

# **Resilient Airport Systems: Integrating Model-Based Analysis with Simulation for Blackout and Cyber Attack Response**

**Tobias Koch**

Vollständiger Abdruck der von der Fakultät für Bauingenieurwesen und Umweltwissenschaften der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

angenommenen Dissertation.

- Gutachter:
1. Univ.-Prof. Dr.-Ing. Alexander Popp
  2. Prof. Dr. rer. nat. Andreas Deutschmann
  3. Univ.-Prof. Dr.-Ing. habil. Michael Schultz

Die Dissertation wurde am 21. Mai 2025 bei der Universität der Bundeswehr München eingereicht und durch die Fakultät für Bauingenieurwesen und Umweltwissenschaften am 24.12.2025 angenommen. Die mündliche Prüfung fand am 02.02.2026 statt.



---

# Zusammenfassung

---

Die Komplexität des Systems Flughafen und dessen Abhängigkeit von elektrischer Energie und Informations- und Kommunikationstechnologie (IKT) nimmt zu. Infolgedessen stellen Stromausfälle oder Cyberangriffe eine enorme Bedrohung dar. Bisherige Ansätze des Krisenmanagements an Flughäfen berücksichtigen die komplexen Zusammenhänge zwischen der Flughafeninfrastruktur und den Flughafenprozessen nicht.

Im Rahmen dieser Arbeit wurde ein neuartiger Ansatz entwickelt, der es ermöglicht den Flughafen als ein komplexes cyberphysisches System (CPS) zu beschreiben, das als mehrdimensionaler Netzwerkgraph dargestellt wird, welches die elektrische und IKT-Infrastruktur repräsentiert. Durch die Einführung von Prozessschichten und deren Verbindung mit den CPS-Schichten wurde der Flughafen als sozio-technisches System beschrieben und mit Modellen angereichert, um das Systemverhalten während Stromausfällen und Cyberattacken abzubilden. Dafür wurden State-of-the-Art Modelle zur Bewertung des Verhaltens von Stromnetzen und der Ausbreitung von Malware in IKT-Netzwerken mit Modellen zur Beschreibung der Interaktion zwischen diesen Schichten kombiniert. Diese Modelle wurden als zusammenhängendes Simulationsframework implementiert, welches eine Prognose der Verfügbarkeit der Prozessressourcen ermöglicht. Das Framework wurde anschließend anhand von Minimalbeispielen verifiziert.

Die resultierende zeitabhängige Ressourcenverfügbarkeit kann dann als Input dienen, um Flughafenprozesse auf zwei Arten zu simulieren: als flussbasierter Ansatz, der das Verhalten einzelner Passagiere vernachlässigt, und als mikroskopische agentenbasierte Simulation. Durch die Kombination dieser Simulationen wurde eine ganzheitliche Pipeline entwickelt, die die Bewertung von Notfallplänen für Stromausfälle und Cyberangriffe (z.B. Lastabwurf oder Netzisolierung) unter Verwendung klassischer Key Performance Indicators (KPIs) für die Performanz von Flughäfen ermöglicht.

Neben dem innovativen methodischen Ansatz wurden die folgenden wichtigen Erkenntnisse aus einer umfassenden Risikoanalyse gewonnen. Während Stromausfälle in Ländern der ersten Welt häufig durch Bau- und Wartungsarbeiten verursacht werden, leiden Flughäfen in Ländern mit einer hohen Häufigkeit und Dauer von Stromausfällen unter großflächigen Stromausfällen und einer unzureichender Notstromversorgung. Die Stress-Zentralität der Knoten innerhalb eines IKT-Netzwerkgraphen hat sich als guter Indikator für eine kosteneffiziente Stärkung der Widerstandsfähigkeit des Gesamtnetzes gegenüber Cyberattacken erwiesen. Mit Hinblick auf die Auswirkung von Ressourcenknappheit auf die Passagierabfertigung hat die Analyse in dieser Arbeit gezeigt, dass dysfunktionale Sicherheitskontrollen

einen Flaschenhalseffekt erzeugen und dadurch die größten Auswirkungen auf die Flughafenleistung haben.

Trotz der fehlenden Validierung anhand einer realen Infrastruktur und eines realen Szenarios wurde in dieser Arbeit ein neuartiger Ansatz zur Erhöhung der Widerstandsfähigkeit von Flughäfen vorgestellt, indem diese als ganzheitliches System betrachtet werden, welches die Flughafeninfrastruktur, die Flughafenprozesse und das Verhalten der Passagiere kombiniert.

---

# Abstract

---

The complexity of airports and their dependency on electrical energy and information and communication technology (ICT) is rising. Consequently, they are becoming increasingly exposed to blackouts or cyber-attacks. Current approaches to tackle this issue do not take into account the interconnection between the airport infrastructure and airport processes.

A novel approach has been developed within this work, treating the airport as a complex cyber-physical system (CPS) represented as a multiplex network graph representing the electrical and ICT infrastructure. By introducing process layers and connecting them to the CPS-layers, the airport was described as a socio-technical system. Models for the interaction between these layers have been described and combined with common approaches to evaluate the behavior of power grids or the propagation of malware through ICT networks. These models have been implemented as an integral simulation framework and verified using minimum examples.

The resource availabilities resulting from the simulation on infrastructure level are being used to simulate airport processes in two ways: as a flow-based approach neglecting passenger behavior, and as a microscopic agent-based simulation. By combining these simulations, a holistic pipeline has been developed that allows for the evaluation of emergency plans for blackouts and cyber attacks (e.g., load shedding or network isolation) using classical key performance indicators (KPIs) used to describe airport performance.

Apart from the innovative methodological approach, the following key findings have been obtained from a comprehensive risk analysis. While blackouts in first-world countries are often caused by construction and maintenance works, airports in countries with a high occurrence rate and duration of blackouts suffer under large-area blackouts and insufficient emergency power supply. The stress centrality of the nodes within an ICT network graph has been found to be a good indicator for cost-efficient strengthening of vulnerable points. With respect to the impact on airport processes, the analysis in this work has shown that dysfunctional security checks induce a bottleneck effect and therefore result in the highest impact on airport performance.

Despite the lack of validation on a real-world infrastructure and real scenarios, a novel approach to increase the resilience of airports has been introduced within this work by expressing them as a holistic system combining the airport infrastructure, airport processes, and passenger behavior.



---

# Contents

---

|          |                                                                       |           |
|----------|-----------------------------------------------------------------------|-----------|
| <b>1</b> | <b>Critical Infrastructure Protection</b>                             | <b>1</b>  |
| 1.1      | Critical Infrastructures and their Role for Society . . . . .         | 1         |
| 1.2      | Incidents and Attacks connected to Critical Infrastructures . . . . . | 4         |
| 1.3      | Increasing Blackout and Cyber Crime Probability . . . . .             | 6         |
| 1.4      | Outline . . . . .                                                     | 7         |
| <b>2</b> | <b>The Airport as a Critical Infrastructure</b>                       | <b>9</b>  |
| 2.1      | Airport System . . . . .                                              | 9         |
| 2.2      | Airport Infrastructure and Passenger Processing . . . . .             | 13        |
| 2.3      | Modeling and Simulation of Airport Processes . . . . .                | 18        |
| 2.4      | Safety and Security Issues at Airports . . . . .                      | 19        |
| 2.4.1    | Aircraft Operation . . . . .                                          | 20        |
| 2.4.2    | Airport Infrastructure . . . . .                                      | 22        |
| 2.4.3    | Cyber Security at Airports . . . . .                                  | 23        |
| 2.5      | Emergency Management and Management Systems . . . . .                 | 24        |
| 2.5.1    | Emergency Management of Power Systems . . . . .                       | 26        |
| 2.5.2    | Cyber Security Measures at Airports . . . . .                         | 31        |
| <b>3</b> | <b>Modeling the Airport as a Dynamic Cyber-Physical System</b>        | <b>33</b> |
| 3.1      | The Airport Infrastructure as a Cyber-Physical System . . . . .       | 34        |
| 3.1.1    | Modeling Malware Intrusion and Propagation within ICT Networks        | 37        |
| 3.1.2    | Modeling Power Supply and Distribution at Airports . . . . .          | 41        |
| 3.1.2.1  | The Airport as a Microgrid . . . . .                                  | 43        |
| 3.1.2.2  | Power Grid Analysis using Power Flow Analysis . . . . .               | 45        |
| 3.2      | Layer Interaction and Dynamics of the Cyber-physical System . . . . . | 49        |

---

|          |                                                                                |           |
|----------|--------------------------------------------------------------------------------|-----------|
| <b>4</b> | <b>Improving Robustness of the Airport against Blackouts and Cyber Attacks</b> | <b>53</b> |
| 4.1      | Risk and Impact Analysis for Blackouts at Airports . . . . .                   | 53        |
| 4.1.1    | Methods . . . . .                                                              | 54        |
| 4.1.2    | Probabilistic Risk Assessment and Mitigation . . . . .                         | 56        |
| 4.1.2.1  | Likelihood of Occurrence . . . . .                                             | 57        |
| 4.1.2.2  | Magnitude Evaluation . . . . .                                                 | 61        |
| 4.1.3    | Risk Mitigation . . . . .                                                      | 66        |
| 4.2      | Strengthening ICT Networks through Vulnerability Analysis . . . . .            | 71        |
| 4.2.1    | Quantification of Network Security and Junction Point Detection . .            | 71        |
| 4.2.2    | Increasing Network Strength with Minimum Costs . . . . .                       | 75        |
| 4.2.3    | Solving the Optimization Problem . . . . .                                     | 76        |
| 4.2.4    | Advise for ICT Network Strengthening and Design . . . . .                      | 79        |
| <b>5</b> | <b>Holistic Approach towards Impact Forecasting using Simulation</b>           | <b>83</b> |
| 5.1      | Simulating the Operability State on Infrastructure Basis . . . . .             | 85        |
| 5.1.1    | Implementation as a Python-based Simulation Tool . . . . .                     | 85        |
| 5.1.2    | Verification of the Simulation Model . . . . .                                 | 90        |
| 5.2      | From Infrastructure to Processes through Process Network Objectification .     | 95        |
| 5.2.1    | Process-Oriented Grouping . . . . .                                            | 95        |
| 5.2.2    | From Grouping to Resource Management . . . . .                                 | 97        |
| 5.3      | Impact Simulation in an Airport Terminal . . . . .                             | 98        |
| 5.3.1    | Static Impact Estimation and Optimization using Linear Algebra . .             | 99        |
| 5.3.1.1  | Emergency Planning Options . . . . .                                           | 110       |
| 5.3.2    | Impact Estimation using a Microscopic Agent-based Simulation Model             | 113       |
| 5.3.2.1  | Model Description, Implementation and Input Data . . . .                       | 114       |
| 5.3.2.2  | Application of the Simulation for KPI-driven Impact Esti-<br>mation . . . . .  | 123       |
| 5.4      | KPI-driven Emergency Plan Evaluation . . . . .                                 | 128       |

---

|          |                                                                  |            |
|----------|------------------------------------------------------------------|------------|
| <b>6</b> | <b>Discussion and Outlook</b>                                    | <b>131</b> |
| 6.1      | Discussion . . . . .                                             | 131        |
| 6.2      | Outlook and Possible Ways of Application in the Future . . . . . | 133        |
| <b>7</b> | <b>Conclusion</b>                                                | <b>137</b> |
| <b>A</b> | <b>Appendix</b>                                                  | <b>139</b> |
| A.1      | Additional Scenarios for the Static Impact Analysis . . . . .    | 139        |
| A.2      | Software Implementation . . . . .                                | 141        |
| A.3      | Scenario Cologne-Bonn . . . . .                                  | 147        |
| A.4      | AnyLogic Implementation Details . . . . .                        | 150        |
|          | <b>References</b>                                                | <b>153</b> |



---

# List of Figures

---

|     |                                                                                                                                                       |    |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1.1 | CI sector division as used by the U.S. Government . . . . .                                                                                           | 3  |
| 2.1 | Model of the airport system . . . . .                                                                                                                 | 11 |
| 2.2 | System architecture for ICT systems at airports . . . . .                                                                                             | 13 |
| 2.3 | Schematic by of the structure of the airport infrastructure . . . . .                                                                                 | 14 |
| 2.4 | Schematic sketch of an airport terminal . . . . .                                                                                                     | 17 |
| 2.5 | Power system emergency states in decision and control . . . . .                                                                                       | 27 |
| 2.6 | Power system operation by decision and control . . . . .                                                                                              | 28 |
| 3.1 | Passenger trajectory through an airport terminal under full performance<br>(top) and disturbed conditions (bottom) . . . . .                          | 35 |
| 3.2 | Overview of graph types and their features . . . . .                                                                                                  | 36 |
| 3.3 | Two-layer network structure showing the ICT and power grid layer . . . . .                                                                            | 37 |
| 3.4 | Categorization of malware types . . . . .                                                                                                             | 38 |
| 3.5 | ICT layer structure represented as a graph with objects as nodes and infec-<br>tion time as edge weights under conditions of a cyber attack . . . . . | 40 |
| 3.6 | One-line diagram of a microgrid structure . . . . .                                                                                                   | 42 |
| 3.7 | Exemplary airport power system setup . . . . .                                                                                                        | 44 |
| 3.8 | Working scheme of dynamic network stability analysis . . . . .                                                                                        | 50 |
| 4.1 | Map overview showing IATA regions airport locations where incidents were<br>recorded . . . . .                                                        | 57 |
| 4.2 | Evolution of the number of incidents in the regions over time . . . . .                                                                               | 59 |
| 4.3 | Source location of recorded incidents as a cumulative bar chart for each region                                                                       | 59 |

---

|      |                                                                                                                                 |    |
|------|---------------------------------------------------------------------------------------------------------------------------------|----|
| 4.4  | Affected parts of airport operation caused by blackouts . . . . .                                                               | 62 |
| 4.5  | Consequences on flight operation for all incidents . . . . .                                                                    | 63 |
| 4.6  | Blackout duration time as box plots for all incidents and by region . . . . .                                                   | 65 |
| 4.7  | Percentages of world-wide blackout causes . . . . .                                                                             | 68 |
| 4.8  | Blackout source location distinguished by cause of the outage . . . . .                                                         | 69 |
| 4.9  | Example ICT networks consisting of 7 to 4 nodes as a weighted graph . . .                                                       | 73 |
| 4.10 | Number of iterations for the optimization with the graphs from Figure 4.9 .                                                     | 78 |
| 4.11 | Number of iterations for the network with six nodes under the conditions of<br>different costs for node five . . . . .          | 79 |
| 4.12 | Improved nodes (left) and the stress centrality before and afterwards at<br>equal costs . . . . .                               | 80 |
| 4.13 | Improved nodes (left) and the stress centrality before and afterwards at costs<br>of 1.1 c.u. and 1.2 c.u. . . . .              | 81 |
| 4.14 | Leftover cost units for the cases with equal costs and increased costs . . . .                                                  | 82 |
| 5.1  | Pipeline for the KPI-based evaluation of emergency plans using infrastruc-<br>ture simulation and impact forecasting . . . . .  | 84 |
| 5.2  | Schematic of the simulation workflow regarding software architecture . . .                                                      | 87 |
| 5.3  | ICT Network structure with objects as nodes and infection speed as edges .                                                      | 90 |
| 5.4  | Time-dependent power demand for the devices during the working day and<br>the corresponding power factor . . . . .              | 91 |
| 5.5  | Time-dependent power generation during the working day . . . . .                                                                | 92 |
| 5.6  | Changes in operating states during the day under the conditions of a cyber<br>attack . . . . .                                  | 93 |
| 5.7  | Changes in operating states during the day under the conditions of a cyber<br>attack only affecting windows computers . . . . . | 93 |
| 5.8  | Evolution of the voltage magnitudes at all objects throughout the day at each<br>component . . . . .                            | 94 |
| 5.9  | Process stations within a generic airport departure terminal split into process<br>groups and process group objects . . . . .   | 96 |

---

|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 5.10 Multiplex network graph showing the relation between 12 devices in the CPS and the process groups . . . . .                                                          | 96  |
| 5.11 Process capacities for two check-in process groups over time . . . . .                                                                                               | 99  |
| 5.12 Four investigated scenarios (disruptive airport states) used for impact forecasting . . . . .                                                                        | 104 |
| 5.13 Increase in total waiting time calculated considering load-shedding and optimization mode . . . . .                                                                  | 112 |
| 5.14 Simulation logic for the departure process . . . . .                                                                                                                 | 115 |
| 5.15 Number of passengers arriving before departure accumulated over 10 minutes according to the five generated databases . . . . .                                       | 119 |
| 5.16 Three-dimensional parameter space of the study spanned by the number of check-in counters, the number of security controls and number of passport controls . . . . . | 125 |
| 5.17 Results of the parameter study showing the averaged seat load factor and its standard deviation in dependence of the service stations configurations . . . . .       | 126 |
| 5.18 Workflow for KPI-based emergency plan evaluation . . . . .                                                                                                           | 129 |
| A.1 Screenshots of the GUI Editor and visualization of the ICT and power layer . . . . .                                                                                  | 144 |
| A.2 Screenshots of the network object editor and object group editor . . . . .                                                                                            | 145 |
| A.3 Screenshots of the emergency management editor and cyber attack configurator . . . . .                                                                                | 146 |
| A.4 Implementation scheme of the simulation using AnyLogic. . . . .                                                                                                       | 152 |



---

# List of Tables

---

|     |                                                                                                                                            |     |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1.1 | Extreme events overview incl. terrorism and natural disasters . . . . .                                                                    | 6   |
| 2.1 | Control methods for grid operation on low-voltage networks . . . . .                                                                       | 30  |
| 3.1 | Overview of possible type of components of a bus system . . . . .                                                                          | 47  |
| 4.1 | Cause categories for blackouts . . . . .                                                                                                   | 55  |
| 4.2 | Overview of IATA regions . . . . .                                                                                                         | 56  |
| 4.3 | Overview of regional distribution of the incidents, total number of airports<br>in the region and the normalized incident number . . . . . | 58  |
| 4.4 | System Average Interruption Duration Index (SAIDI) for all IATA regions . .                                                                | 61  |
| 4.5 | Prevention index by country considering expected and suffered blackout<br>times with more than 1 incident . . . . .                        | 67  |
| 4.6 | Graph properties of the networks in Figure 4.9 . . . . .                                                                                   | 74  |
| 5.1 | Structure of the network_object class used to represent the CPS . . . . .                                                                  | 86  |
| 5.2 | Process Assignment Matrix for the system setup from Figure 5.9 . . . . .                                                                   | 97  |
| 5.3 | Process sequence matrix $\mathbf{P}_{Seq}$ . . . . .                                                                                       | 102 |
| 5.4 | Waiting time distributions as input for the process groups . . . . .                                                                       | 104 |
| 5.5 | Waiting time matrix $\mathbf{P}_W$ in minutes . . . . .                                                                                    | 106 |
| 5.6 | Results for all scenarios in minutes . . . . .                                                                                             | 107 |
| 5.7 | Results for all scenarios with respect to processes in minutes . . . . .                                                                   | 108 |
| 5.8 | Optimization Results for n shed devices with and without load shedding mode                                                                | 111 |

---

|      |                                                                                                                                                                        |     |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 5.9  | Number of combinations dependent with increasing number of dysfunctional devices for a system of 22 devices . . . . .                                                  | 111 |
| 5.10 | Overview of the input parameters used to generate the properties of each passenger generated for the simulation as well as to calculate the processing times . . . . . | 122 |
| 5.11 | Assessment of the number of available service stations at passenger handling processes as uncritical, critical and insufficient to maintain flight operations          | 128 |
| A.1  | Process sequence matrix $\mathbf{P}_{Seq}$ weighted by process. . . . .                                                                                                | 139 |
| A.2  | Results for all scenarios with respect to processes in minutes . . . . .                                                                                               | 140 |
| A.3  | Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2 . . . . .                                         | 147 |
| A.3  | Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2 . . . . .                                         | 148 |
| A.3  | Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2 . . . . .                                         | 149 |
| A.3  | Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2 . . . . .                                         | 150 |

---

# Nomenclature

---

## Abbreviations

|       |                                           |
|-------|-------------------------------------------|
| $R$   | Electrical resistance                     |
| BIM   | building information model                |
| BLF   | breakeven load factor                     |
| CI    | Critical Infrastructure                   |
| CIP   | Critical Infrastructure Protection        |
| EASA  | European Union Aviation Safety Agency     |
| ECI   | European Critical Infrastructure          |
| EU    | European Union                            |
| GUI   | Graphical User Interface                  |
| ICAO  | International Civil Aviation Organization |
| ICT   | Information and Communication Technology  |
| KPI   | Key Performance Indicator                 |
| PAPI  | Precision Approach Path Indicator         |
| PBB   | Passenger Boarding Bridge                 |
| PCN   | Pavement Classification Number            |
| RON   | Remain Overnight                          |
| SCADA | Supervisory Control and Data Acquisition  |
| SLF   | seat load factor                          |
| UPS   | Uninterrupted Power Supply                |

## Mathematical Symbols

|          |                                               |
|----------|-----------------------------------------------|
| $\delta$ | Voltage angles                                |
| $c_b$    | betweenness centrality of a vertex in a graph |

|                |                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------|
| $c_e$          | eccentricity centrality of a vertex in a graph                                                  |
| $c_s$          | stress centrality of a vertex in a graph                                                        |
| $d_{ij}$       | distance between two vertices in a graph, i.e, the sum of all edge weights on the shortest-path |
| $e_{v_i, v_j}$ | edge of a graph connecting vertices i and j                                                     |
| $I$            | Electric current                                                                                |
| $P$            | Real power                                                                                      |
| $p$            | Prevention index determining the preparedness of airports towards blackouts                     |
| $Q$            | Reactive power                                                                                  |
| $U$            | Voltage                                                                                         |
| $v_i$          | vertex of a graph                                                                               |
| $w_{i,j}$      | edge weights of a weighted graph connecting vertices i and j                                    |
| $X$            | Electrical reactance                                                                            |
| $Z$            | Electrical impedance                                                                            |

# Critical Infrastructure Protection

---

A power outage at Newark International Airport, New York, USA in January 1995 caused by construction works raised questions regarding the robustness of power supply at airports. The reporter Robert Hanley from the New York Times posed these queries: "Is it wise for an airport to have both its main power source and the auxiliary source lying side by side? Are the airport's backup power sources sufficient? Was the location of the cables clearly made known to the construction company, as required by Public Service Electric and Gas?". A recent incident at Heathrow Airport on March 20th 2025, where a fire at a nearby electrical substation caused a blackout that affected around 200,000 travelers (CBS News, 2025), underline that, nearly 25 years later, the answers to these questions regarding preventive measures in the emergency management of airports remain unknown. Moreover, blackouts are not explicitly named as an off-aircraft emergency within the emergency planning guidelines from the International Civil Aviation Organization (ICAO) International Civil Aviation Organization (1991). A lack of clarity persists in this area. Within this work, this issue is addressed by modeling the airport as a cyber-physical system using a multi-layer modeling approach and investigating the effect of blackouts and cyber attacks on the airport system.

## 1.1 Critical Infrastructures and their Role for Society

Critical Infrastructures (CI) play an important role in supplying resources such as electrical power, water, heating, communication, financial services, transportation, and healthcare to our everyday life. However, a dysfunction of CI results in a large impairment of society, earning it the designation critical. In response, the U.S. government (U.S. GAO, 2004) and the European Union (EU) (European Commission, 2008a, 2013) have initiated programs for critical infrastructure protection (CIP). While in most cases the society is considered as the population of a state, the European Union distinguishes between critical infrastructures (CI) and European critical infrastructures (ECI), whereas the latter is defined as an infrastructure whose loss would impact at least two member states of the European Union (European Commission, 2008a). Air transport is a notable example of this interconnectedness across state borders and globally.

The classification of CI as critical remains subjective, prompting the German Federal Office of Civil Protection and Disaster Assistance to publish a living guideline for identifying CIs (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021b). The guideline proposes a three-step approach to identification, comprising three key questions, whereas two of these consider qualitative criteria and one a quantitative criterion.

The key question involves identifying services that are urgently demanded by society. This demand is confirmed if a malfunction of the infrastructure could pose:

- Danger to life,
- Threats to public order and security,
- Significant impacts on everyday life,
- And/or interdependencies lead to cascading effects impacting other critical services.

The second criteria considers the processes within the infrastructure are demanded to fulfill its purpose for society. Therefore, the second step is the identification of

- Subprocesses that are necessary for providing critical services,
- And/or stakeholders that are directly connected to these services.

In the final phase, thresholds are defined to filter the impact of CI on the population based on the number of affected people. However, no single threshold exists, as it must be context-dependent and aligned with the scale being investigated. The German Federal Office for Information Security has established a threshold of approximately 500,000 affected people at the national level in Germany (BSI, 2021).

In addition to identifying CIs, their services are classified into different sectors. Figure 1.1 illustrates the classification used by the U.S. Government for assigning protection to various national departments, including the Department of Homeland Security. While many infrastructure sectors are also considered critical in Germany, the Federal Office of Civil Protection and Disaster Assistance does not classify commercial and industrial facilities as such (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021a). This highlights the variation in criteria used across societies for identifying critical infrastructures and the added complexity introduced by the dependencies between and within infrastructure systems.



Figure 1.1: CI sector division as used by the U.S. Government (U.S. GAO, 2018) and the agencies responsible for the protection of CIs within the sector.

## 1.2 Incidents and Attacks connected to Critical Infrastructures

Critical infrastructure protection is a highly prioritized topic today, because of the manifold of hazards and threats that CIs are exposed to. One of them and maybe one of the potentially least forecastable is human error, or sometimes also referred to as human failure. There exists no consistent definition of human error, but Kanki (2018) presents a concise overview of the history and evolution of the term. However, the definition given by Hollnagel (1996) fits well within the context of critical infrastructure protection:

*“Either an action that is not intended or desired by the human or a failure on the part of the human to perform a prescribed action within specified limits of accuracy, sequence, or time that fails to produce the expected result and has led or has the potential to lead to an unwanted consequence.”*

The definition contains the clear distinction from security threats, such as sabotage or terrorism, by clarifying the action as unintended. Furthermore, possible sources of error are named, which may be a lack of performance (accuracy), unfollowed process sequences (sequence) or temporal issues (time). A perfect example for a human error is the Blackout in Arizona and California in 2011, which was caused by an employee who switched off a piece of equipment at a power substation in southwest Arizona (The Guardian, 2011). The local outage caused a cascading effect by affecting important transmission lines connecting Arizona and California and therefore cut the inflow of electric power into southern California. Although, California introduced tougher regulatory measures since the Northeast Blackout in 2003 that affected about 40 million people and cost about 6 billion \$, the blackout in 2011 is still one of the strongest blackouts in Californian history with an estimation of 5 million affected people.

The most significant safety issue is the malfunction of technical equipment. While maintenance, standardized production, and testing can mitigate the risk of technical malfunctions, the incident at Air France Flight 447 in 2009 demonstrates that unknown issues can still occur. On that fateful day, the airplane’s pitot tubes were blocked due to ice crystallization, leading to false sensor output for aircraft velocity. This caused the autopilot to be deactivated, and the pilots received misleading information, which ultimately led to an aerodynamic stall and a fatal crash into the Atlantic Ocean (BEA, 2012). Since then, airlines have taken steps to prevent similar incidents by heating pitot tubes during flight to keep them ice-free.

A striking example of technical failure occurred in 1988 at Clapham Junction near London, where a train crashed into another stationary train due to a signal failure caused by a wire fault (Hidden, 1989). Although fallback solutions were developed afterwards, the European Union has been working on the rollout of the unified European Train Control System (ETCS), which was specified in 2006 (European Commission, 2006). However, this process highlights one of the key challenges in critical infrastructure protection: the long life cycle of the infrastructure, which can slow down the adoption of new technologies.

Moreover, the age of the infrastructure increases the risk of failures due to wear and tear. For instance, a blackout at Hamburg Airport in 2018 was caused by a short-circuit due to isolation issues (Witte, 2018; tagesschau.de, 2018).

In addition to technological failures, environmental hazards such as geomagnetic storms (Kappenman, J. G. and Zanetti, L. J. and Radasky, W. A., 1997) earthquakes, tsunamis, floodings, or storms (Urlainis et al., 2014) pose a diverse range of threats to critical infrastructures (CIs) across different spatial and temporal scales. This spectrum can encompass everything from localized heavy rainfalls to globally significant incidents. However, the field of describing and analyzing environmental hazards is inherently complex and continues to evolve rapidly due to climate change. As a result, the United Nations Environment Programme (UNEP) and the World Meteorological Organization (WMO) established the Intergovernmental Panel on Climate Change (IPCC) to investigate this dynamic landscape. The most recent report from 2022 the Intergovernmental Panel on Climate Change (2022) summarizes the current state of their research, including current risk assessments and projections for future developments due to climate change. This includes examining global trends as well as regional patterns, in addition to proposing mitigation and adaptation strategies.

In addition to safety hazards, critical infrastructures (CIs) are also vulnerable to man-made attacks due to their significant impact on society in the event of a successful attack. The 9/11 attacks on the World Trade Center in 2001 remain one of the most devastating terrorist incidents in modern history, resulting in approximately 2,764 human casualties and 9,349 injured people (Kean et al., 2004; Wikipedia, 2022). The 9/11 attacks were a pivotal moment in the development of critical infrastructure protection programs globally. The United States' response to this attack led to the establishment of the United States Critical Infrastructure Protection Programme (U.S. GAO, 2004). Terrorist groups frequently employ bombs as their preferred method of attack, particularly in the transportation sector where high passenger turnover makes thorough security checks challenging. However, a notable exception is the 1988 bombing of Pan Am Flight 103 over Scotland, which claimed around 270 human lives. This incident led to significant improvements in civil aviation security standards, largely due to the efforts of the International Civil Aviation Organization (ICAO) and its Annex 17 (International Civil Aviation Organization, 2011). Despite the increased security measures implemented in response to this attack, subsequent incidents, such as the Madrid train bombings in 2004 and the London bombings in 2005, highlighted the need for enhanced security protocols across all modes of transportation. Notably, adapting existing security standards from aviation to train stations has proven to be a complex challenge (Asmer et al., 2019).

The table created by Urlainis et al. (2014) and shown in Table 1.1 compares the impact of man-made terrorist attacks and natural disasters. It is evident that the order of magnitude in human casualties differ by at least two orders of magnitude comparing the heaviest man-made incident with the strongest natural disaster. This is directly related to the affected area and their population, as e.g., the Indian Ocean Tsunami flooded large areas of the highly populated regions in Indonesia, India and Thailand and even had impact on East-African states such as Somalia.

Table 1.1: Comparison of extreme events caused by Man-made terrorist attacks and natural disasters. Reprinted from Urlainis et al. (2014), with permission from Elsevier.

| Extreme Event            | Year | Type     | Affected Areas                                            | Estimated damage and loss (10 <sup>6</sup> \$US) | Death and missing | Injured  | Return Period of similar events (years) | Average annual Loss (10 <sup>6</sup> \$US) |
|--------------------------|------|----------|-----------------------------------------------------------|--------------------------------------------------|-------------------|----------|-----------------------------------------|--------------------------------------------|
| Oklahoma City Bombing    | 1995 | Man-made | Oklahoma City, Oklahoma, USA                              | 650                                              | 167               | 684      | -                                       | -                                          |
| Izmit Earthquake         | 1999 | Natural  | Izmit, Turkey                                             | 6,000                                            | 17,000            | 50,000   | <10                                     | 600                                        |
| World Trade Center       | 2001 | Man-made | New York City, NY, USA                                    | 22,000                                           | 2,764             | 9,349    | -                                       | -                                          |
| Indian Ocean Tsunami     | 2004 | Natural  | Several Countries among India Ocean                       | 11,000                                           | 228,000           | 500,000  | <25                                     | 440                                        |
| Hurricane Katrina        | 2005 | Natural  | 5 Countries (mostly Florida, Louisiana, Mississippi), USA | 130,000                                          | 1,833             | Hundreds | <15                                     | 8,600                                      |
| London July 7th Bombings | 2005 | Man-made | London, England                                           | 2,500                                            | 56                | 700      | -                                       | -                                          |
| Haiti Earthquake         | 2010 | Natural  | Port-au-Prince, Haiti                                     | 7,800                                            | 316,000           | 300,000  | >100                                    | <780                                       |
| Fukushima Daiichi        | 2011 | Natural  | Fukushima Daiichi, Japan                                  | 309,000                                          | 20,350            | 5,314    | <60                                     | 5,000                                      |

Nevertheless, the impact of terrorist attacks should not be underestimated. Furthermore, while in the past terrorism has been primarily conducted in a physical form and is still threatening CIs (Zoli et al., 2018), the continuing digitalization results in an increasing vulnerability towards cyber crime via, e.g., Supervisory Control and Data Acquisition (SCADA) Systems (Stamp et al., 2009b). The consequences of successful cyber attacks are very diverse ranging from train signal (Hancock, 2003) and traffic light manipulation (McMillan, 2007) over hijacked water service control systems (Abrams and Weiss, 2008) up to disrupting nuclear power plants (Kesler, 2011).

### 1.3 Increasing Blackout and Cyber Crime Probability

The final examples in Section 1.2 illustrate the dependence on functioning information and communication technology (ICT) systems. However, the scope of resources required to operate critical infrastructure is vast, encompassing natural resources such as water and gas, electrical power, software, and human resources. The availability of these resources is highly interdependent.

Electrical power plays a central role in connecting all other resources, as pumps are necessary for transporting water and oil/gas throughout the infrastructure, while heat/air conditioning is often linked to electric power or relies on thermal power stations. Due to

---

this critical role, the focus of this work is to ensure the reliability of electrical power supply and ICT systems.

The growing interconnectedness of ICT systems (e.g., internet of things, smart grid) increases the likelihood of cyber crime. The concept of tomorrow's smart cities (European Commission, 2011) implies an inevitable increase in infrastructure interconnectivity (Batty et al., 2012). Although there is no universally accepted definition of a "smart city" by now, most planning approaches involve the idea of smart grids and intelligent mobility. Smart grids refer to decentralized electricity production that responds to consumption patterns, enabling efficient, environmentally friendly use of electricity with minimal losses.

For this purpose, sensors (smart meters) must measure and regulate energy consumption while communicating with each other (Palensky and Dietrich, 2011). This leads to increased exposure to cyber attacks not only within critical infrastructure but also in smart homes (Anwar and Mahmood, 2014; Möller and Vakilzadian, 2014; Eckert and Krauß, 2011). The concept of intelligent mobility, which uses ICT systems to optimize transfer, waiting, and door-to-door times, further increases data collection and interconnectivity.

The development of non-blackstart-capable renewable energy sources and reduced power reserves exposes the power grid to numerous safety and security concerns. As a result, the risk of blackouts rises.

For safety and security analysis, critical infrastructure (CIs) must be considered as cyber-physical systems (Möller, 2016). This is due to the high number of interconnected embedded systems within modern CIs and the growing trend towards both ICT and physical systems being vulnerable to threats. In the context of Industry 4.0 (Hermann et al., 2016), which involves periodic conditions and a low amount of unpredictable factors, data-driven approaches are used to detect uncommon or conspicuous system behavior (Niggemann et al., 2015). However, this approach is limited if smart technologies interact with or depend on human behavior, as seen in the transport sector.

To address these challenges, a classical, two-layered, process-oriented approach to model CIs as cyber-physical systems at the example of an airport structure is proposed within this work (Koch et al., 2017, 2018).

## **1.4 Outline**

This study begins with a comprehensive introduction to the airport infrastructure, which is presented as a complex system comprising multiple technical and economic systems, as well as numerous processes involving a large number of stakeholders. The aim of this research is to enhance safety and security at airports, and therefore, possible attack scenarios and current state-of-the-art concepts for emergency management and critical infrastructure resilience are also highlighted.

The increasing complexity of infrastructures necessitates the development of decision support and planning tools to protect airports as critical infrastructures by evaluating preventive and reactive measures. To provide these tools, the airport system is first described as a cyber-physical system (CPS), including its interconnected electrical and ICT infrastructure.

A crucial factor in successful prevention is the identification of possible hazards or threats, from which realistic scenarios can be conducted. Therefore, risk analysis based on worldwide blackout incidents in the past years (as described in Section 4.1) allows for the proposal of appropriate mitigation measures. Additionally, improving preparedness to cyber attacks is also a priority, and a graph-based approach to identify and strengthen network security based on graph properties is introduced in Section 4.2.

Due to the high interconnectedness and complexity of the airport infrastructure, evaluating single aspects of the complex system is insufficient. Hence, a model-based approach to forecast the impact of blackouts and cyber attacks on airports. First, a two-layered modeling approach for the airport infrastructure is explained in Section 3.1, which enables simulation of the impact of blackouts and cyber attacks on the electrical and ICT systems of the airport infrastructure.

The transfer and implementation of these models into a component-based simulation tool, including verification, are performed in Section 5.1. The important factors in decision-making for airport operators are not the availability of infrastructure resources but the effects of resource scarcity on processes, which is why an approach called process-oriented network objectification is introduced, connecting resources to their corresponding processes and allowing evaluation of mitigation measures using common key performance indicators in Section 5.2.

To concretize the use of these tools in the field of critical infrastructure protection, they are integrated into a workflow that connects infrastructure simulation with process and passenger flow simulation at the example of a real airport infrastructure in Section 5.3. Furthermore, a mathematical approach is introduced to estimate consequences of disruptions on passenger flows, and the results are compared to simulation-based results.

This study enables the detection of vulnerable points in the process chains at airports and provides support for possible mitigation measures and evaluation of emergency plans (as described in Section 5.4).

Furthermore, a discussion of this work is provided in Chapter 6, highlighting the most important outcomes of this research, stating unanswered questions within this field, and outlining potential enhancements and integration possibilities into other fields of research, such as digital twins.

# The Airport as a Critical Infrastructure

---

This chapter outlines the structure of an airport, its processes, and communication systems, providing a comprehensive understanding of their interconnectedness. The interconnections between energy infrastructure, information and communication technology (ICT), and airport processes are highlighted, which enables the description of the performance of the airport system. Furthermore, an overview is provided of the stakeholders involved, law regulations governing airport operations, and current state-of-the-art crisis management procedures.

## 2.1 Airport System

The Convention on International Civil Aviation, also known as the Chicago Convention, was adopted in 1947 by the International Civil Aviation Organization (ICAO), which has since become the primary global authority for civil aviation. The ICAO is a subsidiary of the United Nations (UN) and all its member states have ratified the convention. Since then, the ICAO has been responsible for establishing International Standards and Recommended Practices regarding rules of airspace, aircraft registration, and safety, security, and sustainability, as well as provisions pertaining to taxation, and outlining the rights of signatories in relation to air travel (International Civil Aviation Organization, 2006) .

ICAO standards and recommended practices were developed to provide a comprehensive framework for civil aviation. These standards and practices are complemented by regulations set within the European Union (EU), which are enforced by the European Union Aviation Safety Agency (EASA) since 2002.

The terms "aerodrome" and "airport" are often used synonymously, but their meanings differ slightly. According to ICAO, an aerodrome is defined as "A designated area on land or water (including any buildings, installations, and equipment) intended to be used either wholly or in part for the arrival, departure, and surface movement of aircraft" (International Civil

Aviation Organization, 2018). The term "airport", however, is not specified by the ICAO. Instead, it was defined by the U.S. Government in 49 U.S. Code § 40102 as “a landing area used regularly by aircraft for receiving or discharging passengers or cargo”. Furthermore, the World Health Organization (WHO) has clarified that the term "airport" refers specifically to any airport where international flights arrive or depart (World Health Organization, 2005) .

In this work, an airport is considered to be an infrastructure that services commercial air traffic and corresponds to German law, following the term "Verkehrsflughafen" declared in §38 Abs. 2 Nr. 1 LuftVZO. This definition encompasses not only the physical infrastructure but also all services defined in ICAO's Airport Services Manual, Part 8: Airport Operational Services (International Civil Aviation Organization, 1983), which are required to be provided by the airport operator. These services include the conception of an airport emergency plan, the provision of fire and rescue services, and conducting security measures in accordance with legal requirements.

The airport operator is considered a crucial stakeholder in crisis management at airports due to their responsibility for ensuring compliance with regulations and standards. Furthermore, airlines play an essential role as stakeholders from an economic perspective, generating a constant income through fees for aircraft services such as landing, parking, fueling, passenger handling, and freight transportation.

Economical factors have gained importance in recent years, particularly in relation to the environment. Airlines' carbon emissions and noise levels now directly impact starting and landing fees, highlighting the significance of ecological considerations. Moreover, the transition to renewable energies has created a tight coupling between electrical energy and ecology, which will continue to influence airport operation.

Considering the various aspects of the airport system, a qualitative model was developed that represents the influences and relations between energy and ICT infrastructures with airport performance, as shown in Figure 2.1. The five main factors depicted in blue are the electrical energy and ICT infrastructure themselves, as well as the previously mentioned economy and ecology, and air traffic. At a more fine-grained abstraction level, air traffic can be separated into passenger and freight transport (red), which are embedded within the economy through airline companies. This generated traffic leads to emissions, which in turn influence the environment. Environmental changes, such as weather, climate, or extreme weather events, directly affect air traffic (Koch et al., 2017).

The development of a smart energy management system is essential to provide a safe and secure power supply for airport services, as all processes now rely on electrical devices. The need for efficient energy management has become crucial due to the increasing dependence on electricity for airport operations.

The ICAO establishes guidelines for a secondary power source as a fall-back solution, requiring a rapid switch-over time for lighting and radio navigation aids to ensure minimum

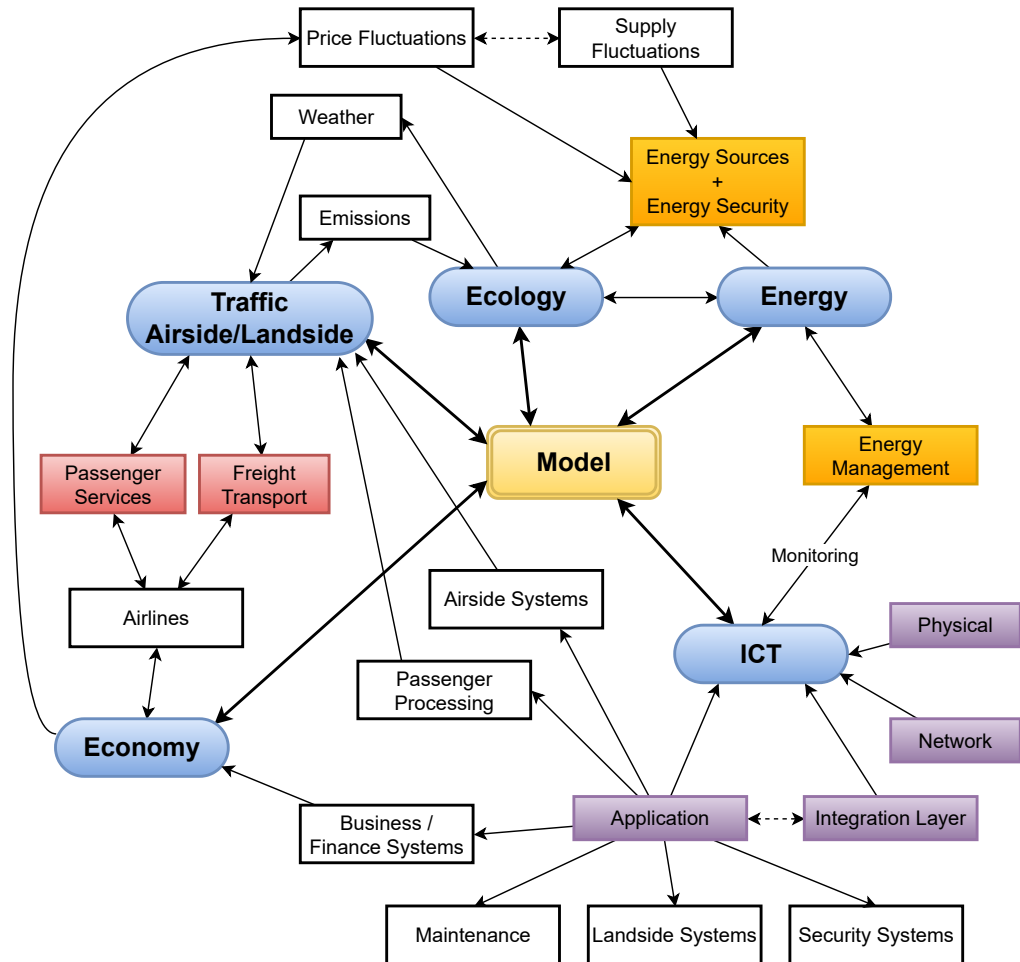


Figure 2.1: The general understanding of an airport includes the 5 main factors on a high abstraction level (blue), e.g., energy, ICT, economy, traffic and ecology, which are highly interconnected with each other as well as with external factors (e. g. energy supply fluctuations or airlines). For energy, ICT and traffic the airport may be divided into subsystems, here depicted in orange (energy), purple (ICT) and red (traffic) (Koch et al., 2017, ©IEEE 2017).

operation in case of emergency. However, there are no regulations governing the integration of this secondary power source into the airport system. In contrast, two independent external power sources are recommended, which would enable a constant power supply during grid failures. Furthermore, an uninterrupted power supply (UPS) is essential to fulfill the required switch-over times until the new power source can be connected.

Common solutions for secondary power supplies include diesel generators or small thermal power plants. The ICAO provides guidelines for electrical circuits for lighting and radio navigation aids, but does not address the overall airport infrastructure, particularly the terminal building. A study by Ortega Alba and Manana (2016) highlights the dominance of the terminal building in energy management, as it consumes approximately 76% of the airport's total energy demand, while airfield lighting and radio navigation systems account for only about 12%. Thus, compliance with ICAO requirements ensures a safe landing or departure of aircraft, but neglects all processes within and around the airport terminal.

The second infrastructure component in Figure 2.1 is the information and communication technology (ICT) used within the airport. The Transportation Research Board and National Academies of Sciences, Engineering, and Medicine (2012) depicts the ICT system architecture as a layered system consisting of physical, networking, application, and integration layers (see Figure 2.2). The physical layer contains all physical connections, such as copper wires or fiber optic cables, which enable direct physical communication. The networking layer comprises electronic devices that either send signals over the physical layer or generate new wireless communication networks, controlling communication within the network. This communication forms the basis for the functioning of the interconnected application layer. According to the Transportation Research Board and National Academies of Sciences, Engineering, and Medicine (2012), the application layer is divided into different fields of application. One field includes airside systems, which control radio and navigation systems, visual aids, fueling, and aircraft handling on both the ground and in the air. In contrast, landside systems control applications located within the publicly accessible part of the airport, including parking access and guidance systems. The passenger processing layer enables successful handling of passengers and baggage by allowing airlines to handle and exchange data, thereby facilitating interactions between passengers and airlines. Business and Financial systems include all administration processes by the airport operator, ranging from financial management to human resource administration and mail or file storage. Due to its criticality and authority involvement, safety and security systems are separated from other processes. These include fire and rescue services, CCTV, access control systems, and mechanical system maintenance, which must be supervised to ensure operating states. At last, the integration layer coordinates interaction between these different applications, enabling information exchange between them. As depicted in the model (see Figure 2.1), the application layer has a direct influence on air traffic through passenger processing systems and airside systems control. Furthermore, business and financial systems incorporate relevant information for economical factors.

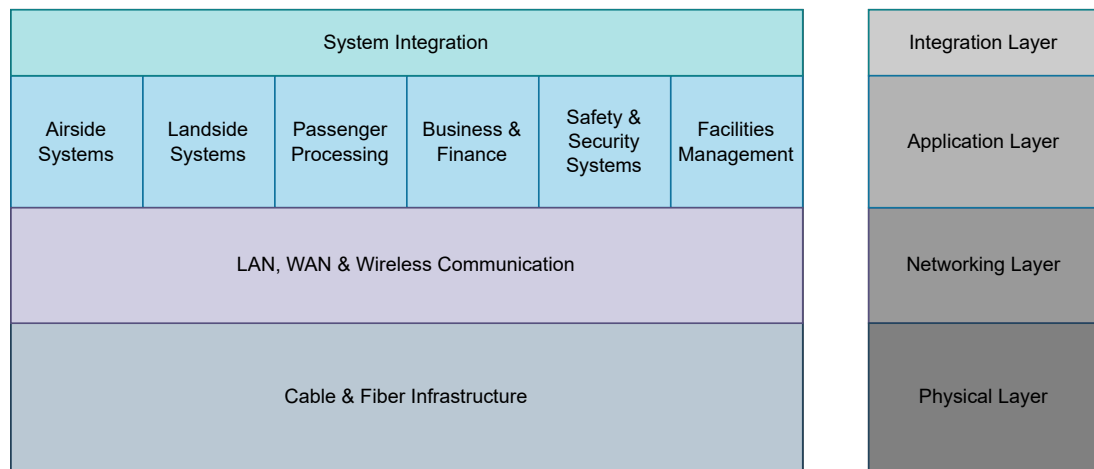


Figure 2.2: System architecture for ICT systems at airports after Transportation Research Board and National Academies of Sciences, Engineering, and Medicine (2012).

## 2.2 Airport Infrastructure and Passenger Processing

The previously mentioned systems are distributed over the entire airport area. In the following section, more insight will be provided into the structure of airports and passenger processing.

A schematic by Aehnelt (2011) in Figure 2.3 illustrates the structure of an airport divided into movement areas (yellow) and infrastructure facilities (red). The core of all aircraft-related activities at the airport is the runway and the corresponding visual and navigational aids. A detailed understanding of their functionality is necessary to comprehend their importance for a safe airport operation, although this topic is outside the scope of this work.

The runway lighting (1) is used during night to guide arriving aircraft towards the runway threshold (9). The Precision Approach Path Indicator (PAPI) (4) assists pilots by indicating the relation of the current descent angle towards the designated glide path, which is calibrated on the aiming point (8). Due to differences in aircraft properties, the designated touchdown zone (7) varies depending on the type of aircraft and deviates from the aiming point. The stopway (10) serves as a safety zone to enable aircraft to stop in case of an aborted take-off. Center lines (6) and edge markings (12) on movement areas assist pilots in aligning the aircraft by center, thereby ensuring that overlapping wings do not leave obstacle-free areas (clearance distance). After landing, aircraft use taxiways to reach the apron/ramp, which are designated for loading or unloading passengers, mail, or cargo, fueling, parking, or maintenance (International Civil Aviation Organization, 2018). Although terms such as maneuvering area or movement area are often used synonymously (Civil Aviation Authority, 2018), the ICAO explicitly defines the maneuvering area to include all parts of the movement area, except the apron (International Civil Aviation Organization, 2018).

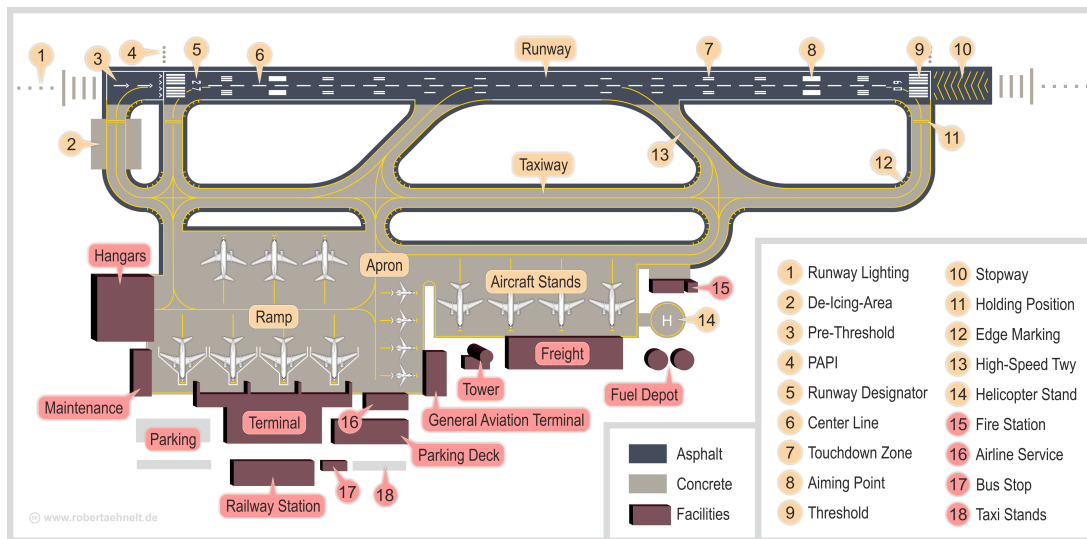


Figure 2.3: Schematic by Aehnelt (2011) of the structure of an airport including landside and airside infrastructure divided into movement areas (yellow) and infrastructure facilities (red).

Aircraft stands or parking gates are designated areas on the apron for aircraft parking and enable embarking or disembarking of passengers. The FAA distinguishes between four types of aircraft parking gates: contact, ground-loaded, and remote gates, as well as remain overnight (RON) positions Federal Aviation Administration (2018). While contact gates allow direct entry into aircraft via passenger boarding bridges (PBB), ground-loaded gates require passengers to walk onto the concourse and use stairs to enter the aircraft. Remote-gates are also located further away from the terminal and necessitate passenger transfer by bus to the aircraft stand. RON positions are used to park non-active aircrafts away from the terminal.

The servicing of aircraft on ground during parking times is referred to as aircraft ground handling, which includes fueling, aircraft maintenance, loading/unloading, cleaning, and catering (International Civil Aviation Organization, 2018). Although ground handling services themselves are not a native task of the airport operator, airports must provide necessary facilities. One exception is the provision of fire and rescue services, which is regulated in Annex 14 provided by the International Civil Aviation Organization (2018).

The following section will focus on the processes within the airport terminal. A typical structure of an airport terminal has been depicted in Figure 2.4. To optimize passenger flow and fulfill all security requirements, a physical separation is done for departing and arriving passengers, who deviate from each other. The ground level floor serves departing passengers, while the first floor handles arriving passengers. However, the structural realization is influenced by various factors, including planning, which is a trade-off between costs, design, and regional laws. While the exact layout must be taken into account when considering physical protection, it is irrelevant to understand the key processes and workflows.

Chronologically, departing processes start with passenger arrival at the airport via different modes of transport. Therefore, sufficient capacities must be available to reach the airport. As a result, airports need to provide parking decks and taxi stands for individual transport. Moreover, most airports are connected to regional and long-distance public transport through buses or a railway station. These facilities are located outside the terminal buildings, as shown in 2.3 (17), (18). Although these facilities are directly connected to the supply grid of the airport and have a connection to ICT systems in the terminal, their power demand for lighting, guiding systems, etc., corresponds to only 4.5% of the total power demand of the airport (Ortega Alba and Manana, 2016). From a modeling perspective, these infrastructures can be summarized under the term "external infrastructure" as they are located outside of the considered system boundary. These external infrastructures are depicted in pink in Figure 2.4.

During the check-in process, passenger identities are validated and boarding passes are printed. Nowadays, the identification process and boarding pass printing can be fully digitized and done electronically before arrival. Passengers who have not checked in before arrival head to the check-in counters, which are shown in light blue in Figure 2.4. Furthermore, hold baggage can be dropped off at the check-in counters. The EU distinguishes between hold baggage, intended to be carried within the hold of the aircraft, and cabin baggage, often referred to as carry-on baggage, as passengers can take along the baggage within the cabin of the aircraft European Commission (2008b). As passengers have access to the baggage in critical parts of the airport, security standards for cabin baggage are higher (see lists of prohibited articles in European Commission (2015) attachment 5-b for hold baggage and attachment 4-C for cabin baggage). Thus, passengers traveling with hold baggage need to head to the check-in counters after arrival.

Passengers and cabin luggage must be "screened prior to boarding an aircraft departing from a security-restricted area" (International Civil Aviation Organization, 2011). The screening measures prescribed by the European Union to prevent illegal transfer of prohibited articles into security-restricted areas are further defined in Commission Implementing Regulation (EU) 2015/1998 of the European Commission (2015). For this purpose, the airport operator provides certified screening devices in areas that enable passenger transfer into secured areas. These areas are referred to as security checks or security controls and their locations are marked in purple in Figure 2.4. After passing security checks, departing passengers head to the gate allocated to their flight. The airport operator must ensure that passengers and their cabin baggage, which have been screened, are protected from unauthorized interference from the point of screening until they board their aircraft (International Civil Aviation Organization, 2011). Moreover, before boarding, boarding passes are checked to prevent aircrafts being entered by people not assigned to the corresponding flight. Today, boarding passes are scanned electronically and verified by comparison with airline databases. Furthermore, this step can be used to track the progress of the boarding process and data about passengers within the aircraft. These boarding pass controls are conducted at the gates. In the sketched airport example, these are located directly in front of the passenger boarding bridge and marked in green. In case of international flights, travel documents such as passport and visa must be controlled by the competent

authorities. Thus, the terminal is divided into a part with domestic flights and international flights, whereas passport control separates them and is depicted in dark blue in Figure 2.4. To simplify traveling within Europe, on 14 June 1985, the Schengen Agreement was signed, setting the foundation for the Schengen Area, which enables the absence of border control of persons crossing internal borders between Member States. Thus, the terms "domestic" and "international" are often replaced by "Schengen" and "Non-Schengen" within the Schengen Area.

Passengers disembarking from an arriving aircraft with its origin in a contracting state of the Convention on International Aviation (International Civil Aviation Organization, 2006) and their cabin baggage are considered screened and therefore allowed to directly enter secured areas. However, airports must prevent unauthorized interference with non-screened passengers or baggage.

There are three cases for arriving passengers: final destination, transfer, and transit. Transit passengers depart on the same aircraft as that on which they arrived, often on long-distance flights divided into multiple legs. Reasons for these transit stops may be technical (e.g., refueling, maintenance) or operational (e.g., route optimization, personnel exchange). In contrast, transfer passengers depart on an aircraft other than that on which they arrived (European Commission, 2008b). If transfer passengers are changing from an international to a domestic flight, they must undergo immigration processing (indicated in dark blue in Figure 2.4) to be granted entry into the country. While some transfer passengers may need to pick up their hold baggage and undergo a second screening, most cases involve automatic routing of hold baggage to another aircraft (European Commission, 2008b). Special one-way passages are built to enable the transfer of these passengers from the arrival to the departure terminal (marked in orange in Figure 2.4).

Immigration is also mandatory for passengers arriving at their final destination with an international flight, before they can pick up their hold baggage within designated areas (see light blue in Figure 2.4). Custom controls (green area in Figure 2.4) are conducted on a random basis and in suspicious cases, before passengers are allowed to exit the terminal. Disembarking passengers from domestic flights are directly cleared to pick up their hold baggage and leave the airport.

The airport can be divided into airside and landside. The Civil Aviation Authority of the United Kingdom defines the airside as part of an aerodrome intended for the surface movement of aircraft, including the maneuvering area, aprons and any part of the aerodrome provided for the maintenance of aircraft (Civil Aviation Authority, 2018). The European Union adds the condition that access is restricted within this areas (European Commission, 2008b). This border is depicted in Fig. 2.4 as the red dotted line. Within the departure terminal, access to the airside is limited to screened departing passengers with valid flight tickets. For arriving passengers, the public and restricted areas are separated by a one-way exit, which may include customs control. It is essential to note that this design prevents unauthorized persons from interfering with luggage or reaching the departure terminal through reserved transfer passages.

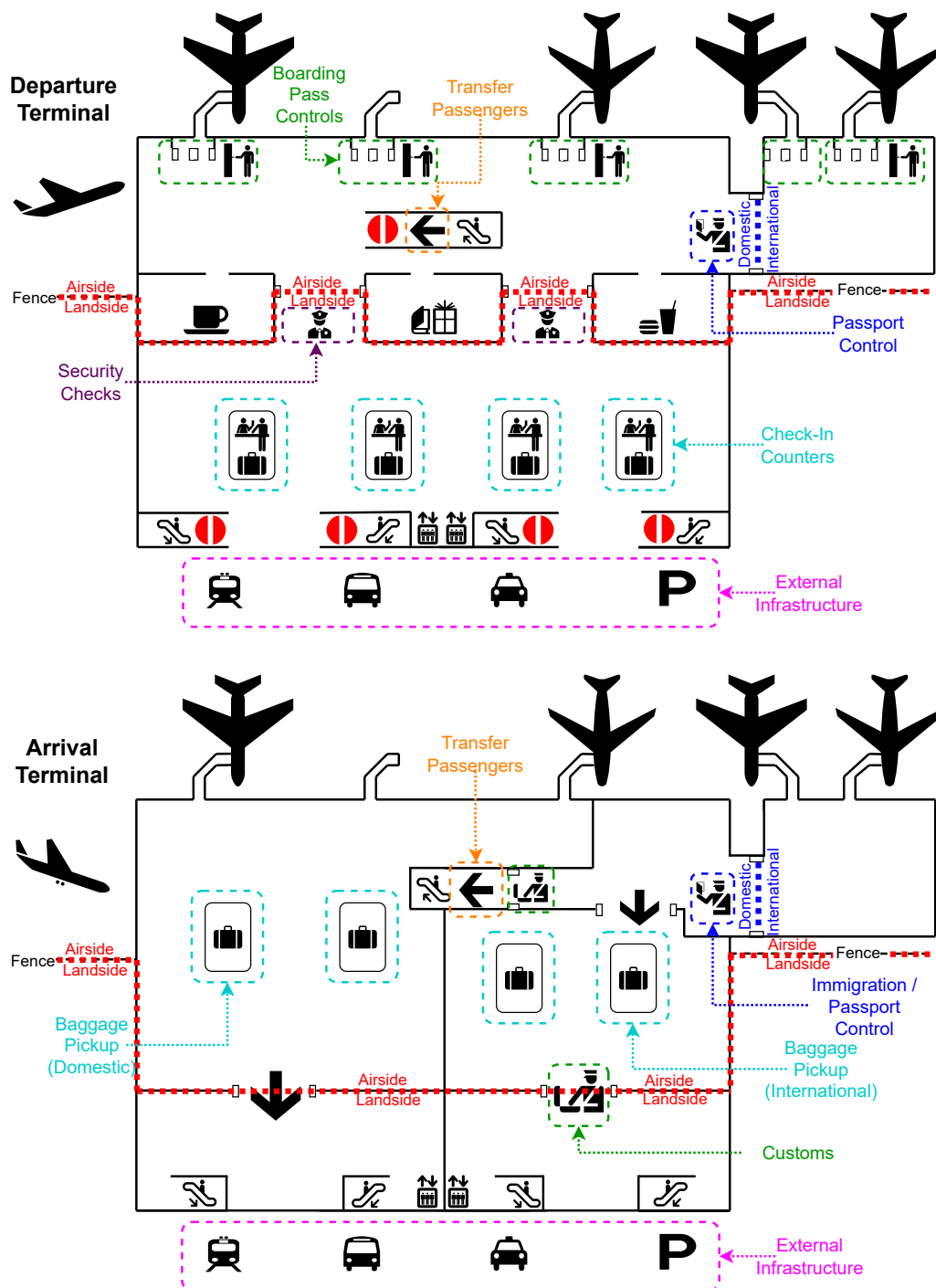


Figure 2.4: Schematic sketch of an airport terminal. Departures and arrivals are located on different floor levels to separate departing and arriving passengers, as they undergo different processes. Division into airside and landside is shown by the red dotted line.

Certain parts of the airside are designated as critical, defined by the European Union as “all parts of an airport accessible to screened departing passengers and all parts through which screened departing hold baggage may pass or be held, unless it concerns secured baggage” (European Commission, 2015). Temporary establishment of these critical areas for specified periods is allowed, provided previous conditions are met. However, this is not feasible for larger airports due to the need for security searches beforehand, as these areas might become contaminated with lower security standards.

## **2.3 Modeling and Simulation of Airport Processes**

Simulations are a powerful tool to optimize efficiency and support decision-making during the design process, normal operations, or crisis situations. According to Winsberg (2003), computational intensive methods such as simulations and numerical experiments are used to learn about the behavior of systems driven by mathematical models. However, these models themselves are based on theoretical foundations.

Stachowiak (2012) has defined three main characteristics of models. Firstly, models are always models of something - illustrations or re-representations of natural or artificial originals. These models contain a finite number of attributes of the original, which are represented by linguistic symbolizations named predicates. The sets of attributes and their predicates form an attributive system.

Secondly, models generally do not capture all attributes of the original, but rather only those that seem relevant to the respective model creators and/or users. The chosen attributes are highly dependent on the system boundaries and the goal that should be achieved.

Thirdly, models are not clearly assigned to their originals per se, but instead fulfill a replacement function for a specific user, a certain period of time, and/or under consideration of specified mental or actual operations.

Applying this understanding to the modeling of passenger processes, including passenger flows, Schultz (2010) identified several requirements for an application-oriented model:

1. The movement behavior of passengers must be based on a microscopic model approach, which enables the mapping of essential characteristics of the passenger;
2. A separation must be made between the modeling of handling processes and the mapping of passenger movement to facilitate efficient analysis;
3. All specific process- and passenger-related properties (parameters) must be collected and analyzed through targeted empirical measurements;
4. Validation of models developed for handling processes and passenger movement mapping is essential to ensure that application in a practical environment leads to sustainable and high-quality results.

---

To develop a model pipeline for the whole traffic chain from door to door, Widemann and Möller (2013) included the way to the airport in their model, but neglected the individual movement of passengers and their interaction. However, they approximated passenger movement between processes using statistical data. Other researchers, such as Curcio et al. (2007), have implemented models using software like AnyLogic (The AnyLogic Company, 2024), which include passengers, baggage, and aircraft flows within the airport, while accounting for traffic flow to the airport and passenger movement. These examples illustrate that the goal of investigation and system boundaries strongly influence the choice of modeling approach and selected attributes. The modeling approach used in the application case will be further described in Chapter 5.

## 2.4 Safety and Security Issues at Airports

This section addresses common hazards and threats at airports. Hazards are events or conditions that have the potential to cause harm, damage, or loss without any intentionality behind them. They refer to undesirable occurrences with uncertain consequences but no malicious intent. For example, extreme weather conditions can be considered a hazard because they pose danger to people, aircrafts, and airport infrastructure. Moreover, hazards differ from failures as failures can occur without resulting in a hazard, and a hazard may occur without any preceding failures (Leveson, 2012; Pettersen Gould and Bieder, 2020; International Civil Aviation Organization, 2012).

Threats, on the other hand, are deliberate acts or intentions by individuals or groups to cause harm, damage, or loss. They involve active planning and execution of actions with malicious intent (Mentges et al., 2023). For instance, if a person plans to cause an explosion at the airport, that individual becomes a threat because they have intentions of causing casualties and structural damage.

In summary, the main difference between hazard and threat is that a hazard refers to an undesirable situation or event without any intentionality behind it, while a threat involves deliberate actions with malicious intent to cause harm, damage, or loss. Within cyber security the term cyber threat is explicitly referring to computer viruses and more malicious deliberate attacks on computer systems (Lim, 2014).

The concept of safety encompasses the state of being protected from harm or injury caused by hazards. In contrast, security involves the process of protecting assets, resources, or individuals from potential threats. Safety focuses on minimizing hazards and ensuring a safe environment, whereas security involves taking measures to prevent deliberate acts of harm or damage caused by threats (Mentges et al., 2023).

The concept of risk includes the fact that an exposure, such as the degree to which a system is subject to hazards or threats, does not necessarily lead to harm or loss but generates a potential for negative impact. Risk is the potential for an event to have a negative impact

or cause harm, damage, or loss. It involves evaluating and quantifying the likelihood of a hazard or threat occurring and its possible consequences (Aven, 2011).

Incidents are unplanned events that disrupt normal operations without necessarily resulting in negative consequences. For example, a power outage during a storm would be considered an incident because it caused disruption to the electrical supply but did not result in casualties or significant damages.

Accidents, however, are unplanned events that result in harm, damage, or loss due to chance or error. They occur when someone makes a mistake or when circumstances beyond their control lead to undesirable outcomes. For instance, if a technical failure at an aircraft leads to a crash, it was not a deliberate act but rather the result of unforeseen events.

Attacks are planned actions with malicious intent (security-related) to have negative impact. They involve targeting individuals, property, or systems for the purpose of inflicting injury, destruction, or disruption (Mentges et al., 2023; Bieder and Pettersen Gould, 2020). Cyber attacks, which are often specified as ICT infrastructure targets, are a type of attack that involves malicious electronic attacks on electronic systems (Lim, 2014). The protection of electronic systems from malicious electronic attack and dealing with the consequences of such attacks is encompassed by the term cyber security. (Centre for the Protection of National Infrastructure, 2012)

To successfully protect the airport system from incidents and guarantee safety, security, and cyber security, it is essential to identify known hazards and threats. In the following sections, known hazards and threats for aircraft operation, airport infrastructure, and ICT systems will be discussed.

### **2.4.1 Aircraft Operation**

A data-driven risk assessment was conducted by Distefano and Leonardi (2014) to identify potential hazards for aircraft operation. A total number of 1749 accidents and serious incidents were analyzed between 1980 and 2010 to gain quantitative knowledge about the probability and severity of different risks.

The incidents were dissected into seven distinct flight phases, namely parking, taxiing, take-off, landing, and assigned to separate scenarios (landing short, landing veer-off, landing overrun, take-off veer-off, take-off overrun, ground collision in landing/take off). The terms "short", "veer-off", and "overrun" all refer to situations where the aircraft leaves its intended area for take-off or landing on the runway. Landing short means missing the runway threshold, while veer-off refers to a situation where the aircraft leaves the runway sideways, and overrun is an accident during a landing or an aborted takeoff when the pilot cannot prevent the aircraft from leaving the paved surface of the runway (Distefano and Leonardi, 2014).

Furthermore, the incidents were classified as possibly caused by environmental conditions, runway conditions, aircraft performance characteristics, human factors, or unknown reasons. The presence of certain conditions during the incidents was considered relevant, with heavy rain and crosswinds posing a major issue during the landing phase with an impact probability above 10%, leading to landing short, veer-off, or overrun (Distefano and Leonardi, 2014). Conversely, fog resulted in a significant number of ground collisions. Regarding runway conditions, aquaplaning and the related longer braking distances were present during 18.31% of landing overruns, while Distefano and Leonardi (2014) leave out whether the aquaplaning occurred during heavy rainfall or afterwards. The analysis of aircraft performance characteristics revealed that engine failures and resulting thrust imbalance on both sides of the aircraft led to 27.78% take-off veer-off incidents, while landing gear failures posed problems for landing veer-off as well as take-off veer-off (Distefano and Leonardi, 2014). Inadequate crew competence was found to have the highest probability of causing incidents during landing and take-off, with little relevance during ground navigation.

Although many incidents could not be categorized due to unknown causes, the probability assessment provided a comprehensive overview of the challenges in aircraft operation. Passive risk assessment tools, such as fishbone diagrams, were used to identify cause-and-effect relationships between hazards and effects, enabling preventive measures to mitigate these issues (Distefano and Leonardi, 2014).

Different classes of aircraft operations (e.g., general aviation, commuter aircrafts, short-range, long-range flights) were employed to quantify the severity, categorized based on maximum takeoff weight and flight distance. Severity was qualitatively measured and assigned a rating (negligible, minor, major, hazardous, catastrophic) according to the ICAO recommendations (International Civil Aviation Organization, 2012). Although no visible trend emerged, the prevalence of incidents had a significant impact on system performance, highlighting the need for stringent safety management standards.

Moreover, the increasing presence and advancement in drone technology pose threats to airport safety and security. Unmanned aircraft systems (UAS), also known as drones, can interfere with critical airport systems such as air traffic control, radar systems, and communication networks, potentially leading to incidents and accidents (Wild et al., 2016; Lykou et al., 2020). Investigations by Pyrgies (2019) identified an increased collision risk during landing, as the aircraft gains height faster during take-off and collisions are more probable below 1 km altitude (Distefano and Leonardi, 2014). To mitigate these threats, airports must invest in advanced detection and countermeasure systems that can identify and intercept drones before they cause harm. Collaboration between airport operators, law enforcement agencies, and national security organizations is essential to share information and develop effective strategies against drone threats (Lykou et al., 2020). Countermeasures for mitigating drone threats range from electronic interdiction/signal jamming to kinetic physical methods like UAS net capturing and kinetic electronic (e.g., high power microwave or laser guns). The primary responsibility for ensuring safety and security lies with the airline during non-airport phases, which are outside the scope of this work.

### **2.4.2 Airport Infrastructure**

The airport infrastructure, which includes both physical assets and technical systems, serves as the backbone for aircraft operation. The reference to purely physical assets encompasses buildings, fences, pavement, while also including technical systems such as electrical or communication systems.

Structural fires and failures pose a general risk to all types of infrastructures, including airport terminals, as demonstrated by the collapse of the Dubai Airport terminal in 2004 (Coppola, 2020). Possible hazards encompass design, geographic location, climate, seismicity, construction materials, maintenance, and safety standards employed at the infrastructure (Coppola, 2020). Apart from safety concerns, incidents such as the suicide bomber attack in public areas of the airport terminal building in Brussels in 2016 (Price and Forrest, 2016) highlight the need for countermeasures to ensure physical infrastructure integrity and demonstrate the importance of maintaining structural integrity.

Extreme weather events, sea-level rise, and other climate-change induced effects threaten structural integrity, leading to loss of infrastructure or physical damage (Voskaki et al., 2023). This physical damage may cascade through the system, causing power outages or ICT system failures due to cut wiring as well as water system leakages from damaged pipes. The causes for blackouts will be further investigated in Section 4.1 and a closer look at the ICT infrastructure is taken in Subsection 2.4.3.

Apart from airport buildings, movement areas are responsible for ensuring continuity of aircraft operation. The runway is exposed to strong short-term impacts during take-off and landing, as well as vibrations from aircraft operations and environmental factors on the long-term (Meng et al., 2023). To ensure pavement sufficiency for corresponding aircraft types, the ICAO introduced the pavement classification number (PCN), including information about pavement type (rigid or flexible), subgrade strength category (modulus of subgrade reaction  $k$  quantifies the support of the pavement from the surface below as a spring constant), maximum allowable tire pressure category, and evaluation method (technical evaluation or operational experience) (International Civil Aviation Organization, 2018). However, runways are not designed to resist extreme loads such as rough impacts or explosions. The development of models to forecast runway behavior under various conditions and loads using numerical models is an ongoing field of research.

Radio and navigational aids distributed throughout the airport are exposed to various conditions, making all risks applicable to them. To mitigate equipment failure or malfunctioning, regular checks and maintenance work are conducted. However, human error during these tasks poses a problem, as accidental damage may occur. Regarding security, intentional damage poses a risk, while also interference signals emitted by UAS (Lykou et al., 2020). Moreover, cascading effects from other systems such as power-outages or cyber-attacks might be the cause for failures of radio and navigational aids.

Perimeter protection is an essential measure to mitigate unauthorized access to critical areas. The ICAO stipulates fencing of all these areas, including a cleared area on both sides of

the fence or barrier, to facilitate patrols and make trespassing more difficult, accompanied by security lighting to guarantee illumination (International Civil Aviation Organization, 2011). However, fences also mitigate the hazard of wildlife entering movement areas and colliding with aircraft.

### 2.4.3 Cyber Security at Airports

Cyber-security has gained importance in recent decades due to the increasing number of cyber attacks on information systems and networks (Pricewaterhouse Coopers International, 2014). The National Institute of Standards and Technology defines cyber security as “the ability to protect or defend the use of cyberspace from cyber attack”, whereas the latter are “targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information” (Joint Task Force Transformation Initiative, 2012).

The CIA model provides a framework for describing three attributes that are crucial to security: confidentiality, integrity, and availability. Confidentiality refers to protecting sensitive information from unauthorized access or disclosure, which can be achieved through measures such as encryption, access controls, and user authentication (Priyadarshini, 2019). Integrity ensures consistency, trustworthiness, and accuracy of data, while availability focuses on the accessibility of data and services when needed by authorized users. Measures such as digital signatures, hashing algorithms, and input validation can prevent unauthorized modifications or tampering with information (Priyadarshini, 2019).

Cyber security measures aim to conserve CIA by deploying various countermeasures. The successful establishment of these measures involves the 3Ps: people, plan, and practice. People play an important role in cyber security either in defense or as victims. A plan should exist that predefines organizational as well as technical response to an attack. Regular practice should be done to test the functionality of countermeasures and train involved personnel (Priyadarshini, 2019).

Cyber attacks have been spread via large interconnected networks, including the internet, since their first occurrence in 1834 in France. The brothers Blanc invaded the semaphore telegraph network to steal information about stock market changes in Paris by installing a man-in-the-middle system (Šimkevičiūtė, 2020). Nowadays, various types of cyber attacks exist and can be divided into passive and active attacks.

Passive attacks attempt to gather and make use of information, while active attacks alter the system. Insider attacks occur when an attack is initiated from within the organization, whereas outsider attacks are launched from outside. In this context, inside refers not to a spatial location, but to authorized access to the attacked system (Shirey, 2000).

As information and computer systems of critical infrastructures are complex and highly interconnected, the number of possible attack vectors is endless. Nevertheless, some of

these have to be highlighted, as there is evidence that critical infrastructures are vulnerable with regard to this type of attacks.

Supervisory control and data acquisition (SCADA) systems build the interface between the physical and cyber levels, making them a prime target for cyber attacks. Cyber attacks on these control systems have occurred in various critical infrastructures, such as water services, nuclear power plants, and electricity distribution stations (Abrams and Weiss, 2008; Kesler, 2011; EISAC, 2016). Therefore, deploying cyber security measures at all critical infrastructures is inevitable.

To protect airport systems from cyber threats, a risk assessment must be conducted. The Airport Cooperative Research Program (ACRP) provides best practice guidelines for this purpose Murphy et al. (2015), collected from various sources including the National Institute of Standards and Technology (Joint Task Force Transformation Initiative, 2012), MITRE (MITRE Corporation, 2014), Verizon, and others. Countermeasures can be categorized into management measures (e.g., risk or security assessment), operational measures (such as training or incident response), and technical measures (e.g., access control/authentication). A study by Lykou et al. (2018) comparing "classic"/less digitized airports with modern smart airports suggests that, though smart airports have a higher exposure to possible cyber attacks, they also prepare themselves better by introducing strict policies regarding software use, data encryption and by establishing highly elaborated cyber security management systems. However, "Bring-your-own-device" controls (e.g., self-check-in via smartphone) introduces numerous new attack vectors. Following Lykou et al. (2018) "major cyber security threats against IoT applications in smart airports can be segregated into the following categories: (i) Network and communication attacks; (ii) Malicious software; (iii) Tampering with Airport Smart Devices; (iv) Misuse of Authorization; and (v) Social and Phishing attacks".

Countermeasures against cyber attacks on airports include physical separation of networks or end-point systems, software solutions such as anti-malware software or security updates, limiting connections, and training IT personnel. However, a complete protection from cyber attacks is impossible, and proper early detection, response, and recovery methods become important (Murphy et al., 2015). Technical solutions, such as anomaly detection and antivirus and malware detection software, can be implemented alongside training processes or cyber security policies as part of a cyber security management system.

## **2.5 Emergency Management and Management Systems**

While the term resilience is a relatively new concept in the context of critical infrastructure protection, research continues to explore its various definitions (Mentges et al., 2023). In contrast, emergency and crisis management have been well-established tools for operators to prepare for any incident. For the specific application case in this work, a closer examination will be conducted on safety and security management systems at airports, providing an overview of handling emergency situations within the power grid.

---

In aviation safety and security, distinct regulations govern separate aspects of management. The ICAO and European Union have prescribed the establishment of a safety management system (International Civil Aviation Organization, 2012; European Commission, 2017). In the early stages, these systems must ensure proper maintenance to mitigate technical failures. Later on, human factors became the primary focus, with standard operating procedures introduced as a key component. Today, safety management systems must also address organizational factors that may contribute to crisis situations, such as insufficient communication or unclear responsibilities. Proper risk assessment assures to be aware of the most common threats (International Civil Aviation Organization, 2012).

From a regulatory perspective (See European Union Aviation Safety Agency, 2023, Annex VII Section 2), a safety management system for airports must incorporate the following aspects to obtain certification:

- Clear description of responsibilities and documentation, especially with contractors fulfilling safety relevant tasks at the airport, such as aircraft ground handling;
- A mechanism to guarantee that contractors are operating compliant to the arrangement;
- A wildlife management system to mitigate risks, such as bird strike or collisions with deer;
- Coordination of aircraft, vehicles and personnel on the movement areas, that are not covered by air navigation services;
- Operating procedures in winter, adverse weather conditions, low visibility and night;
- Proper storage and handling of fuel;
- Availability and application of manuals regarding maintenance and repairs;
- An emergency plan covering emergencies at the airport and its surroundings;
- Provision of adequate rescue and firefighting services including training of the fire fighting personnel;
- Training and qualification standards for all personnel involved in airport operation;
- Access rules to keep inadequately trained personnel away from movement areas;
- An occurrence reporting system and analysis to guarantee continuous improvement of the safety management system.

In depth details including a closer look at ground handling and apron management can be found in the EASA guidelines (European Union Aviation Safety Agency, 2023). Although a lot of urgent risks are covered by these measures, apart from proper maintenance, none of these measures are handling power outages in particular.

From security point of view, current regulations concentrate on establishing measures to prevent acts of unlawful interference, i.e., acts such as to jeopardize the safety of civil aviation and air transport (See International Civil Aviation Organization, 2020, Chapter 1), which includes:

- unlawful seizure of aircraft in flight;
- unlawful seizure of aircraft on the ground;
- hostage-taking on board aircraft or on aerodromes;
- forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility;
- introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes;
- communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

Thus, the prescribed measures (See European Commission, 2015, Chapter 1) concentrate on procedures for

- access to airside and security restricted areas including requirements for identification of crew and staff members as well as vehicles,
- screening of all persons (passengers and staff) granted access to these areas to find prohibited articles,
- screening of baggage,
- examination of vehicles entering these areas,
- screening and protection of cargo and mail,
- surveillance and physical controls of restricted areas.

### **2.5.1 Emergency Management of Power Systems**

Some measures, such as preventing physical access to exposed electrical equipment or detonations damaging cables and disrupting power supply, may support mitigating the risk of a power outage. However, existing measures are unable to tackle this issue directly, as they can be easily evaded by cutting supply cables outside restricted areas or causing an electrical surge at devices in public areas. Additional preventive measures would be considered voluntary, but are often deemed uneconomic due to the estimated low probability

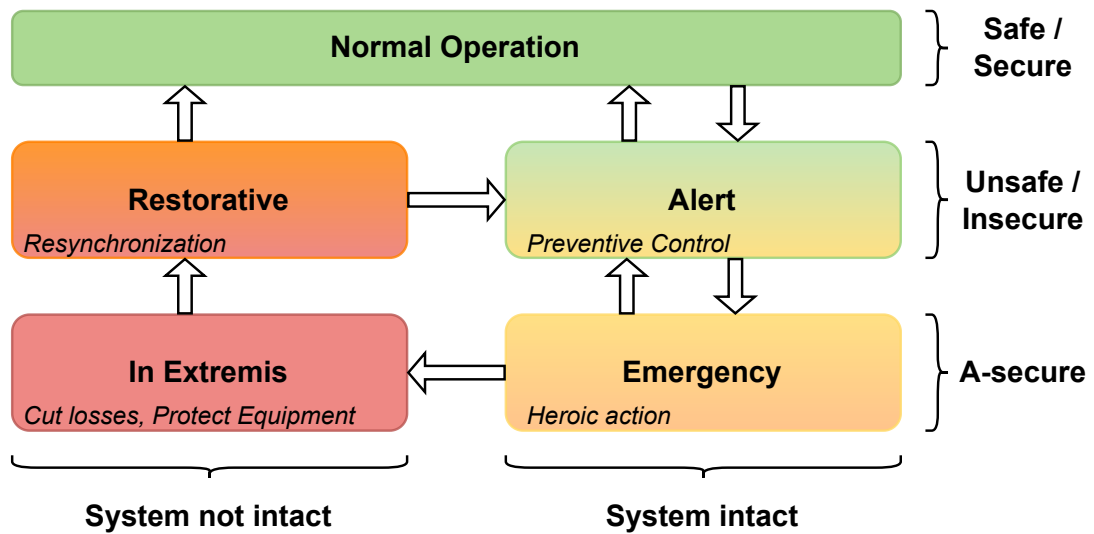
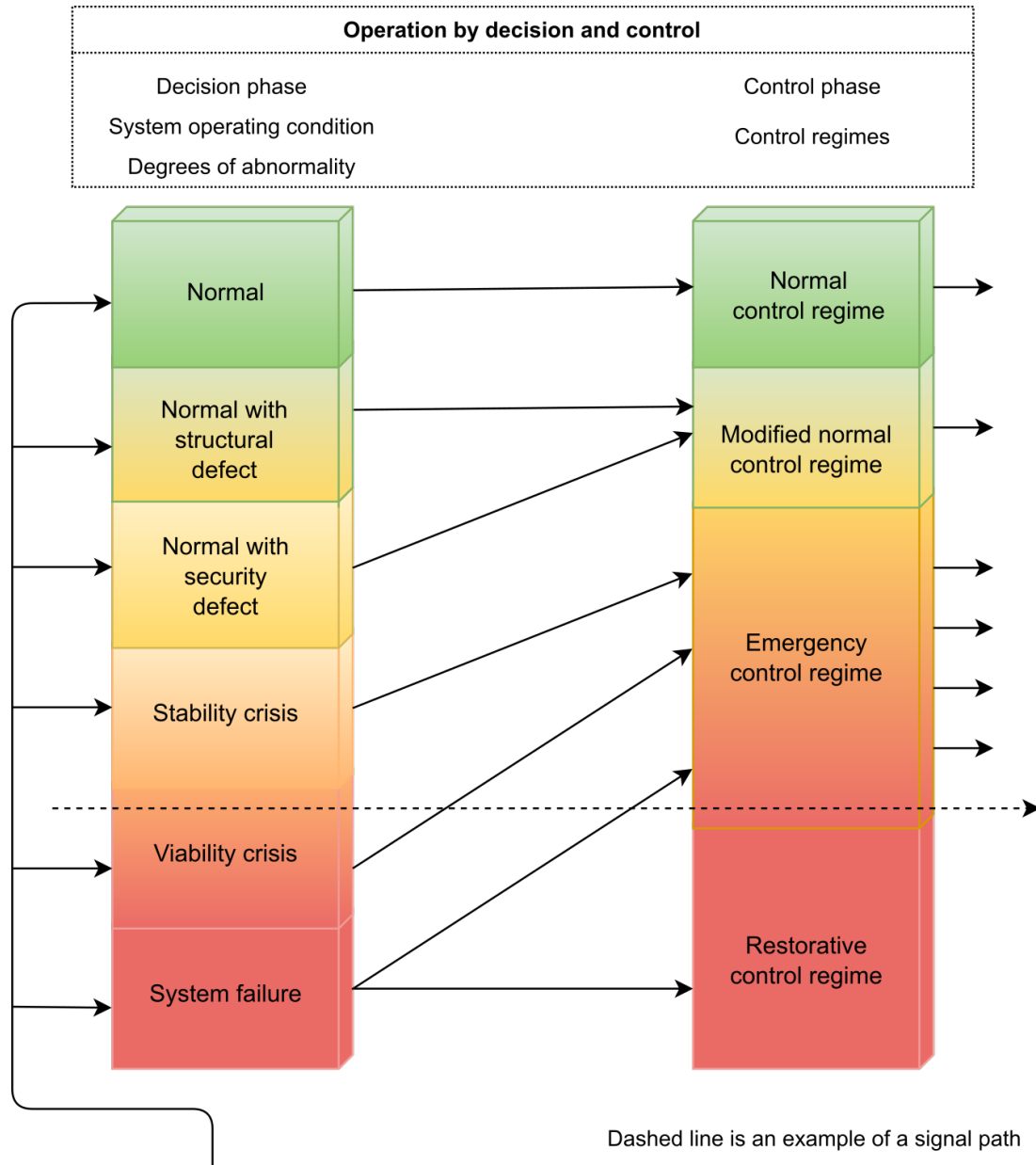


Figure 2.5: System operating states as defined by Fink and Carlsen (1978). The color scheme is modified to emphasize criticality (from green=normal to red=critical).

of outages. Nevertheless, the increasing amount of information and digitization render manual crisis management of large interconnected infrastructure systems no longer feasible. Even with the assistance of an advisory body, this infeasibility persists. Consequently, the possibility of computer-assisted help for crisis units must be considered.

The approaches employed by operators of critical infrastructures within the power supply sector have been established through experience and innovation. The concept of operation by decision and control was introduced by Zaborszky et al. (1980) to address the increasing complexity of power grids and ensure a safe and secure operation of large interconnected power systems. The underlying principles of this approach were further developed, including the identification of operational states of a power system as described by Fink and Carlsen (1978) and is depicted in Figure 2.5. These operational states include normal operation, characterized by a stable power equilibrium, where frequency and voltages are maintained within prescribed limits while providing power to all connected loads. Typically accepted voltage variations during normal operation are within 2% or 0.002 per unit (Ilić and Zaborsky, 2000). In contrast to crisis situations, economic factors play a significant role in grid operation during normal operation, influencing the allocation of resources to minimize costs and maximize profit.

An unexpected behavior or loss of equipment may destabilize conditions, leading to a power imbalance if either more power is generated than needed or too much power is consumed. A frequency increase may result from an oversupply of power, while a decrease occurs with a shortage (Kruse et al., 2021). Such deviations trigger the alert state and demand for preventive control to restore previously defined limits and achieve normal operation. Tolerable deviations during alert mode typically reach up to  $\pm 5\%$ , before system state changes into emergency mode (Ilić and Zaborsky, 2000). If emergency measures fail, and



At sample time, enter data, measurements

Figure 2.6: System operation by decision and control after Ilić and Zaborsky (2000). The color scheme is modified by Koch et al. (2019b, ©IEEE 2019) to emphasize criticality (from green=normal to red=critical).

---

a recovery of the system back to the alert state cannot be achieved, the system state transitions into the in extremis state as defined by Fink and Carlsen (1978). This leads to the collapse of the power grid or at least parts of it. To prevent further damage, protection of equipment has top priority during this system state. If there are capabilities left to restart the system and the source of stress on the system has been removed, the system can enter the restorative state. From this point, it may transition to either normal or alert operation Fink and Carlsen (1978).

The concept of decision and control plays a crucial role in handling actions taken during transitions between phases. A schematic representation of these state transitions is provided in Figure 2.6. During the decision phase, continuous surveillance and monitoring are conducted to determine the system's condition (left side in Figure 2.6) and select the best regime of actions (right side in Figure 2.6) (Zaborszky et al., 1980). Subsequently, adequate actions are taken during the control phase. The distinction between direct control using logic trees for automatic decision, optimizing control, i.e., solving for the best control decision using a mathematical model before taking action, and adaptive control is made by Dy Liacco (1967). Adaptive control refers to a man-machine combination where the human adjusts settings, parameters, and logic used during direct and optimizing control.

This work concentrates on blackouts or power shortages, which result in either UPS and emergency power generators taking over or the grid power supply being insufficient for full operation. In both cases, a complete system failure has not occurred. However, the viability and stability of the power system are threatened, demanding measures within the emergency control regime. According to Ilić and Zaborsky (2000), this includes the control methods presented in Table 2.1. However, these measures are proposed for large-interconnected power systems on an energy distribution level and not for small-scale low-to-medium voltage networks, rendering some of them inapplicable for internal infrastructure control.

Summarizing Table 2.1, the measures that an airport operator can initiate at an infrastructure level are very limited. Regulating the injected power from either the grid or emergency generators is a way to increase grid stability. Although this approach may seem straightforward, in practice, buying and maintaining emergency power generators is extremely expensive, leading to a conclusion that they should only fulfill basic needs as prescribed by law, such as for evacuation purposes or safety procedures. Moreover, most emergency generators operate on diesel, resulting in an increased demand for storage capacities and a constant external supply of diesel.

Disconnection of parts of the infrastructure's electrical system may enhance grid stability by reducing load and rebalancing injected and demanded power or removing faulty components that cause short circuits. Although this strategy appears promising to ensure grid stability, the structure of subsidiary circuits is driven by structural conditions of the infrastructure rather than being designed from a system performance perspective. Therefore, disconnecting these circuits may lead to an unpredictable, cascading effect on the infrastructure's performance.

Table 2.1: Control methods proposed by Ilić and Zaborsky (2000) and their corresponding measure and applicability in low-voltage networks:

| Control Method                                                                                                                | Applicable?                     | Corresponding measure                                     |
|-------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-----------------------------------------------------------|
| Protective relaying or minor restructuring to eliminate faulty components from the system                                     | Yes                             | Turn off subsidiary circuits                              |
| Use Flexible AC transmission systems, breaking resistors, load skipping                                                       | No                              | -                                                         |
| Load shedding or major structural changes that put the system into an integrity crisis mode                                   | No                              |                                                           |
| Frequency reduction                                                                                                           | Partially, dependent on devices |                                                           |
| Use of reserves                                                                                                               | Yes                             | Regulate power generation from emergency power generators |
| Fast turbine run back at power plants                                                                                         | No                              |                                                           |
| Help from neighboring areas (energy market)                                                                                   | No                              |                                                           |
| Exploiting time-limited overload capability of the equipment                                                                  | No                              |                                                           |
| First-stage structural control (starting new generation, returning equipment from maintenance or load shedding)               | Yes                             | Turn loads and/or generators on/off                       |
| Second stage structural control-islanding (separation of power network into parts, some of which are not supplied with power) | Yes                             | Turn off subsidiary circuits                              |

---

Turning single loads on and off can rebalance injected and demanded power. In contrast to removing subsidiary circuits, concentrating on single loads has only a limited impact on reducing demanded power, but it is a more controlled approach. However, to achieve controlled and efficient load shedding, the choice of these loads must be based on knowledge about their impact on system performance.

### **2.5.2 Cyber Security Measures at Airports**

Regarding cybersecurity, no state-of-the-art emergency plan exists. The International Civil Aviation Organization (2011) has recommended in Annex 17, point 4.9, that each Contracting State should develop measures to protect ICT systems used for civil aviation purposes from cyber threats that may compromise safety. However, a worldwide prescription for implementing cyber security measures does not currently exist. The EU has incorporated detailed cyber security measures into an amendment to European Commission (2015) in September 2019 (European Commission, 2019), which includes the following tasks for airport operators:

- Critical information and communication technology systems and data are identified and protected from cyber attacks that could affect civil aviation security;
- Measures are detailed in the security programme to ensure protection from, detection of, response to, and recovery from cyber attacks;
- Systems and data are identified, developed, and implemented with measures to protect them from unlawful interference, based on a risk assessment carried out by the airport operator;
- Enhanced or standard background checks are conducted for persons with administrator rights or unsupervised and unlimited access to critical information and communication technology systems and data used for civil aviation security purposes;
- Persons with roles and responsibilities related to cyber threats receive training.

As a result, EU airport operators are required to adapt their security programmes to comply with the law. However, these formulations focus on organizational measures, leaving room for interpretation from a technical perspective.



# Modeling the Airport as a Dynamic Cyber-Physical System

---

Within Chapter 2 , the airport system has been introduced as a critical infrastructure, along with the processes necessary to ensure its service as such. The importance of airports as part of the air transport system, handling aircrafts and passengers, has also been highlighted. Furthermore, the vulnerability of airports as critical infrastructures has been emphasized in terms of safety and security concerns, including aircraft operation, airport systems, power supply and ICT infrastructure. Pursuant to emergency management frameworks, prescribed measures have been evaluated for their added value in preventing or responding to blackouts or cyber attacks. However, current state-of-the-art management systems solely meet basic needs to ensure aviation safety and security without considering the impact on airport systems. Nevertheless, a successful Critical Infrastructure Protection (CIP) system is expected to ensure the availability of critical services during crisis situations.

The first step in guaranteeing this is to understand the impact of crises and reactive measures on the airport system. In this work, a pipeline is proposed that can evaluate and propose suitable preventive and reactive measures for blackouts and cyber attacks. The pipeline's features include:

- Identification of threats and hazards causing blackouts to reason preventive measures;
- Identification of vulnerabilities within ICT systems to strengthen the system;
- Modeling the impact of blackouts or cyber attacks on airport performance;
- Modeling the impact of reactive measures (e.g., load shedding to stabilize the power grid) on airport performance;
- Evaluate measures using key performance indicators (KPIs).

Today, airports operate as complex, interconnected systems that rely on reliable power and data distribution. The majority of processes are digitized, with computers playing a crucial role in managing security scanners, processing information, and controlling other electrical devices. However, if these systems fail, critical data fails to reach relevant stakeholders, compromising the integrity of airport operations.

In order for the model to be effective, it must be able to handle such scenarios and ensure that essential data is disseminated to those who need it. This requires a robust framework that can navigate the complexities of digitized processes and provide timely, accurate information to support informed decision-making. Therefore, the model used for decision support must be able to

- model single devices with its electrical and ICT properties,
- mirror the dependencies of its interconnections,
- describe the interaction of these devices with regard to system properties,
- and transfer changes of these properties on the airport processes.

### 3.1 The Airport Infrastructure as a Cyber-Physical System

The term cyber-physical system (CPS) was described in the Acatech report “agendaCPS – Integrated research agenda Cyber-Physical Systems” as a system that connects the physical world with the world of information technology, describing its complex interactions (Geisberger et al., 2015). More concretely, a cyber-physical system can be characterized as a system with complex interactions between embedded systems, application systems, and infrastructures, along with their connections to the Internet, based on networking and integration. Furthermore, a CPS involves human-machine interaction (HMI) within the application domain (Geisberger et al., 2015). As this description aligns with the previously defined model criteria, the airport has to be considered as a cyber-physical system.

Figure 3.1 shows a passenger’s journey through the departure area of the Suvarnabhumi International Airport in Bangkok, starting at the escalators/elevators (blue) and ending at the boarding area (purple). The path (orange dashed line in 3.1) involves various steps, including check-in (brown), security checks (dark green), and gate arrival. Throughout these steps, passengers or personnel interact with electrical devices and ICT systems, such as elevator control units, computers, luggage conveyor belts at the check-in counter, body scanners, and boarding pass scanners.

In Figure 3.1, these electrical devices or ICT systems are depicted as dots, with their color indicating operating status (green for on, red for off). Figure 3.1 (bottom) shows the same process steps under disturbed conditions, where some devices are out of order. Possible scenarios causing this disruption could be power shortages or outages of ICT systems.

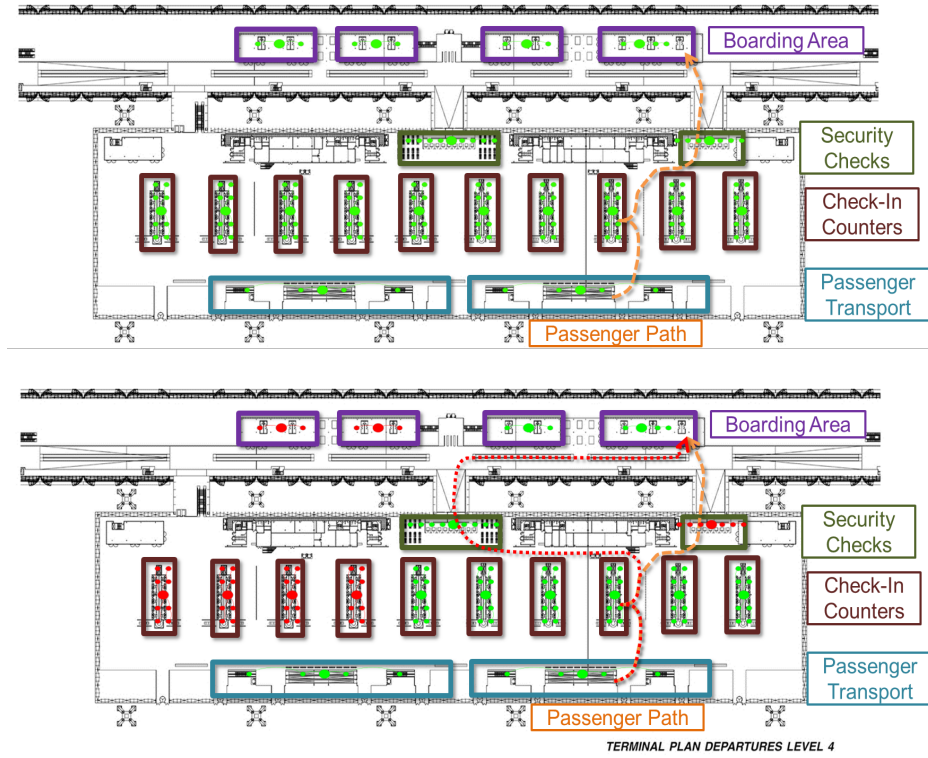


Figure 3.1: Passenger trajectory through an airport terminal under full performance (top) and disturbed conditions (bottom). Green and red dots represent operating and non-operating objects within the CI. Rectangles represent groups of objects connected to a certain process (Koch et al., 2018, ©IEEE 2018).

For the passenger, these disruptions result in a detour (red dotted line) due to security check outages, leading to an extended walking distance and potential bottleneck effects as the number of passengers per available security check increases. This may cause a delayed arrival at the boarding area, potentially resulting in missing the flight (Koch et al., 2019b, 2018).

This example illustrates the tight coupling between the airport's infrastructure and the processes taking place, including human behavior, which is revealed through its intricate relationship with electrical and ICT devices that form a complex infrastructure network.

A common way to describe such complex systems is to employ graphs (Sayama, 2015). A graph is a mathematical structure consisting of a set of vertices that are connected by a set of edges. In Figure 3.2 (a), a basic graph featuring seven vertices connected by nine edges is depicted. Assigning labels to vertices or edges, as shown in Figure 3.2 (b), enables the graph to store more information about vertex types and edge properties.

The edges in Figure 3.2 (b) contain weights that allow for the addition of information about edge properties relevant to graph algorithms, such as traffic speed for routing algorithms.

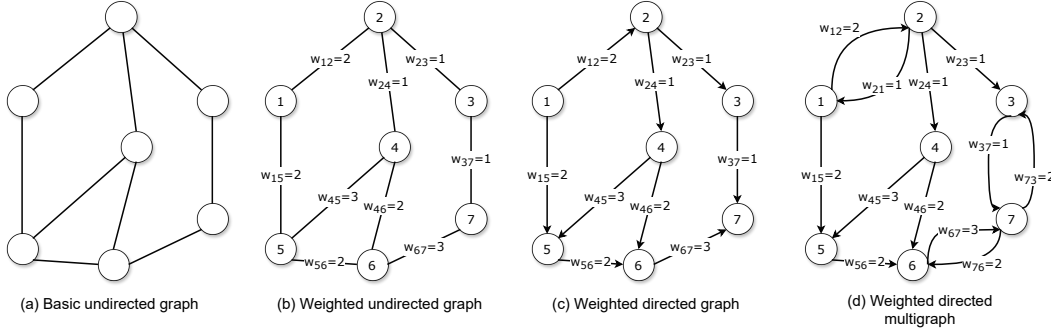


Figure 3.2: Schematic showing different types of graphs and their features.

This results in a weighted undirected graph. In some use cases, vertices may not have bi-directional connections, e.g., one-way streets in road networks connecting two crossings. To address this, directions can be assigned to the edges, resulting in a directed graph or digraph, which is illustrated in Figure 3.2 (c).

If multiple connections between nodes have different properties, a multigraph such as that shown in Figure 3.2 (d) may be employed to represent these relationships. The edge weights in a multigraph depend on the direction of the connection.

Mathematically a graph  $G(v_1, \dots, v_n, e_{v_i, v_j})$  is defined by either a list of edges  $e_{v_i, v_j}$  each vertex  $v_i$  is connected to or its adjacency matrix  $\mathbf{A}$ :

$$\mathbf{A} = \begin{pmatrix} e_{v_1, v_1} & e_{v_1, v_2} & \cdots & e_{v_1, v_n} \\ e_{v_2, v_1} & e_{v_2, v_2} & \cdots & e_{v_2, v_n} \\ \vdots & \vdots & \ddots & \vdots \\ e_{v_n, v_1} & e_{v_n, v_2} & \cdots & e_{v_n, v_n} \end{pmatrix} \quad (3.1)$$

The entries of the adjacency matrix may indicate just a connection between two vertices (1 for a connection or 0 for no connection) or, in case of a weighted graph, the corresponding edge weights  $w_{i,j} = e_{v_i, v_j}$ . Entries on the matrix diagonal stand for self-connections (also called loops). While the adjacency matrix is symmetrical for non-directed graphs, this does not hold for digraphs.

Applying this knowledge to airports, the infrastructure model can be designed as electrical infrastructure and ICT systems represented by two graphs consisting of electrical or ICT devices and their interconnections. A closer examination of the separate networks reveals that an essential component of ICT devices is electrical power supply. Therefore, ICT devices are at least a subset of electrical devices, and they are highly dependent on the power grid. However, there are two different interaction types between the vertices within the layers, where one is the transmission of power between devices (power grid layer) and the other is the communication of data (ICT layer). Networks with multiple types of relations between vertices are referred to as multiplex networks. Battiston et al. (2017) defined a

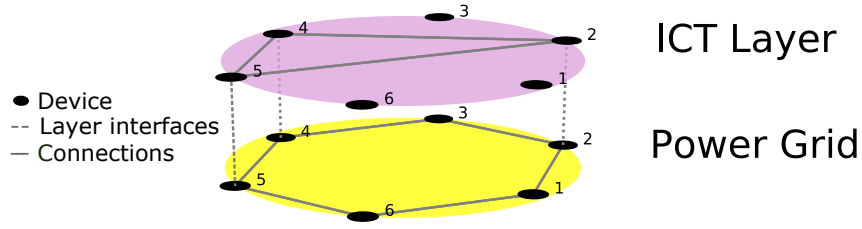


Figure 3.3: Two-layer network structure showing the devices (vertices) and their interconnections (solid edges) within the ICT (light purple) and power grid layer (yellow). Devices having properties on both layers build the layer interface (dashed lines) (Reprinted from Koch et al. (2019b) with the permission of Springer Nature)

multiplex network  $\mathbf{M}$  containing  $M$  layers describing different types of relations, which is defined by a set of adjacency matrices:

$$\mathbf{M} = \{\mathbf{A}^{[1]}, \mathbf{A}^{[2]}, \dots, \mathbf{A}^{[m]}\} \quad (3.2)$$

or weighted adjacency matrices  $\mathbf{W}$ , if edge weights are relevant for the interaction. This notation assumes that each vertex is present on all layers. At a deeper level, modern electrical devices often include ICT in the form of embedded controllers, which undertake tasks such as power switching, regulating charging rates, or other basic operations. Thus, the system can be described as a two-layered multiplex system consisting of an ICT layer and a power grid layer, as depicted in Figure 3.3.

Due to the possibility of powerline communication edges on the power grid layer are replicated onto the ICT layer. The example in Figure 3.3 shows a system consisting of six devices in a power circuit forming connections on the power grid layer (yellow), whereas only three of them are communicating within the ICT layer (light purple). To emphasize that only these devices interact on both layers, they are connected by dashed lines representing this layer interface.

However, the interactions between vertices on each layer follow different rules, resulting in the need for a separate modeling approach. Consequently, a successful interaction model for both the ICT layer and the power layer will be described in the following two Subchapters.

### 3.1.1 Modeling Malware Intrusion and Propagation within ICT Networks

Within this work, the impact of cyber attacks using malicious software (Malware) on ICT networks will be modeled by determining the operability of single systems within the infrastructure. The need to distinguish different types of malware has been identified, whereas malware is defined as a “piece of code or program that can cause minor to significant

| Malware     |      |                    |               |             |              |            |         |                                              |
|-------------|------|--------------------|---------------|-------------|--------------|------------|---------|----------------------------------------------|
| Replicators |      | Remotely Attackers |               | Differenter |              | Autonomous |         | Direct Stealer                               |
| Virus       | Worm | Ransom-ware        | Backdoor/Bots | Logic Bombs | Trojan Horse | Adware     | Rootkit | Sniffers, Password hash grabbers, Keyloggers |

Figure 3.4: Categorization of malware types as done by Poudyal et al. (2019).

damage to the user, computer or network” (Poudyal et al., 2019). A categorization of malware types has been shown in Figure 3.4 by (Poudyal et al., 2019), dividing them into five classes: replicators, remotely attackers, differenter, autonomous and direct stealers. These generalized categories have been derived based on typical behavior of the malware, though malware may exhibit the behavior of several categories.

The replicative behavior of viruses and worms has led to their classification as replicators. The propagation of these malicious entities has been facilitated by their ability to replicate within the same machine caused by a trigger, such as opening a file, and propagate to other devices by sending the malicious file. In contrast, worms have autonomously executed themselves and propagated throughout the network, infecting other connected machines.

The behavior of logic bombs and trojan horses has resulted in their use of changing the code of a program in a way that it either executes code if a predefined condition is met (logic bomb) or to hide inside an app and gain intel through recording the taken actions (trojan horse). The encryption of user data by ransomware has enabled attackers to blackmail data owners remotely by offering data decryption in exchange.

The creation of backdoors has allowed remote connections to user machines without further authentication, thereby enabling attackers to execute local commands. The propagation of adware has resulted in unwanted popups of advertisements or information, which have lured people to click on the advert and get directed to malicious sites, stealing information or executing malicious code.

The deployment of rootkits has enabled unauthorized access to systems, often used to hide or spread other malware types. Direct stealers, such as sniffers, keyloggers, and password hash grabbers, have been designed to steal user names, passwords, etc., through direct logging of typing or other system events (Poudyal et al., 2019).

To mimic the effect of this behavior in an abstract manner, the following aspects have to be considered:

- Network intrusion: The ICT layer represents only an internal system description, whereas most devices have internet access or connections to other external devices (e.g, via WiFi, Bluetooth). Thus, the model has to be capable of handling this exposure through the corresponding attack vectors.

- Network propagation: Malware types as worms have the ability to infect connected devices. Thus, a model for the propagation within the network has to be introduced.
- Infection probability and impact: In case of a large-scale attack a manifold of devices are attacked at once or through propagation of the malware throughout the network. However, malware is designed to use specific insecure code pieces in running software or operating systems. Thus, devices on which this code is not executed, e.g., because of a different operating system or it being an embedded system without application software, are not infected and therefore the malware does not impact the machines operability. Nevertheless, similar to virus diseases devices may act as a carrier of the worm by transmitting the malicious data without being impacted itself.

Thus, the model must cover the range of possible scenarios, from an attack on a single machine spreading through network connections to a large-scale attack without propagation.

Considering the external layer as one vertex connected to the ICT layer, the exposure of the ICT layer can be described using a corresponding attack vector consisting of zeros and ones containing the vertices it is connected to.

Fred Cohen was the first to demonstrate the propagation of computer viruses in the way that they induce a virus into machine A and detect it on a machine C, although A and C had only an indirect connection via a machine B (Cohen, 1987). Therefore, network propagation can be described as a flow inside the ICT layer from one vertex to its neighbors. Differential equation-based approaches are commonly used in epidemic modeling (Martcheva, 2015), however, these are not able to include network topology and cannot mimic this behavior. Thus, a graph-based network flow (Ahuja et al., 1999) approach based on weighted edges similar to those explained in Chen and Carley (2001), Lloyd and Valeika (2007) and Kephart, Jeffrey O. and White, Steve R. (1993) is used (Koch et al., 2019b, 2018).

The main assumption that must be made is that an infection can propagate to every connected object within a finite amount of time without any countermeasures. Although these infection times may be very high, modern malicious software is often designed to be mutable and adaptive, and therefore able to outwit barriers. In addition, the transmission of malicious software from one object to another is assumed to start when the virus is triggered at the first object. As the goal is to consider the effect on airport processes and neglect processes within the ICT object itself, it is not considered that the dormant or propagation virus phase occurs within single objects. Therefore, a state variable  $\text{infected}_i = \text{true}$  is given to each object that has been triggered. In this case, the capacities at the edges symbolize the infection speed towards the connected system - in network flow theory sometimes referred to as capacity. These capacities are introduced to combine all factors affecting propagation time, such as the OS, computer architecture, data transfer rate, type of connection, used protocols and encryptions or security precautions, into one macroscopic measure (in an arbitrary time unit (t.u.)) being a weighting parameter  $w_{ij}$  for the edge between objects  $i$  and  $j$ . If objects  $i$  and  $j$  are not connected, then  $w_{ij}$  is set to infinity (Koch et al., 2017).

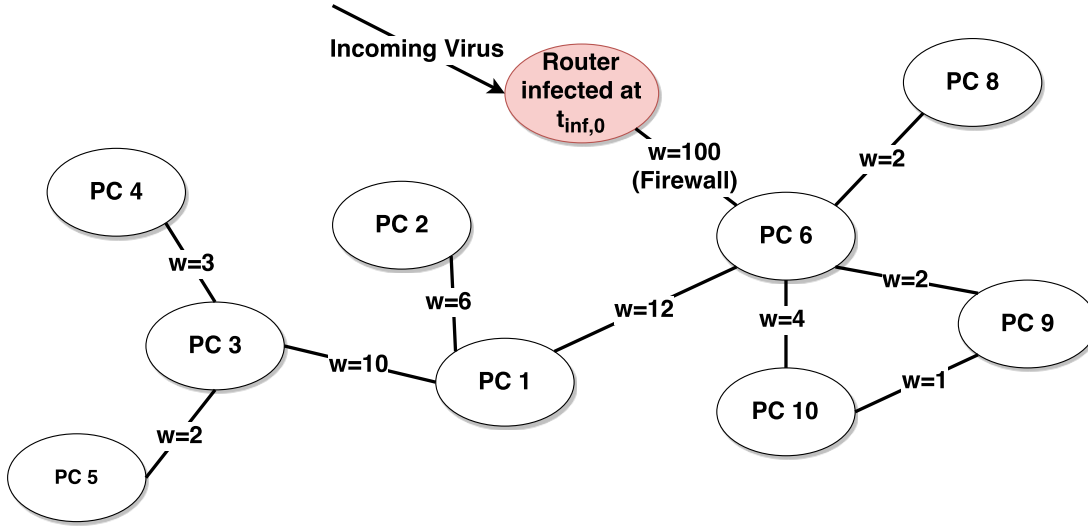


Figure 3.5: ICT layer structure represented as a graph with objects as nodes and infection time as edge weights under conditions of a cyber attack. After the infection of the router (red), the virus starts to propagate through the network.

Furthermore, an infection probability is added to the nodes since not every attack on an ICT system is successful.

Figure 3.5 shows an example of an ICT network structure consisting of ten personal computers using one router to access the internet via a router that gets infected at a time  $t_{inf,0}$  (red). As only PC 6 is directly connected to the Router, the firewall between the router and PC 6 is first attacked. After a successful infection of PC 6, the malware spreads to every neighbor at once, i.e., at  $t = t_{inf,0} + 100 \text{ t.u.}$  the infection spreads towards PCs 1, 8, 9, and 10. In this example, the router is predefined as the point of attack. In real networks, attack vectors are not limited to one point of attack, and many points of attack can be predefined.

With the help of shortest-path algorithms such as Dijkstra or Floyd-Warshall algorithms (Dijkstra, 1959; Floyd, 1962; Cormen et al., 2001), the infection time of each node is calculated and assigned to the node. After time evolves beyond the node's infection time, the device is considered as infected.

By varying weight edges, points of attack, and infection probabilities, a manifold of different types of cyber attacks can be depicted. E-mail-based attacks, for instance, may have a low probability to infect a computer but multiple points of attack simultaneously, whereas viruses typically have only one or few points of attack and are more dependent on propagation behavior. In the former case, the probability is highly dependent on user behavior and their knowledge about cyber-security. As a result, companies are advised to educate their staff on detecting suspicious e-mails, web pages, etc.

Moreover, an infected device is not necessarily a dysfunctional device, as in some cases only certain software may be affected by the infection. Therefore, devices require a list

of applications being used on this device ( $\text{applications}_i$ ) and a list of affected programs (affected applications) to be assigned as malware properties. An example is the ransomware WannaCry, which targeted Deutsche Bahn AG but only shut down some screens and ticket vending machines without affecting traffic (Karabasz et al., 2017; Koch et al., 2019b).

To identify dysfunctional devices, objects need to check all elements of the list  $\text{applications}_i$ , for whether one of the necessary applications is infected. Under these conditions, the property  $\text{working\_status\_cyber}_i$  is set to true (Koch et al., 2018):

$$\begin{aligned} & \text{infected}_i = \text{false} \\ & \text{infected}_i = \text{true} \quad \wedge \quad \text{applications}_i \notin \text{affected applications} \end{aligned} \quad (3.3)$$

, where  $\wedge$  denotes the logical conjunction.

Regarding the system architecture for ICT systems at airports, as described in section 2.1 being divided into physical, networking, application, and integration layers (see Figure 2.2), the network flow model can model the propagation of malware on the physical and networking layers, while modeling the dysfunctionality of a device due to an infection on the application layer.

Thus, the propagation model fulfills the predefined requirements and is able to model the intrusion through an attack vector, the propagation using a weighted network graph and the infection probability and impact through device internal attributes.

### 3.1.2 Modeling Power Supply and Distribution at Airports

As introduced in Section 2.1, airports rely on an external main grid for power, but a critical infrastructure requires a backup solution. Typically, these fall-back solutions are implemented in the form of an uninterruptible power supply (UPS) during switch-over times and one or more diesel generators that enable the operation of critical systems. Larger airports increase their redundancy by installing a second, independent power grid connection or operating their own power plants. Moreover, several large airports, such as Vienna Airport and Denver International Airport, have established large solar farms, although the construction process is complex due to safety concerns related to reflectivity and communication system interference (Federal Aviation Administration, 2010). Consequently, airport electrical infrastructure must coordinate distributed energy resources to accommodate a high number of spatially distributed loads and be capable of islanding, i.e., operating without an external power supply. Electrical grids that meet these criteria are often referred to as microgrids (Hatziargyriou et al., 2007).

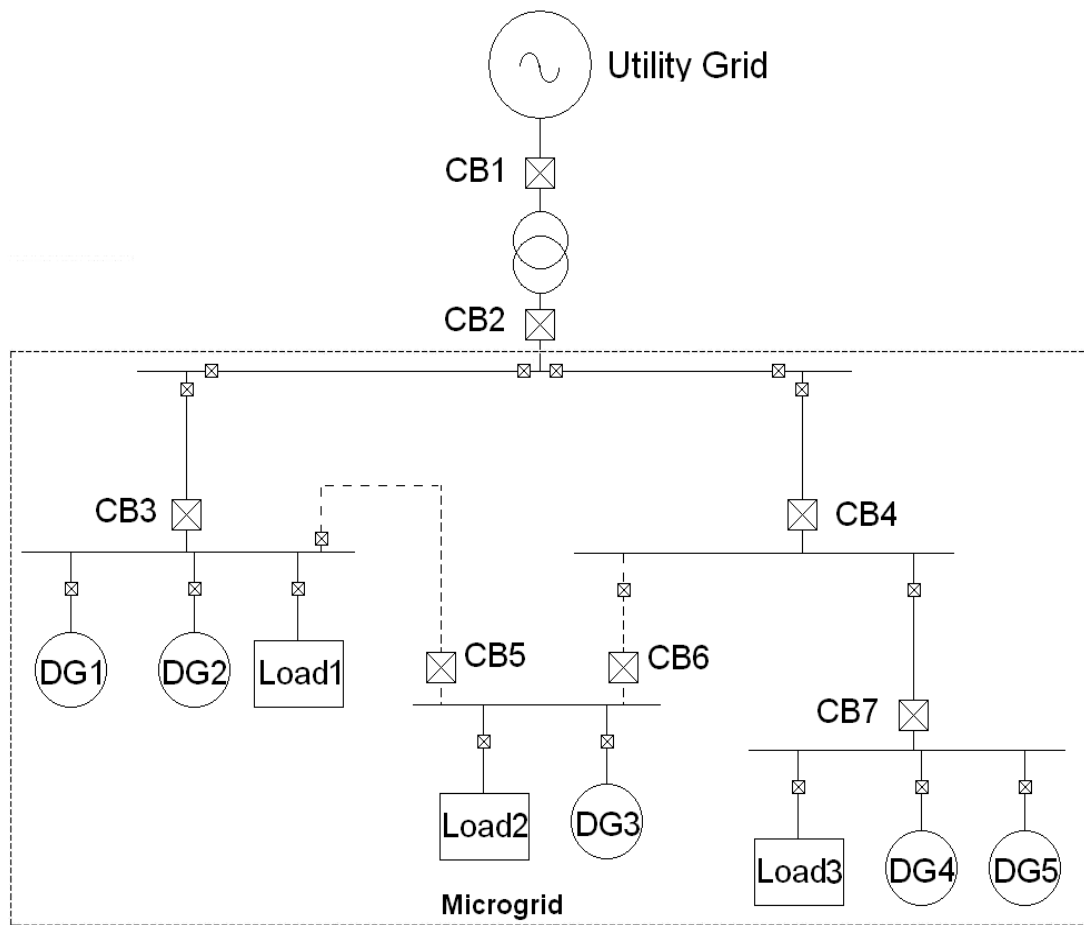


Figure 3.6: One-line diagram of a microgrid structure that is connected to the utility grid as depicted by Ustun et al. (2011). The microgrid in the dashed box consists of five buses divided by circuit breakers (CB). At three buses power is not only consumed by loads, but also distributively generated (DG).

### 3.1.2.1 The Airport as a Microgrid

A one-line diagram is a simple form to depict the structure of a power grid, as it reduces the grid to the basic power flow of one phase (von Meier, 2006). An example of a one-line-diagram of a microgrid is provided in Figure 3.6. One-line diagrams facilitate the representation of relay hierarchy, which is of great importance in cases of faults and demands for isolation. Power flows from top to bottom through the horizontal lines, which represent buses, i.e., common connections at key points of the system. In cases where the system spans over different voltage levels, the voltages should be indicated at the buses. The crossed squares in Figure 3.6 mark circuit breakers (CB), which can be opened and closed to protect parts of the grid and are triggered by a relay when a defined threshold of upstream or downstream current through the relay is exceeded (Grainger and Stevenson Jr., 1994). Loads (boxes) and distributed generators (circles) are connected to buses through circuit breakers, allowing for load shedding or connecting and disconnecting power sources.

Although one-line diagrams are a very basic representation of the power circuit, the contained information about subsystems and relay hierarchy can be used to analyze changes in microgrid structure using graph theory by removing connections between buses and determining the power flow using shortest-path algorithms (Ustun et al., 2011). This approach is especially important while investigating islanding conditions within a microgrid. Figure 3.6 illustrates a microgrid system connected to an external power grid through a voltage transformer (two overlapping circles), which is protected by CB 1 and CB 2. If a fault is detected at one of these CBs, the microgrid (big dashed box) operates under islanding conditions.

In the context of the airport system, a blackout of the power grid would lead to a loss of an external power supply. In 2018, the Civil Aviation Regulatory Commission (CARC) (2018) published guidance material for the installation of electrical systems at airports, proposing a microgrid structure depicted in Figure 3.7. For redundancy, they suggest two independent connections to the public source feeding one main distribution ring bus. Furthermore, switches at the middle of the main and ring bus enable a manifold of network setups, allowing continuous operation during faults within parts of the system. Most airport loads are directly connected to the main distribution bus, but for safety-critical systems such as airfield lighting or navigation systems, two encapsulated electrical vaults including an UPS are intended to guarantee robustness of the system. Additionally, the ringbus is connected to the main distribution bus and the electrical vaults by transformers, capable of transporting power at higher voltage levels and therefore reducing power loss.

However, this proposed architecture did not include a diverse set of additional power sources spread around the airport infrastructure. Continuous operation of terminal ICT systems would require an additional UPS connected to the main bus, as switch-over times for the airport emergency generator are too high, resulting in potential loss of data or even damaged equipment. Comparing microgrid structures in Figure 3.6 and Figure 3.7 reveals a manifold of design possibilities and failure scenarios, and therefore each airport system must be individually analyzed. To facilitate such an analysis, a model is needed that can

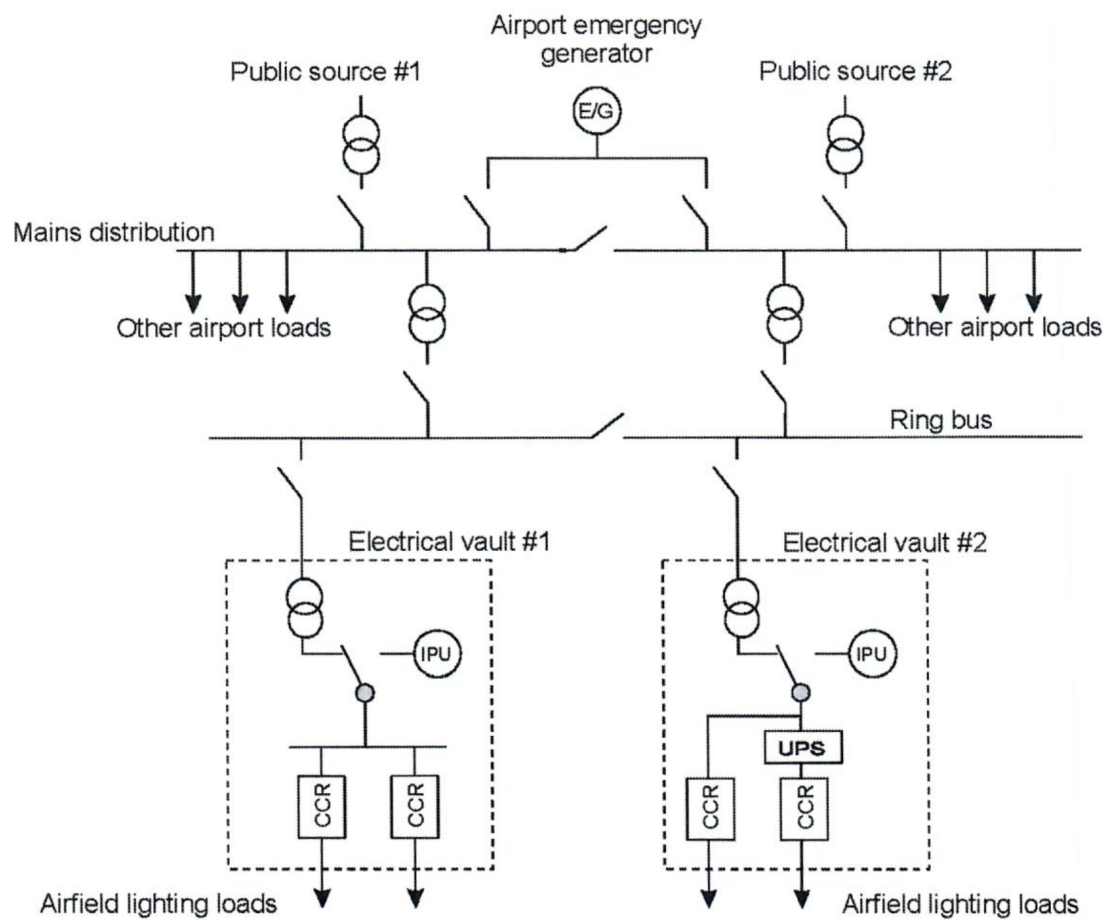


Figure 3.7: Airport power system setup as suggested by the Civil Aviation Regulatory Commission (CARC) (2018) using two public sources and two separate electrical vaults for the airfield lighting loads.

analyze the operating state of the power system under given conditions and is compatible with the two-layer approach.

### 3.1.2.2 Power Grid Analysis using Power Flow Analysis

A common state-of-the-art method for analyzing the present operating state of a system, given certain known quantities, is the power flow analysis (von Meier, 2006). The basis for this analysis lies in a network representation on a bus level, which has been introduced before. The fundamental principle of the analysis involves checking the balance of the grid by ensuring that all generators collectively supply power in exactly the amount demanded by loads, plus the amount lost on transmission lines. Thus, known real power  $P$  and reactive power  $Q$  flows at each bus, as well as explicit voltage magnitudes  $U$ , are used to calculate the remaining voltage magnitudes  $U$  and all voltage angles  $\delta$ . After this, current magnitudes and angles are calculated (von Meier, 2006). To achieve this, buses are categorized into three types. At a generator bus, real power  $P$  and voltage  $U$  are provided. Loads attached to a load bus consume certain real and reactive power, resulting in the provision of real power  $P$  and reactive power  $Q$  at that load bus.

The behavior of a load is defined by its impedance  $Z_i = R + jX$ , where  $R$  refers to resistance and  $X$  to reactance of the load, with alternating current circuits involving frequency-dependent reactance. In reality, loads may exhibit mixed behavior, but they can be categorized into three different load types based on dominating properties. Resistive loads, characterized by conductors generating heat from electrical currents, are distinguished from inductive loads, which involve alternating currents inducing changes in magnetic fields and causing phase shifts. Conversely, capacitive reactance leads to phase shifts in the opposite direction, driven by changing electrical fields within a capacitor. This behavior defines capacitive loads, commonly found in power supplies of consumer electronics (e.g., notebooks) (von Meier, 2006).

As the power flow analysis searches for balance without prior knowledge of transmission losses, one generator bus is left with undefined real power, referred to as a slack bus and serving as the system's reference point. In this scenario, the utility grid is typically taken as the reference bus (Suresh et al., 2019). A summary of different load and bus types is presented in Table 3.1.

The complex power  $S_i$  generated or consumed at each bus  $i$  is equal to the product of voltage  $U_i$  and the complex conjugate (denoted by an asterisk) of electric current  $I_i$ , as revealed in Eq. 3.4.

$$S_i = U_i I_i^* \quad (3.4)$$

Using Ohm's law  $I = VY$  with  $Y$  being the complex admittance of the transmission line,  $I_i$  in Eq. 3.4 can be replaced by the sum of all currents injected or consumed by directly

connected buses  $k$ , where  $Y_{ik}$  refers to the admittance of the transmission line between the two buses. This yields:

$$S_i = U_i \left( \sum_{k=1}^n Y_{ik} U_k \right)^* \quad (3.5)$$

Conjugation of both sides and inserting  $S_i = P_i + jQ_i$  yields:

$$P_i - jQ_i = U_i^* \sum_{k=1}^n Y_{ik} U_k \quad (3.6)$$

Expanding Eq. 3.6 and equating real and reactive parts, two sets of equations are obtained:

$$P_i = \sum_{k=1}^n |Y_{ik} U_i U_k| \cos(\theta_{ik} + \delta_k - \delta_i) \quad (3.7)$$

$$Q_i = - \sum_{k=1}^n |Y_{ik} U_i U_k| \sin(\theta_{ik} + \delta_k - \delta_i) \quad (3.8)$$

This set of  $2n$  equations Eq. 3.7 and Eq. 3.8 are commonly referred to as the power flow equations. The power flow equations are a set of non-linear algebraic equations, which can only be solved using iterative numerical techniques (Kothari and Nagrath, 2003).

A widely employed technique for solving power flow equations is the Newton–Raphson method also referred to as Newton’s method. The Newton’s method is a root-solving algorithm that is used to find roots  $f(x) = 0$  by iteratively improving an initial guess for the state variables using the derivatives of the corresponding function (Tinney and Hart, 1967). To address multi-dimensional mismatch problems  $\mathbf{f}(\mathbf{x})$ , the corresponding equation system can be formulated using the Jacobian matrix  $\mathbf{J}$ . The resulting equation

$$\Delta \mathbf{x} = -\mathbf{f}(\mathbf{x}) \mathbf{J}(\mathbf{x})^{-1} \quad (3.9)$$

rearranged to

$$\mathbf{J}(\mathbf{x}) \Delta \mathbf{x} = -\mathbf{f}(\mathbf{x})$$

yield a Jacobian matrix that relates the changes in the state variables  $\mathbf{x}$  to the changes in the objective function  $\mathbf{f}(\mathbf{x})$ .

In the context of power flow problems, the voltages  $U_i$  and voltage angles  $\delta_i$  serve as state variables, which can be represented as a state vector  $\mathbf{x} = [\boldsymbol{\delta}, \mathbf{U}]^T$ . By considering the slack

Table 3.1: Descriptive overview of possible type of components of a bus system as described by Grainger and Stevenson Jr. (1994):

| Type | Subtype         | Description                                                                                                                                      | Airport example                                         |
|------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| Bus  | generator bus   | Also called P, V bus as the real power and voltage is given                                                                                      | Emergency generator                                     |
|      | load bus        | Bus at which the power consumption in form of real and reactive power is given through the connected loads (also known as P, Q bus)              | Main distribution bus                                   |
|      | slack bus       | Balances the system, neither P nor Q is defined                                                                                                  | Public source                                           |
| Load | Resistive load  | Loads consisting basically of a heated conductor                                                                                                 | Airstrip and other non-LED lighting                     |
|      | Inductive loads | Most common and include all types of motors, fluorescent lights, and transformers like those used in power supplies for lower voltage appliances | Air conditioning                                        |
|      | Capacitive load | Use capacitors to store electrical charge                                                                                                        | Monitors, computers and other ICT devices; LED lighting |

bus as the reference point, the voltage at this bus is known that the corresponding voltage angles are zero, thereby reducing the number of unknowns in the state vector to  $N - 1$ . The equations governing power flow, namely Eq. 3.7 and Eq. 3.8, can be transformed into a set of mismatch equations by comparing the current estimate with the iteratively computed values:

$$\Delta P_i(\mathbf{x}) = P_i - P_i(\mathbf{x}) = P_i - \sum_{k=1}^n |Y_{ik} U_i U_k| \cos(\theta_{ik} + \delta_k - \delta_i) \quad (3.10)$$

$$\Delta Q_i(\mathbf{x}) = Q_i - Q_i(\mathbf{x}) = Q_i - \sum_{k=1}^n |Y_{ik} U_i U_k| \sin(\theta_{ik} + \delta_k - \delta_i) \quad (3.11)$$

For brevity Eq. 3.10 and 3.11 are referred to as mismatch vectors  $\Delta \mathbf{P}(\mathbf{x})$  and  $\Delta \mathbf{Q}(\mathbf{x})$ , respectively. The Jacobian matrix for these equations is obtained by applying the Jacobian operator to the original equations. The resulting Jacobian matrix consists of four partitions for the derivatives  $\partial \mathbf{P}(\delta, U) / \partial \delta$ ,  $\partial \mathbf{P}(\delta, U) / \partial U$ ,  $\partial \mathbf{Q}(\delta, U) / \partial \delta$  and  $\partial \mathbf{Q}(\delta, U) / \partial U$ . Each partition comprises rows corresponding to the  $\delta_i$  or  $U_i$  values and columns corresponding to the  $P_i$  or  $Q_i$  values for all buses, excluding the slack bus (von Meier, 2006).

The equations can be combined into a matrix equation of the form:

$$\begin{bmatrix} \frac{\partial \mathbf{P}}{\partial \delta} & \frac{\partial \mathbf{P}}{\partial U} \\ \frac{\partial \mathbf{Q}}{\partial \delta} & \frac{\partial \mathbf{Q}}{\partial U} \end{bmatrix} \begin{bmatrix} \Delta \delta \\ \Delta U \end{bmatrix} = \begin{bmatrix} \Delta \mathbf{P}(\mathbf{x}) \\ \Delta \mathbf{Q}(\mathbf{x}) \end{bmatrix} \quad (3.12)$$

By applying the Newton's Method to this equation, an approximate solution for all demanded voltages  $U_i$  and voltage angles  $\delta_i$  can be obtained at each load bus (P-Q-bus) and  $\delta_i$  and  $Q_i$  at every generator bus (P-V-bus). The real power at the slack bus can also be calculated by inserting known values into Eq. 3.7. Comparing this with the total consumed power at the loads allows for the determination of the system's power loss.

Furthermore, the voltage angles  $\delta_i$  and voltages  $U_i$  at each bus provide sufficient information to calculate the power injected into each transmission line and the outflow at the end of each transmission line using Ohm's law. This enables the calculation of real and reactive losses in each transmission line, thereby completing the output of the power flow analysis.

Finally, the results can be checked for compliance with external limitations by applying additional constraints to the solution.

System stability of an AC power system is ensured if the system maintains synchronization and balanced power generation and consumption. A state of angle stability is achieved when the system components remain at a given frequency (von Meier, 2006). While 50 Hz is typically used for power grids in Europe, Asia, and Africa, 60 Hz is common in North and South America. The topic of angle stability and frequency regulation is important in

large power systems, but airport operators face limitations due to the externally regulated power grid supply or prefabricated devices with limited operational control options.

A comprehensive angle stability analysis would require sophisticated models for all airport power sources, which is beyond the scope of this work (von Meier, 2006). Moreover, consumer electronics commonly employ switched-mode power supplies, which convert alternating current into direct current and render devices resistant to frequency changes.

However, voltage stability, i.e., the ability of a power system to maintain acceptable voltage magnitudes at all buses under normal conditions and after disturbances (Kothari and Nagrath, 2003), is crucial for airport operators. Consumer technologies have limited tolerance to voltage magnitude deviations, with international standards recommending no more than  $\pm 10\%$  deviation without causing damage (see (Partha Sarathy, 2018) for an overview of common standards). Additionally, most devices are equipped with integrated protection mechanisms that shut them down if the voltage exceeds a safe threshold.

The voltage at load buses can be determined using the previously presented power flow analysis. A threshold for acceptable voltage amplitude can be established and used to check for voltage stability at all buses, thereby determining the operability state. Moreover, the real power demanded from the supply  $P_{d,\text{supply}}$  should be limited to a maximum supply power  $P_{\text{supply,max}}$ . Therefore, the object property `working_status_physicali` is set to true if the following conditions are fulfilled:

$$\begin{aligned} U_{\min} &< U_i < U_{\max} \\ P_{d,\text{supply}} &< P_{\text{supply,max}} \end{aligned} \quad (3.13)$$

### 3.2 Layer Interaction and Dynamics of the Cyber-physical System

In the previous section, the airport was described as a cyber-physical system consisting of a power layer and an ICT-layer. Furthermore, interactions between ICT devices (Subsection 3.1.1) and the system behavior on a power layer (Subsection 3.1.2) were described. However, the interaction between the two layers has not been explicitly addressed.

While purely electrical devices do not interact with the ICT network, most stationary ICT devices rely on power supply. Consequently, a correlation exists between the results of the power flow analysis and the working state of these devices. The network flow analysis introduced in Subsection 3.1.1 is used to determine the current working state on the cyber layer (`working_status_cyberi`) using Eq. 3.3. The electrical properties of the device are used to conduct the power flow analysis and check for stability using Eq. 3.13 to gain the working state on the electrical layer (`working_status_physicali`). Subsequently, the working state (`working_statei`) of the device is set to true if:

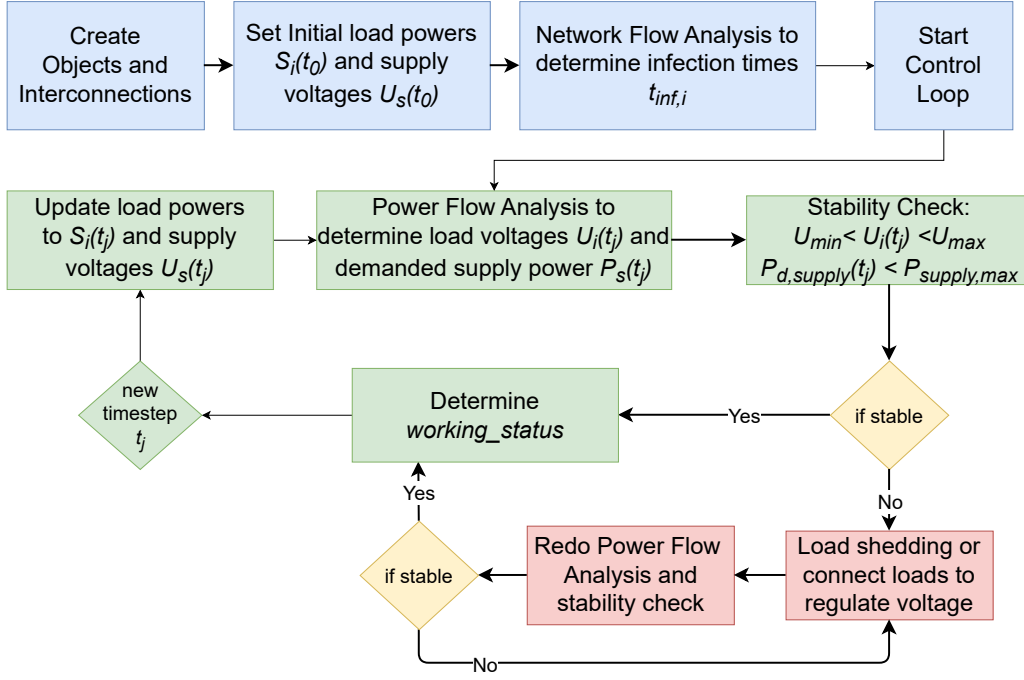


Figure 3.8: Working scheme of dynamic network stability analysis: After setting up the simulation (blue), grid stability is checked using the power flow analysis, the dynamic load conditions are updated before the new time step is started. Green colors mark iterative processes without control measures, while red boxes include event-based system changes. Path decisions are made at yellow if-statements (Modified from Koch et al. (2018)).

$$\text{working\_status\_cyber}_i = \text{true} \quad \wedge \quad \text{working\_status\_physical}_i = \text{true} \quad (3.14)$$

where  $\wedge$  denotes the logical conjunction.

Using previously described methods allows to determine the working state of each network object (vertex) in the multiplex network representation of the CPS under steady-state conditions. However, neglecting dynamic effects within the power grid, system state changes can be considered as a quasi-stationary process. Therefore, the power flow analysis is embedded into an iterative decision and control loop to introduce time-dependency.

Figure 3.8 shows the time-dependent simulation control loop system (Modified from Koch et al. (2018)). After network setup and initialization (blue), which includes the calculation of infection times, the control loop starts with the power flow analysis. Afterwards, stability is checked (yellow) using Eq. 3.13 to determine the system state analogous to the process of decision and control presented in Section 2.5. If the condition check fails, the control loop (red) starts to enable grid adaptation. Possible solutions include load shedding, starting additional power supply, or network restructuring to increase/decrease load voltages or

---

to fall below the maximum power supply. After applying the control measures, the analysis is redone and stability is checked again. This is repeated until stability is reached. Subsequently, the working status of each object is updated according to Eq. 3.14 to complete the time step. After each time step, the power demands, supply voltages, and power supply limits are updated, i.e., the power flow analysis is driven by dynamic boundary conditions (Koch et al., 2018).



---

# Improving Robustness of the Airport against Blackouts and Cyber Attacks

---

Within the previous chapter, the airport infrastructure was modeled as a cyber-physical system represented by a multiplex network graph, consisting of a cyber and electrical layer. Furthermore, network flow analysis (see Subsection 3.1.1) and power flow analysis (see Subsection 3.1.2.2) were presented to model interactions on the corresponding layers. The interaction between the layers was outlined, and the model was enhanced by the introduction of a decision and control loop that evaluated system state at discrete time steps.

Thus, the model is capable of evaluating which components within the airport infrastructure are available at discrete time steps, if their corresponding load power and supply voltage are known. Predefined cyber attacks can be used to model the impact of these attacks on the operability of devices. Summarizing, this model enables forecasting of resource availability within the airport infrastructure under predefined scenarios.

To gain information about reasonable scenarios that suit the use-case of a blackout at airports, an in-depth analysis of previous blackouts at airports should be conducted. Furthermore, a generalized risk and impact analysis may provide further insights into possible mitigation methods and control measures on a broader scale, i.e., without modeling the singular airport infrastructure. Therefore, Section 4.1 conducts a classical risk and impact analysis to assess realistic sources for blackouts and gather intelligence about impacted processes. Additionally, this knowledge should be used to improve the preparedness of the airport.

While the lack of data regarding cyber attacks at airports prevents a data-driven analysis, Section 4.2 presents a graph theory-based approach that is capable of detecting vulnerabilities within ICT networks and thus strengthening the preparedness towards cyber attacks as well as defining cyber attack scenarios hitting critical spots within the airport's ICT system.

## 4.1 Risk and Impact Analysis for Blackouts at Airports

The performance of prevention measures is directly connected to the consequences of real-life incidents. The evaluation of these incidents plays a major role in the preparedness

cycle introduced by Pelfrey (2005). In the past, collections of previous incidents have been successfully used to assess risks on the flight operation side. This approach has been employed by various studies, including Distefano and Leonardi (2014), Guerra et al. (2008) and Spriggs (2002), to identify hazards during all flight phases and assess their risk.

In this context, preliminary incident data was used to assess the risks originating from blackouts, following the guidelines for safety management planning outlined by ICAO Neubauer et al. (2015). The potential outcomes associated with these risks were categorized according to the ICAO guidelines, which include consequences for people (injury, death), assets (property/equipment loss, operating funds), environment, reputation, and mission, i.e., the airport's ability to move people and cargo.

As a result of this analysis, measures are proposed to mitigate these risks in the future.

#### **4.1.1 Methods**

To conduct this reverse risk assessment, a total number of 175 incidents worldwide were collected. Information sources encompassed governmental investigation reports, press releases, and social media posts. Although the latter ones may be questioned in their credibility, social media has evolved to become a predominant tool in company-customer communication. Private posts were only included for the detection of blackout occurrences and supported by press articles. As incident investigation reports are commonly not publicly available, despite some governmental exceptions, press articles served as the major source for data collection.

Blackouts may be triggered by a broad range of sources. Furthermore, to mitigate them, it is essential to distinguish between power outages caused within the airport and therefore limited to the airport itself, and external sources causing large-area blackouts. Consequently, the source location was categorized into internal, external (blackout not caused by an internal source, but no other customers affected), regional, and nationwide. During the investigation, 14 cause categories were identified that occurred at least twice and the remaining 5 causes were summarized in a category labeled "others". Further analysis revealed specific reasons within this group, including destruction by hurricane, flood, explosion, pole fire, and water leak. A comprehensive list, including descriptions and examples, is provided in Table 4.1.

Furthermore, the emergency management on the land-side of the airport system is highly influenced by regional laws, as well as personal experience from everyday life. Regional differences in response to power grid interruptions are also observed in Western Europe, where a continuous supply of electrical power is seen as the regular case. In contrast, people from developing countries are accustomed to short power outages and may be more inclined to take steps for sufficient emergency power supply (Doing Business, 2016). Hence, it becomes essential to investigate regional differences considering the treatment of blackout prevention.

Table 4.1: Cause categories for blackouts:

| Cause category                | Description                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------|
| unknown                       | -                                                                                                         |
| construction/maintenance work | workers accidentally cut power line during work or generator failed during testing                        |
| fire                          | blackout caused by fire                                                                                   |
| weather                       | severe weather conditions led to a blackout                                                               |
| circuit breaker               | includes short-circuits, overloads or voltage sags/dips inside the airport with unknown cause             |
| power cable interruption      | power cable interruption on low voltage level                                                             |
| transmission line failure     | interruption or failure of transmission lines on high or medium voltage level                             |
| generator failure             | relating to airport related generators or block heat and power plant (not external power plant failures)  |
| grid failure                  | including power plant failures                                                                            |
| technical failure             | any technical failure causing a system collapse reaching from broken light over defect air conditioning   |
| transmission station failure  | failures in electrical transmission stations including voltage transformers, whether internal or external |
| human error                   | wrong decision of personal leading to blackout                                                            |
| sabotage/security             | any intentional, planned attack causing a blackout, even if the airport is not the main target            |
| others                        | not assignable single causes                                                                              |

Table 4.2: Overview of IATA regions:

| IATA Region Code | Region Name              | Color in Figures |
|------------------|--------------------------|------------------|
| SWP              | South West Pacific       | violet           |
| SEA              | South East Asia          | gold             |
| SAS              | South Asian Subcontinent | lavender         |
| SOA              | South America            | light green      |
| NOA              | North America            | salmon           |
| MDE              | Middle East              | tan              |
| JAK              | Japan and Korea          | palegoldenrod    |
| EUR              | Europe                   | lightskyblue     |
| CAR              | Caribbean Sea            | aquamarine       |
| AFR              | Africa                   | peru             |

To achieve this, region codes from the International Air Transport Association (IATA) are used, as listed in Table 4.2. An overview of the regions including incidents is provided in Figure 4.1, where single incidents are depicted in red circles and yellow circles represent clustered groups of incidents. This division of the world appears to be feasible, as it is influenced by geographical borders as well as political and economic connections between countries. The airline industry also employs this classification system to determine flight charges and differentiate between domestic and intercontinental flights. For instance, connections between Europe and Russia are used to categorize flights to Moscow as continental, whereas flights to Siberia are regarded as intercontinental. Similarly, due to the historical linkage between Egypt and the Middle East, Egypt is assigned to the Middle Eastern region.

Moreover, for a successful risk assessment, data on incident consequences are required. Consequently, information about affected airport parts, airport sizes, duration of power outages (if available), and results for flight operations, including flight cancellations, delays, or diversions were recorded.

#### 4.1.2 Probabilistic Risk Assessment and Mitigation

An initial overview of the data has been provided in Figure 4.1. An interactive map of the data was created as a Leaflet map using the Python package Folium (Story, 2013) and is available online via Zenodo accommodated by the data set (Koch, 2025) (short access to the map via scanning the QR-code in the top left corner of Figure 4.1). The density of markers was calculated, resulting in clusters indicated by circles with numbers representing the amount of incidents within each region. Circle colors were assigned based on incident numbers: green for low values (below 10) and yellow for high values (above 10). Hotspots were identified in decreasing order of incidence rates.

The search of press articles was conducted in English, German, and Spanish. The language of the media is found to be relevant for regional incidents. Language usage varies

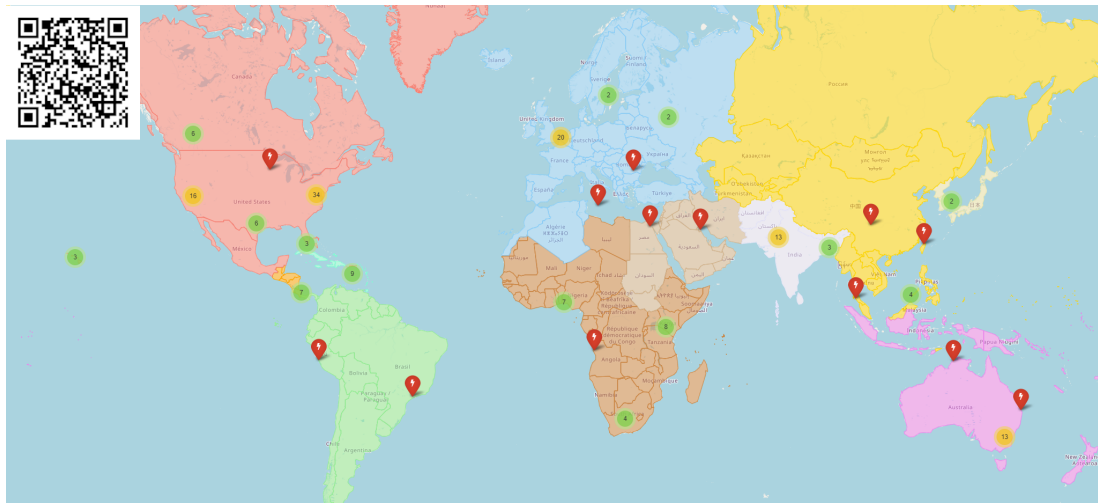


Figure 4.1: Map overview showing IATA regions color coded using the colors given in Table 4.2 and the airport locations where incidents were recorded. Single incidents are shown in red and near together incidents are clustered with numbers showing the number of incidents. QR-code to interactive map can be found in the top left corner.

across regions: English predominates in North America and Europe, while being an official language in many countries (India, Pakistan), Australia (SWP), or Africa (Kenya, Nigeria, South Africa). Incidents at Paris Charles de Gaulle airport were only reported in French, while those in Germany and Switzerland were reported in German. In contrast, incidents in Latin America are often reported in Spanish.

Another factor contributing to differences in incident numbers is the variation in region size, population, or geographical area, which affects air traffic demand. This results in a heterogeneous distribution of airports per region.

#### 4.1.2.1 Likelihood of Occurrence

Normalization by airport number was performed for comparability among regions. The absolute numbers of recorded incidents, their percentage of all incidents, and the normalized values are presented in Table 4.3. The importance of the normalization as an integral part becomes clear, when comparing before and after values for the European Region (EUR) and Central America (CEM). Prior to normalization, EUR ranked second, with 71 incidents and 26 recorded incidents, whereas CEM had only four incidents. However, when accounting for airport numbers, EUR's normalized value was significantly lower than CEM's. This highlights a higher probability of power outages in CEM compared to EUR.

The region with the highest probability is on the South Asian Subcontinent (SAS) (0.13), followed by North America (NOA) (0.09). Africa (AFR) and SWP are also among the top three, while the Caribbean Islands (CAR), EUR, the Japan Korea Sub-Area (JAK), and South

Table 4.3: Overview of regional distribution of the incidents, total number of airports in the region and the normalized incident number:

| IATA region                                          | AFR   | CAR  | CEM  | EUR   | JAK  | MDE  | NOA   | SOA  | SAS  | SEA  | SWP  |
|------------------------------------------------------|-------|------|------|-------|------|------|-------|------|------|------|------|
| Number of incidents                                  | 20    | 4    | 4    | 26    | 2    | 2    | 71    | 8    | 16   | 7    | 15   |
| Percentage                                           | 11.4% | 2.3% | 2.3% | 14.9% | 1.1% | 1.1% | 40.6% | 4.6% | 9.1% | 4.0% | 8.6% |
| Number of airports                                   | 251   | 122  | 20   | 901   | 79   | 125  | 751   | 239  | 120  | 411  | 202  |
| $\frac{\text{incidents}}{\text{number of airports}}$ | 0.08  | 0.03 | 0.20 | 0.03  | 0.03 | 0.02 | 0.09  | 0.03 | 0.13 | 0.02 | 0.07 |

America (SOA) have lower probabilities, with a value of 0.03. The Middle East (MDE) and South East Asia (SEA) have the lowest probabilities, tied at 0.02 each. However, it is noted that values for JAK and MDE may be questionable due to the small number of recorded incidents (2) and potential language biases in the research, as the search did not include Japanese, Korean, Arabic as well as Chinese and Russian.

Furthermore, a possible evolution over time should be investigated to determine its impact on airport emergency management. Therefore, in Figure 4.2, a cumulative bar chart showing the composition of incidents by region has been plotted, displaying the number of incidents over the years. The first interesting observation is an increase in registered incidents starting from the year 2007/2008. It is worth noting that this does not necessarily mean an increase in the total number of incidents in this period. Rather, it is likely that the digitization of former print media has led to an increase in worldwide media access. In addition, social media has made it impossible for airports to conceal even small recognizable outages, as every passenger can now publish the occurrence and encourage incident investigations by journalists. This trend can be illustrated using the data from NOA as a case study: in March 2019, Facebook had 168 million users, while Instagram had 121 million users (Clement, 2019), which corresponds to 51% and 37% of the US population. NOA and EUR are the predominant contributors to the total data, but there is no observable change in the composition over the years.

Despite this increase in media access, research by McCarthy and Mahoney (2013); Stamp et al. (2009a,b) has demonstrated that the ongoing digitization poses a risk for electrical systems and will likely continue to increase in the future with the implementation of smart grids. The exposure to cyber attacks or failures of ICT systems is also accompanied by an increased reliance on electrical devices and power demand (Morley et al., 2018). However, this trend cannot be explicitly deduced from the data due to two main limitations: firstly, the limited availability of information, and secondly, the chosen abstraction level at which the infrastructure composition of individual airports has not been fully resolved.

To distinguish between pro-active and reactive mitigation measures, it is necessary to determine whether power outages are self-inflicted or not. Therefore, a categorization based on source location has been created, where internal caused incidents only require pro-active

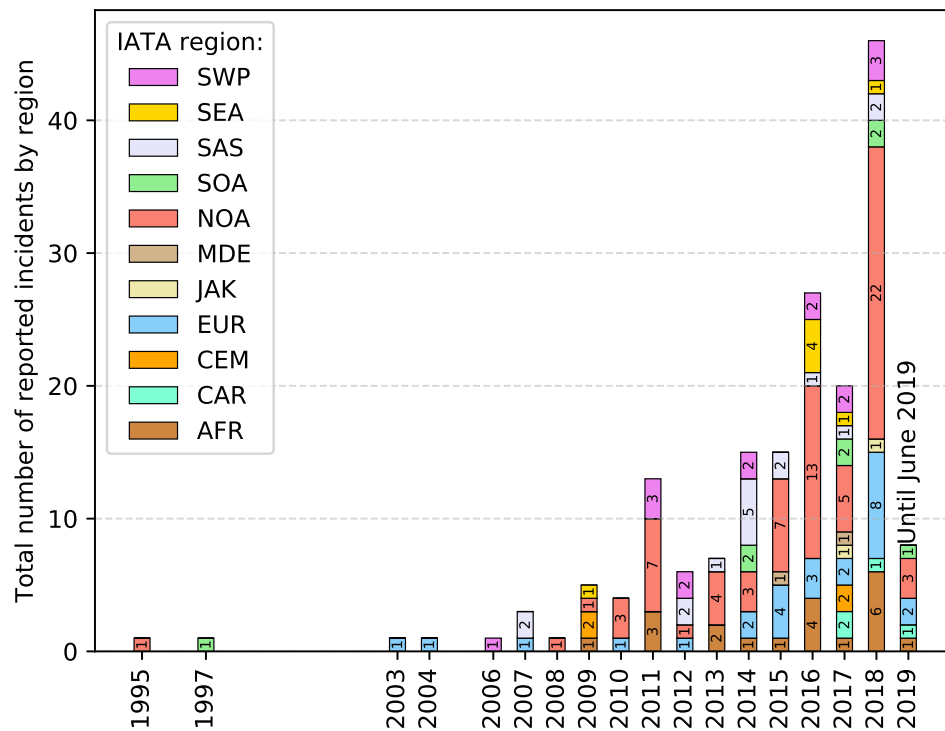


Figure 4.2: Evolution of the number of incidents in the regions over time.

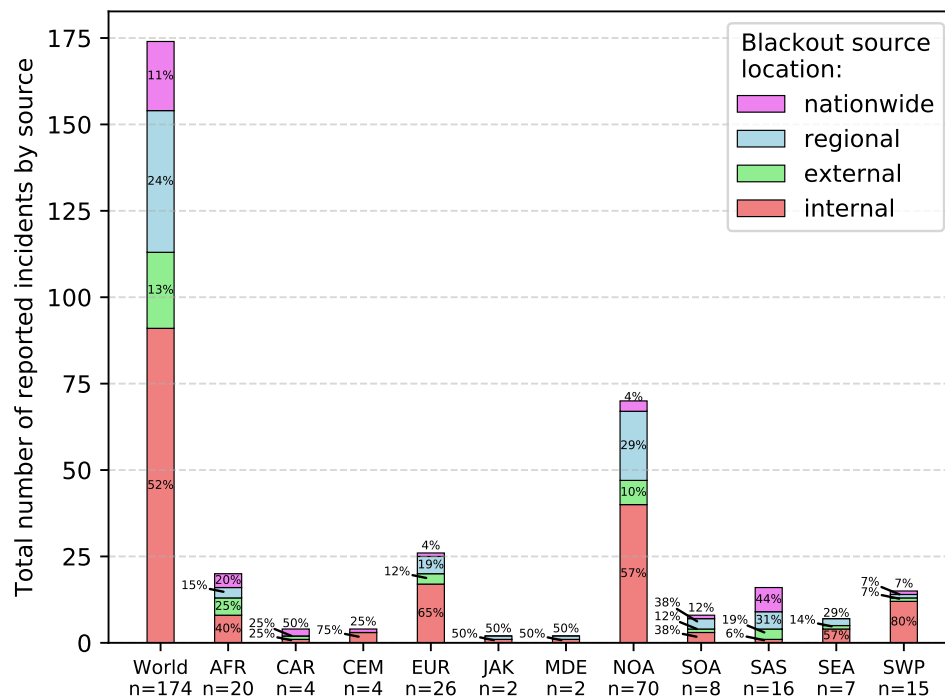


Figure 4.3: Source location of recorded incidents as a cumulative bar chart for each region.

measures, while external, regional, and nationwide outages demand for reactive measures. As shown in Figure 4.3, world-wide 52% of all incidents were categorized as internal. The percentages of self-inflicted cases are above average for SWP (80%), which in the data only contains incidents from Australia.

The categorization between regional and nationwide outages is challenging, particularly in countries with large federal states such as the USA, Australia, India, etc., where state-wide power outages were categorized as nationwide to enable a comparison w.r.t. area and population to outages within much smaller countries or even small islands. Regional and nationwide outages are predominant in the regions of SAS (75%), CAR (50%), SOA (62%), and AFR (60%). Adding also externally caused cases, it becomes clear that airports in SAS (94%), CAR (75%), SOA (62%), and AFR (60%) seem to face strong issues regarding power grid reliability.

The most common IEEE Standard for grid reliability evaluation is the System Average Interruption Duration Index (SAIDI), which refers to the cumulative duration of all blackouts per customer over a year. Table 4.4 shows the calculated SAIDI for each region based on data from Doing Business (2016) in tabular form, including median, average, and standard deviation. Outliers with a SAIDI above 100 hours a year are also mentioned. However, the mean value is strongly influenced by these outliers, which can be seen by the low ratio between mean and standard deviation. Therefore, using the median as a more stable value to represent most region values is recommended, although caution should be taken when considering single country data. Further, the lack of data for some regions highly reduces its representativeness, e.g., for SAS, no data for Bangladesh, Pakistan, Afghanistan, and Nepal is available. Although India is predominant regarding its population, this results in the number of included countries being reduced to four out of nine. High standard deviation values may imply that grid reliability within IATA regions is diverse, only 20 countries exceed a SAIDI larger than 31 hours per year. The African region grids (44 h/a) have by far the lowest reliability, followed by CEM (10.45 h/a), CAR (6.10 h/a), SWP (5.75 h/a), SOA (5.05 h/a), and SAS (4.70 h/a). Grids are most reliable in JAK (0.05 h/a), EUR (0.70 h/a), and SEA (0.85 h/a). The U.S. Energy Information Administration found that within the USA, without major events, grid reliability varied strongly in 2016 depending on the U.S. state, spanning from 27 minutes in Nebraska to 6 hours in West Virginia (U.S. EIA, 2018).

Comparing the SAIDI ranking with the findings for external source locations, it has been proven that there is a correlation between high percentage of external sources and low grid reliability for SAS, CAR, SOA, and AFR. However, an exceptional case is CEM, where most incidents were self-inflicted despite unstable grids. This result is likely due to local infrastructure problems at the Airport of San Salvador (IATA-Code: SAL) in El Salvador, where three out of four incidents occurred. On the other hand, low SAIDI values in EUR and SEA as well as NOA coincide with the findings that incidents in these regions are mostly self-inflicted. The highest percentage (80%) of self-inflicted blackouts is found in SWP, whereas the SAIDI of SWP is the third worst. However, the SAIDI of Australia is 1.2 hours a year (Doing Business, 2016) and therefore underlies similar conditions as in the NOA region.

Table 4.4: System Average Interruption Duration Index (SAIDI) for all IATA regions:

| Region | Number of Values | Median | Mean  | Std    | number of Values larger y <sub>lim</sub> = 100 |
|--------|------------------|--------|-------|--------|------------------------------------------------|
| World  | 138              | 2.70   | 24.32 | 89.27  | 5                                              |
| AFR    | 19               | 44.00  | 47.94 | 55.58  | 1                                              |
| CAR    | 8                | 6.10   | 19.10 | 27.53  | 0                                              |
| CEM    | 6                | 10.45  | 61.18 | 95.33  | 1                                              |
| EUR    | 46               | 0.70   | 4.45  | 12.13  | 0                                              |
| JAK    | 2                | 0.05   | 0.05  | 0.05   | 0                                              |
| MDE    | 12               | 2.15   | 6.77  | 15.72  | 0                                              |
| NOA    | 5                | 1.30   | 4.50  | 5.24   | 1                                              |
| SOA    | 12               | 5.05   | 18.57 | 38.91  | 1                                              |
| SAS    | 4                | 4.70   | 56.10 | 89.90  | 1                                              |
| SEA    | 16               | 0.85   | 64.36 | 229.16 | 1                                              |
| SWP    | 8                | 5.75   | 17.57 | 26.08  | 0                                              |

#### 4.1.2.2 Magnitude Evaluation

The next step in risk assessment, after identifying a description for risk likelihood, is to determine its consequences, also referred to as magnitude or severity. The consequences are evaluated from two different perspectives: first, limitations in infrastructure performance in terms of which areas are disabled due to lack of power, and second, the impact on airport performance with regard to flight cancellations, delays, or diversions.

In 21 out of 175 incidents, airport operation was unaffected. In 13 cases, it is not known whether the blackout impacted the airport, potentially indicating either no effect or unreported information. However, in 141 cases, a clear description of affected areas within the airport exists. It is worth noting that only explicitly named parts of the airport were included, and multiple mentions are possible. The infrastructure components are assigned to partial processes of airport operation, as depicted in Figure 4.4.

A distinction is made between complete airport stop (orange), infrastructure responsible for passenger (yellow) and cargo (brown) processing, flight operations (light blue), indispensable infrastructure (gold) such as communication infrastructure and supporting infrastructure (light green) facilitating traveling comfort. It is observed that passenger processing (yellow bars) is most likely to be affected, while the flight operation infrastructure is only affected by a low percentage. The reason for this is largely due to the strict ICAO rules for air side infrastructure power backup systems prescribed by the International Civil Aviation Organization (2018), wherein minimum requirements inside the terminal are limited to fire protection and evacuation measures.

In most cases, airport operators prefer to take the risk of stopped airport operation rather than investing in expensive backup supply for passenger processing infrastructure. This decision is further complicated by the digitization of processes, which impedes manual

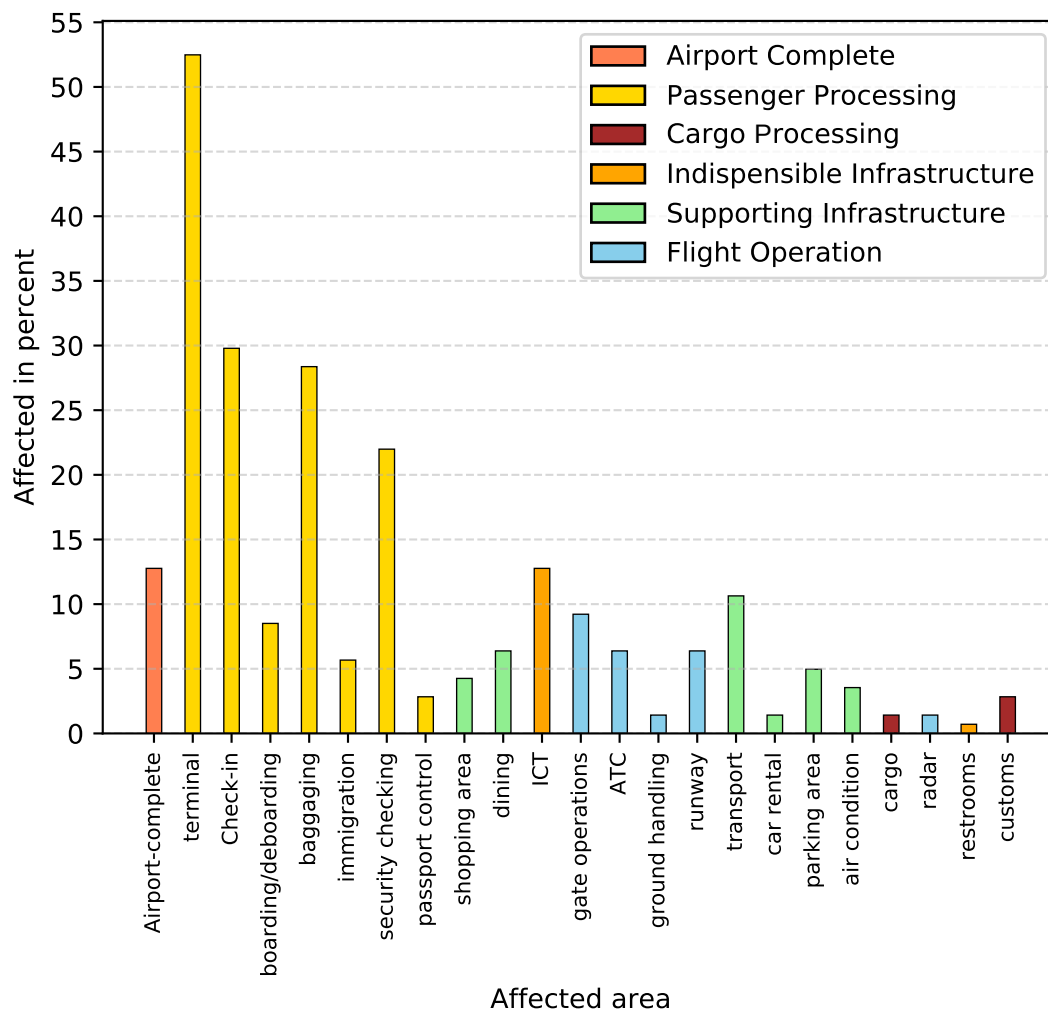


Figure 4.4: Percentage of cases in which parts of airport operation were affected, divided into complete airport disruption (salmon), passenger (yellow) or cargo (dark red) processing, ICT infrastructure (orange), supporting infrastructure (light green) and flight operation (light blue).

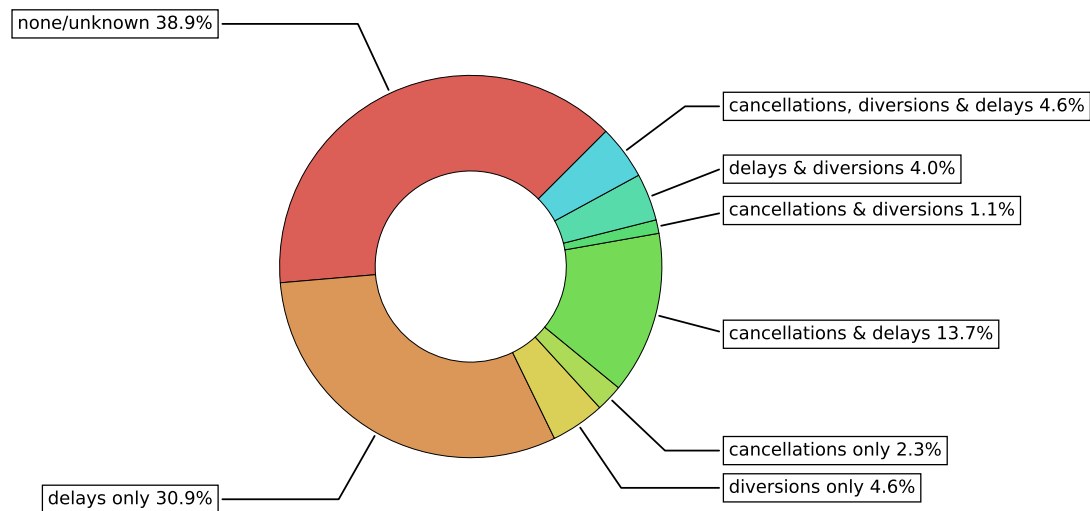


Figure 4.5: Consequences on flight operation for all incidents (n=175), i.e., disruptions leading to cancellations, diversions or delays.

backup procedures such as pen and paper check-in, security controls, or passport controls. Electronic baggage handling completely fails without power, resulting in laborious replacement procedures including transportation and sorting.

The low percentage of impacted cargo operation may contribute to a low public interest in news reports on cargo operations unless a shortage of goods occurs. Surprisingly, 12.8% of information and communication systems are out of order. Although it is unclear whether an emergency communication system exists, successful emergency management requires sufficient communication channels.

Although a loss of passenger comfort or a decrease in airline or airport reputation may lead to a long term decline in sales, the short-term monetary impact on stakeholders requires evaluation of flight operations' consequences. Therefore, it is necessary to focus on the impact of flight disruptions, such as cancellations, diversions, and delays, on flight schedules and timeliness. The percentage of cases with these issues is presented in Figure 4.5. In 38.9% of cases, no delays, cancellations, or diversions were reported. However, this absence of incidents does not necessarily imply that there was no adverse effect on flight operations; hence, such cases are labeled as "none" and "unknown". In most known cases, the consequences have been delays (30.9%) or a combination of delays and cancellations (13.7%).

It has been observed that in 19.4% of all incidents, no infrastructure was affected or an impact was not mentioned. Comparing these percentages, a comparison between the values of 19.4% without infrastructure effect and 38.9% without impact on flight operations may lead to the conclusion that this gap results in efficient emergency management, including sufficient emergency backup systems and replacement of automated processes with manual processing. To verify this, an examination of 68 incidents without impact on flight operations was conducted to determine whether sources mentioned emergency backup power

supplies. In 40 articles (58.8%), no information about backup supplies was provided, while 22 cases (32.4%) reported successful activation of the emergency backup system. However, in six instances (8.8%), the emergency system failed. Consequently, it can be inferred that only around 12.6% of all incidents had impact on flight operations prevented by a backup system.

Despite this, other measures such as manual passenger processing or baggage handling may have prevented delays or cancellations, and the fact that flights were not affected under circumstances of a failed emergency power supply raises doubts about the completeness of blackout consequences data. Future investigations may address this question by examining delay codes of flights during and shortly after blackout time for delays connected to terminal related processes.

Additionally, an investigation into blackout duration may gather more intelligence on reactive measures. The duration between first interruption and complete restoration of regular power supply is defined as blackout time. Figure 4.6 presents box plots for all regions, displaying inter-quartile ranges with median as yellow line, whiskers representing data range, i.e., data points lying within 1.5 times the inter-quartile range from the box, and outliers indicated by crosses. The median value is also listed in the box above. World-wide, the duration median was found to be 2 hours. The duration was highest in JAK (20.5 hours), followed by SAS region (4.8 hours) and AFR region (3.8 hours). However, only two cases were recorded in JAK, which may not be representative due to their catastrophic nature being of world-wide interest. All other regions reported durations on average or below.

A correlation between regional grid reliability variation and the source of blackout has been shown before. However, it remains a matter of interest whether regions with low grid reliability suffer from long blackout duration times. Blackout duration and SAIDI data are available for 31 countries. As incidents within a country may be distributed over several years and several customers, cumulative outage time  $t_{\text{total}}$  cannot be compared to the SAIDI of one year, but rather to an expected outage time  $t_{\text{expected}}$ . This yields in a dimensionless value which is define as prevention index  $p$ . The prevention index is based on the assumption that every customer, here the airport, in a country is exposed to a yearly outage risk in the order of the SAIDI accumulating to the expected outage time  $t_{\text{expected}}$  and indicates how well the prevention measures of airports worked out by comparing the actual outage time to the exposed risk, as stated in Eq. 4.1.

$$p = \frac{t_{\text{expected}}}{t_{\text{total}}} = \frac{\sum_{\text{years}} n_{\text{customers,year}} \cdot \text{SAIDI}}{t_{\text{blackout}}} \quad (4.1)$$

However, it has been noted that only years with registered incidents are considered in the expected outage time, as the data does not allow a continuous treatment. In addition, a fixed beginning point cannot be defined and possible SAIDI fluctuations cannot be considered. It has been observed that grid reliability is either stable or improves (Doing Business, 2016) particularly in developing countries. Therefore, the prevention index might

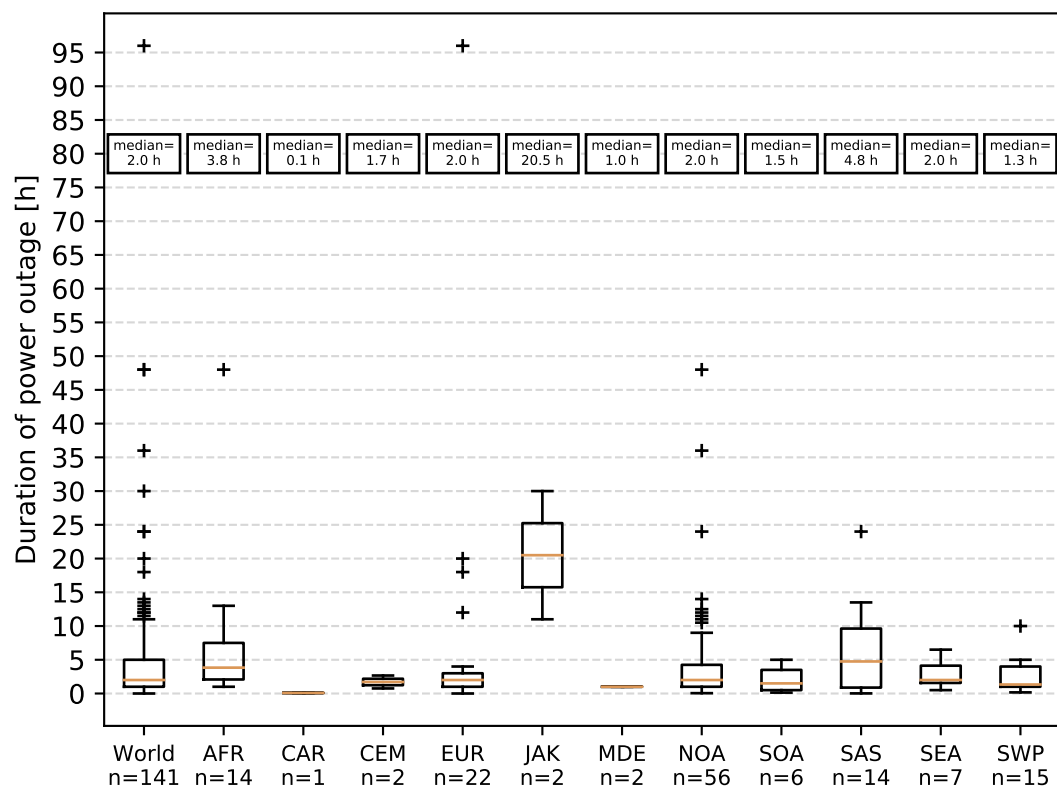


Figure 4.6: Blackout duration time as box plots for all incidents and by region including its written-out median in the upper box.

be corrected for these countries, as the expected outage time may be underestimated. The prevention index  $p$  gives a first guess about whether customers were able to limit the actual outage time to the exposed risk, which is the case for values above 1 or suffer from enhanced outage times at values below.

Complete data is available for 31 countries. Out of these, 10 were able to achieve a prevention index above 1 and therefore have well-performing either reactive or preventive measures to keep outage times low. While 5 countries suffer from outage times ten times higher than the expected outage time, 16 countries have a prevention index within the range of 0.61 to 0.1. As the representativeness of single incidents for their country might be questioned, these are explicitly excluded in the discussion. The resulting values are summarized in Table 4.5. Kenya (11.62), South Africa (6.09), Colombia (4.31) and El Salvador (1.96) have been able to confine their total outage time and therefore performed well under emergency conditions. All four countries have a SAIDI higher than 4.6 hours, which is far above the average of 2.7 hours (as a matter of fact, Kenya and South Africa have the highest SAIDI values overall with 60 and 44 hours, respectively).

On the other hand, the three countries with the lowest SAIDI i.e., UK (0.3 hours), Germany (0.2 hours) and Russia (0.3 hours) were not able to prevent long power interruptions yielding prevention indexes of below 0.1. It has been concluded that a high grid reliability results in a bad performance during emergency situations due to the low awareness for blackouts as a risk, while countries where power outages are common have established good preventive and reactive emergency measures. However, Puerto Rico is an exception with a SAIDI of 14.4 hours, but a prevention index of 0.4.

In addition to risk awareness, another important factor are financial resources. The Puerto Rican Electric Power Authority (PREPA) was greatly indebted (Lambert and Adler, 2014) and the infrastructure suffered from lack of investment until a nearly complete destruction by the hurricanes Irma and Maria in September 2017. While the government - in cooperation with Siemens - is working on the rebuilt of a resilient microgrid system (Siemens, 2018), the grid still poses an exceptional risk for infrastructure operators. Nevertheless, Puerto Rico still performed better than Australia (0.39), the USA (0.28) and the Netherlands (0.27). The bad performance of especially high-income European and North American countries should attract attention to the lack of a high-quality emergency management system in these countries. Therefore, new measures should be considered with regard to establishing a resilient airport system.

#### **4.1.3 Risk Mitigation**

To successfully find mitigation measures, a detailed analysis of the outage's cause is required. An overview of all found causes is presented in Figure 4.7. The reason for the outage remains unknown or uncommunicated to the public in 30% of cases. Clear-up rates are below average in SWP (47%) and NOA (45%). Transmission line failures, power grid failures, transmission station failures, and construction/maintenance work are found

Table 4.5: Prevention index  $p$  by country considering expected and suffered blackout times with more than one incident.

| Country            | Country Code | IATA region | $t_{\text{total}}$ | n  | SAIDI  | $t_{\text{expected}}$ | $p$   |
|--------------------|--------------|-------------|--------------------|----|--------|-----------------------|-------|
| Kenya              | KEN          | AFR         | 25.82 h            | 5  | 60.0 h | 300.0 h               | 11.62 |
| South Africa       | ZAF          | AFR         | 21.67 h            | 3  | 44.0 h | 132.0 h               | 6.09  |
| Colombia           | COL          | SOA         | 2.13 h             | 2  | 4.6 h  | 9.2 h                 | 4.31  |
| El Salvador        | SLV          | CEM         | 3.42 h             | 2  | 6.7 h  | 6.7 h                 | 1.96  |
| Canada             | CAN          | NOA         | 14.67 h            | 10 | 0.9 h  | 9.0 h                 | 0.61  |
| Philippines        | PHL          | NOA         | 7.25 h             | 2  | 3.9 h  | 3.9 h                 | 0.54  |
| Belgium            | BEL          | EUR         | 3.00 h             | 2  | 0.7 h  | 1.4 h                 | 0.47  |
| India              | IND          | SAS         | 26.47 h            | 6  | 4.0 h  | 12.0 h                | 0.45  |
| Malaysia           | MYS          | SEA         | 3.13 h             | 2  | 0.7 h  | 1.4 h                 | 0.45  |
| Puerto Rico        | PRI          | NOA         | 72.00 h            | 2  | 14.4 h | 28.8 h                | 0.40  |
| Australia          | AUS          | SWP         | 37.08 h            | 15 | 1.2 h  | 14.4 h                | 0.39  |
| USA                | USA          | NOA         | 198.22 h           | 44 | 1.3 h  | 54.6 h                | 0.28  |
| Netherlands        | NLD          | EUR         | 4.50 h             | 2  | 0.6 h  | 1.2 h                 | 0.27  |
| UK                 | GBR          | EUR         | 26.50 h            | 8  | 0.3 h  | 2.4 h                 | 0.09  |
| Germany            | DEU          | EUR         | 20.17 h            | 2  | 0.2 h  | 0.4 h                 | 0.02  |
| Russian Federation | RUS          | EUR         | 100.00 h           | 2  | 0.3 h  | 0.6 h                 | 0.01  |

to be responsible for 13.1%, 9.7%, 9.1%, and 8.6% of all incidents, respectively. The often-mentioned force majeure, encompassing categories such as weather, fire, sabotage/security, and others, is surprisingly only responsible for 14.9% of all incidents. In the remaining cases, passengers or airlines may claim compensation, which can result in significant monetary losses for the polluter.

Investigation into the causes of outages has revealed that identifying responsible stakeholders is crucial to implement mitigation measures, as the ability to do so varies among individuals and organizations. The analysis further determines which of the causes has led to internal, external, regional, and nationwide outages. Figure 4.8 presents the results of this investigation, where internal sources are colored in light coral, external in light green, regional in light blue, and nationwide in violet.

Figure 4.7 reveals that 30.3% of all incidents were categorized as unknown reasons for the outage. Breaking down these 52 incidents into different source locations yields that nearly 85% of them were caused by the airport itself, as shown in Figure 4.8. This conclusion may be drawn without sufficient airport investigations or airports failing to release investigation results, which makes them vulnerable to criticism about their emergency management and leaves customers dissatisfied. Furthermore, a lack of thorough investigation prevents airports from defending themselves in case of claims for compensation. It is highly advised that either clear-up rates are increased or, if the cause is known, it is communicated to the public. On the other hand, clear-up rates in case of nationwide or regional outages are relatively high, contributing only 2% and 6% to unknown cases, respectively.

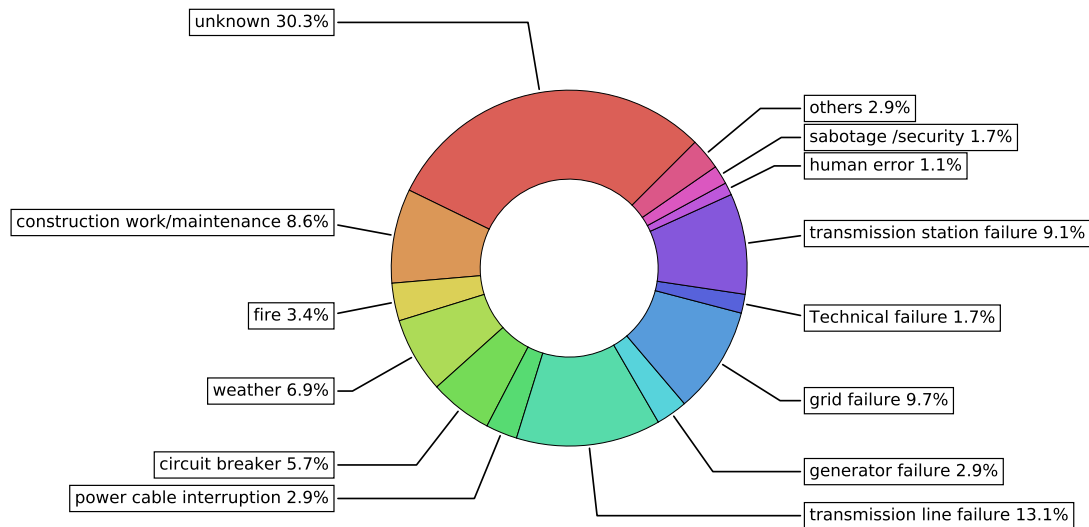


Figure 4.7: Percentages of world-wide blackout causes.

Certain causes can be identified as typically leading to internally or externally caused outages. Grid failures, such as power plant failures or necessary load shedding, are by definition external causes. However, weather-related issues, particularly for external polluters, contribute significantly to cumulative nearly 84% and 96%, respectively.

Regions exposed to extreme weather conditions, such as wind or flooding, benefit from reducing overhead cabling to minimize the risk of transmission line cuts. The implementation of microgrid structures, as planned in Puerto Rico by Siemens (2018), can help to increase grid resilience. In large area countries like the USA, distributed energy production and creation of interconnected microgrid structures can decrease dependence on single transmission lines.

While sabotage or security issues occur to 100% of the external grid level, it is unclear whether they are a commonly non-communicated reason to prevent exposing vulnerable infrastructure points. Approximately 60% of outages due to construction/maintenance work and 50% due to fire pose opportunities for significant improvement measures in grid operation. Improved planning strategies using simulation techniques can prevent non-resilience after stress tests, while better information flow between grid operators and construction/-maintenance companies can reduce the risk of power cables being cut by excavators. The use of fireproof materials, sun protection, sufficient cooling, and regular maintenance lower the risk of fire ignition, although it cannot be eliminated entirely when using electric devices.

In addition to a low clear-up rate of internal causes, the infrastructure operator views circuit breakers (90%), power cable interruptions (80%) generator or technical failures (100% each) and transmission station failures (69%) as dominant reasons for outages. While circuit breakers occasionally occur, sufficient capacities of an uninterrupted power supply (UPS) should be available for especially ICT systems to prevent long rebooting phases or

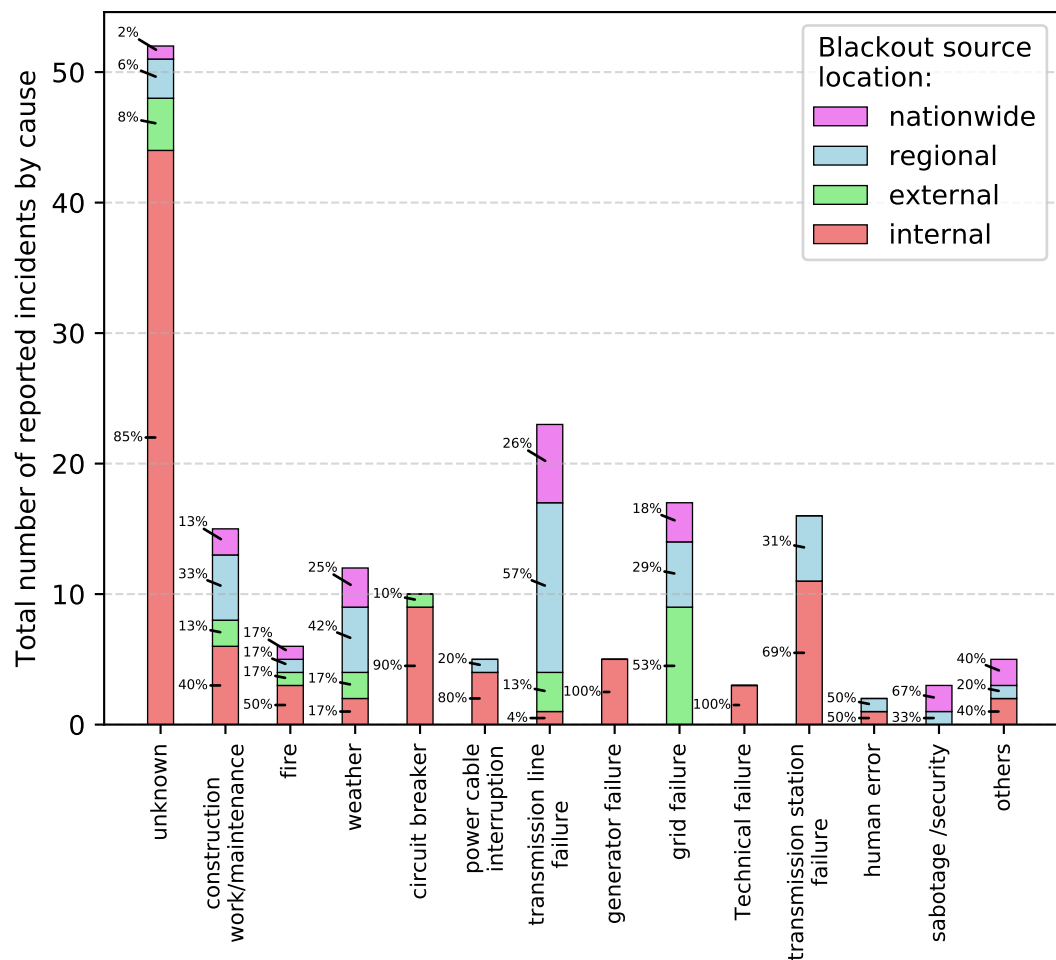


Figure 4.8: Source location distinguished by cause of the outage.

even data loss. In addition, short-circuit localization methods (Zhou et al., 2011; Mohammadpour and Dashti, 2011) are necessary to improve reaction speed.

Aging infrastructure is found to go hand in hand with insulation becoming detached and therefore causing cable faults. However, localization of power cable interruptions is the most important step, as it can prevent the operator from replacement of a large amount of cables. Thus, pulse-reflection or transient methods should be known by the crisis unit and the necessary equipment such as a time-domain reflectometer should be available. Moreover, preventive maintenance using simulations may assist to monitor the infrastructure and forecast cable abrasion or similar issues to repair or replace cables efficiently.

While failing of technical devices cannot be prevented, strategic planning of the electrical circuit structure in form of a controlled multi-bus microgrid (Hamzeh et al., 2012; Yunwei Li et al., 2004) enables, first, insulation in case of local dysfunctions, and second, strengthens the efficiency of a secondary power utility supply as proposed by the International Civil Aviation Organization (2017). The lack of a secondary utility supply magnifies the impact of a generator failure and therefore should be considered in the calculations of the capacity of the emergency power supply, which may be supported using modeling and simulation techniques (Koch et al., 2017, 2018). A secondary supply access point also mitigates the risk of severe consequences due to transmission station failures, which are located at the interface between utility grid and infrastructure. An additional interface works as a backup system as long as both suppliers are independent and capable of providing sufficient power for the whole airport system.

The evaluation of the applicability of proposed measures is highly dependent on individual airport properties, such as size, financial resources or geographic and political conditions. These properties determine the measure costs as well as the economic benefit. An individual risk assessment from an airport side is therefore highly recommended for the risks pointed out in this work. Airport simulation tools can be used to assess the impact of mitigation measures on individual airport systems. However, common interests among stakeholders need to be defined beforehand, also with regard to contractual arrangements.

In future work, correlations between airports size, cause and impact should be investigated to further improve risk probabilities by transferring fixed probability to a function of airport size. Within this work, airport sizes ranging from 6000 passengers per year to 107 million passengers per year (including one airport without scheduled services) have been covered, although press releases tend to focus on major airports (48.6% of all registered airports handled more than 20 Mio. passengers a year and 76.1% more than 5 Mio. passengers a year). Web mining can be used to enhance the database, but its success depends on evaluation with regard to precision of cause and source categorization beforehand. Search agent functions should also be created to feed the database with most recent data. Furthermore, additional languages may be used to supplement the database, especially in Russia, Africa or the Middle-East.

## 4.2 Strengthening ICT Networks through Vulnerability Analysis

The graph-based representation and propagation model of the ICT layer as introduced in subsection 3.1.1 allows to determine the impact of cyber attacks on the ICT infrastructure of airports. However, it does not allow to identify weaknesses or vulnerabilities in the system, which is an important capability to improve network security. In this section, a first quantitative metric is proposed that allows to

- measure the vulnerability of the system,
- compare the security of different network structures,
- and evaluate the effect of network changes or mitigation measures on the system vulnerability.

Based on this metric, most vulnerable points can be detected and used to deduce measures that help strengthen the ICT system. However, mitigation measures are expensive, whereas the cost-benefit ratio is important to evaluate the reasonableness of the measure. Therefore, an optimization problem is deduced that searches for the most improvement at lowest costs, i.e., cost efficiency. In application, this could be the case where replacing a router is a lot cheaper than replacing a server system.

### 4.2.1 Quantification of Network Security and Junction Point Detection

In graph theory, a manifold of properties exist that describe the graphs interconnectedness or analyses its structure. As the infection times in the propagation model are based on shortest-paths within a weighted graph, the metrics are based on either the distance  $d_{ij}$ , i.e., the sum of all weights on the shortest-path  $\sigma_{ij}$  (propagation time) between two vertices, or the importance of single vertices within the network structure (centrality indices). The betweenness centrality (Freeman, 1977) is an often used measure to describe the importance of a vertex within a network. The idea behind the betweenness centrality  $c_b$  for a given vertex is that how many pairs of vertices in the network are connected through the shortest path to each other passing the vertex. Thus, it is a perfect measure for the analysis of social network structures, connectivity analysis of metro systems (Derrible, 2012) or even the human brain (Joyce et al., 2010). The purpose of the stress centrality  $c_s$ , introduced by Shimbel (Shimbel, 1953) was to describe the “work” done by each device within a communication network. Similar to the model used in this work, Shimbel assumed that communication is done on the shortest-path and he therefore proposed the number of shortest paths through a vertex as a metric (Ghasemi et al., 2014). A typical problem in operations research is to find the optimum site for a facility on the basis of a specific criterion, e.g., the minimum response time to incident locations in case of a hospital. This

problem is solved by minimize the maximum distance to any other node within the network (Hage and Harary, 1995). As stated above in a connected graph the distance  $d_{ij}$  is the sum of all edge weights on the shortest-path from vertex  $v_i$  to vertex  $v_j$ . Based on this problem Hage and Harary (1995) introduced the eccentricity centrality  $c_e$ . Adopted to the propagation of malware within an ICT network, this eccentricity centrality can identify the best attack point for a malware as the time at which all devices are infected is minimum. The betweenness, stress and eccentricity centralities can be calculated using Eq. 4.2, Eq. 4.3, Eq. 4.4, respectively, where  $\sigma_{jk}$  denotes the total number of shortest-paths from vertex  $v_j$  to  $v_k$ ,  $\sigma_{jk}(v_i)$ , the ones passing vertex  $v_i$  and  $V$  all vertices within the graph.

$$c_b(v_i) = \sum_{j \neq i \neq k \in V} \frac{\sigma_{jk}(v_i)}{\sigma_{jk}} \quad (4.2)$$

$$c_s(v_i) = \sum_{j \neq i \neq k \in V} \sigma_{jk}(v_i) \quad (4.3)$$

$$c_e(v_i) = \sum_{j \neq i \in V} d_{ij} \quad (4.4)$$

The previously described metrics enable to analyze the structure of the ICT layer and identify important devices within the network. However, they do not quantify the impact of the malware infection on the operability of the devices during time. Thus, possible quantitative measures could also be

- the minimum distance  $\min\{d_{ij}\}$ , i.e., the point in time, where the first device is infected and the impact on the system starts,
- the maximum distance  $\max\{d_{ij}\}$ , i.e., the point in time, at which all devices are infected and therefore the impact is maximum,
- and the mean shortest-path length  $\bar{d}$ , i.e., the arithmetic mean of all shortest-path distances  $d_{ij}$  within the network.

A property that is suitable should be able to quantify the impact of slight network changes, while delivering robust results. Furthermore, the property is intended to evaluate the spreading through the network in case of an infection. Thus, the minimum distance is inappropriate as it refers to the time before the spreading starts.

To further evaluate the applicability of the other previously described properties, a graph is generated consisting of seven nodes and manipulated in a way that the last node is cut off. In this way a set of four networks is obtained, that differ in structure and size, while representing a similar network. The low number of nodes was chosen to enable a

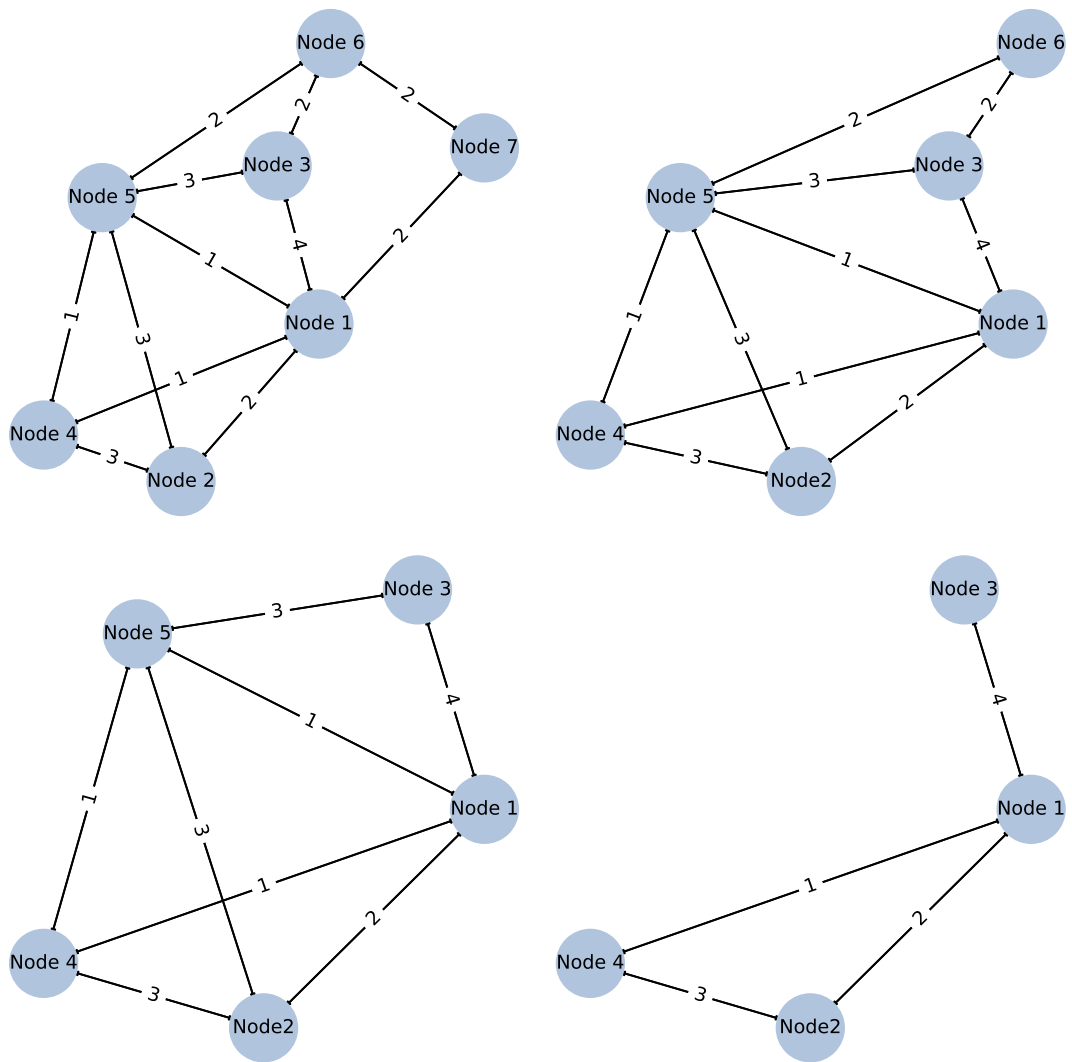


Figure 4.9: Example networks consisting of 7 to 4 nodes as a weighted graph. The smaller graphs are generated by cutting the last node off in each step.

Table 4.6: Resulting properties of the networks from Figure 4.9:

| property                                   | node  | n=7      | n=6       | n=5      | n=4      |
|--------------------------------------------|-------|----------|-----------|----------|----------|
| stress<br>centrality $c_s$                 | $n_1$ | 8        | 2         | 2        | 4        |
|                                            | $n_2$ | 0        | 0         | 0        | 0        |
|                                            | $n_3$ | 0        | 0         | 0        | 0        |
|                                            | $n_4$ | 0        | 0         | 0        | 0        |
|                                            | $n_5$ | 8        | 8         | 2        | -        |
|                                            | $n_6$ | 2        | 0         | -        | -        |
|                                            | $n_7$ | 0        | -         | -        | -        |
| betweenness<br>centrality $c_b$            | $n_1$ | 10.3     | 4.3       | 3.3      | 5        |
|                                            | $n_2$ | 0        | 0         | 0        | 0        |
|                                            | $n_3$ | 0        | 0         | 0        | 0        |
|                                            | $n_4$ | 0        | 0         | 0        | 0        |
|                                            | $n_5$ | 10.3     | 10.3      | 4.3      | -        |
|                                            | $n_6$ | 0        | 0         | -        | -        |
|                                            | $n_7$ | 2        | -         | -        | -        |
| eccentricity<br>centrality $c_e$<br>[t.u.] | $n_1$ | 4        | 4         | 4        | 4        |
|                                            | $n_2$ | 6        | 6         | 6        | 6        |
|                                            | $n_3$ | 6        | 6         | 6        | 6        |
|                                            | $n_4$ | 4        | 4         | 4        | 5        |
|                                            | $n_5$ | 3        | 3         | 3        | -        |
|                                            | $n_6$ | 4        | 5         | -        | -        |
|                                            | $n_7$ | 5        | -         | -        | -        |
| graph density                              | -     | 0.57     | 0.6       | 0.8      | 0.6      |
| $\max\{d_{ij}\}$                           | -     | 6 t.u.   | 6 t.u.    | 6 t.u.   | 6 t.u.   |
| $\bar{d}$                                  | -     | 2.9 t.u. | 2.86 t.u. | 2.8 t.u. | 3.5 t.u. |

comprehensible visualization. However, the scalability is only limited by computational resources. The resulting networks are depicted in Figure 4.9.

The stress (Shimbel, 1953), betweenness (Freeman, 1977) and eccentricity (Hage and Harary, 1995) centralities of all nodes in the networks as well as the graph density, maximum distance as well as mean shortest-path length for the four networks are given in Table 4.6. The direct comparison emphasizes the high influence of network topology on the stress and betweenness centrality of the nodes, as these are changing significantly with decreasing network size. Although node 1 stays prominent for all networks with a high centrality, cutting node 7 to obtain the network with 6 nodes yield in a switch of node 5 having a significantly higher stress and betweenness centrality. When the network size is decreased further to six nodes, the stress centralities of nodes 1 and node 5 are equal, while the betweenness centrality of node 5 stays slightly higher. As the eccentricity centrality is only influenced by a node deletion if there is a shortest path through the node, the values for the eccentricity only change when deleting node 7 and node 5.

The graph density is around 0.6 for the networks with seven, six and four nodes and 0.8 for the network with five nodes. There is no direct connection to the infection times, but

it indicates a high degree of interconnectedness of the network. A highly interconnected network tends to be less dependent on certain nodes, which corresponds to the lower absolute numbers in stress and betweenness centrality. Thus, the density might be an indicator to decide, if measures that would only improve the security of certain nodes, are even applicable, as more dense networks will not profit from them as much as less interconnected networks. The maximum distance stays at 6 t.u. for all networks as these are equivalent to the highest eccentricity centrality. The changes in mean shortest-path length  $\bar{d}$  range from 2.8 t.u. to 3.5 t.u. for the networks with 5 and 4 nodes, respectively. Comparing the evolution of the mean shortest-path length to the stress and betweenness centralities of the networks yield that a small amount of high centrality values may cause a raise of the average shortest-path length through a bottleneck effect, here especially due to the high weight between node 3 and its neighbors. This coupling between centralities and average shortest-path lengths can be used to efficiently detect these bottlenecks and use them to improve the overall network.

All of the properties can be used to describe the system and its overall robustness, whereas the stress and betweenness centrality show a high potential for the detection of points that have a large impact on the average shortest-path length. Conversely, the eccentricity centrality directly hints where to attack with maximum impact. Thus, the centrality values are able to detect junction points within the ICT network and therefore help to propose preventive measures that make the system more durable against cyber attacks by enhancing the time that is needed to infect the system.

#### 4.2.2 Increasing Network Strength with Minimum Costs

Graph properties can be used to detect vulnerable points within a network and can therefore yield as a basis for an efficient improvement of the ICT infrastructure. Although improving the security of a junction point is supposed to be most efficient with respect to the overall effect, it might be expensive. Thus, there is an urgent need for a method that combines these properties with costs, especially while treating with a limited budget. In the following, this issue will be described as a mathematical optimization problem and applied on the networks described in Figure 4.9 to demonstrate its feasibility.

Assuming that the weights of the graph determine the propagation properties and strengthening the system is done by modifying these weight, an improvement of singular components can be described as a increase of all weights connected to this node. Mathematically this translates to a modification of the adjacency matrix (see Eq. 3.1). More specifically improving a vertex  $v_l$  by a value  $s$  leads to adding  $s$  to column and row  $l$  of the adjacency matrix apart the value on the diagonal. To enable the improvement of multiple nodes at the same time, the strengthening values  $s_k$  can be represented by a strengthen vector  $\mathbf{s} = [s_1, s_2, \dots, s_{m-1}, s_m]$  with  $m$  equal to the number of nodes. Combining both can transform a given previous graph  $\mathbf{G}_{\text{pre}}$  to a graph of the strengthened system  $\mathbf{G}_s(\mathbf{G}_{\text{pre}}, \mathbf{s})$  with entries  $w_{s,i,j}$ .

$$w_{s,i,j} = \begin{cases} w_{\text{pre},i,k} + s_k & \text{for } k = 1, \dots, m, k \neq i \\ w_{\text{pre},j,k} + s_k & \text{for } k = 1, \dots, m, k \neq j \\ 0 & i = j \end{cases} \quad (4.5)$$

In Subsection 4.2.1 it has been shown that the average shortest-path length  $\bar{d}$ , is a suitable quantitative measure for network security. Thus, the average improvement per shortest-path seems a reasonable measure to determine the increase in robustness. The matrix containing all shortest paths of a graph  $\mathbf{G}$  is also referred to as distance matrix  $\mathbf{D}(\mathbf{G})$  with the entries  $d_{i,j}$  are given by the shortest-path length between vertices  $i$  and  $j$ . Thus, the improvement of the shortest paths can be written as

$$\Delta \mathbf{D} = \mathbf{D}(\mathbf{G}_s) - \mathbf{D}(\mathbf{G}_{\text{pre}}) \quad (4.6)$$

The sum of all entries of this matrix yields the total path length improvement  $\Delta d_{\text{total}} = \sum_{i,j} \Delta d_{i,j}$ . To get the average improvement per path as a comparable value to the average shortest-path length,  $\Delta d_{\text{total}}$  is divided by the number of possible paths  $N$ , i.e., the size of the distance matrix, which yields

$$\overline{\Delta d}(\mathbf{G}_{\text{pre}}, \mathbf{s}) = \frac{\Delta d_{\text{total}}}{N} \quad (4.7)$$

To elaborate the maximum improvement within a certain cost limit, a cost vector  $\mathbf{c}$  is introduced, whereas the entries  $c_i$  are representing the costs for the improvement of vertex  $i$  by 1 t.u., i.e., the dot product of the improvement and cost vectors yield the total costs for the improvement. In the following, this ratio of costs per time unit is referred to as cost units (c.u.). Defining a cost limit  $c_{\text{lim}}$ , the maximum average improvement per path while being in the budget mathematically translates to the optimization problem given in Eq. 4.8.

$$\max \left\{ \overline{\Delta d}(\mathbf{G}_{\text{pre}}, \mathbf{s}) \mid \mathbf{s} \cdot \mathbf{c} < c_{\text{lim}} \right\} \quad (4.8)$$

### 4.2.3 Solving the Optimization Problem

The optimization problem was solved by employing the brute force approach sketched in Algorithm 4.1. A Python generator iterator scheme was used to loop over all possible combinations, which allowed determining the maximum improvement of each node, as well as setting up a pool of combinations that covers all combinations within the specified cost limit (lines 4-8). However, improving multiple nodes would exceed the cost limit, whereas reducing the combinatorial space could be achieved by checking whether the total costs exceed the cost limit (line 9). Lowering the number of combinations was also possible

---

**Algorithm 4.1** Algorithm to solve the optimization problem given in Eq. 4.8:

---

```

1: maximum_solutions=[0] * len(G_pre)
2: D_pre = calc_distance(G_pre)
3: pool = list()
4: for i in range(0,len(G_pre)) do
5:   maximum_solutions[i] = int(ma.trunc(c_lim/c_array[i]))
6:   pool.append(list(range(0,int(maximum_solutions[i])+1)))
7: end for
8: combination = itertools.product(*pool)
9: combination_filtered = filter(lambda x: sum([a*b for a,b in
   zip(c_array,x)]) <= c_lim,combination)
10: combination_filtered = filter(lambda x: sum([a*b for a,b in
   zip(c_array,x)]) > min_spent_money,combination_filtered)
11: combination_filtered = filter(lambda x: sum(x) !=
   0.0, combination_filtered)
12: for i in combination_filtered do
13:   s_temp = list(i)
14:   G_s = strengthen_nodes(G_pre,s_temp)
15:   D_s = calc_distance(G_s)
16:
   Delta_D, improvement_per_path_temp, improvement_of_node_n_temp,
   average_improvement_per_node_temp = calc_Delta_D(D_s,D_pre)
17:   costs_temp = sum([a*b for a,b in zip(c_array,i)])
18:   if costs_temp != 0.0 then
19:     cost_efficiency_temp =
   improvement_per_path_temp/costs_temp
20:   else
21:     cost_efficiency_temp = 0.0
22:   end if
23:   if improvement_per_path_temp > max(improvement_per_path)
   then
24:     overwrite current values...
25:   end if
26: end for

```

---

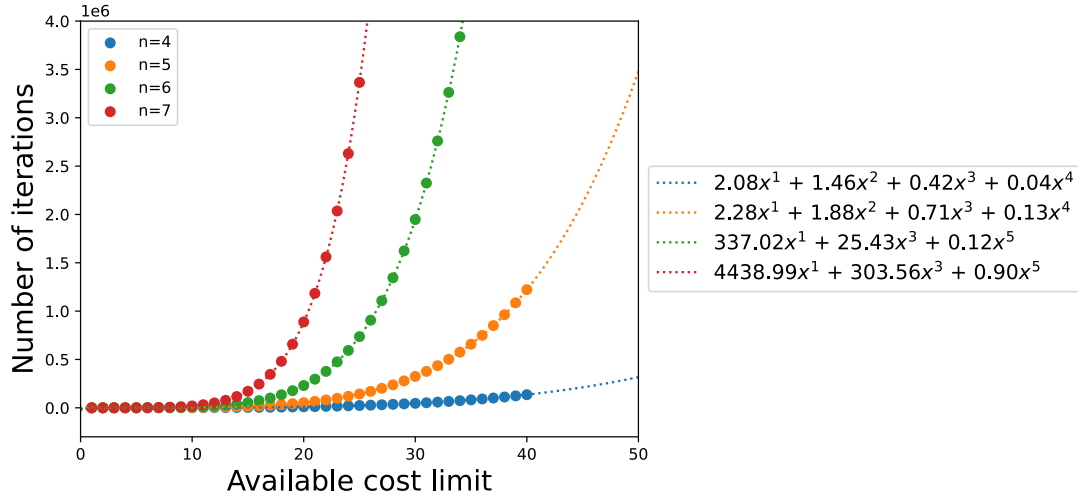


Figure 4.10: Number of iterations for the optimization with the graphs from Figure 4.9.

if a minimum amount of money was defined (line 10), and combinations yielding zero improvement were excluded (line 11). Iterating over all possible combinations (lines 12-26) and comparing the improvement (line 23) resulted in the optimal solution.

To benchmark the scalability of the approach with respect to the number of nodes, the algorithm was applied to the example networks shown in Figure 4.9, which featured a cost limit up to 40 c.u. and a cost vector consisting of ones.

The number of combinations can be mathematically described by the discrete volume of an  $n$ -dimensional simplex (Haase and Kiefer, 2016), where  $n$  referred to the number of nodes in the graph and the ratios of the cost limit and the cost vector entries spanned the simplex along the corresponding unit vectors. As the exact calculation of this integral polytopes is complex, the number of iterations were counted during code execution. A least squares polynomial fit was done without constraints on the order of the polynomials to obtain an impression of the difference in magnitude and be able to interpolate for other cost limits. The resulting number of iterations, i.e., number of possible combinations, were depicted in Figure 4.10. While the number of iterations for four nodes can be described by a polynomial of degree four (nearly degree three as the fourth order coefficient is very small), adding three nodes to the graph yield in an increase of iterations up to a fifth degree polynomial.

The impact of increasing the number of costs for the improvements of a node was investigated by analyzing the decrease in the number of possible combinations that resulted from lowering the ratio between the cost limit and the costs per improvement. This analysis was conducted by repeating the procedure while maintaining a constant number of nodes at six and incrementally increasing the costs for node five from 1 c.u. to 1.2 c.u. The resulting number of iterations and polynomial coefficients were visualized in Figure 4.11. The analysis revealed that, across all three setups, the polynomial fit yielded a fifth-order polynomial with minimal variations in the fifth-order coefficient. This finding indicated that

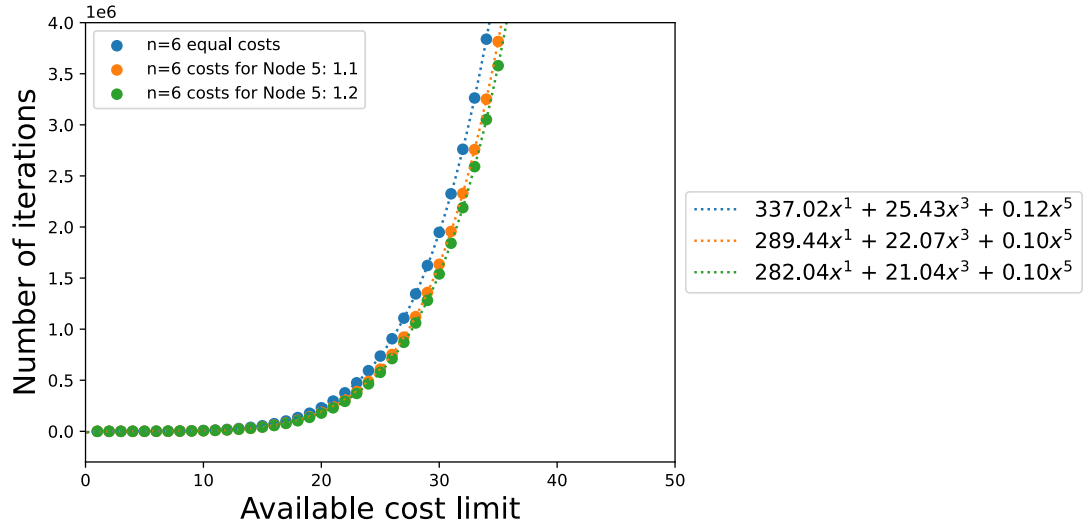


Figure 4.11: Number of iterations for the network with six nodes under the conditions of different costs for node five.

increasing the costs had only a modest influence on the number of combinations compared to the order of the graph.

#### 4.2.4 Advise for ICT Network Strengthening and Design

The proposed optimization problem was solved using brute force methods, resulting in a high number of combinations that had to be tried out. Although the duration for one iteration was on a millisecond scale, the high number of iterations made the approach inapplicable for large-scale networks, rendering it ineffective. The results, however, were utilized to answer questions regarding whether graph properties such as centralities allowed for efficient improvement of the network, and whether this held true when treating with different costs per node. Therefore, the resulting optimal solutions and their dependency on stress centrality were investigated using an example network with six nodes, as depicted in Figure 4.9 (top right). Scaling the cost limit up to 40 c.u. was considered for equal costs for each node, leading to an interchanging improvement of nodes 1 and 5, as evident from Figure 4.12, left side. Notably, only in the first two steps did node 5 experience improvements in a row.

A comparison of centralities before and after improvement was conducted, shown in Figure 4.12 right side, indicating that an additional improvement by the node with the currently highest stress centrality yielded the optimal solution. The first iteration relied on the stress centrality values listed in Table 4.6, where the stress centrality of node 5 was highest, underscoring this correlation. At steps where the stress centralities of node 5 and node 1 were equal, improving node 1 was found to be the optimal solution.

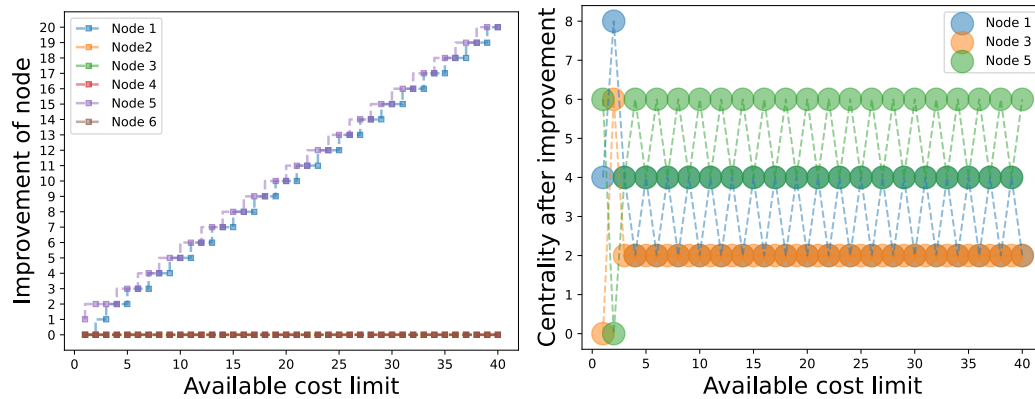


Figure 4.12: Improved nodes (left) and the stress centrality before and afterwards at equal costs for the improvement of a node.

The pattern was investigated to determine whether it holds for different costs. Consequently, two different cost vector variations were examined, with the results presented in Figure 4.13. The top row corresponds to a cost increase of 1.1 c.u. per improvement for node five, while the bottom row represents an increase of 1.2 c.u.

Due to the increased costs, improvements for node five were no longer feasible during the first iteration, as the costs exceeded the cost limit. In contrast, improving node one, which had the second highest stress centrality, yielded optimal results. At a cost limit of 2 c.u., only node five was chosen for improvement, although the cost limit would have allowed improvements of two other nodes instead. This process was repeated until node one held the highest stress centrality at a cost limit of 3 c.u.

Following this, an alternating improvement between node 5 and node 1 occurred until a cost limit of 20 c.u. was reached. After this point the improvements for both nodes stagnated. Instead, node three received improvements, despite having lower stress centrality than node 5.

The results for increased costs of 1.2 c.u. per node for node 5 showed a similar pattern (as seen in Figure 4.13, bottom row). However, the cost limit at which improvements for both nodes one and five ceased was reached at a cost limit of 10 c.u.

This pattern can be explained when examining the cost units that are leftover. Figure 4.14 depicts the evolution of unspent cost units while increasing the available cost limit. The optimal result yielded by improving node 5 initially, rather than two other nodes, created a financial buffer that was gradually depleted each time node 5 was improved. Consequently, the alternating stress centrality patterns in Figure 4.13 (right column) led to strengthening node 5 at each second step. The depletion of the financial buffer occurred at cost limits of 20 c.u. and 10 c.u., respectively, for increased costs of 0.1 c.u. and 0.2 c.u. Subsequent improvements of node 3 were undertaken three times, after which a financial buffer was rebuilt.

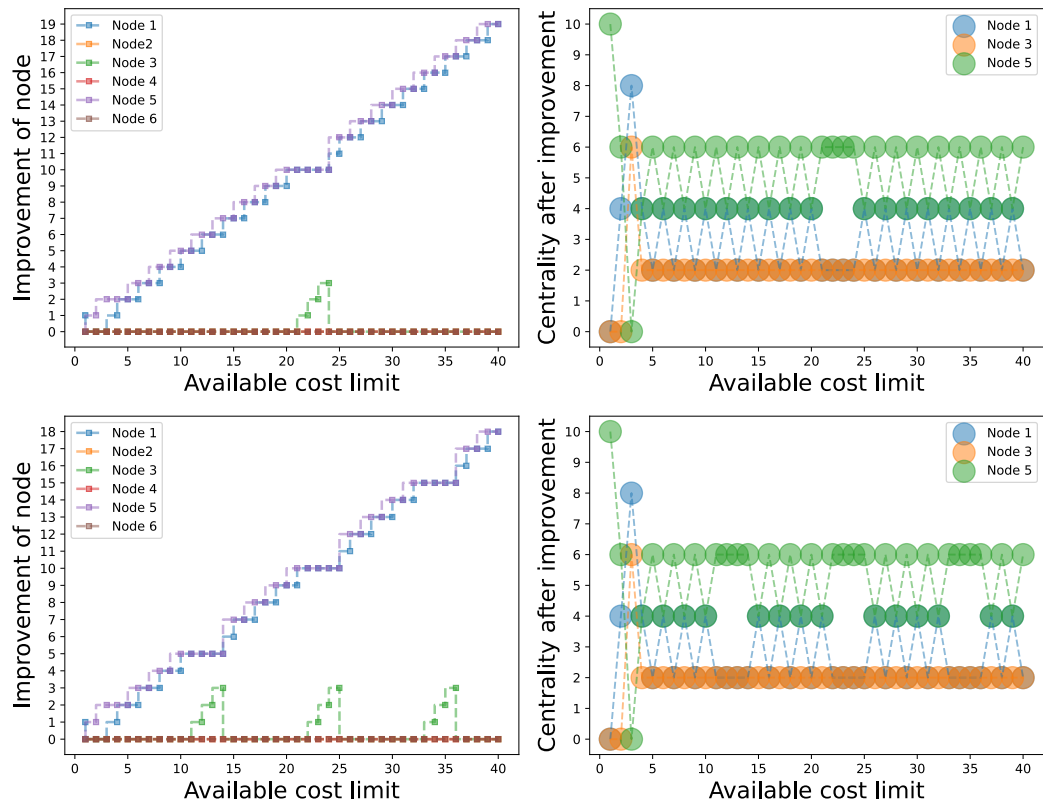


Figure 4.13: Improved nodes (left) and the stress centrality before and afterwards at costs of 1.1 c.u. (top row) and 1.2 c.u. (bottom row) for the improvement of node 5.

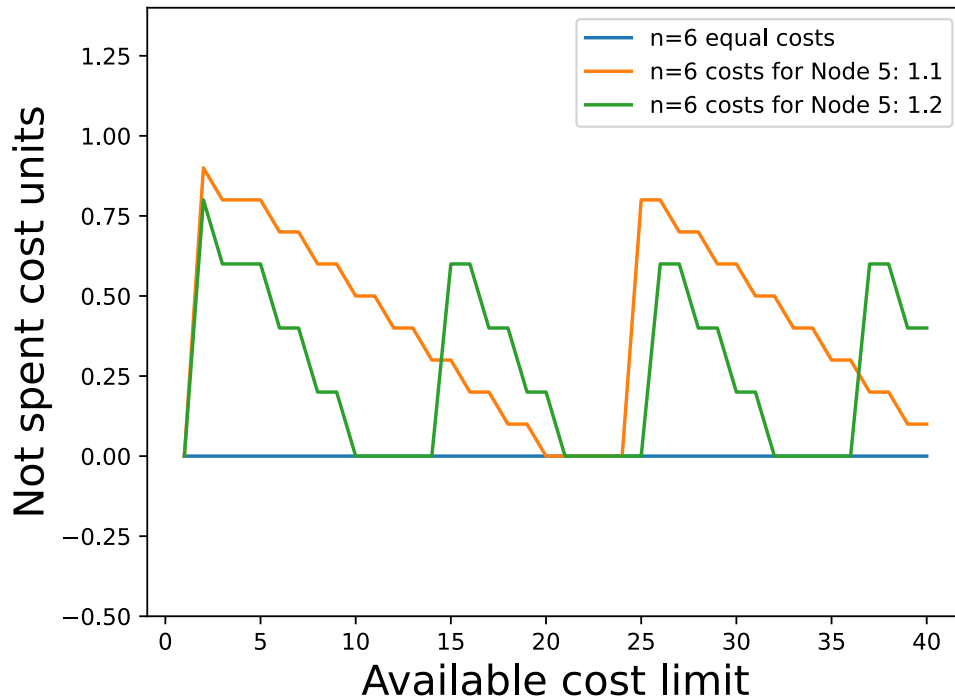


Figure 4.14: Leftover cost units for the cases with equal costs (blue) and increased costs for node 5 of 1.1 c.u.(orange) and 1.2 c.u.(green).

In summary, this section investigated whether stress centrality serves as a valid indicator for efficiently strengthening ICT networks by introducing an optimization problem that maximizes the improvement of average propagation times within the network under a limited amount of costs.

The optimization algorithm was implemented using a brute force approach for a small example network to explore whether stress centrality remains a viable indicator for maximum improvement, while differing costs are incurred for strengthening nodes within the network. Although the interdependencies between stress centrality and average shortest path improvement appear to be more complex when introducing deviating costs, it was proven that stress centrality is a feasible indicator for maximizing the efficiency of investments into ICT security.

However, the introduced optimization algorithm guarantees best results, but solving this optimization problem is related to high computational costs that render the approach impractical for large networks. Therefore, either optimized solvers are needed or a trade-off must be made between achieving perfect efficiency, i.e., solving the optimization problem, and using the fast-to-calculate stress centrality as an indicator for efficient improvement.

## Holistic Approach towards Impact Forecasting using Simulation

---

The scenarios and vulnerabilities identified in Section 4.1 are a solid basis to identify preventive safety and security actions. However, to establish reasonable and effective measures the impact of the scenarios on the airport as well as the effect of the actions has to be determined adequately. Nowadays, the impact estimation is often still based on expert knowledge or measures are selected to be in compliance with the regulatory prescribed standards. Although this was a good approach in the past, the increasing complexity of the infrastructure as well as the cascading effects demand for a holistic simulation approach that is capable to forecast the effect of blackouts and cyber attacks and therefore guarantee the effectiveness of preventive and reactive measures.

Within this chapter, the pipeline shown in Figure 5.1 is introduced, which allows an impact prediction based on simulation. In a first step, the CPS model introduced in Chapter 3 with its multiplex layer structure and its dynamics (see Section 3.2) is implemented to simulate the impact of blackouts and cyber attacks on the infrastructure level, i.e., to estimate the operational state of devices at airports during crisis situations. Moreover, a bridge to the airport processes is built through the concept of process-oriented grouping of network objects (Koch et al., 2019a) and therefore gain the availability of resources to continue airport operation (Section 5.2). Furthermore, the pipeline is enhanced by two approaches (Section 5.3) that are capable to forecast feasible key performance indicators to estimate the impact. While the first method described in Subsection 5.3.1 estimates the effect by solving a linear-algebra problem (Koch et al., 2019a), the second one presented in Subsection 5.3.2 is an agent-based simulation using the software AnyLogic to depict pedestrian flows and processes at a medium-sized airport inspired by Cologne-Bonn Airport ((Brause et al., 2020). Lastly, the simulation results are used to evaluate emergency measures based on their impact on the key performance indicators (KPIs).

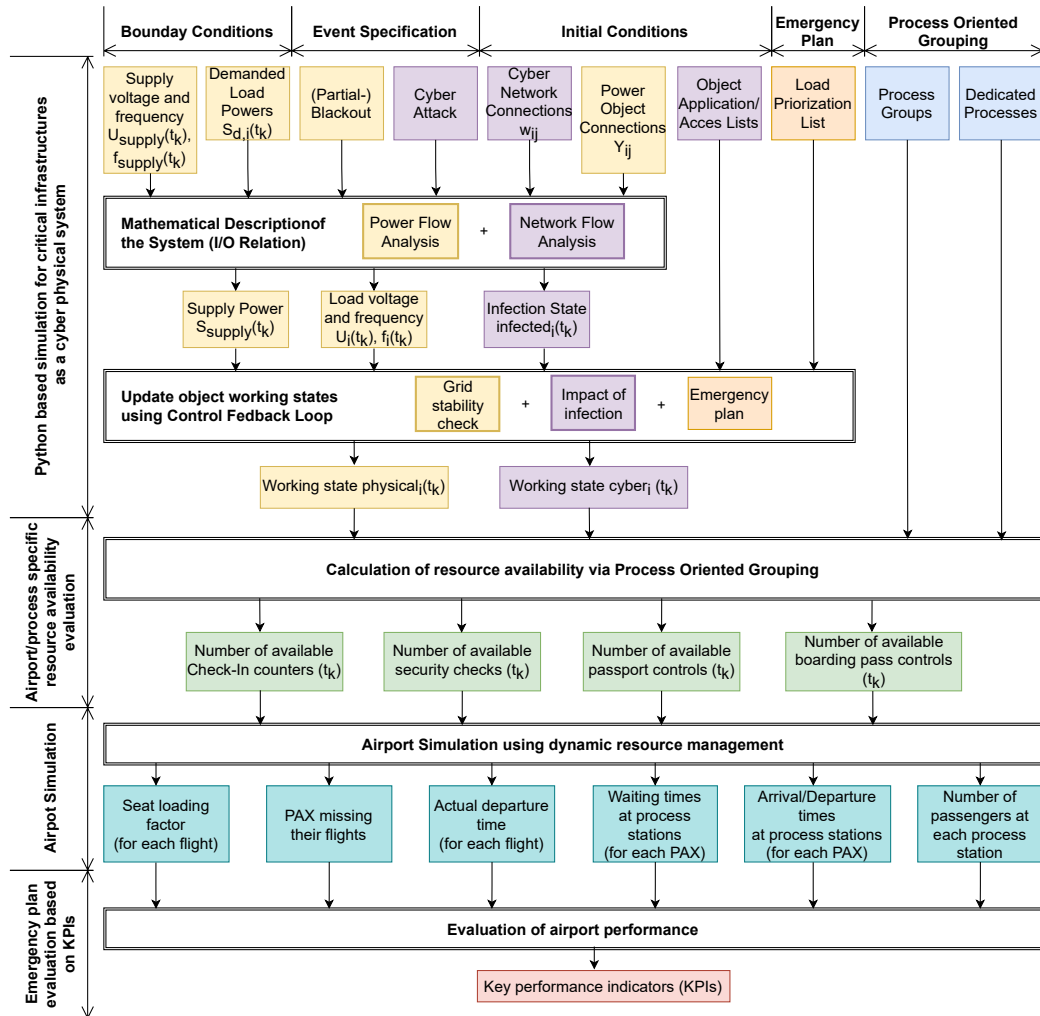


Figure 5.1: Input (top) can be divided into initial and boundary conditions for electrical (yellow) and cyber (purple) properties. Dynamically occurring events are given by special event input and knowledge about emergency measures and processes is needed. Electrical and cyber properties are used as input for the power-flow analysis and the network flow analysis. and fed into the control loop to gain information about operability states (Koch et al., 2018, 2017). The resulting device states are amalgamated into numbers of available resources (green) through process-oriented grouping. Simulations are used during the third phase to determine typical airport performance variables (blue) related to passenger processing as well as aircraft operation, which then are fused into KPIs (red).

## 5.1 Simulating the Operability State on Infrastructure Basis<sup>1</sup>

The first part of the holistic approach involves the investigation into the current physical status of the infrastructure in terms of operability. This is achieved through the implementation of the models described in Chapter 3 as a simulation tool, which is written in Python. Additionally, the functionality of the tool is validated through testing with a simple power grid and ICT network setup.

### 5.1.1 Implementation as a Python-based Simulation Tool

The implementation is fully completed in Python 3.7.9. A detailed overview of the Python environment and versions of all packages is provided in the Appendix (see A.2). The graphical user interface (GUI), based on wxPython (wxPython, 2022), was developed to facilitate the creation of a network setup without requiring programming knowledge, utilizing point-and-click functionality with direct visualization of the network through the use of the Python package NetworkX (Hagberg et al., 2008). The choice of the Floyd-Warshall algorithm for finding shortest paths was preferred over other alternatives due to its ability to reconstruct paths, which is essential for further network analysis (e.g., the vulnerability analysis explained in Section 4.2).

An interface to the PyPower package was created to solve the power flow problem, leveraging the Python port of MATPOWER (Zimmerman et al., 2011). The software architecture is oriented around a central class named `network_object`, which basically translates to the vertices of the graph in the multilayer network as depicted in Figure 3.3. Through the GUI, a pool of network object instances is initialized and used throughout the simulation to persist input and output values. The class contains information about the object itself, e.g., identifier, name, and operability state, as well as information relevant for the ICT and electrical layer. A total overview about the contained attributes, their type, unit, and a short description is provided in Table 5.1. Cyber attacks (in form of attack vectors, infection starting times etc.) and emergency plans (in form of an infrastructure prioritization list) are generated that define the investigated scenario. Additionally, network objects can be grouped and assigned to airport processes.

The GUI solely provides an editor mode, and instances of the classes `object_group`, `network_objects`, `cyber_attack`, and `emergency_management` are generated for use within this context. The GUI is continuously updated during editing mode to visualize the current network structure. Screenshots of the main GUI, the network object editor, and the object group editor are provided in the appendix (see Figure A.1 and Figure A.2, respectively). The parameters for cyber attack scenarios are chosen, and the load prioritization in case of emergencies is defined before starting the simulation (see Figure A.3 for screenshots). The simulation starting and ending time, as well as the step size, are also defined. After the system description is completed, the simulation phase is initiated. A presentation of the simulation workflow from a software perspective can be found in Figure 5.2.

<sup>1</sup>Parts of this subsection are reprinted with permission from Koch et al. (2018)© 2018, IEEE

Table 5.1: Structure of the network\_object class used to represent the CPS:

| network_object |                      |                |         |                                                                                                                         |
|----------------|----------------------|----------------|---------|-------------------------------------------------------------------------------------------------------------------------|
| domain         | attribute            | type           | unit    | description                                                                                                             |
| general        | iteration            | int            | -       | current iteration                                                                                                       |
|                | time                 | float          | s       | current simulation time                                                                                                 |
|                | dt                   | float          | s       | time step size                                                                                                          |
|                | added_element        | string         | -       | name of the device                                                                                                      |
|                | no_number            | int            | -       | identifier of the device                                                                                                |
|                | working_status       | bool           | -       | contains the operating state of the device (true = operating)                                                           |
| ICT            | connected_nodes      | dict           | - / s   | dictionary containing the names of the connected nodes and weights of the edges                                         |
|                | infection_status     | dict           | - / -   | dictionary of booleans stating whether the object is infected by each malware (multiple attacks)                        |
|                | infection_time       | dict           | - / s   | dictionary of times at which the object is infected for each cyber attack scenario                                      |
|                | applications_running | list           | -       | list with software names necessary for the object to operate                                                            |
|                | working_status_cyber | bool           | -       | determines whether the object is capable to fulfil its purpose on the IT-layer                                          |
| power grid     | bus_type             | str            | -       | string with the bus type of the NO ("load" = load; "gen" = generator; "ref" = reference bus; "isolated" = isolated bus) |
|                | voltage              | float          | -       | current voltage in per unit system                                                                                      |
|                | vmax                 | float          | -       | maximum allowed voltage in per unit system                                                                              |
|                | vmin                 | float          | -       | minimum allowed voltage in per unit system                                                                              |
|                | phase                | float          | -       | current phase shift                                                                                                     |
|                | demanded_power       | [float, float] | [W, VA] | apparent power demand containing real and reactive power demand                                                         |
|                | power_out            | [float, float] | [W,VA]  | generated apparent power in case of power sources                                                                       |

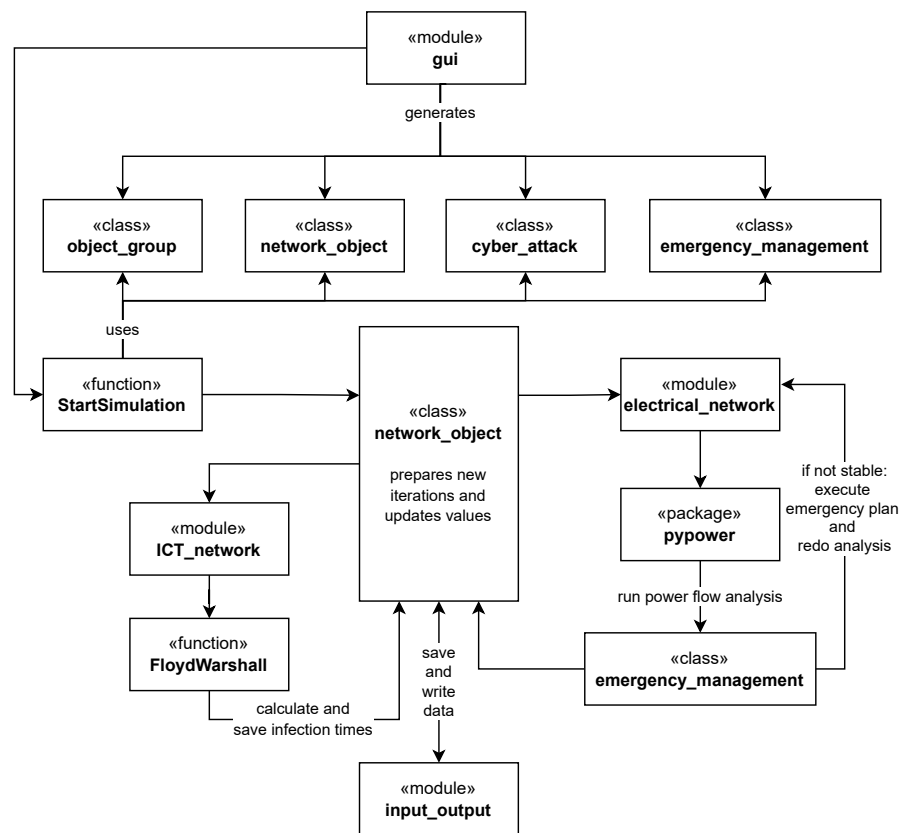


Figure 5.2: Schematic of the simulation workflow regarding software architecture.

At the first iteration, the infection times are calculated via the corresponding function in the `ICT_network` module (see left lower part in Figure 5.2). This calculation is performed by conducting the following workflow for each attack:

1. Graph representation: The adjacency matrix of the ICT layer graph is generated from the information stored within the pool of network objects;
2. Shortest-Path Calculations: Predecessor and Distance Matrix are calculated using the Floyd-Warshall Algorithm (see Algorithm A.1 for implementation);
3. Determination of infection times: The shortest times to all nodes are checked for all attack points, and for each node, the shortest time from one of the attack points to this node is selected as the infection time of the node;
4. Persist infection times in network objects: The infection times are saved within the network object for further use within the simulation.

A detailed overview of the algorithm is provided in Algorithm 5.1.

At each iteration of the simulation, a power flow analysis is conducted using the workflow depicted in Figure 3.8. The Python package PyPower (Zimmerman and Murillo-Sánchez, 2024) is utilized to perform this analysis.

A case file must be generated for conducting a power flow analysis in PyPower. Consequently, the data stored in the network objects has been transformed into a compatible data structure. The case files consist of three matrices that include all information regarding buses, generators, and branches. Furthermore, it has been ensured that units are adjusted to conform to the units used in PyPower. A comprehensive overview of the data structure of PyPower/Matpower can be found in the Appendix of the Matpower User Manual (Zimmerman and Murillo-Sánchez, 2024). The `electrical_network` module (right lower side in Figure 5.2) drives the following workflow:

1. Case file generation: The data in the network objects is transformed into three matrices corresponding to the case file structure. Units are adjusted to fit the PyPower requirements;
2. Power flow analysis: A power flow analysis is performed using the case file, yielding updated values;
3. Retransformation: A reverse version of step one is called to convert the data structure;
4. Stability Check: Stability is checked via the `emergency_management` module;
5. (Optional) Emergency Measure: In case of an unstable grid, measures such as load shedding are applied, and the workflow is restarted at step one;
6. Updating values: Values are written to network objects.

After each iteration, the working states are updated as described in Section 3.2. Moreover, the `input_output` module is utilized to save the results and update time series values, e.g., changing power demand and/or generation.

---

**Algorithm 5.1** Algorithm to calculate the infection times for a cyber attack:

---

```

1: for attack in list_of_cyber_attacks do
2:   shortest_times =
     numpy.full(number_of_network_objects, float("nan"))
3:   adjacency_matrix, labels = create_adjacency_matrix()
4:   pred, distance = fw.FloydWarshall(adjacency_matrix)
5:   for attack_point in attack.attack_points do
6:     for instance in list_of_network_objects do
7:       if instance.added_element == attack_point then
8:         attack_index =
           list_of_network_objects.index(instance)
9:         temp_shortest_times = distance[attack_index,:]
10:        for i in range(0, len(temp_shortest_times)) do
11:          if temp_shortest_times[i] < shortest_times[i] or
             ma.isnan(shortest_times[i]) then
12:            shortest_times[i] = temp_shortest_times[i]
13:          end if
14:        end for
15:      end if
16:    end for
17:  end for
18: end for
19: for instance in list_of_network_objects do
20:   index = list_of_network_objects.index(instance)
21:   instance.infection_time[attack.name] =
     (shortest_times[index] + attack.infection_starting_time)
22: end for

```

---

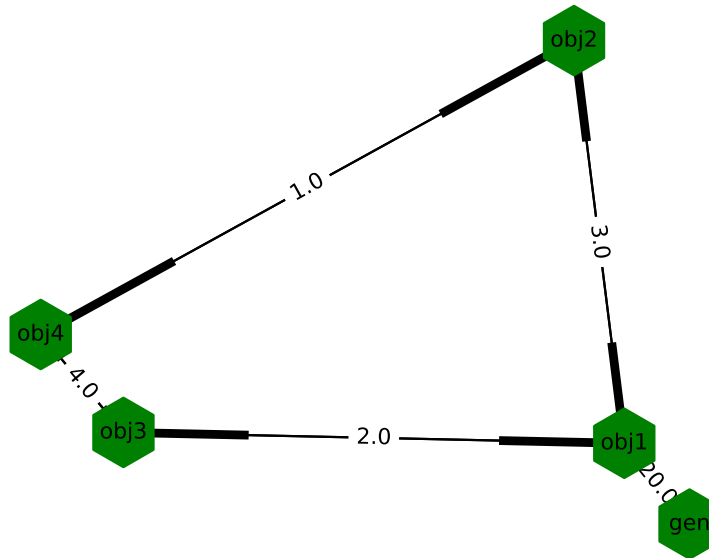


Figure 5.3: ICT Network structure with objects as nodes and infection speed as edges (Koch et al., 2018, ©IEEE 2018).

### 5.1.2 Verification of the Simulation Model

A minimal example is chosen to verify the implementation. As the determination of infection times and power flow equations does not change with scale, this verification is deemed sufficient. Additionally, the calculation of infection times for small systems can be done manually to confirm the implementation.

The test setup consists of four loads (named obj1, obj2, obj3, obj4) and a power source (gen), as depicted in Figure 5.3. In the context of airport infrastructure, this could represent a series of check-in counters containing four personal computers necessary for performing check-in. To simulate the system behavior throughout a day, a simulation time of 24 hours is chosen with discrete steps of 10 minutes (600 seconds).

The testing goal is to monitor the operating conditions of this group for one working day. Working hours are assumed to be normally distributed around 7:30 am and 5:00 pm, respectively, with a variance of half an hour. Based on data from Menezes et al. (2013), time series for the entire day are generated with a sampling rate of 600 s, featuring triangular shapes within working hours with a mean apparent power demand of 200 W and added randomly distributed noise of intensity 5 W. The power factor of the devices is randomly taken from a uniform distribution between 0.9 and 0.96 and used to divide the apparent power into real and reactive power. Obj2 of the devices is assumed to be shut down and rebooted in between. Figure 5.4 displays the time series for the apparent (blue), real (green) and reactive (red) power demand for the objects 1 to 4 from top to bottom.

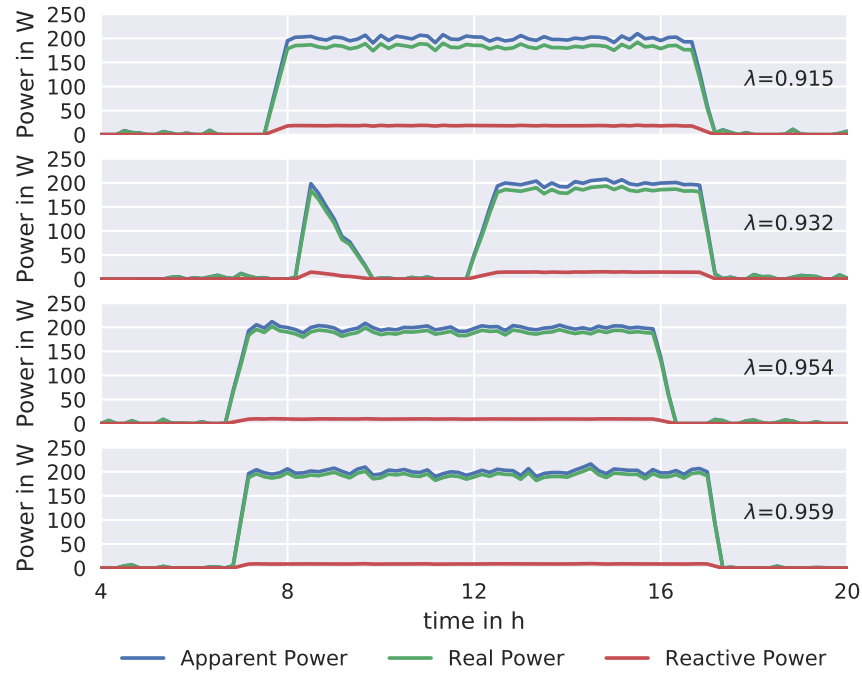


Figure 5.4: Showing time-dependent power demand for obj1 to obj4 (from top to bottom) during the working day and the corresponding power factor on the right (Koch et al., 2018, ©IEEE 2018).

As short transmission lines are treated, capacitive effects can be neglected. To minimize effects occurring from power transmission, connections are assumed to be nearly lossless transmission lines, but numerical issues require a small resistance of  $0.5 \text{ m}\Omega$  per unit length. The power supply voltage and frequency are chosen to be constant at 230 V and 50 Hz, corresponding to German grid values. Furthermore, power shortages are not included in this run, so the time series for injected power at gen is created with a mean power of 1000 W, random noise of 50 W, and a power factor of 0.9 throughout the day (Koch et al., 2018). The corresponding time series for power generation is presented in Figure 5.5.

### Verification of Infection Propagation

The weights in the ICT network representation depicted in Figure 5.3 determine the propagation times between nodes in hours, i.e., an infection spreads from e.g. obj2 to obj4 in 1 hour. A test scenario involving a cyber attack starting at  $t = 8$  hours at the attack point obj1 is chosen. Through manual calculation, the predicted infection times of the network components are calculated as follows: obj3 at  $t = 10$  hours, obj2 at  $t = 11$  hours, and obj4 at  $t = 12$  hours. This aligns with the working state changes within the simulation, which are represented in Figure 5.6. The correctness of the shortest path algorithm is ensured by this alignment. Under the given conditions, the network group becomes completely inop-



Figure 5.5: Showing time-dependent power generation at gen during the working day.

erable at  $t = 12$  hours. The infection of gen is out of the simulated time frame (Koch et al., 2018).

Furthermore, the application dependence is tested by adding operating systems to the computers. While obj1, obj3, and obj4 operate under Windows, obj2 operates based on Linux. The cyber attack is designed to start propagating at  $t = 0$  hours from the attack point (obj1) while only influencing Windows computers. The resulting evolution of the working states of the devices is presented in Figure 5.7. The infection times are calculated correctly, with obj1 being infected at  $t = 0$  hours, obj3 at  $t = 2$  hours, and obj4 at  $t = 4$  hours. Although the malware propagates through obj2 to reach obj4 in time, its working state remains unaffected, proving the intended behavior.

### Verification of the power flow analysis

The PyPower package is in wide-spread use for scientific work and has been tested in the context of a manifold of peer-reviewed publications (e.g., Jin et al. (2023); Yusuff et al. (2021)). Therefore, if the case file is generated correctly from the network objects, the power flow results are assumed to be correct. Thus, the matrix transformation was checked manually by comparison of the matrices and the corresponding network objects using the minimum example. For the bus matrix the transformation results in a  $4 \times 17$  matrix containing the 4 buses and the 17 attributes demanded by PyPower (see Table B-1 in Zimmerman and Murillo-Sánchez (2024)). The generator matrix includes the generator and its 21 attributes (see Table B-2 in Zimmerman and Murillo-Sánchez (2024)), yielding a  $1 \times 21$

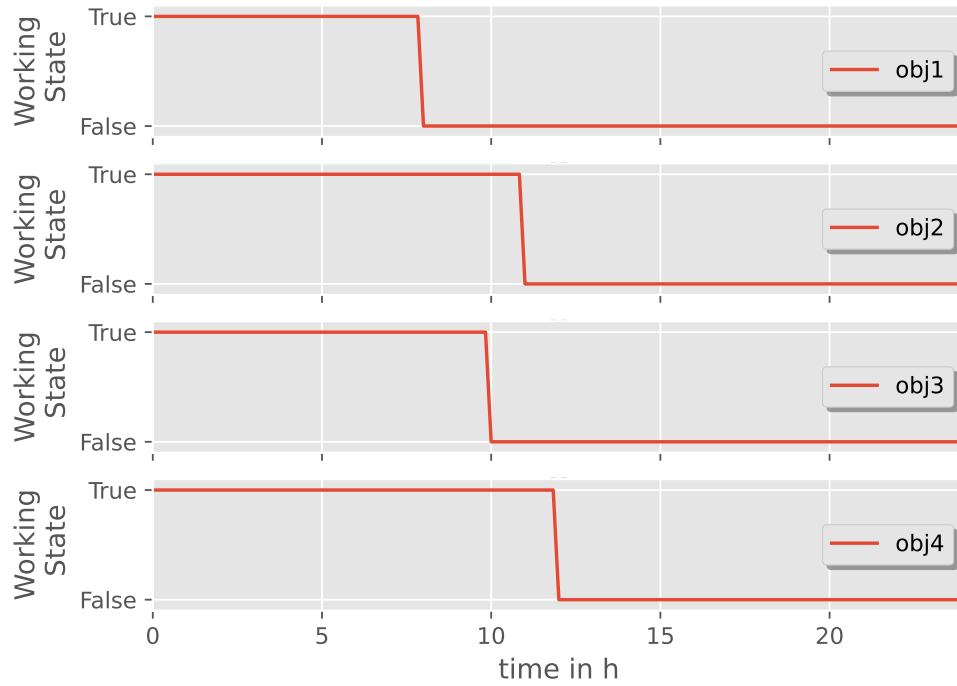


Figure 5.6: Changes in operating states during the day under the conditions of a cyber attack at  $t = 8$  h at the attack point *obj1*.

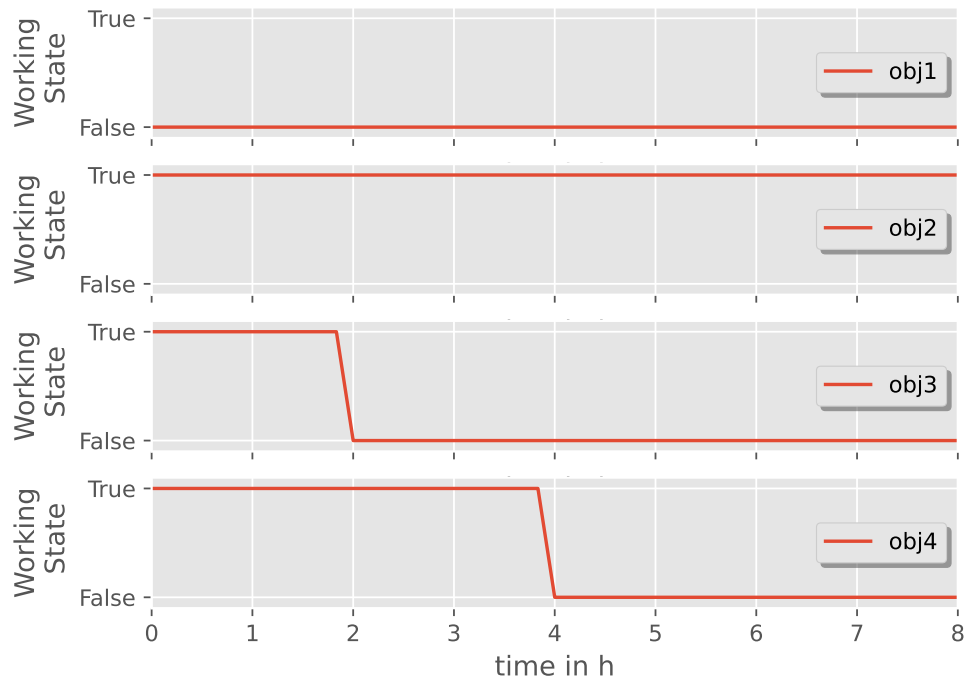


Figure 5.7: Changes in operating states during the day under the conditions of a cyber attack at  $t = 0$  h at the attack point *obj1* that only affects windows computers.

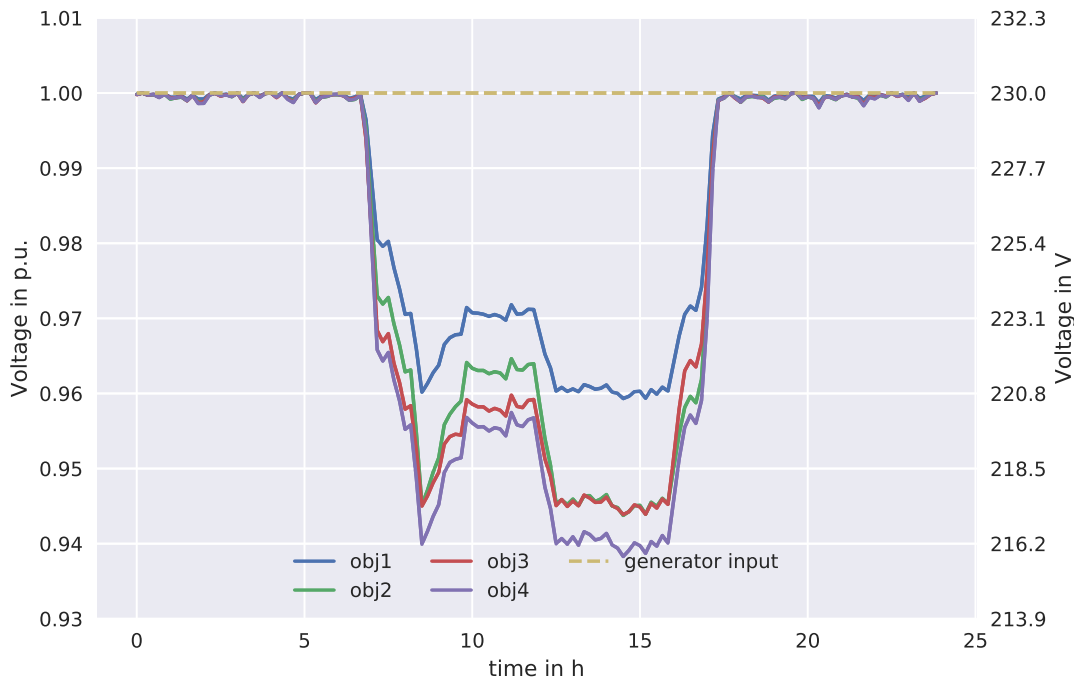


Figure 5.8: Evolution of the voltage magnitudes at all objects throughout the day at each component of the network. During working hours (6-8 h to 17:30 h) the increasing power demand causes a voltage drop at the loads. Within the phase in which *obj2* goes into standby (around 10 h to 12 h), the decreasing power demand result in a rise in voltage magnitude. Differences in the Voltage drop yield from the network geometry and cabling properties (Koch et al., 2018, ©IEEE 2018).

matrix. The five edges of the graph are transformed into a  $5 \times 21$  branch matrix (see Table B-3 in Zimmerman and Murillo-Sánchez (2024) for branch attributes).

To further validate the results of the analysis, the resulting voltage of the power flow analysis are analyzed. The daily evolution of the voltages applied at the objects is shown in Figure Zimmerman and Murillo-Sánchez (2024) given in p.u. (left scale) and volts (right scale) with a conversion factor of 230 V. While the voltage of the supply at gen is constantly 1.0, the voltages at the network objects drop with the start of the working hours at around 7-8 am to a minimum of 0.94 p.u. or 216 V, respectively. Between  $t = 9$  h and  $t = 10$  h the voltage increases due to the decreasing load, as *obj2* goes into standby mode until  $t = 12$  h. Then the voltage decreases again to the minimum of 0.94 p.u. until the end of working hours at around 5:30 pm. The different shapes at the start and end of working hours result from the shift difference between the start of power loading at the different objects. Moreover, the network structure influences the voltages in the way, that to *obj1* the highest voltage is applied, as it is directly connected to the power source. Furthermore, the lowest voltage is given at *obj4*, because the loads *obj2* and *obj3* are interposed. Other differences in voltage yield from the deviations in the demanded load power at the objects. Thus, the power flow analysis give meaningful results.

## 5.2 From Infrastructure to Processes through Process Network Objectification

As in the preceding section, only single devices have been considered. The transition from an operability state of individual objects to a process availability state is now demonstrated. Furthermore, the methods are explained through examples, including a generic test airport and a model generic medium-sized airport inspired by Cologne-Bonn Airport.

### 5.2.1 Process-Oriented Grouping

The information about device dysfunctions, power shortages, or other situations constraining the operation of single or multiple devices is often unused, although it may serve as an indicator for an upcoming problem within the processing chain. This omission results in a lack of comprehensive understanding of the process, highlighting the need to bridge the gap between single device operation and passenger processing. To address this issue, single devices are considered part of a higher level process group.

A vivid example from airport application illustrates the benefits of process-oriented grouping, as seen in Figure 5.9. This figure shows the grouping of single check-in counters to a process group, which is especially suitable for dedicated process groups such as check-in, which may be assigned to specific airlines or even certain flight numbers. The time consumption to undergo the process chain is highly dependent on the number of functioning devices within the same process group.

For the application example, a maximum of five check-in counters per check-in group (two groups) are selected, accompanied by four security checks, four passport controls split into two manual and two automated control points, and two boarding pass control devices at two gates each. Process shortcuts (CI: check-in; SC: security check; PC: passport control; APC: automated passport control; BPC: boarding pass control) are used to encode names, followed by the process group number and device number.

Although individual check-in counters comprise multiple devices, the approach of process-oriented grouping can be applied twice, first grouping single devices to a counter and then counters to a group, with reapplication on different levels. The setup in Figure 5.9 represents the initial state, where all devices are operating, with operating devices indicated in green (Koch et al., 2019a).

The grouping of the ICT layer and power grid layer, as introduced in Chapter 3, corresponds to an additional two-layer structure that projects physical and ICT resources onto process group objects and superior process groups. This structure is depicted in Figure 5.10. The light green layer in Figure 5.10 is aligned with the green circles in Figure 5.9, and its operability state is dependent on several devices within the CPS (e.g., devices 1,2, and 3 are assigned to process group object Check-In 1-1).

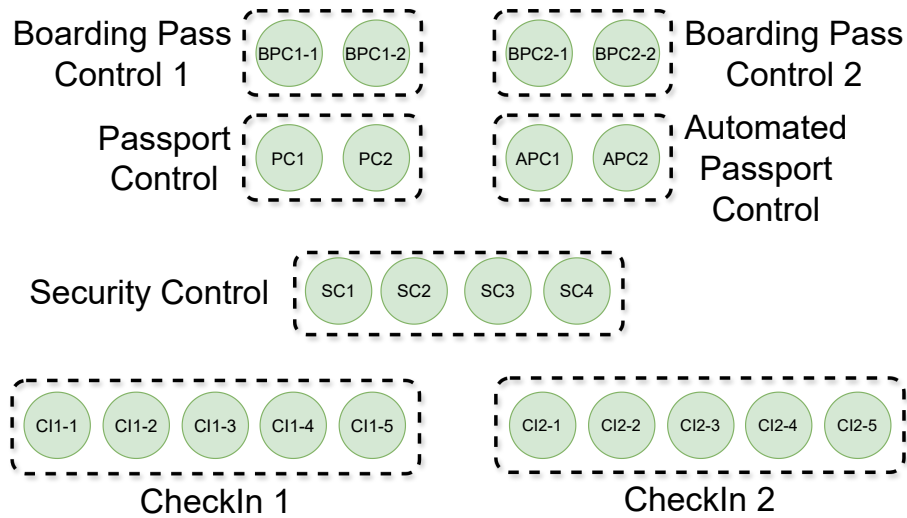


Figure 5.9: Process stations within a generic airport departure terminal consisting of two check-in counter groups, one security check group and two boarding pass control groups. Passport control is split into an automated and a manual passport control group. Each process group consists of several devices named by the process abbreviation, group number and device number. Green color indicates positive operating state of the devices. (Koch et al., 2019a, ©IEEE 2019)

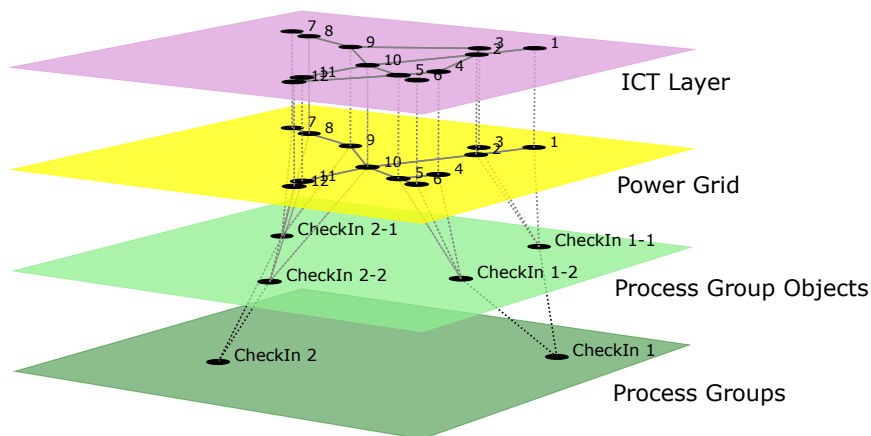


Figure 5.10: Multiplex network graph showing the relation between 12 devices in the CPS (ICT layer in purple and the power grid layer in yellow) and the process groups. Four devices are assigned to each process group object (light green), each, whereas they themselves form two process groups (darkgreen)

Table 5.2: Process Assignment Matrix  $\mathbf{P}_A$  for the system setup from Figure 5.9. (Koch et al., 2019a, ©IEEE 2019)

|                            | CI1-1 | CI1-2 | CI1-3 | CI1-4 | CI1-5 | CI2-1 | CI2-2 | CI2-3 | CI2-4 | CI2-5 | SC1 | SC2 | SC3 | SC4 | PC1 | PC2 | APC1 | APC2 | BPC1-1 | BPC1-2 | BPC2-1 | BPC2-2 |
|----------------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-----|-----|-----|-----|-----|-----|------|------|--------|--------|--------|--------|
| Check-In 1                 | 1     | 1     | 1     | 1     | 1     | 0     | 0     | 0     | 0     | 0     | 0   | 0   | 0   | 0   | 0   | 0   | 0    | 0    | 0      | 0      | 0      | 0      |
| Check-In 2                 | 0     | 0     | 0     | 0     | 0     | 1     | 1     | 1     | 1     | 1     | 0   | 0   | 0   | 0   | 0   | 0   | 0    | 0    | 0      | 0      | 0      | 0      |
| Security Control           | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 1   | 1   | 1   | 1   | 0   | 0   | 0    | 0    | 0      | 0      | 0      | 0      |
| Passport Control<br>(PC)   | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0   | 0   | 0   | 0   | 1   | 1   | 0    | 0    | 0      | 0      | 0      | 0      |
| Automated PC               | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0   | 0   | 0   | 0   | 0   | 0   | 1    | 1    | 0      | 0      | 0      | 0      |
| Boarding Pass<br>Control 1 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0   | 0   | 0   | 0   | 0   | 0   | 0    | 0    | 1      | 1      | 0      | 0      |
| Boarding Pass<br>Control 2 | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0     | 0   | 0   | 0   | 0   | 0   | 0   | 0    | 0    | 0      | 0      | 1      | 1      |

To associate devices with their respective process groups, a process group assignment matrix  $\mathbf{P}_A$  is introduced, denoted as Eq. 5.1. This matrix establishes a connection between network objects (represented by columns) and process groups (arranged in rows). A value of 1 in entry  $P_{A,i,j}$  assigns object  $j$  to process group  $i$ .

$$\mathbf{P}_A = \begin{pmatrix} P_{A,11} & P_{A,12} & \cdots & P_{A,1m} \\ P_{A,21} & P_{A,22} & & P_{A,2m} \\ \vdots & & \ddots & \vdots \\ P_{A,n1} & P_{A,n2} & \cdots & P_{A,nm} \end{pmatrix} \quad (5.1)$$

The rank of matrix  $\mathbf{P}_A$  is equal to the number of linearly independent column vectors, which corresponds to the number of distinct network object types and can thus serve as a measure of object diversity. The process assignment matrix for this specific case from Figure 5.9 is provided in Table 5.2.

### 5.2.2 From Grouping to Resource Management

To use the previously introduced process oriented grouping within resource management, the state of the devices and the process groups have to be linked. In Section 3.2, an approach to determine the operability state of the devices using a feedback loop was introduced. The result of this CPS analysis framework can be denoted as a state vector  $\mathbf{s}$  consisting of zeros and ones, where  $s_j$  refers to the working status of the network object and 1 is equal to working and 0 means out of order. Thus, the operability state of a system consisting of  $m$  network objects can be written as Eq. 5.2.

$$\mathbf{s} = [s_1, s_2, \dots, s_{m-1}, s_m] \quad (5.2)$$

Multiplying the state vector  $\mathbf{s}$  in transposed form and the process assignment matrix  $\mathbf{P}_A$  as introduced before, yields the product  $\mathbf{P}_A \cdot \mathbf{s}^T$ , which corresponds to the capacity  $\mathbf{p}_c$  of available resources for all  $n$  process groups:

$$\mathbf{p}_c = \mathbf{P}_A \cdot \mathbf{s}^T = [p_1, p_2, \dots, p_{n-1}, p_n]^T \quad (5.3)$$

The case of full operation (as shown in Fig. 5.9) yields in the total possible capacity of  $\mathbf{p}_{c,max} = \mathbf{P}_A \cdot \mathbf{1}_{m \times 1}^T$  with  $\mathbf{1}_{m \times 1}$  being an  $m \times 1$  column vector with all entries being 1.

Therefore, the method of process oriented grouping enables to link the outcome of the cyber-physical system airport model introduced in Chapter 3 with process capacities. This is especially important as it enables the use within common simulation models used to analyze passenger flows within airports, as these are the foundation for the impact analysis within this work. Within the evaluation pipeline depicted in Figure 5.1 the process oriented grouping enables the calculation of resource availability and therefore yields the number of available resources for each process group (corresponding to the green boxes).

### 5.3 Impact Simulation in an Airport Terminal

Impact estimation refers to the effect of system state changes on system performance. Applied to the airport system with focus on terminal operation, this corresponds to implications for passenger handling due to dysfunctional devices. Thus, using the previously introduced notation, changes of the state vector  $\mathbf{s}$  result in an adjustment of the process group capacities, as illustrated in Figure 5.11. The scenario is a disruptive event at a time  $t_1$  that leads to a dysfunctionality of devices within the airport system (here two counter in two check-in process groups). As the state of these devices are connected to the process capacity via Eq. 5.3, the process capacity decreases as illustrated in Figure 5.11. However, two different types of changes have to be distinguished:

- The set of devices of dysfunctional objects is determined by the event itself. This is the case for cyber attacks, damaged electrical devices or short circuits disconnecting a bus from the grid. Referring to the process capacity time series in Figure 5.11, the decrease reflects dysfunctional devices due to a cyber attack or device failure within these process groups and the increase equals repair measures of certain devices.
- In case of operation by decision and control as introduced in Section 2.5, however, the set of devices is determined by the decision maker, Control measures as load shedding or restructuring fall into this category. With respect to the scenario in Figure 5.11 devices within the two check-in process groups are actively chosen for load shedding at time  $t_1$  and restoration at time  $t_2$ . The control measures applied at  $t_1$  allow continuous airport operation with reduced process capacities under emergency conditions. At time  $t_2$  more power becomes available and some devices can be re-connected to the grid allowing reduced operation.

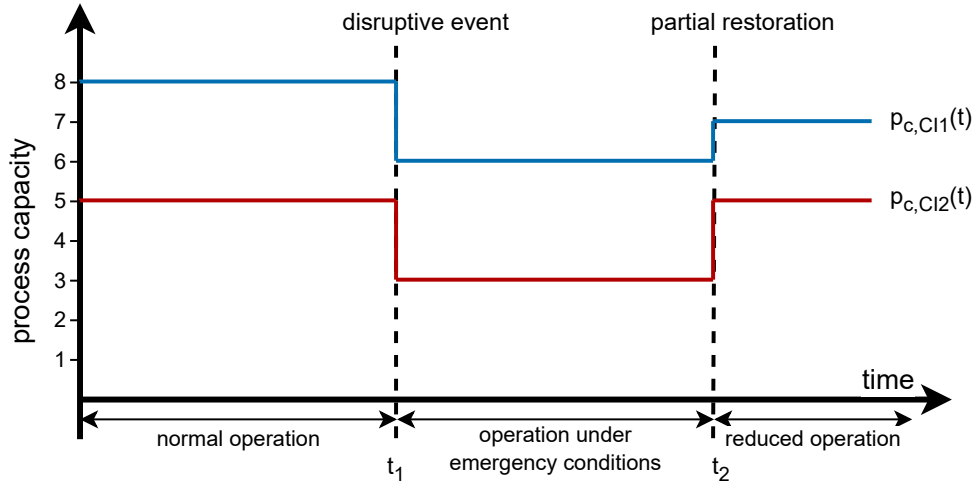


Figure 5.11: Process capacities  $p_c$  for two check-in process groups over time. A disruptive event demands for a control measures at time  $t_1$  lead to a decrease in process capacities for both check-in groups. At time point  $t_2$  conditions allow a partial restoration of the system.

In the context of impact estimation, these cases lead to two use cases for decision making support tools that have to be considered and differ in their requirements. The first one is a near-real time decision making support in situations with insufficient power supply, which requires load shedding. Proper estimation of the impact may help to determine which loads could be shed with a minimum impact on passenger processing. The near-real time criterion demands for a method that is capable to estimate the impact fast, however, should consider the whole process chain and their cascading effects. The second use case is the provision of more accurate and sophisticated models to forecast the impact of the dynamic process capacities on the airport system on a microscopic basis. Therefore, Within this section, two methods are introduced, whereas the first allows a fast forecast snapshot analysis, and the second one a microscopic simulation model including pedestrian dynamics.

### 5.3.1 Static Impact Estimation and Optimization using Linear Algebra<sup>2</sup>

In a very simplistic form airport processes can be considered as a sequence of processes with a constant throughput of passengers. Neglecting passenger interaction on their way through the airport and assuming a constant walking speed, time losses only happen due to either waiting in front of a process or by undergoing such a process. In the following, it is assumed that processes are conducted under the FIFO (first in, first out) principle, i.e., the passenger that waited longest in the queue gets served. Although processing times vary on an individual basis, they can be considered as constant on average and do not depend on the amount of people in the queue or the number of parallel processes. Thus, waiting

<sup>2</sup>Parts of this subsection are reprinted with permission from Koch et al. (2019a)© 2019, IEEE

times are the factor that order passenger flow within their process chain and waiting times are affected by the number of process capacities available.

In case of service processes, the approach of process-oriented grouping and resource management explained in section 5.2 can be enhanced by incorporating the waiting times at the process steps. For this static approach waiting times at the stations as well as process capacities are considered to be a snapshot out of the current state of the airport.

The current waiting times can be expressed in the form of a waiting time matrix  $\mathbf{P}_W$  with waiting times  $p_{w,ij}$  in time units (t.u.) for the corresponding process group  $i$  at service station  $j$ :

$$\mathbf{P}_W = \begin{pmatrix} p_{w,11} & p_{w,12} & \cdots & p_{w,1m} \\ p_{w,21} & p_{w,22} & & p_{w,2m} \\ \vdots & & \ddots & \vdots \\ p_{w,n1} & p_{w,n2} & \cdots & p_{w,nm} \end{pmatrix} \quad (5.4)$$

The Hadamard-product  $\mathbf{a} \circ \mathbf{b}$ , Hadamard-division  $\mathbf{a} \oslash \mathbf{b}$ , square root  $\mathbf{a}^{\circ \frac{1}{2}}$  and Hadamard-square  $\mathbf{a}^{\circ 2}$  notations as defined by Reams (1999) refer to element-wise operations of two matrices. For cases, in which the divisor of the Hadamard-division contains zero entries, holds  $a_i / b_i = 0$  if  $b_i = 0$ .

Combining the process waiting matrix  $\mathbf{P}_W$  (Eq. 5.4) and process assignment matrix  $\mathbf{P}_A$  (Eq. 5.1), the average waiting times  $\bar{\mathbf{w}}_{group}$  in t.u. for process group  $i$  can be calculated by

$$\bar{\mathbf{w}}_{group} = [(\mathbf{P}_A \circ \mathbf{P}_W) \cdot \mathbf{s}^T] \oslash (\mathbf{P}_A \cdot \mathbf{s}^T) \quad (5.5)$$

where  $[(\mathbf{P}_A \circ \mathbf{P}_W) \cdot \mathbf{s}^T]$  corresponds to the cumulative waiting time and  $(\mathbf{P}_A \cdot \mathbf{s}^T)$  to the current resource capacity  $\mathbf{p}_c$ . The Hadamard multiplication is necessary to exclude waiting times at service stations, which are not operating at the moment. As waiting times might strongly differ, it is necessary to include the standard deviation to later interpret the mean values. Starting with the definition of the standard deviation

$$s = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2}$$

with  $n$  being the number of values,  $x_i$  the single values and  $\bar{x}$  the mean value, the deviation term  $x_i - \bar{x}$  is described in matrix form  $\mathbf{P}_{W,dev}$  using the mean value  $\bar{\mathbf{w}}_{group}$  and the single values included in  $\mathbf{P}_W$ :

$$\mathbf{P}_{W,dev} = \mathbf{P}_W - (\bar{\mathbf{w}}_{group} \otimes \mathbf{s}^T) \circ \mathbf{P}_A$$

where  $\otimes$  is the dyadic product. Squaring the Matrix entries and sum up row-wise yields the standard deviation  $\Delta \bar{\mathbf{w}}_{group}$ :

$$\Delta \bar{\mathbf{w}}_{group} = \sqrt{[(\mathbf{P}_{W,dev} \circ \mathbf{P}_{W,dev}) \cdot \mathbf{1}_{m \times 1}^T] \oslash \mathbf{p}_c} \quad (5.6)$$

However, these waiting times need to be managed. Thus, in the next step the amount of waiting time for process group  $i$  in t.u., which needs to be redistributed towards the other service stations of the same type, has to be calculated by

$$\mathbf{w}_{unassigned,group} = \mathbf{P}_W \cdot (\mathbf{1}_{m \times 1} - \mathbf{s}^T) \quad (5.7)$$

with  $\mathbf{1}$  being a  $m \times 1$  column vector with all entries being 1.

However, sometimes it is necessary to detect the network object  $j$  at which the unassigned waiting times occur. Therefore, the waiting times of process group  $i$  at network object  $j$  are represented as a matrix  $\mathbf{W}_{unassigned}$ , which yields:

$$\mathbf{W}_{unassigned} = \mathbf{P}_W - \mathbf{P}_W \cdot \text{diag}(\mathbf{s}) \quad (5.8)$$

Assuming that the unassigned waiting time is distributed equally over the network objects within the process group and no change of processing time, the additional waiting time in t.u. per operating process group object is equal to:

$$\mathbf{w}_{add,group} = \mathbf{w}_{unassigned,group} \oslash \mathbf{p}_c \quad (5.9)$$

Combining mean process group time and additional time distributed towards the process group object, yields in the total process group time in t.u.:

$$\mathbf{w}_{total,group} = \bar{\mathbf{w}}_{group} + \mathbf{w}_{add,group} \quad (5.10)$$

$$\Delta \mathbf{w}_{total,group} = \Delta \bar{\mathbf{w}}_{group} \quad (5.11)$$

For some applications such as the passenger processing at airports, network object groups might be subordinated to a process within a chain, i.e., not every process groups waiting time contributes to the overall process time of one single passenger. Thus, a consecutive order of processes and the process structure has to be defined. Staying with linear algebra notation, a process sequence matrix  $\mathbf{P}_{seq}$  is defined to assign the process group  $i$  to one of the  $p$  processes. In the previously introduced airport example, the sequence contains check-in, security control, passport control and boarding pass control. The corresponding process sequence matrix is given in Table 5.3.

In the sequence matrix shown in Table 5.3 passengers are equally distributed over all process stations. However, modeling real airport operation requires to consider more process properties, such as not all gates, check-in counters etc. are used by all passengers equally, as some counters are assigned to certain airlines or flights not being distributed equally over all gates. This can be considered by replacing the entries in the process sequence matrix by weights representing the percentage of passengers assigned to the process. By adding an additional column with zero entries as waiting times, passengers can even skip a process.

Table 5.3: Process sequence matrix  $\mathbf{P}_{seq}$  (Koch et al., 2019a, ©IEEE 2019):

|                       | CI 1 | CI 2 | SC | PC | APC | BPC 1 | BPC 2 |
|-----------------------|------|------|----|----|-----|-------|-------|
| Check-In              | 1    | 1    | 0  | 0  | 0   | 0     | 0     |
| Security Check        | 0    | 0    | 1  | 0  | 0   | 0     | 0     |
| Passport Control      | 0    | 0    | 0  | 1  | 1   | 0     | 0     |
| Boarding Pass Control | 0    | 0    | 0  | 0  | 0   | 1     | 1     |

An example for this is given in the appendix in Table A.1, depicting a situation in which passengers from domestic flights do not need to participate in boarding pass controls.

Subsequently, the mean additional waiting time  $\mathbf{w}_{add,process}$  for each process concludes from the cumulative waiting times of all process groups belonging to the process divided by the number of process groups assigned to the process:

$$\mathbf{w}_{add,process} = (\mathbf{P}_{seq} \cdot \mathbf{w}_{add,group}) \oslash (\mathbf{P}_{seq} \cdot \mathbf{1}_{m \times 1}) \quad (5.12)$$

Likewise, the mean waiting time per process yield:

$$\bar{\mathbf{w}}_{process} = (\mathbf{P}_{seq} \cdot \bar{\mathbf{w}}_{group}) \oslash (\mathbf{P}_{seq} \cdot \mathbf{1}_{m \times 1}) \quad (5.13)$$

The standard deviations for equations 5.12 and 5.13 are given by Eq. 5.14 and 5.16.

$$\Delta \mathbf{w}_{add,process} = \left[ [(\mathbf{W}_{add,process,dev} \oslash \mathbf{W}_{add,process,dev}) \cdot \mathbf{1}_{m \times 1}^T] \oslash (\mathbf{P}_{seq} \cdot \mathbf{1}_{m \times 1}) \right]^{\frac{1}{2}} \quad (5.14)$$

with

$$\mathbf{W}_{add,process,dev} = (\mathbf{P}_{seq} \cdot \mathbf{w}_{add,group}) - (\mathbf{w}_{add,process} \otimes \mathbf{1}_{p \times 1}^T) \oslash \mathbf{P}_{seq} \quad (5.15)$$

and

$$\Delta \bar{\mathbf{w}}_{process} = \left[ [(\bar{\mathbf{W}}_{process,dev} \oslash \bar{\mathbf{W}}_{process,dev}) \cdot \mathbf{1}_{m \times 1}^T] \oslash (\mathbf{P}_{seq} \cdot \mathbf{1}_{m \times 1}) \right]^{\frac{1}{2}} \quad (5.16)$$

with

$$\bar{\mathbf{W}}_{process,dev} = (\mathbf{P}_{seq} \cdot \bar{\mathbf{w}}_{group}) - (\bar{\mathbf{w}}_{process} \otimes \mathbf{1}_{p \times 1}^T) \oslash \mathbf{P}_{seq} \quad (5.17)$$

Finally, the total waiting time per process can be calculated by adding the additional waiting time to the mean waiting time:

$$\mathbf{w}_{total,process} = \bar{\mathbf{w}}_{process} + \mathbf{w}_{add,process} \quad (5.18)$$

Using error propagation the uncertainty is given by:

$$\Delta w_{total,process} = \left[ \Delta \bar{w}_{process}^2 + \Delta w_{add,process}^2 \right]^{\circ \frac{1}{2}} \quad (5.19)$$

As quantitative performance measure the cumulative waiting time and its error for a single passenger is used:

$$w_{total} = \sum_i w_{total,process,i} \quad (5.20)$$

$$\Delta w_{total} = \left[ \sum_i \Delta w_{total,process,i} \cdot \Delta w_{total,process,i} \right]^{\circ \frac{1}{2}} \quad (5.21)$$

Moreover, for the application on process chains the readability of the matrix representation might be increased by resorting the process rows in chronological form. Therefore, a matrix  $\mathbf{P}_{order}$  is introduced which is able to order the process group rows by left multiplication. Formally, this is a transformation matrix of dimension  $i \times i$  leading to a change of base. The first step to determine  $\mathbf{P}_{order}$  is to determine an ordering vector  $o_k \forall k \in \{1, \dots, n\}$  containing the consecutive order of the processes groups with regard to their row number in  $\mathbf{P}_A$ . From there on  $\mathbf{P}_{order}$  yields as

$$\mathbf{P}_{order,ij} = \begin{cases} 1 & \text{if } i = o_k \wedge j = k \\ 0 & \text{else} \end{cases} \quad (5.22)$$

## Scenarios

To investigate the impact of system deviations on airport performance, three scenarios differing from the initial state (Figure 5.12 top left) are chosen. For reasons of comparison the same number of dysfunctional devices are used for each scenarios and chose the number of five, which corresponds to a percentage of around 22% of dysfunctional devices. In scenario 1 (Figure 5.12 top right) the dysfunctional devices are chosen to concentrate on the security checks with three non-operating devices, building a bottleneck within the process chain, and distributed the remaining two equally to the check-in counters. Scenario 2 (Figure 5.12 bottom left) represents a situation with a limited number of check-in counters being available, with a dysfunction of two out of five at each group and one defect automated passport control point. The last scenario 3 (Figure 5.12 bottom right) concentrates on the last processing steps with a dysfunction in both passport control types and at one boarding pass control at both gates each. The remaining dysfunction occurs on a check-in counter of check-in group one.

Although during the mathematical formulation neutral time units (t.u.) were used, waiting times are considered to be given in minutes for the application case. Waiting times have



Figure 5.12: Based on the layout given in Figure 5.9 the four used scenarios are displayed (initial state: top left; scenario 1: top right; scenario 2: bottom left; scenario 3: bottom right). While all scenarios, except the initial state scenario contain a cumulative number of five malfunctioning devices (indicated in red), the devices are distributed differently over the process groups. (Koch et al., 2019a, ©IEEE 2019)

Table 5.4: Waiting time distributions (in minutes) as input for the process groups:

| Process group         | CI 1 | CI 2 | SC   | PC  | APC  | BPC 1 | BPC 2 |
|-----------------------|------|------|------|-----|------|-------|-------|
| mean waiting time     | 6.8  | 7.2  | 12.0 | 9.5 | 3.0  | 1.25  | 2.0   |
| standard distribution | ±1.5 | 0.5  | ±1.9 | 2.5 | ±0.5 | ±0.25 | 0.0   |

been generated out of a normal distribution with the means and standard deviations given in Table 5.4. To prevent deviations due to random generation, a constant seed for all scenarios is used.

The corresponding entries of the waiting time matrix  $\mathbf{P}_W$  are given in Table 5.5.

The idea behind this combination of waiting times and scenarios are:

1. to create an exaggerated bottleneck at the security checks in scenario 1 and to check whether the approach is feasible to detect it;
2. to investigate whether the bottleneck also occurs when shifting the dysfunctions to a process consisting of two process groups as done in scenario 2;
3. to investigate the impact of dysfunctions being equally distributed over the last two steps of the process chain, which only consist of two process group objects, as done in scenario 3.

## Results

The mathematical approach has been implemented as a Python script and has been applied to the previously described scenarios to prove its capability for impact forecasting.

Table 5.6 shows the results on the process group level for all four scenarios, i.e., the mean group waiting times and their corresponding standard deviations  $\mathbf{w}_{group} \pm \Delta\mathbf{w}_{group}$ , additional waiting time per group  $\mathbf{w}_{add,group}$  and the total group waiting time with standard deviation  $\mathbf{w}_{total,group} \pm \Delta\mathbf{w}_{total,group}$  in minutes. In full operating state (initial state) the mean check-in times are  $6.9 \pm 1.5$  min and  $7.1 \pm 0.7$  min at check-in group 1 and 2, respectively. The security check is considered to be the most time-consuming processing step with mean waiting times of  $11.4 \pm 2.3$  min. Manual passport control is assumed to be more laborious with a mean waiting time of  $9.5 \pm 2.8$  min compared to the automated passport control with a waiting duration of  $2.7 \pm 0.2$  min. The shortest waiting times are assumed to occur at the boarding pass controls with mean waiting times of  $1.3 \pm 0.1$  min for BPC 1 and  $2.0 \pm 0.0$  min for BPC 2.

The dysfunction of one check-in counter at CI 1 and CI 2 each and three security checks leads to an increase of waiting times in case of scenario 1 mainly focused on the security checks. While mean waiting times at CI 1 and CI 2 increase to values of  $8.6 \pm 1.6$  min and  $8.8 \pm 0.7$  min, the waiting time at the security check is prolonged by 34.2 min to a total waiting time of  $45.6 \pm 0.0$  min.

In case of two non-operating check-in counters within CI 1 and CI 2 each and one dysfunctional automated passport control as described in scenario 2 the average waiting times

Table 5.5: Waiting time matrix  $\mathbf{P}_W$  in minutes (for better readability in transposed form):

|        | Check-In 1 | Check-In 2 | Security Control | Passport Control (PC) | Automated PC | Boarding Pass Control 1 | Boarding Pass Control 2 |
|--------|------------|------------|------------------|-----------------------|--------------|-------------------------|-------------------------|
| CI1-1  | 9.2        | 0          | 0                | 0                     | 0            | 0                       | 0                       |
| CI1-2  | 5.9        | 0          | 0                | 0                     | 0            | 0                       | 0                       |
| CI1-3  | 6.0        | 0          | 0                | 0                     | 0            | 0                       | 0                       |
| CI1-4  | 5.2        | 0          | 0                | 0                     | 0            | 0                       | 0                       |
| CI1-5  | 8.1        | 0          | 0                | 0                     | 0            | 0                       | 0                       |
| CI2-1  | 0          | 6.0        | 0                | 0                     | 0            | 0                       | 0                       |
| CI2-2  | 0          | 8.1        | 0                | 0                     | 0            | 0                       | 0                       |
| CI2-3  | 0          | 6.8        | 0                | 0                     | 0            | 0                       | 0                       |
| CI2-4  | 0          | 7.4        | 0                | 0                     | 0            | 0                       | 0                       |
| CI2-5  | 0          | 7.1        | 0                | 0                     | 0            | 0                       | 0                       |
| SC1    | 0          | 0          | 14.7             | 0                     | 0            | 0                       | 0                       |
| SC2    | 0          | 0          | 8.1              | 0                     | 0            | 0                       | 0                       |
| SC3    | 0          | 0          | 11.4             | 0                     | 0            | 0                       | 0                       |
| SC4    | 0          | 0          | 11.3             | 0                     | 0            | 0                       | 0                       |
| PC1    | 0          | 0          | 0                | 12.3                  | 0            | 0                       | 0                       |
| PC2    | 0          | 0          | 0                | 6.8                   | 0            | 0                       | 0                       |
| APC1   | 0          | 0          | 0                | 0                     | 2.9          | 0                       | 0                       |
| APC2   | 0          | 0          | 0                | 0                     | 2.6          | 0                       | 0                       |
| BPC1-1 | 0          | 0          | 0                | 0                     | 0            | 1.3                     | 0                       |
| BPC1-2 | 0          | 0          | 0                | 0                     | 0            | 1.4                     | 0                       |
| BPC2-1 | 0          | 0          | 0                | 0                     | 0            | 0                       | 2                       |
| BPC2-2 | 0          | 0          | 0                | 0                     | 0            | 0                       | 2                       |

Table 5.6: Results for all scenarios in minutes:

|               |                          | CI 1      | CI 2      | SC        | PC        | APC       | BPC 1     | BPC 2     |
|---------------|--------------------------|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| Initial State | $w_{group}$              | 6.9       | 7.1       | 11.4      | 9.5       | 2.7       | 1.3       | 2.0       |
|               | $\Delta w_{group}$       | $\pm 1.5$ | $\pm 0.7$ | $\pm 2.3$ | $\pm 2.8$ | $\pm 0.2$ | $\pm 0.1$ | $\pm 0.0$ |
|               | $w_{add,group}$          | 0.0       | 0.0       | 0.0       | 0.0       | 0.0       | 0.0       | 0.0       |
|               | $w_{total,group}$        | 6.9       | 7.1       | 11.4      | 9.5       | 2.7       | 1.3       | 2.0       |
|               | $\Delta w_{total,group}$ | $\pm 1.5$ | $\pm 0.7$ | $\pm 2.3$ | $\pm 2.8$ | $\pm 0.2$ | $\pm 0.1$ | $\pm 0.0$ |
| Scenario 1    | $w_{group}$              | 7.1       | 7.0       | 11.4      | 9.5       | 2.7       | 1.3       | 2.0       |
|               | $\Delta w_{group}$       | $\pm 1.6$ | $\pm 0.7$ | $\pm 0.0$ | $\pm 2.8$ | $\pm 0.2$ | $\pm 0.1$ | $\pm 0.0$ |
|               | $w_{add,group}$          | 1.5       | 1.8       | 34.1      | 0.0       | 0.0       | 0.0       | 0.0       |
|               | $w_{total,group}$        | 8.6       | 8.8       | 45.6      | 9.5       | 2.7       | 1.3       | 2.0       |
|               | $\Delta w_{total,group}$ | $\pm 1.6$ | $\pm 0.7$ | $\pm 0.0$ | $\pm 2.8$ | $\pm 0.2$ | $\pm 0.1$ | $\pm 0.0$ |
| Scenario 2    | $w_{group}$              | 6.8       | 7.1       | 11.4      | 9.5       | 2.6       | 1.3       | 2.0       |
|               | $\Delta w_{group}$       | $\pm 1.7$ | $\pm 0.8$ | $\pm 2.3$ | $\pm 2.8$ | $\pm 0.0$ | $\pm 0.1$ | $\pm 0.0$ |
|               | $w_{add,group}$          | 4.7       | 4.7       | 0.0       | 0.0       | 2.9       | 0.0       | 0.0       |
|               | $w_{total,group}$        | 11.5      | 11.8      | 11.4      | 9.5       | 5.5       | 1.3       | 2.0       |
|               | $\Delta w_{total,group}$ | $\pm 1.7$ | $\pm 0.8$ | $\pm 2.3$ | $\pm 2.8$ | $\pm 2.2$ | $\pm 0.1$ | $\pm 0.0$ |
| Scenario 3    | $w_{group}$              | 7.1       | 7.1       | 11.4      | 12.3      | 2.6       | 1.4       | 2.0       |
|               | $\Delta w_{group}$       | $\pm 1.6$ | $\pm 0.7$ | $\pm 2.3$ | $\pm 0.0$ | $\pm 0.0$ | $\pm 0.0$ | $\pm 0.0$ |
|               | $w_{add,group}$          | 1.5       | 0.0       | 0.0       | 6.8       | 2.9       | 1.3       | 2.0       |
|               | $w_{total,group}$        | 8.6       | 7.1       | 11.4      | 19.1      | 5.5       | 2.7       | 4.0       |
|               | $\Delta w_{total,group}$ | $\pm 1.6$ | $\pm 0.7$ | $\pm 2.3$ | $\pm 0.0$ | $\pm 0.0$ | $\pm 0.0$ | $\pm 0.0$ |

Table 5.7: Results for all scenarios with respect to processes in minutes:

|               |                                    | Check-In  | Security Check | Passport Control | Boarding Pass Control | Total processing time |
|---------------|------------------------------------|-----------|----------------|------------------|-----------------------|-----------------------|
| Initial State | $\bar{\mathbf{w}}_{process}$       | 7.0       | 11.4           | 6.1              | 1.7                   | 26.2                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.4$        | $\pm 0.2$             | $\pm 2.4$             |
|               | $\mathbf{w}_{add,process}$         | 0.0       | 0.0            | 0.0              | 0.0                   | increase              |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.0$ | $\pm 0.0$      | $\pm 0.0$        | $\pm 0.0$             | by                    |
|               | $\mathbf{w}_{total,process}$       | 7.0       | 11.4           | 6.2              | 1.6                   | —                     |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.4$        | $\pm 0.2$             |                       |
| Scenario 1    | $\bar{\mathbf{w}}_{process}$       | 7.1       | 11.4           | 6.1              | 1.7                   | 62.1                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.4$        | $\pm 0.2$             | $\pm 2.4$             |
|               | $\mathbf{w}_{add,process}$         | 1.7       | 34.2           | 0.0              | 0.0                   | increase              |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.1$ | $\pm 0.0$      | $\pm 0.0$        | $\pm 0.0$             | by                    |
|               | $\mathbf{w}_{total,process}$       | 8.7       | 45.6           | 6.1              | 1.7                   | 137.2 %               |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.4$        | $\pm 0.2$             |                       |
| Scenario 2    | $\bar{\mathbf{w}}_{process}$       | 6.9       | 11.4           | 6.1              | 1.7                   | 32.2                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.5$        | $\pm 0.2$             | $\pm 2.7$             |
|               | $\mathbf{w}_{add,process}$         | 4.7       | 0.0            | 1.5              | 0.0                   | increase              |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.0$ | $\pm 0.0$      | $\pm 1.0$        | $\pm 0.0$             | by                    |
|               | $\mathbf{w}_{total,process}$       | 11.6      | 11.4           | 7.5              | 1.7                   | 23.0 %                |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 0.1$ | $\pm 0.0$      | $\pm 2.7$        | $\pm 0.2$             |                       |
| Scenario 3    | $\bar{\mathbf{w}}_{process}$       | 7.1       | 11.4           | 7.4              | 1.7                   | 34.8                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 0.0$ | $\pm 0.0$      | $\pm 3.5$        | $\pm 0.2$             | $\pm 3.8$             |
|               | $\mathbf{w}_{add,process}$         | 0.7       | 0.0            | 4.8              | 1.6                   | increase              |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.5$ | $\pm 0.0$      | $\pm 1.5$        | $\pm 0.3$             | by                    |
|               | $\mathbf{w}_{total,process}$       | 7.8       | 11.4           | 12.3             | 3.3                   | 33.1 %                |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 0.5$ | $\pm 0.0$      | $\pm 3.7$        | $\pm 0.3$             |                       |

at check-in groups CI 1 and CI 2 increase to  $11.5 \pm 1.7$  min and  $12.8 \pm 0.8$  min, while the waiting time at the automated passport control is prolonged to  $5.5 \pm 0.0$  min.

The failure of CI1-2 during scenario 3 causes an extension of the waiting time to  $8.6 \pm 1.6$  min at CI 1. However, the dysfunction of a manual passport control leads to the largest increase in waiting time of 6.8 min yielding a total group waiting time of  $19.1 \pm 0.0$  min for PC. Furthermore, APC, BPC 1 and BPC 2 are delayed by 2.9 min, 1.3 min, 2.0 min resulting in waiting times of  $5.5 \pm 0.0$  min,  $2.7 \pm 0.0$  min and  $4.0 \pm 0.0$  min, respectively.

The results with combined process groups are shown in Table 5.7 for all scenarios. In addition, the cumulative processing time  $\mathbf{w}_{total,process} \pm \Delta\mathbf{w}_{total,process}$  is listed in the last column together with a relative increase in waiting time compared to the initial state (scenario working).

Under full operation conditions the waiting times of  $7.0 \pm 0.1$  min for the check-in process,  $11.4 \pm 0.0$  min at the security checks,  $6.2 \pm 2.4$  min at the passport control and  $1.6 \pm$

0.2 min at the boarding pass control sum up to a total processing time of  $26.2 \pm 2.4$  min. The standard deviation of 2.4 min at the passport controls reflects the large difference between the waiting times at the manual and the automated passport control points, while the low standard deviations of 0.1 min and 0.2 min at the check-in and boarding pass control show the equal distribution of waiting times that have been chosen for the setup.

The exaggerated bottleneck effect, induced for scenario 1, becomes clearly visible by the additional waiting time of  $34.2 \pm 0.0$  min at the security check, while the dysfunction of one check-in counter at CI 1 and CI 2 each results in only  $1.7 \pm 0.1$  min additional time for the check-in process. These effects accumulate to a total processing time of  $62.1 \pm 2.4$  min, which corresponds to a percentage increase of 137.2%.

The focus on dysfunctions of the check-in process in case of scenario 2 results in an increase of  $4.7 \pm 0.0$  min, whereas the failure of an automated passport control leads to a gain of waiting time by  $1.5 \pm 1.0$  min. This yields a total processing time of  $32.2 \pm 2.7$  min under the conditions given in scenario 2, which is equivalent to a percentage increase by 23.0% with respect to the initial state.

In case of a distributed set of device failures as given by scenario 3 waiting times are prolonged by  $0.7 \pm 0.5$  min,  $4.8 \pm 1.5$  min and  $1.6 \pm 0.3$  min for the processes of check-in, passport control and boarding pass control, respectively. Therefore, the total processing time is enhanced by 33.1% to an absolute value of  $34.8 \pm 3.8$  min.

The three scenarios deviating from the initial state have been chosen to represent a bottleneck at the security checks (scenario 1), a focus on the check-in process (scenario 2) and a distributed failure of devices at passport and boarding pass controls (scenario3). The increase in total processing time of 137.2% with respect to the initial conditions clearly shows the bottleneck role of the security checks and would in reality highly impact airport operation, as prolonged processing times will either cause flight delays or passengers will miss their flights. The focus on dysfunctions at the check-in counters leads to an increase of 23.0%, which is the lowest of all three constellations. Thus, considering redundancy, the check-in seems to be most redundant. However, the increase of 33.1% in case of scenario 3 is still acceptable. Furthermore, the results of scenario 2 and 3 are linked to higher standard deviations, which coincides with the observation made while analyzing the process groups by itself: higher number of process capacities as well as process groups per process go hand in hand with higher standard deviations. However, the standard deviations have to be interpreted carefully as they are highly influenced by the choice of waiting times at the process group objects.

Regarding possible skipping of processes, a different setup using the process sequence matrix in Table A.1 is constructed, while keeping waiting times and scenarios given above. However, it is assumed that 20% of the passengers have already checked-in online before arriving at the airport. Furthermore, 75% are considered domestic flights (or flights within the Schengen zone), i.e., they do not have to undergo a passport control. The results show that the bottleneck for scenario 2 persists (increase of 177.4% of total processing time),

whereas some passengers skipping the passport control and check-in counters suppress the effect in scenarios 3 and 4 with an increase of 20.6 % and 18.5 % in total processing time, respectively. Further details of the results underlining this are given in Table A.2.

The previously explained approach is a simple and fast way to estimate the impact occurring from lost resources, reaching from partial failures within the infrastructure or limited availability of personnel. Therefore, it allows quick decision support while dealing with crisis situations or optimizing airport business operation. With the chosen scenarios it has been proven that the method is capable to detect bottlenecks within the process chain (scenario 1) as well as underlining the redundancy of process groups through multiple counters (scenario 2). For analysis/optimization purposes and to provide these to the passengers modern airports measure/estimate waiting time data (e.g., Frankfurt Airport<sup>3</sup>). Thus, the current waiting times as well as the available/active resources are available as an input for the proposed approach.

### 5.3.1.1 Emergency Planning Options

Referring back to the times  $t_1$  or  $t_2$  in Figure 5.11, i.e., at the time of the disruptive event or the partial restoration, airport operators are able to determine the impact of the situation. In situations, where load shedding is needed the operator can specifically search for the resources having the least impact on the total process time. Therefore, knowing the number of objects that have to be set out of order, regardless of the reason, a state vector (see Eq. 5.2) can be generated by setting a number of entries corresponding to the number of objects out of order to zero. As the number of possible state vectors is finite, iterating over the combinations and calculating the increase in total processing time, a minimization problem can be deduced. Solving this minimization problem allows to find the combination that leads to the lowest increase in total processing time and suggest it to the operator.

However, in case of load shedding, starting and disabling devices is stressing the grid. To avoid this, the number of objects out of order should be set to one, while repeating the minimization and using the resulting state vector as input for the next step in the loop. Repeating this leads to a suggested load shedding plan, based on the minimized loss of the next load. In Table 5.8 the resulting plans for the previously used scenario setup from Figure 5.12 are shown. Although the outcome is quite similar for a low number of dysfunctional objects, the differences become clearly visible in cases with 5 or even 10 dysfunctional devices.

Figure 5.13 shows the increase in total waiting time that results from the deactivation of the devices according to the previously calculated emergency plan. The blue line refers to the plan derived from the load shedding algorithm and the orange line from the optimization approach. Starting from  $w_{total} = 26.2$  min in the initial state, the total waiting time increases slowly for the first two iterations reaching 28.6 min and 27.7 min following the

<sup>3</sup><https://www.frankfurt-airport.com/wartezeiten/public?lang=en>

Table 5.8: Optimization Results for  $n$  shed devices with and without load shedding mode:

| Mode                  | Load Shedding   |                                            |                                                                                       | No Load Shedding |                                            |                                                                                        |
|-----------------------|-----------------|--------------------------------------------|---------------------------------------------------------------------------------------|------------------|--------------------------------------------|----------------------------------------------------------------------------------------|
| Dysfunctional devices | $n = 2$         | $n = 5$                                    | $n = 10$                                                                              | $n = 2$          | $n = 5$                                    | $n = 10$                                                                               |
| List of devices       | BPC1-1<br>CI1-4 | BPC1-1<br>CI1-4<br>CI2-1<br>BPC2-1<br>APC2 | BPC1-1<br>CI1-4<br>CI2-1<br>BPC2-1<br>APC2<br>CI1-2<br>CI2-5<br>SC-1<br>PC-2<br>CI1-3 | BPC1-1<br>CI1-4  | CI1-2<br>CI2-1<br>APC2<br>BPC1-1<br>BPC2-1 | CI1-2<br>CI1-3<br>CI1-5<br>CI2-1<br>CI2-4<br>CI2-5<br>SC-1<br>APC2<br>BPC1-1<br>BPC2-1 |

Table 5.9: Number of combinations dependent with increasing number of dysfunctional devices for a system of 22 devices:

| number devices | 1  | 2   | 3   | 4     | 6      | 8       | 10        |
|----------------|----|-----|-----|-------|--------|---------|-----------|
| load shedding  | 22 | 43  | 63  | 82    | 117    | 148     | 175       |
| optimization   | 22 | 220 | 253 | 1.793 | 35.442 | 600.369 | 1.744.435 |

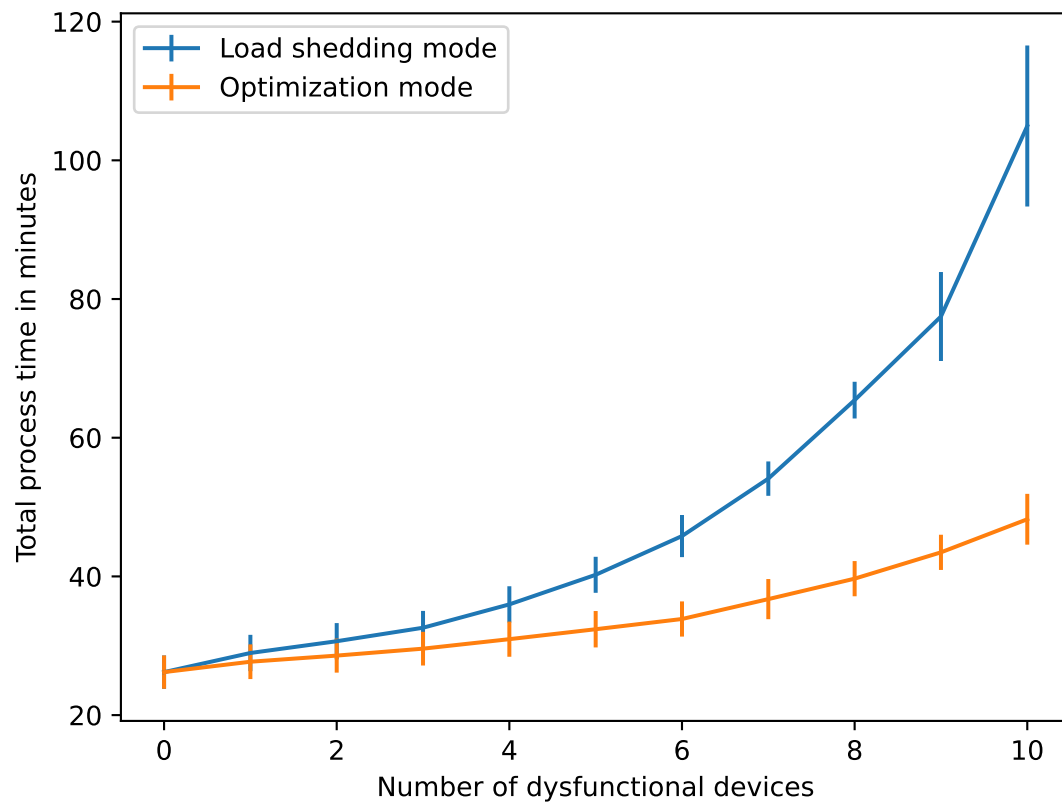
order provided by the load shedding and optimization algorithm, respectively. For the next iterations the difference between the modes increases further ending in a total difference of around 56.7 min, showing that solving the optimization problem gains much better results with respect to passenger processing.

However, the better results are tied to higher computational costs. In Table 5.9 the number of combinations that need to be evaluated to solve the optimization problem for the test system of 22 devices are given. Even for the small test system used here the optimization algorithm is not feasible for fast-paced decision making, which is essential in the case of a power shortage. Though, parallelization and implementation optimization, e.g., using a faster programming language for implementation, such as C++, might improve the situation, the scalability to large systems would be sufficient as the complexity of the algorithm scales with the number of nodes according to Eq. 5.23, with  $n$  being the number of total devices in the system and  $r$  the maximum number of dysfunctional devices.

$$N_{combinations} = \sum_{i=1}^r \frac{n!}{(n-i)!i!} \quad (5.23)$$

Summarizing, in this subsection a static impact estimation algorithm was introduced, that is capable to calculate the impact of single or multiple device dysfunctions based on the given waiting time and a redistribution on other stations within the same process group. The approach supports the airport operator during fast-paced decision making as it enables

Figure 5.13: Increase in total waiting time calculated considering load-shedding (blue) and optimization mode (orange)



to use the current waiting times as input and forecast the impact of the loads he or she has chosen for load shedding or saving resources. Enhancing this to an optimization problem that minimizes the impact of one or multiple dysfunctional devices, allows suggesting decisions or even setting up emergency plans. However, finding the optimal configuration in large systems might be an issue. This and the fact that fast changes in the grid (either switching on or off devices) may cause instabilities, iterating the algorithm step by step can be done to create a load shedding plan. This allows fast calculation and prevents multiple devices switching on/off during one step. However, the discrepancy in the increase of the resulting total waiting time, leads to the conclusion that both modes have their own purpose and application:

- Load-Shedding control - During instable grid situations the load-shedding algorithm can be used to create a list of loads that are the best choice based on the current real waiting time data. This application seems reasonable as the load shedding is intended to absorb small amounts of stress on the power grid, i.e., the number of shed loads should be low. The algorithm could be deployed in form of an automated control loop initiated inside the system.
- Resource management and optimization - The optimization algorithm is able to forecast prolonged waiting times of passengers based on saved resources. Thus, if the airport operator accepts a certain amount of additional time, i.e., a slight decrease of comfort for the passenger, the algorithm helps to select the resources that are expendable under a given threshold.

### 5.3.2 Impact Estimation using a Microscopic Agent-based Simulation Model<sup>4</sup>

The static impact algorithm introduced in Subsection 5.3.1 can be considered as a powerful support tool for decision makers. However, system dynamics (in form of time dependencies) are completely neglected and single passenger behavior cannot be taken into account. In the domain of pedestrian flow simulations, these models are referred to as microscopic models (Kneidl, 2013; Schultz, 2010). Therefore, in this subsection an agent-based microscopic simulation model is introduced, which allows to include individual passenger behavior and properties, such as

- individual arrival time at the airport,
- modes of transportation for arrival,
- travel information about destination in form of airline and flight number,
- traveling with or without luggage,

<sup>4</sup>Parts of this subsection are reprinted with permission from Brause et al. (2020) published in SpringerOpen under the CC BY 4.0.

- use of online check-in capabilities,
- and individual movement speed within the airport.

Furthermore, the model enables to incorporate information about airport operation, such as

- airport geometry,
- flight plans,
- individual processing times at each processing step,
- available resources in form of process capacities.

To incorporate these information in the impact estimation and make it as adaptive as possible, a model of a generic medium-sized commercial airport was developed, which is based on components of real airports. The advantage of a generic model is the flexibility, i.e., the results can be transferred to all medium sized airports. Furthermore, customization of the airport parameters allows a transfer of the model to smaller and larger airports. Because of the amount of data open to the public, these components were taken from Cologne-Bonn Airport and are based on public information. Due to the international standards for airport operations, e.g., those set by the ICAO Annex 9 (International Civil Aviation Organization, 2022) or the European Commission (European Commission, 2015), it can be assumed that the data is transferable to other medium sized airports. The passengers are modeled individually, but their behavior is subject to statistical distribution functions regarding baggage claim or check-in at the airport terminal. Interactions between passengers are only partially taken into account, i.e., at the process stations only one passenger can be handled at a time and the passengers have to wait in queues for a free service station. However, passenger interactions between the process stations are neglected due to the assumption, that the dimension of the terminal is sufficient to avoid passenger congestion (Brause et al., 2020).

#### **5.3.2.1 Model Description, Implementation and Input Data**

In the following, a detailed description of the simulation logic behind the microscopic agent-based impact estimation is given, as well as its implementation using a java-based simulation framework. Furthermore, the input data is described that is used to model the airport processes and passenger behavior based on available operational data at the example of a medium-sized airport.

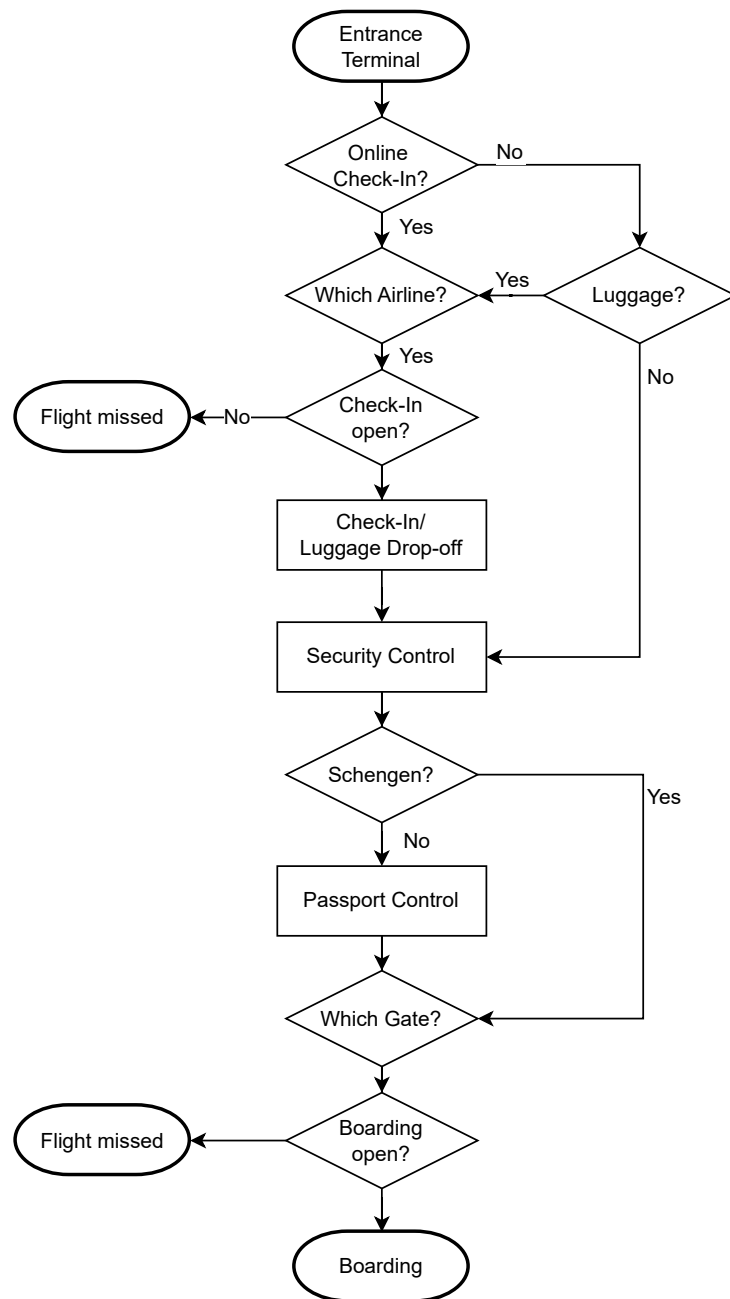


Figure 5.14: Simulation logic for the departure process with ellipses as source/sinks, diamonds as decision spots, and rectangles depicting processes after Brause et al. (2020).

## **Simulation Logic**

Figure 5.14 illustrates the simulation logic of the model, which outlines the process for passenger arrival and processing through the terminal. Upon arrival, passengers are generated according to their scheduled flight time at the airport. Those who have not checked in online or need to check-in their baggage proceed to the designated check-in counters. The number of available counters is determined by the airline's capacity, i.e., the process capacity of the process group the airline is assigned to. However, within this model, automatic check-in is not considered an option, because it is not provided at all airports or offered by all airlines, so it has been omitted.

Passengers who have already checked in prior to their arrival or are arriving from outside the terminal do not exhibit different behavior and are thus integrated into the existing process. Furthermore, the model assumes that baggage can only be checked-in at designated check-in counters, simplifying the situation by neglecting separate counters for luggage or vending machines. The check-in counters open 2 hours before departure (Reisen-Experten.de, 2022) and close 30 minutes prior to takeoff. Passengers arriving after this window miss their flight and are removed from the simulation immediately.

The model features a centralized security checkpoint with multiple screening lanes, which all passengers must pass through independently of their flight. Each control lane allows four passengers to deposit and pick up their personal belongings simultaneously, while only one individual can undergo screening at any given time. Depending on whether the passenger is traveling within or outside the Schengen area, they will need to present their passport before proceeding to their gate.

Boarding commences 60 minutes prior to departure and concludes 20 minutes before take-off (KLM Royal Dutch Airlines, 2024; Iberia, 2024). If there are still passengers in line for boarding when this time arrives, the boarding desk remains open until all passengers have cleared the queue. Passengers arriving at the gate after the boarding window has closed will be removed from the simulation.

## **Implementation**

The model was implemented using the AnyLogic simulation software (The AnyLogic Company, 2024), a commercial, java-based platform that offers various libraries and function blocks for customization via Java code. In this instance, the Process Modeling Library is utilized to create a flowchart representation of the airport's model. In contrast to the Pedestrian Library, the Process Modeling Library enables us to neglect passenger interaction during processes to make the model less dependent on the accurate geometry and therefore better transferable to other airports. The characteristics and behaviors of passengers are defined through a database, which serves as a central repository for storing and retrieving information.

The simulation begins with the generation of passengers at the terminal entrance, where their arrival times are determined according to the data stored in the database. Sink blocks are employed throughout the simulation whenever passengers are removed due to various reasons, such as arriving too late for check-in or boarding, or being already processed through the boarding process.

Check-in, security check, passport control, and boarding are implemented as separate service stations, each with customizable durations and available capacity. The passenger processing system is modeled as a single queue multiple server (SQMS) system, where only one passenger can be served at a time, and others must wait in line for an open service station. Priority is determined by the first-in-first-out principle, in analogy to the static approach introduced in Section 5.3.1. To accommodate the diverse number of airlines present at medium-sized airports, three separate groups based on the number of passengers served on a reference day are established. Airlines are assigned to these groups solely on the basis of passenger numbers, disregarding their type or other attributes. This categorization ensures that passengers arriving before check-in counters open will encounter waiting loops, where they periodically monitor the status of available counters. Upon discovering an open counter, they exit the loop and join the queue for processing. Conversely, passengers arriving after check-in counters have closed are removed from the simulation by a sink block and counted as passengers who missed their flight. The boarding process is implemented individually for each flight at separate boarding counters, mirroring the procedure used for check-in in terms of queues and delayed passengers.

To segment passengers according to specific criteria defined within the database, such as Schengen vs. non-Schengen travelers, select output blocks are utilized. Visual representations are employed in Figure 5.14: sink and source blocks are depicted by ellipses, service stations by rectangles, and selectOutput devices by diamonds. A more detailed explanation and depiction is given in the Appendix (Section A.4).

### **Input Data**

Due to the limitations in publicly available data and airport privacy policies, precise measurement data from airports are not available. Instead, data has been obtained from literature references, which provide a valuable foundation for the analysis. However, it is worth noting that airports may use real-world data to conduct studies using the here described methodology.

In the following, input data is categorized into two types: fixed and process parameters. The fixed input parameters represent the inherent characteristics of the airport environment, which are relatively stable and difficult to change, e.g., the underlying geometry. In contrast, the process parameters indicate the specific details that can be adjusted or optimized within the model. These parameters include the number of service stations at each passenger handling process, which enables to simulate various scenarios and evaluate their

impact on the overall performance of the airport or even change the process capacities over time.

To inform the simulation, a flight plan that outlines departure and arrival times for aircraft at the airport is obtained. The flight plan is based on the Cologne-Bonn Airport schedule dated November 19, 2018, which was randomly selected due to the lack of publicly available data for peak days. The flight plan includes essential information such as flight number, destination (IATA code), departure time, operating airline (ICAO code), and aircraft type. The maximum number of seats available on each flight is determined by the aircraft's configuration and type, which can be obtained through public information provided by the airlines. In this study, it is assumed that flights are not typically fully booked, with an average seat load factor (SLF) of 77.6% in Germany in 2017 (DFS, 2017). This value serves as a basis for generating passenger numbers for each flight, ultimately resulting in a total of 16,136 passengers across 123 flights operated by 17 airlines. Approximately 25% of these passengers are non-Schengen travelers. The complete flight plan including the assumed number of occupied seats for each flight is given in the appendix (see Table A.3).

To obtain representative results, it is essential to determine when passengers arrive at the airport and the time available for completing departure processes. A study by Schultz (Schultz, 2010) conducted at Stuttgart Airport found that the arrival distribution of passengers can be approximated using a normal or Simpson distribution. The measurements also showed that a Weibull-Distribution would be better suited to distinguish between passenger groups, e.g., tourists and business travelers, as it is more flexible regarding its shape. This would be essential to generate a highly accurate model of a specific airport. However, within this work passengers are estimated to be a homogeneous group to have better transferability between airports. Thus, a normal distribution with an expected value of 89 minutes before departure and a standard deviation of 26 minutes is used. The probability density function of a normal distribution in parameterized form is given by Equation 5.24 with  $\mu$  being the mean and  $\sigma$  the standard deviation.

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\left(\frac{x-\mu}{\sigma}\right)^2} \quad (5.24)$$

The mode of transportation used to travel to the airport also influences whether passengers arrive alone or in groups. Passengers traveling by car typically arrive individually or in small groups, while those using public transport arrive with a group of fellow travelers. According to the Arbeitsgemeinschaft Deutscher Verkehrsflughäfen (ADV), approximately 64% of passengers use cars, taxis, or rental cars to reach the airport, whereas 36% opt for public transportation like trains or buses (ADV, 2018). The arrival time at the airport can be determined by leveraging the arrival distribution, information about transport media usage, and flight departure times. A Flight Generator developed by the DLR is employed to calculate the arrival time for each passenger based on pseudorandom numbers within specified parameters (arrival distribution, departure time, and transport medium). To analyze the impact of random numbers on results, five different databases with arrival times were generated. Each database is based on the three aforementioned specifications. Figure 5.15

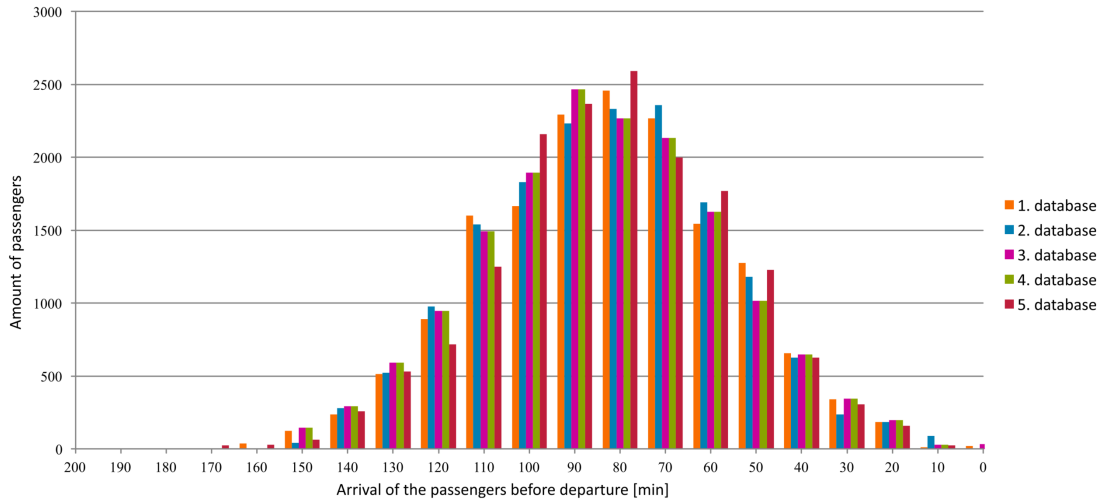


Figure 5.15: Number of passengers arriving before departure accumulated over 10 minutes according to the five generated databases. Input for the generation is a mean of 89 min before departure with a standard deviation of 26 min (Brause et al., 2020).

presents the cumulative arrival times of passengers before departure for the five databases. The x-axis represents the time elapsed before departure, while the y-axis denotes the number of passengers. The bars indicate the cumulative number of passengers arriving at the airport over 10-minute intervals. Differing colors represent the results from each database.

The analysis reveals that the arrival times across the five databases exhibit minimal variations. The distributions conform to a normal distribution (as described in Equation 5.24) and, as expected, the mean arrival time before departure lies between 80 and 90 minutes. Notably, fewer than 150-170 minutes elapse before departure, and no passengers arrive more than 10 minutes prior to departure. The results indicate that approximately 11% of passengers (with a standard deviation of 0.9%) arrive at the airport more than two hours before departure, while about 14% (with a standard deviation of 0.6%) arrive less than one hour before departure, and only about 2% (with a standard deviation of 0.2%) arrive within 30 minutes before departure.

If these passengers still need to undergo the check-in process, they face a significant challenge in reaching their flight, as check-in counters typically close between 30 and 60 minutes before departure, depending on the airline, destination, and other factors. Moreover, boarding often takes place about 20-30 minutes before departure (Asam, 2018).

Passengers who fail to board their flight despite having booked a ticket are referred to as no-shows. There are two primary reasons for no-shows: Firstly, some passengers opt for flexible tickets, which allow them to book and cancel flights without incurring additional costs. This flexibility can sometimes lead to missed connections. Secondly, some passengers arrive at the airport excessively late due to factors such as traffic congestion or public transport delays. This tardiness can result in missed flights.

The percentage of no-shows varies significantly among airlines and routes (Lawrence et al., 2003). Within this model, the no-show rate is represented by passengers who arrive so late that the check-in or boarding service stations have already closed, causing them to miss their flight. The estimated no-show rate for this model is approximately 2%.

In addition to variations in passenger arrival times, other characteristics of passengers are relevant for efficient handling at the airport. For instance, it's essential to distinguish between passengers who have checked-in online beforehand and those who need to check-in at the airport counter. Furthermore, some passengers travel with only hand luggage, while others require baggage check-in. To better understand these factors, existing studies are referred to. According to a study by SITA (Eiselin, 2018), 39% of passengers use online check-in, while 61% still check-in at the airport counters. When it comes to baggage check-in, there is a significant difference between flights within and outside Europe. Many airlines include baggage in the fares for international flights, which means it may be assumed that all passengers with destinations outside Europe will be traveling with checked baggage. In contrast, Ryanair found that only 20% of passengers flying within Europe carry checked baggage (dpa, 2018). The varying passenger characteristics are summarized in Table 5.10. To incorporate these factors into the model, random distribution methods based on the given percentages are used. The Mersenne Twister algorithm (MT 19937) is utilized to generate random numbers for each passenger. By using five different databases, as previously mentioned, the aim is to verify that any changes in output parameters are indeed due to variations in process parameters rather than random fluctuations within fixed input parameters.

The processing time at various airport process stations is influenced by factors such as the previously described passenger characteristics, equipment availability, and personnel working methods. As a result, processing times are prone to fluctuations. According to Schultz' study at Stuttgart Airport (Schultz, 2010), the duration of check-in processes (with or without baggage check-in) follows a normal distribution with an expected value of 58 seconds and a standard deviation of 25 seconds.

The security control process is divided into three distinct sub-processes: disposal of personal belongings, security screening of individuals and their hand luggage, and reception of personal belongings. These times are based on measurements taken at Hamburg Airport as part of the Critical Parts project (Deutschmann et al., 2011). The time for depositing personal belongings falls within a range of 0 to 81 seconds, with a mode of 21 seconds. This variability is attributed to the triangular distribution given by the probability density function from Equation 5.25. The security check involves passing through a metal detector or body scanner, followed by a post-control procedure executed by security personnel if necessary. The processing time for this step varies between 2 and 169 seconds, with a mode of 43 seconds. The subsequent reception of personal belongings and, if required, a baggage inspection, takes place within a specified time frame ranging from 0 to 260 seconds. Notably, the mode for this process is 22 seconds.

$$p(x) = \begin{cases} \frac{2(x-a)}{(b-a)(c-a)} & \text{for } x \in [a, c] \\ \frac{2(b-c)}{(b-a)(b-c)} & \text{for } x \in [c, b] \\ 0 & \text{else} \end{cases} \quad (5.25)$$

In contrast, passport control exhibits uniform distribution characteristics, with an expected processing time between 50 and 60 seconds (Kachlíková, 2011). The probability density function of this uniform distribution is described in Equation 5.26.

$$p(x) = \begin{cases} \frac{1}{(b-a)} & \text{for } a \leq x \leq b \\ 0 & \text{else} \end{cases} \quad (5.26)$$

The boarding process duration follows a normal distribution with an expected value of 5 seconds and a standard deviation of 2 seconds (cf. equation 5.24). A detailed overview of the parameters used to calculate the process times can be found in Table 5.10.

The time passengers need to cover distances ( $t$ ) are calculated with the formula for uniform movement, which depends on the distance between process stations in meters and the individual velocity of the passenger. The speed of movement varies according to a probability distribution, taking into account individual differences among people. Moreover, the distances between process stations are not constant due to factors such as varying entrance locations within the terminal or gate assignments for boarding. As a result, the time passengers need to spend between process stations is not fixed and depends on several variables, including the uncertainty associated with the distance that must be covered and the differences in the individual walking speeds. To account for these uncertainties, Gaussian error propagation is used. This enables to calculate the travel times and their standard deviation using Equation 5.27.

$$t = \frac{s}{v}, \quad dt \sqrt{\left(\frac{1}{v}\right)^2 ds^2 + \left(\frac{s}{v^2} dv\right)^2} \quad (5.27)$$

According to Weidmann from ETH Zurich, the average speed of human movement is 1.34 m/s spanning from 0.97 m/s to 1.65 m/s throughout literature (Weidmann, Ulrich, 1992). Later in his work, he states that single pedestrian movement can be modeled using a mean velocity of 1.34 m/s and a standard deviation of 0.26 m/s (Weidmann, Ulrich, 1992). The distances between process stations in this model are determined by the airport's structure and size. The distance between process stations varies significantly depending on the airport's structure and size. In this model, the distances are based on the structure of the airport Cologne-Bonn and have been measured using Google Maps. An overview of the distances between the process stations and the resulting times is shown in 5.10. Appropriate data for other airports can be calculated the same way with adjusted distances. A detailed overview of these distances is presented in Table 5.10. To accommodate different airports, it is possible to recalculate distances using adjusted values, ensuring that the model remains applicable for other airport configurations.

Table 5.10: Overview of the input parameters used to generate the properties of each passenger generated for the simulation as well as to calculate the processing times:

|                                    | Description                                               | Input Values                                                    | Used in Equation |
|------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------|------------------|
| Passenger characteristics          | Arrival distribution of the passenger at the airport      | $\mu = 89 \text{ min}$ ,<br>$\sigma = 26 \text{ min}$           | Eq. 5.24         |
|                                    | Transportation mode (own car / public transport)          | 64 %/ 36 %                                                      | -                |
|                                    | Online check-in / counter check-in                        | 39 %, 61 %                                                      | -                |
|                                    | Baggage check-in within EU                                | 20 %                                                            | -                |
|                                    | Baggage check-in outside EU                               | 100 %                                                           | -                |
|                                    | Non-schengen passengers                                   | 25 %                                                            | -                |
| Process characteristics            | Duration check-in                                         | $\mu = 58 \text{ s}$ , $\sigma = 25 \text{ s}$                  | Eq. 5.24         |
|                                    | Deposition of personal belongings at the security control | $a = 0 \text{ s}$ , $b = 81 \text{ s}$ ,<br>$c = 21 \text{ s}$  | Eq. 5.25         |
|                                    | Security check of person and luggage                      | $a = 2 \text{ s}$ , $b = 169 \text{ s}$ ,<br>$c = 43 \text{ s}$ | Eq. 5.25         |
|                                    | Receiving personal belongings at the security control     | $a = 0 \text{ s}$ , $b = 260 \text{ s}$ ,<br>$c = 22 \text{ s}$ | Eq. 5.25         |
|                                    | Duration passport control                                 | $a = 50 \text{ s}$ , $b = 60 \text{ s}$ ,                       | Eq. 5.26         |
|                                    | Calculation of delay times in the airport terminal        | $v = 1.34 \text{ m/s}$ ,<br>$dv = 0.26 \text{ m/s}$             | Eq. 5.27         |
| Distances between process stations | Entrance Terminal - Check-in Counter                      | $s = 46 \text{ m}$ , $ds = 26 \text{ m}$                        | Eq. 5.27         |
|                                    | Entrance Terminal - Security Control                      | $s = 153 \text{ m}$ ,<br>$ds = 77 \text{ m}$                    | Eq. 5.27         |
|                                    | Check-in Counter - Security Control                       | $s = 153 \text{ m}$ ,<br>$ds = 77 \text{ m}$                    | Eq. 5.27         |
|                                    | Security Control - Passport Control                       | $s = 90 \text{ m}$ , $ds = 0 \text{ m}$                         | Eq. 5.27         |
|                                    | Security Control - Gate                                   | $s = 106 \text{ m}$ ,<br>$ds = 42 \text{ m}$                    | Eq. 5.27         |
|                                    | Security Control - Gate                                   | $s = 42 \text{ m}$ , $ds = 15 \text{ m}$                        | Eq. 5.27         |

### 5.3.2.2 Application of the Simulation for KPI-driven Impact Estimation

Applying the model described in Subsection 5.3.2.1 and its implementation enables the simulation of the evolution of the airport system throughout the day. Logging the system state during simulation allows to gain information about airport performance in form of time series for KPIs or other valuable information for airport operators, such as

- waiting times at the process stations and their evolution throughout the day,
- times needed for passengers from entering the airport until boarding,
- times spent in different areas within the airport, e.g., passengers waiting for boarding and therefore having time left for duty-free shopping,
- passengers missing/reaching their flight, i.e., aircraft utilization,
- or delayed aircraft due to passengers being late for boarding.

Thus, the airport simulation enables operators to calculate these KPIs based on the number of available resources as depicted in the two stages at the bottom of Figure 5.1. Analogous to the static approach, the simulation can either be used to analyse, improve existing and develop new emergency plans or to support decision making regarding resource optimization. However, due to the rather long simulation and evaluation times (several minutes to an hour depending on the complexity of the chosen scenario), the approach is inappropriate regarding the support of load shedding in real time.

To evaluate the applicability of the airport simulation in this context, a parameter study is conducted, whereas resource availabilities are varied and their impact on the airport performance is measured. To keep the results comparable to the approach presented in Subsection 5.3.1.1, the number of resources at the process station is kept constant throughout the simulation day. However, the individual passenger behavior and operational aspects are considered.

In contrast to the static impact estimation, where the total averaged waiting time was used to measure the impact, a more suitable KPI in form of the seat load factor is applied. The SLF indirectly expresses the number of no-shows as well as the number of passengers missing their flight. Most notably, airlines are interested in keeping the SLF high to maximize revenue. However, also airport operators are encouraged to minimize the impact of people missing their flight due to blackouts or cyber attacks, as airlines may claim for compensation. As the operational costs for the aircraft are independent from the load, if the SLF drops below a certain value, aircraft operation gets unprofitable. This value is known as the breakeven load factor (BLF) (Butler and Keller, 2001). In this study, the BLF was chosen to be 66% (according to Avjobs (2010)), however, the BLF is highly dependent on the individual costs of the airline and tends to be much higher for low-cost carriers.

In the context of resource optimization, the optimization problem can be formulated as follows (Eq. 5.28): resources at passenger handling services are minimized while the seat load factor does not fall below a specified breakeven load factor.

To find the optimal solution for the scenario of the medium sized-airport as presented in Subsection 5.3.2.1, a parameter study is conducted. The process of identifying an approximate solution involves iteratively minimizing resources at check-in, security check, and passport control to emulate resource shortages, e.g., due to necessary load shedding. The minimum configuration of process station and their criticality has been determined through analysis of the output data from all simulations. This information provides valuable decision support for airport operators during system failures, enabling them to decide which service stations are prioritized within passenger handling subprocesses without compromising flight operations.

$$\min(\text{resources} \mid \text{slf} > \text{blf}) \quad (5.28)$$

The range of variability in process parameters is determined by the number of service counters available, specifically 86 check-in counters, 26 security checkpoints, and 6 passport control stations. To maintain flight operations, all processes must continue without interruption. Therefore, at least one service station must be operational at each step. The available check-in counters are categorized into three groups based on the number of passengers they handle on a reference day. Group 1 handles passengers from Eurowings, accounting for 50% of the total passenger volume. Group 2 accounts for 28% of the passenger volume, comprising clients from Lufthansa and Ryanair. The remaining group checks in all passengers from other airlines. The resulting seat load factors for the flights are logged and averaged to assess how varying process parameters affects the proportion of passengers who fail to reach their destination. The covered parameter space is shown in Figure 5.16. For each parameter combination simulations with the five previously generated data sets are conducted to estimate the impact of the random numbers on the results via the standard deviation.

Initially, it was assumed that there was no disruption at the airport and that the maximum number of all service stations was available. However, when a disruption occurred, the available resources for passenger handling decreased, necessitating reductions in the number of service stations. The impact of different processes on flight operations was analyzed through simulations, where reductions in the number of service stations were systematically implemented at one process until the resulting seat load factor (SLF) fell below the break-even threshold. This procedure was repeated five times for each of the different databases, and the resulting SLFs were averaged to obtain a comprehensive understanding of the impact on flight operations. The standard deviation in the average SLF values was calculated to provide insight into the variability induced by the five databases. It was found that reductions in the number of service stations at one process had a significant impact on the SLF.

The initial findings indicated that reductions in the number of check-in counters had little effect on the number of passengers who missed their flight, suggesting that reducing the capacity to 10 counters would have minimal impact. However, further analysis revealed that

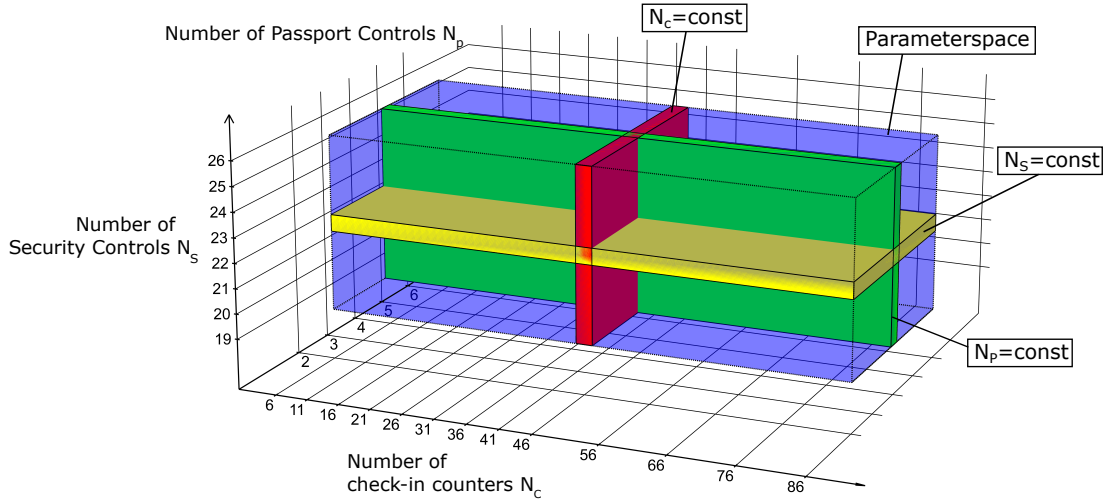


Figure 5.16: Depiction of the three-dimensional parameter space (blue) of the study spanned by the number of check-in counters (yellow), the number of security controls (green) and number of passport controls (red), which are iteratively kept constant.

reductions in the capacity to 46 counters led to more pronounced effects. Consequently, the reduction interval for check-in counters was reduced to 5, and it was found that the break-even SLF was reached with 6 check-in counters, while preserving the resources for security and passport controls.

Similarly, it was observed that reductions in the number of security or passport control stations were implemented until their respective minimum thresholds (19 security checks and 2 passport checks) were reached. This resulted in a significant decrease in the SLF. The simulation strategy was informed by this insight, allowing for critical process points to be targeted while minimizing unnecessary reductions. This yields in a total of 520 simulation runs that were executed for each database, providing a comprehensive output to analyze the impact of different process reductions.

Figure 5.17 presents the mean values for the resulting SLFs (a), and the corresponding standard deviations (b) in the considered parameter space. The x-axis represents the number of check-in counters, the y-axis represents the number of security checks, and the z-axis represents the number of passport control stations. The points on this graph represent the coordinates of the parameter space for which simulation runs were performed. The SLF values resulting from the corresponding combinations of service counters at the three processes are visualized. In Figure 5.17 (a), the mean SLF is color-coded, with a legend provided to explain how the colors correspond to the average SLF of flights over the day. A blue dashed line indicates the maximum SLF possible in the model (77.6%, see Subsection 5.3.2.1), while a red dashed line represents the BLF (66%). Bright dots indicate high SLF values, and darker colors indicate lower SLF values. White or yellow dots signify that the mean SLF is above the BLF of 66%, whereas dark brown and black dots indicate that the mean SLF is below this threshold. Light brown dots represent a SLF value close to the

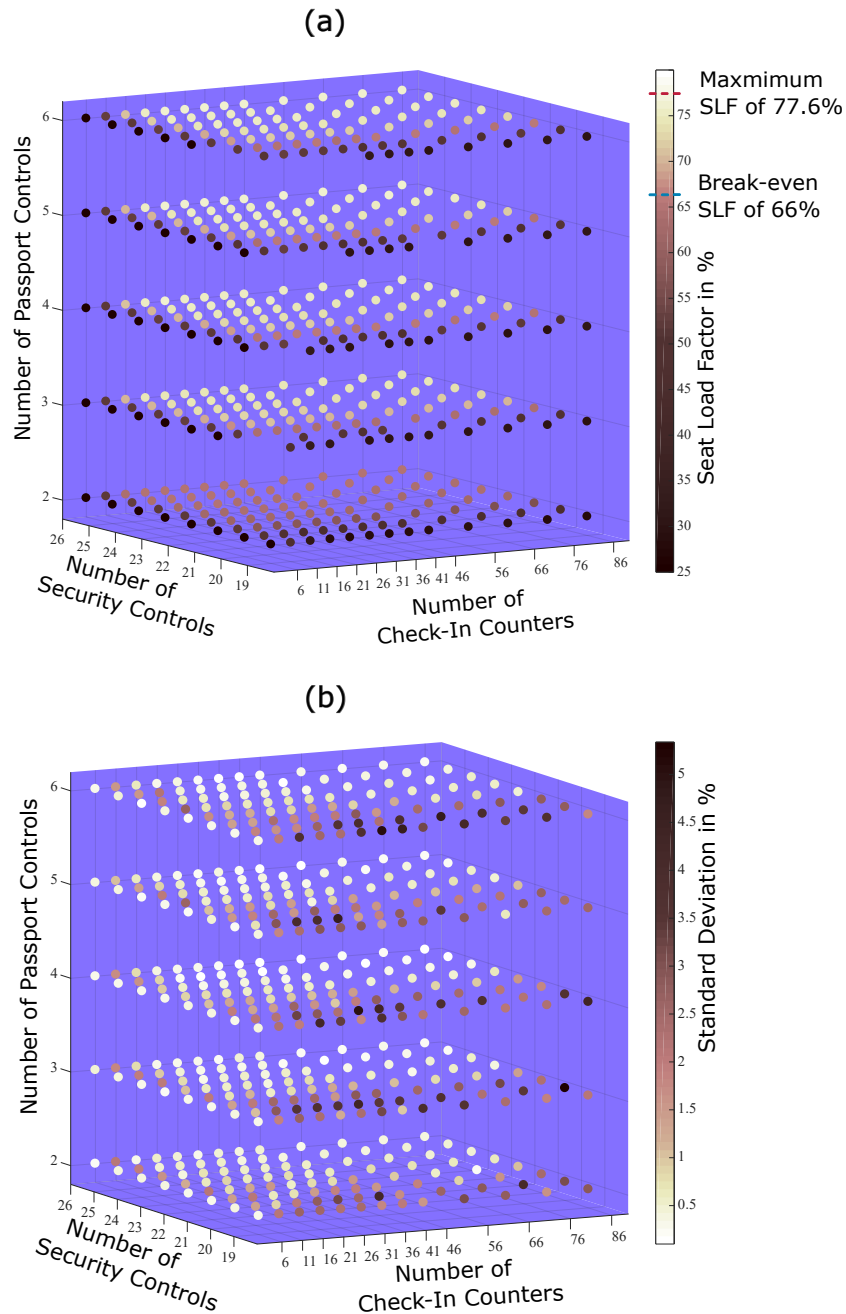


Figure 5.17: Results of the parameter study showing the averaged seat load factor (a) and its standard deviation (b) in dependence of the service stations configurations. Bright dots represent goo airport performance and brown dots indicate operation below the breakeven load factor Brause et al. (2020).

break-even point. The color coding scheme provides a clear visual representation of the relationship between the parameter space and the corresponding SLF values.

If all service stations of the three processes are available, the SLF is between 70% and 76%, resulting in a value above the breakeven SLF. Figure 5.17 (a) shows that initially, no notable change occurs to the SLF when the number of check-in counters is reduced. However, from a certain number of 16 check-in counters onwards, a greater change in the SLF can be observed.

Reductions in the number of security checks below 21 do not lead to a lowering of the SLF below the break-even level. With a number of 19 and 20 available security checks, the SLF falls below the BLF. Further reductions in security checks may result in a significant increase in the number of passengers who miss their flight.

No notable influence on the SLF can be detected when reducing the number of passport controls. A slight change in the SLF is observed only with 2 service counters available. The SLF has a value slightly lower than the BLF in this scenario.

Figure 5.17 (b) presents the differences between simulation results from various databases in terms of standard deviation. The coloring of the dots indicates the percentage standard deviation, with dark dots representing high standard deviations and bright dots symbolizing low standard deviations. The maximum deviation among all parameter combinations is less than 6%. With a large number of service stations at the three processes, the results of simulation runs differ by only less than 1%. Therefore, differences in databases, such as the distribution of arrival times, can be excluded as a cause for the decreasing SLF.

The results indicate that it is possible to reduce the number of check-in counters to 26 without a noticeable increase in the number of passengers missing their flight. However, further reductions in check-in resources may lead to an increase in passengers missing their flights by up to 5%. Based on simulation study findings, a further reduction in the number of check-in counters is not recommended due to the risk of occupying less than the BLF.

A noticeable effect on the number of passengers not reaching their flight occurs with a reduction of just one counter at the security control. Nevertheless, if reductions are unavoidable, security resources can be reduced to 22 available service stations. With 21 service stations at the security control, the average proportion of occupied seats in aircraft is slightly below the break-even SLF. Since random fluctuations of the SLF occur between 2% and 3%, it is not possible to determine whether the BLF is slightly exceeded or undercut. Further reductions in security checks should be avoided, as they can lead to a sharp increase in passengers who do not reach their flight.

The simulation results indicate that a reduction of passport control to 3 service stations is possible without a noticeable increase in delayed passengers. A comparison of the results from the five different databases reveals that with a reduction of resources to 2 passport controls, many non-Schengen passengers miss their flight. As a result, the SLF, both in

Table 5.11: Assessment of the number of available service stations at passenger handling processes as uncritical, critical and insufficient to maintain flight operations (Brause et al., 2020).

|                             | Uncritical | Critical | Insufficient |
|-----------------------------|------------|----------|--------------|
| number of check-in counters | 86-26      | 21-16    | 11-6         |
| number of security controls | 26         | 25-21    | 20-19        |
| number of passport controls | 6-4        | 3        | 2            |

terms of the number of non-Schengen passengers and the total number of passengers, falls below the break-even SLF.

If less resources are available at the airport due to a system malfunction (e.g., power shortage), the number of check-in and passport control service stations may be reduced. A reduction up to 26 service stations at the check-in or 4 at the passport control has only a minor effect on the number of passengers missing their flight. Further reductions in resources may necessitate the reduction of security control service stations. A reduction to fewer than 16 counters for check-in, 21 service stations for security, or 3 for passport control should be avoided. This would result in so many passengers who do not reach their flight that the SLF would fall under the BLF.

Therefore, the simulation results can be used to categorize which variations of the service stations are considered as uncritical (nearly no effect), critical (performance approximately at BLF) or insufficient (below BLF) with regard to a functioning flight operation. This overview of the results is presented in Table 5.11. The results of the parameter study are comparable to the snapshot based approach presented in Subsection 5.3.1, as both results emphasize the bottleneck effect at the security controls and the low impact of a reduced number of check-in counters on the airport performance.

## 5.4 KPI-driven Emergency Plan Evaluation

Within the previous Subsections two methods have been presented that allow the estimation of the impact of disruptions on airport performance at the example of two simple departure process chains. The approach presented in Subsection 5.3.1 minimizes the amount of additional waiting times, while assuming a certain number of dysfunctional devices. To do this, matrix operations are used to represent the redistribution of additional waiting times on other process stations in mathematical form and calculate the total additional waiting time. Subsequently, the optimization problem is solved using a brute-force approach. The tests on a simple departure process chain have shown that for fast-paced decision support, solving the optimization problem is not feasible. However, solving the optimization for one dysfunctional device and keeping this device dysfunctional, reduces the number of combinations by magnitudes without losing too much performance, if considering only a small amount of dysfunctional devices. Thus, it could be used as real-time decision support to

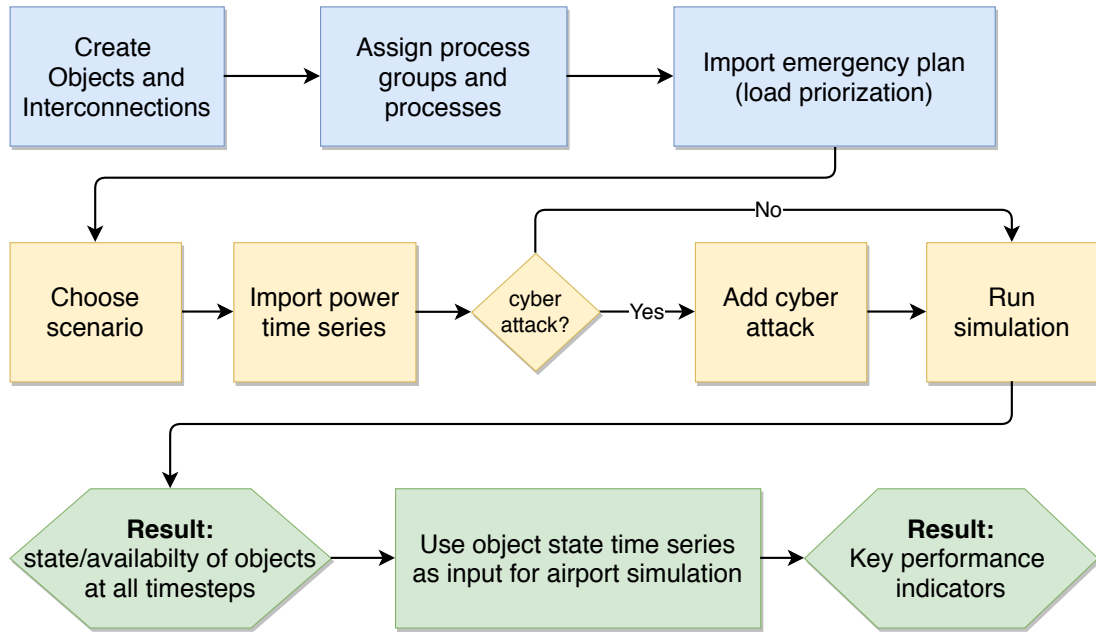


Figure 5.18: Emergency plan evaluation workflow that starts with the system setup (blue), simulates the operability state under given scenarios (yellow), and uses these capacities to determine the impact in form of KPIs.

decide which loads to shed in case of power shortages. However, the microscopic-agent based simulation allows an in depth analysis of multiple KPIs and is capable to consider operational conditions, such as flight plans or even dynamic resource management.

Nevertheless, the approach requires an event-based scenario as input, whereas resource availabilities at each point in time are given. Therefore, in Section 5.1 a simulation model was introduced that allows to simulate the operability state of single devices under given power availability and demand as well as predefined cyber attack scenarios. The process of process-oriented grouping (see Section 5.2) can then be used to transfer this knowledge from a device abstraction level to process capacities.

Combining the approaches presented in this Chapter yields a workflow that allows a KPI-driven evaluation of emergency plans for blackout or cyber attack scenarios. The workflow is shown in Figure 5.18 and consists of three phases:

1. System setup (depicted in blue): First, the airports physical infrastructure and their connections are assessed yielding in a complex network graph representing the airport as a cyber-physical system as described in Section 3.1. Second, the devices are projected on the processes via process-oriented grouping (see Subsection 5.2.1). To be able to apply reactive measures in case of a crisis, an emergency plan is defined, whereas this should at least contain a load prioritization list for load shedding. However, it can also contain measures to separate the network in case of a cyber attack to isolate network parts and prevent further spreading.

2. Determination of system state evolution (yellow): Goal of this phase is to determine the operability state of each device throughout the chosen time frame. Thus, the investigated scenario is defined in form of a time series for the available power (at each power source) and, if applicable, a cyber attack via an attack vector and an attack time. Afterwards, the power demands of all devices are imported. In case of a cyber attack, the attack vector is imported. Conclusively, the simulation framework explained in Section 5.1 is executed to determine the evolution of the operability states.
3. Impact analysis (green): The last phase first translates the operability states from phase two into process capacities applying the method described in Subsection 5.2.2. Lastly, either the static (applied before and after resource changes) or the microscopic impact analysis is used to determine the KPIs under the conditions resulting from phase two. These KPIs enable the evaluation of the emergency plan and allows a comparison of its effectiveness for the specific scenario, or even its adaptability by repeating phases two and three for different scenarios.

---

# Discussion and Outlook

---

Within this Chapter, the methods developed within this work and its findings are critically discussed in Section 6.1. As some parts of this work are several years old, the findings and assumptions are set into technological trends and modern changes. Moreover, an outlook is given in Section 6.2, which emphasizes the necessary steps that need to be undertaken to bring the methods into application and prepare them for operational use. Furthermore, suggestions for possible methodological enhancements are provided.

## 6.1 Discussion

The motivation of this work lies in making airport infrastructure more resilient towards blackouts and cyber attacks. The question may arise whether modern technologies have already solved this issue, especially since the last outages considered in the risk analysis in Chapter 4 occurred in June 2019. However, incidents such as the large blackout at Manchester Airport in June 2024, where 90,000 passengers were stranded due to a malfunctioning cable (Akintade, 2024), indicate that effective emergency management remains an unsolved problem. The heavy impact on airports of the large-scale power outage in Spain and Portugal on April 28, 2025 (Peters, 2025) underlines that airports are not prepared sufficiently. Moreover, it emphasizes that long lasting, large scale blackouts are possible in Europe.

The ongoing decentralization of energy production due to the increasing amount of renewable energies and the development towards smart grids will further increase the complexity of emergency management during blackouts. The risk and impact analysis provided in Section 4.1 can help to establish guidelines for better preventive measures and extend existing guidelines and laws by stricter rules and processes to protect physical infrastructure, such as enhanced planning of construction works.

Regarding cyber attacks, a recent attack on Japan Airlines has highlighted the importance of cyber security in aviation (McDonald, 2024). Although the incident targeted and mainly affected the airline's network, the threat for airports is equivalent. A vulnerability analysis

introduced in Section 4.2 can be adapted to all types of ICT networks and could even be virtually enhanced by ICT networks of all stakeholders. However, this high interconnect-edness further increases the complexity of the system. Therefore, technical support for decision makers becomes inevitable in the future.

The methodological approach to express physical infrastructure as a complex cyber-physical system (see Chapter 3) and use simulations to analyze its operational state (see Section 5.1) yields great potential in understanding this complexity. Furthermore, connecting the operability state of physical infrastructure and airport processes through process-oriented grouping (see Section 5.2) enables a holistic approach towards resource and emergency management. The pipeline introduced in Chapter 5 can be used to evaluate planning and decisions by predicting their impact on airport performance using predefined KPIs.

Despite the proposed methods, several weaknesses are included that should be discussed. The most obvious weakness lies in the missing validation of the holistic pipeline within a real infrastructure. A lack of validation using real-world data is an overall problem while developing modeling and simulation methods that aim to enhance the safety and security of critical infrastructure. Many reasons contribute to this knowledge gap, but these are the most prominent ones:

- Lack of digitization: The life cycles of most critical infrastructures are very long, leading to the fact that most critical infrastructures were built before digitalization in civil and electrical engineering began. Consequently, it is common that the original structure of the infrastructure is not documented in digital form. In most cases, engineering drawings are available as scanned raster-files.
- Evolution over time: Due to the long life cycle, many changes may occur that alter the physical part of the infrastructure. Common reasons for this are either a constant adaptation to demand (e.g., building another terminal at an airport) or moderniza-tion (e.g., renewing the ICT cabling to achieve higher communication speeds). Thus, data might be connected to a certain state of the infrastructure, which does not co-here with the environment of other collected data.
- Multi-faceted scenarios: The models presented in this work refer to the impact of blackouts and cyber attacks in general and claim to be adaptable to be independent of the cause. However, this can only be proven if data for the impact on the same infrastructure under a multi-faceted scenario is available.
- Criticality for Society: A common way to acquire data is through the active manipu-lation of the system into the desired state. In the context of crisis management, this would mean disrupting the infrastructure's functionality until losing integrity. The importance of critical infrastructures makes this impossible, leading to crisis man-agers relying on expert knowledge or a sparse set of data about previous incidents.

The propagation model for cyber attacks described in Subsection 3.1.1 models the prop-agation between objects using time units. However, this time is subject to various factors

such as communication speed, hardware and software dependencies, and the properties of malware, which need to be considered. Aggregating these factors into a single edge property is both a strength and a weakness. On one hand, it simplifies the infection process by providing an understandable system description, enabling quick analysis of the system. On the other hand, malware properties are diverse and often remain undetected, resulting in limited data about infection times. Recreating a concrete scenario with the proposed method requires more effort due to these limitations.

The impact estimation methods described in Section 5.3 only cover departure processes at the airport, limiting the universality of the results. However, the method can be enhanced to include other processes, such as arrival processes or aircraft procedures, which would require expert knowledge about specific airports and an in-depth analysis.

One important point of using modeling techniques is determining the correct abstraction level. This work refers to the general term "device" or "node" without specifying the granularity level. The examples used throughout Chapter 5 consider single devices such as personal computers, as well as aggregated devices into process groups. The multiplex graph introduced in this work has its major strengths in scalability and adaptability, as neither the number of nodes on a layer nor the number of layers is limited. The physical layer, such as the electrical grid, can be split up into more granular and abstract layers, while maintaining the more abstract forms of process groups.

A last weakness of several aspects of this work lies in the demand for computational time necessary to conduct analysis. Parallelization and optimization efforts could address this issue, but it is unclear whether this would make the approaches real-time capable. In its current state, the holistic pipeline developed in this work is limited to planning and preventive measures. However, some parts of the pipeline, such as the method described in Subsection 5.3.1, are capable of being executed in real-time while losing accuracy or being limited to a small number of dysfunctional devices.

Despite these limitations, this work combines methods from several fields into the first holistic pipeline that enables forecasting the impact of blackouts and cyber attacks on airport infrastructure by mapping them onto understandable KPIs. Previous approaches focused solely on developing improved, highly sophisticated modeling and simulation methods for individual layers, such as power grid simulations or malware propagation. By integrating these elements, this work contributes to a better understanding of critical infrastructures and strengthens their protection in the future, supporting decision-makers.

## 6.2 Outlook and Possible Ways of Application in the Future

The results and limitations of this work have given rise to a multitude of new research questions for future work and an urgent demand for new technologies to bring the approach into application.

Modern artificial intelligence holds great potential for the digitization of infrastructures, and its combination with modern measurement technologies has the capability to overcome the problem of model adaptation on different infrastructures by automatically generating corresponding models. A pipeline for the automated generation of simulation models from in situ measurements and engineering drawings using artificial intelligence has been proposed by Koch et al. (2024).

Czerniawski and Leite (2020) treated the automatic digitization of building information models (BIM) via object recognition, which translates in situ measurements, such as point clouds, RGB- or infrared images, into a machine-readable, semantically annotated form. The semantic information and functionality included in the BIM make a major difference to 3D-models generated using photogrammetry. Stürmer et al. (2023) leveraged common methods for the digitization of engineering diagrams to form a pipeline that translates piping and instrumentation diagrams into a graph structure and utilizes this graph to generate a hydraulic simulation. Integrating previous approaches may tackle the issue about data scarcity regarding the physical infrastructure, allowing for a simple adaptation of the methods on all types of critical infrastructures and specific use cases.

Apart from knowledge about the building structure, modeling passenger flows at airports, or critical infrastructures in general, remains a tedious work, as processes may differ in special cases. Therefore, Eftimova et al. (2024) set up a data-driven method to reconstruct processes, such as interaction at counters or queuing in front of them, from passenger trajectories and automatically generated simulations out of the resulting points of interest. In combination with the automatic reconstruction of the building structure, this method can reduce the effort needed to set up the pedestrian flow model required for impact estimation as described in Section 5.3.2. However, one of the key questions in this field will be how the interconnections between the physical infrastructure and the processes are assigned.

The non-real-time capability of the simulation models presented in this work limits its application to prognosis models. Therefore, parallel computing could be used to speed up computation times and enable near real-time applications. Other approaches towards fast computing include model order reduction (Schilders, 2008) or physics-informed machine learning (Raissi et al., 2017), especially with respect to modern pedestrian flow models that incorporate navigation, locomotion, and interaction of all agents, such as the Optimal Steps Model (Kleinmeier et al., 2019). Moreover, the real-time capability is also the first step towards a setup of fully interactive simulation coupling that could replace the sequential approach of the holistic pipeline presented in Chapter 5. Software architectures, such as the one presented in Franke et al. (2023), allow for the interactive coupling of multiple simulations running in parallel by using a broker architecture. Furthermore, communication via a centralized broker architecture would enable an easy integration of multiple simulations, e.g., the water infrastructure or knowledge information transfer between passengers.

Moreover, an important step towards a Digital Twin for Airports would be the successful integration of sensor data for monitoring purposes and to update models. With respect

---

to the electrical infrastructure, smart meter data could be used to assess power demands. In combination with simulation results, anomalies in power consumption can be detected. Camera tracking systems can be used to determine passenger positions, and the resulting data enables the update and validation of pedestrian flow models.

All the previously mentioned enhancements are steps towards the overall integration of this work into a Digital Twin for Airports that enable a bi-directional connection, provide forecasting and prognosis tools, and offer tools for monitoring as proposed by Brucherseifer et al. (2021). In combination with an optimized front-end interface, situational awareness of crisis management teams and decision-making in crisis situations could be brought to a new level.

Lastly, from a less technical but not less important perspective, the results of this and following works should be used to introduce new standards for infrastructure design, including process-oriented factors. This would be essential to tackle the need for more resilience of critical infrastructures as desired by European Commission (2022).



---

## Conclusion

---

The question of how to prepare for and react to blackouts or cyber attacks on airport infrastructure remains unsolved for airport operators. Within this work, this question is addressed in two ways.

First, it is essential to understand the reasons for blackouts and identify vulnerable points within the airport systems, also with respect to cyber attacks. Therefore, a comprehensive risk impact analysis of blackouts at airports is carried out to identify causes of blackouts. The key findings were that maintenance and construction works are the major reasons for blackouts in first-world countries. However, this differs in countries with a high System Average Interruption Duration Index, i.e., countries with a high occurrence rate and long durations of blackouts on the power grid, where dysfunctions on the public grid are the main cause. As a result, prevention strategies should be adapted to external factors.

Moreover, a vulnerability analysis method based on graph properties is introduced to aid in cost-efficient strengthening of the ICT network. The stress centrality was found to be an indicator for a cost-efficient improvement of the network security. However, in cases where investment costs within the network differ strongly, solving the optimization problem introduced within this work yields best results.

Second, a modeling and simulation approach is used to enable impact forecasting of incidents as well as the evaluation of preventive and reactive measures. While power grid operators are constantly working to increase the resilience of their grids and operation researchers are optimizing airport operation with respect to efficient resource management and a good cost-benefit ratio, there is no integrative approach to use this knowledge to improve the resilience of airports. Regulations focus on the prevention of casualties, but neglect business continuity management. Therefore, within this work a holistic approach is described that tackles these issues by representing the airport as a complex cyber-physical system represented by a multiplex network graph including the physical infrastructure and airport processes. The work introduces methods for process-oriented grouping to combine approaches describing the behavior of singular layers, such as power flow analysis for electrical systems, or agent-based approaches to simulate airport processes, to enable an impact estimation in case of blackouts or cyber attacks. The singular parts of the pipeline are verified at minimum examples, and two impact estimations are conducted at different airport

setups. In all cases, security checks have been found to introduce a bottleneck effect, posing a major problem for business continuity management. However, proper adjustment to the specific airport would be necessary to allow an in-depth analysis.

Although the pipeline introduced in this work needs to be validated on a real infrastructure using measured data, it is the first conceptual approach towards treating resilience of airports as a holistic approach that includes the physical infrastructure, airport processes and passenger behavior, and allows for an integral evaluation of emergency plans considering these factors.

# Appendix

## A.1 Additional Scenarios for the Static Impact Analysis

In the following, an additional scenario to the ones presented in Subsection 5.3.1 is defined, to give further insight into the Static impact analysis. The scenario differs by using float values to distribute passengers over the process stations. In the scenario given in Table A.1, 80% of the passengers need to Check-In and are distributed equally over CI 1 and CI 2 (with 40% each), while 20% have already checked in. Furthermore, 75% do not undergo passport controls due to domestic or intra-Schengen flights and the remaining 25% are split over classical and automated passport controls with 12.5% each.

Table A.1: Process sequence matrix  $\mathbf{P}_{Seq}$  weighted by process.

|                       | CI 1 | CI 2 | No CI | SC | PC    | APC   | No BPC | BPC 1 | BPC 2 |
|-----------------------|------|------|-------|----|-------|-------|--------|-------|-------|
| Check-In              | 0.4  | 0.4  | 0.2   | 0  | 0     | 0     | 0      | 0     | 0     |
| Security Check        | 0    | 0    | 0     | 1  | 0     | 0     | 0      | 0     | 0     |
| Passport Control      | 0    | 0    | 0     | 0  | 0.125 | 0.125 | 0.75   | 0     | 0     |
| Boarding Pass Control | 0    | 0    | 0     | 0  | 0     | 0     | 0      | 0.5   | 0.5   |

Table A.2: Results for all scenarios with respect to processes in minutes

|               |                                    | Check-In  | Security Check | Passport Control | Boarding Pass Control | Total processing time |
|---------------|------------------------------------|-----------|----------------|------------------|-----------------------|-----------------------|
| Initial State | $\bar{\mathbf{w}}_{process}$       | 5.5       | 11.2           | 1.3              | 1.6                   | 19.8                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.3$        | $\pm 0.3$             | $\pm 1.9$             |
|               | $\mathbf{w}_{add,process}$         | 0.0       | 0.0            | 0.0              | 0.0                   | increase by           |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.0$ | $\pm 0.0$      | $\pm 0.0$        | $\pm 0.0$             | —                     |
|               | $\mathbf{w}_{total,process}$       | 5.5       | 11.2           | 1.3              | 1.6                   |                       |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.3$        | $\pm 0.3$             |                       |
| Scenario 1    | $\bar{\mathbf{w}}_{process}$       | 5.7       | 11.3           | 1.3              | 1.6                   | 54.8                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.3$        | $\pm 0.3$             | $\pm 2.0$             |
|               | $\mathbf{w}_{add,process}$         | 1.3       | 33.6           | 0.0              | 0.0                   | increase by           |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.3$ | $\pm 0.0$      | $\pm 0.0$        | $\pm 0.0$             | 177.4%                |
|               | $\mathbf{w}_{total,process}$       | 7.0       | 44.9           | 1.3              | 1.6                   |                       |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.3$        | $\pm 0.3$             |                       |
| Scenario 2    | $\bar{\mathbf{w}}_{process}$       | 5.5       | 11.2           | 1.4              | 1.6                   | 23.8                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.3$        | $\pm 0.3$             | $\pm 2.2$             |
|               | $\mathbf{w}_{add,process}$         | 3.8       | 0.0            | 0.3              | 0.0                   | increase by           |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.9$ | $\pm 0.0$      | $\pm 0.4$        | $\pm 0.0$             | 20.6%                 |
|               | $\mathbf{w}_{total,process}$       | 9.3       | 11.2           | 1.7              | 1.6                   |                       |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 1.6$ | $\pm 0.0$      | $\pm 1.4$        | $\pm 0.3$             |                       |
| Scenario 3    | $\bar{\mathbf{w}}_{process}$       | 5.7       | 11.2           | 1.2              | 1.8                   | 23.4                  |
|               | $\Delta\bar{\mathbf{w}}_{process}$ | $\pm 1.4$ | $\pm 0.0$      | $\pm 1.2$        | $\pm 0.2$             | $\pm 2.4$             |
|               | $\mathbf{w}_{add,process}$         | 0.6       | 0.0            | 1.5              | 1.5                   | increase by           |
|               | $\Delta\mathbf{w}_{add,process}$   | $\pm 0.4$ | $\pm 0.0$      | $\pm 1.5$        | $\pm 0.4$             | 18.5%                 |
|               | $\mathbf{w}_{total,process}$       | 6.3       | 11.2           | 2.7              | 3.3                   |                       |
|               | $\Delta\mathbf{w}_{total,process}$ | $\pm 1.5$ | $\pm 0.0$      | $\pm 1.9$        | $\pm 0.4$             |                       |

---

## A.2 Software Implementation

Python environment description in YML form:

```
name: airport simulation environment
channels:
  - conda-forge
dependencies:
  - ca-certificates=2024.12.14=h56e8100_0
  - libsqlite=3.47.2=h67fdade_0
  - openssl=1.1.1w=hcfcfb64_0
  - pip=24.0=pyhd8ed1ab_0
  - python=3.7.9=h7840368_100_cpython
  - setuptools=69.0.3=pyhd8ed1ab_0
  - sqlite=3.47.2=h2466b09_0
  - ucrt=10.0.22621.0=h57928b3_1
  - vc=14.3=ha32ba9b_23
  - vc14_runtime=14.42.34433=he29a5d6_23
  - vs2015_runtime=14.42.34433=hdffcdeb_23
  - wheel=0.42.0=pyhd8ed1ab_0
  - pip:
    - cycler==0.11.0
    - fonttools==4.38.0
    - kiwisolver==1.4.5
    - matplotlib==3.5.3
    - networkx==2.6
    - numpy==1.21.6
    - packaging==24.0
    - pandas==1.3.5
    - pillow==9.5.0
    - pyparsing==3.1.4
    - pypower==5.1.15
    - python-dateutil==2.9.0.post0
    - pytz==2024.2
    - scipy==1.7.3
    - six==1.17.0
    - typing-extensions==4.7.1
    - wxpython==4.2.0
```

---

---

Implementation of the FloydWarshall Algorithm used in Section 5.1:

---

**Algorithm A.1** Implementation of the FloydWarshall Algorithm

---

**Input:** graph (adjacency matrix of a graph)  
**Output:** pred, dist (predecessor and distance matrix)

```

1: function FloydWarshall(graph)
2:   graph_temp = graph.copy()
3:   n = len(graph_temp)
4:   pred = np.zeros(graph_temp.shape)
5:   dist = np.zeros(graph_temp.shape)
6:   for i in range(0,n) do
7:     for j in range(0,n) do
8:       pred[i,j] = i
9:       if i != j and graph_temp[i,j] == 0 then
10:        pred[i,j] = -100000
11:        graph_temp[i,j] = 100000
12:       end if
13:     end for
14:   end for
15:   for k in range(0,n) do
16:     for i in range(0,n) do
17:       for j in range(0,n) do
18:         if graph_temp[i,j] > graph_temp[i,k] +
graph_temp[k,j] then
19:           graph_temp[i,j] = graph_temp[i,k] +
graph_temp[k,j]
20:           pred[i,j] = pred[k,j]
21:           dist[i,j] = graph_temp[i,j]
22:         end if
23:       end for
24:     end for
25:   end for
26:   return pred, dist
27: end function

```

---

Structure of the software folder:

```
main folder
├── scripts
│   ├── __init__.py
│   ├── cyber_attack.py
│   ├── electrical_network.py
│   ├── emergency_management.py
│   ├── floyd_warshall.py
│   ├── ict_network.py
│   ├── input_output.py
│   ├── network_object.py
│   └── object_group.py
├── results
│   ├── scenario 1
│   │   ├── iteration_data
│   │   │   ├── 0
│   │   │   ├── 1
│   │   │   ├── ...
│   │   │   └── n
│   │   └── time_series
│   │       ├── demanded_power.dat
│   │       ├── p_max.dat
│   │       ├── phase.dat
│   │       ├── power_out.dat
│   │       ├── resources.dat
│   │       ├── voltage.dat
│   │       └── working_status.dat
│   └── ...
├── scenario x
├── Actions-go-down-icon.png
├── Actions-go-next-icon.png
├── Actions-go-previous-icon.png
├── Actions-go-up-icon.png
├── gui.py
└── airport_infrastructure_env.yml
```

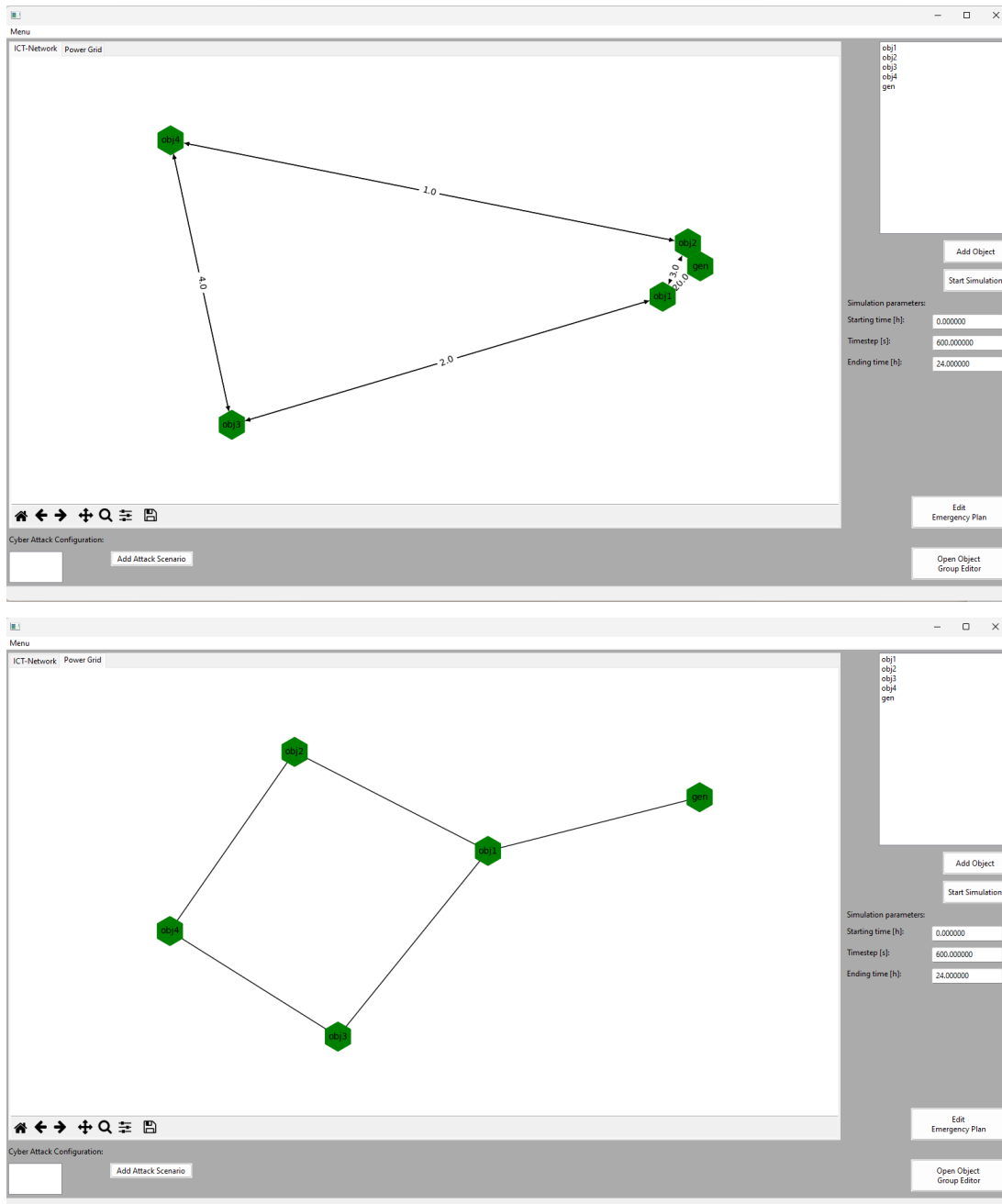


Figure A.1: Screenshots of the GUI Editor and visualization of the ICT (top) and power (bottom) layer

Enter object properties:

Name:  Use the following time series for... power demand:  Browse

Object Type:  power output:  Browse

☒ IT properties voltage control:  Browse

Physical Properties:

|                           |                                        |                            |                                       |                            |                                       |
|---------------------------|----------------------------------------|----------------------------|---------------------------------------|----------------------------|---------------------------------------|
| Frequency:                | <input type="text" value="50.000000"/> | Phase:                     | <input type="text" value="0.000000"/> | Voltage:                   | <input type="text" value="1.000000"/> |
| Demanded Real Power:      | <input type="text" value="0.000000"/>  | Demanded Reactive Power:   | <input type="text" value="0.000000"/> | Real Power Output:         | <input type="text" value="0.000000"/> |
| Reactive Power Output:    | <input type="text" value="0.000000"/>  | Maximum Allowed Voltage:   | <input type="text" value="1.100000"/> | Minimum Allowed Voltage:   | <input type="text" value="0.900000"/> |
| Area:                     | <input type="text" value="1"/>         | Shunt Conductance:         | <input type="text" value="0.000000"/> | Shunt Susceptance:         | <input type="text" value="0.000000"/> |
| Loss Zone:                | <input type="text" value="1"/>         | Minimum Real Power:        | <input type="text" value="0.000000"/> | Maximum Real Power:        | <input type="text" value="0.000000"/> |
| Minimum Reactive Power:   | <input type="text" value="-0.300000"/> | Maximum Reactive Power:    | <input type="text" value="0.300000"/> | Voltage Magn. Setpoint:    | <input type="text" value="1.020000"/> |
| Generator Status:         | <input type="text" value="running"/>   | Lower PQ capability curve: | <input type="text" value="0.000000"/> | Upper PQ capability curve: | <input type="text" value="0.000000"/> |
| Min. power output at PC1: | <input type="text" value="0.000000"/>  | Max. power output at PC1:  | <input type="text" value="0.000000"/> | Min. power output at PC2:  | <input type="text" value="0.000000"/> |
| Max. power output at PC2: | <input type="text" value="0.000000"/>  | Ramp rate AGC:             | <input type="text" value="0.000000"/> | Ramp rate 10 min reserve:  | <input type="text" value="0.000000"/> |
| Ramp rate 30 min reserve: | <input type="text" value="0.000000"/>  | Ramp rate reactive power:  | <input type="text" value="0.000000"/> | Area participation factor: | <input type="text" value="0.000000"/> |

Setup physical connections:

| From Object: | To Object: | Active: |
|--------------|------------|---------|
| 2 - obj3     | 3 - obj4   | Yes     |
| 1 - obj2     | 3 - obj4   | Yes     |

Connect to object... Edit

ICT properties:

Required Applications: ☒ windows ☐ linux

Add Application

Delete Selected Application

Setup ICT network:

| From Object: | To Object: | Weight: |
|--------------|------------|---------|
| 1 - obj2     | 3 - obj4   | 1.0     |
| 2 - obj3     | 3 - obj4   | 4.0     |
| 3 - obj4     | 1 - obj2   | 1.0     |
| 3 - obj4     | 2 - obj3   | 4.0     |

Connect to object... Edit

Apply Reset Delete

Group List:

- Object Groups
  - Check-In1
    - obj1
  - Check-In2
    - obj2
  - Security-Check1
    - obj3
  - BPC 1
    - obj4

Object List:

☐ gen

←

→

Add Group

Delete Group

Choose dedicated process:  Delete Process

Add Process

OK

Figure A.2: Screenshots of the network object editor (top) and object group editor (bottom)

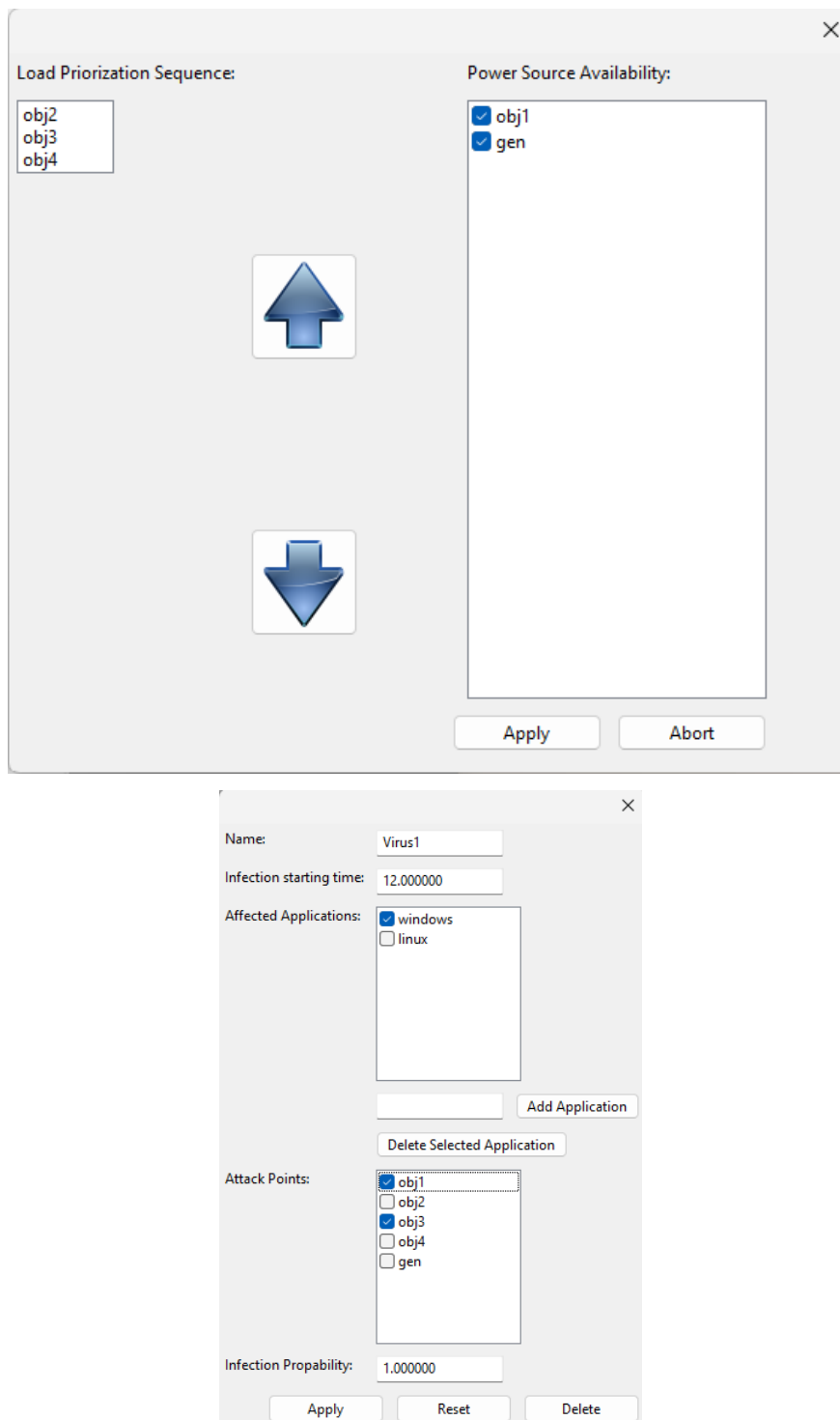


Figure A.3: Screenshots of the emergency management editor (top) and cyber attack configurator (bottom)

### A.3 Scenario Cologne-Bonn

Table A.3: Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2

| Flight number | Destination | Departure Time | Airline | Aircraft Type | Seats | Seats Occupied |
|---------------|-------------|----------------|---------|---------------|-------|----------------|
| EW012         | TXL         | 06:15          | EWG     | A320-200      | 180   | 140            |
| LH1999        | MUC         | 06:20          | DLH     | A321-100/200  | 200   | 155            |
| FR409         | CPH         | 06:25          | RYR     | B737-800      | 189   | 147            |
| EW026         | DRS         | 06:35          | EWG     | A320-200      | 180   | 140            |
| EW072         | LEJ         | 06:40          | EWG     | A319-100      | 150   | 116            |
| FR2813        | STN         | 06:45          | RYR     | B737-800      | 189   | 147            |
| EW824         | MXP         | 06:50          | EWG     | A319-100      | 150   | 116            |
| EW764         | ZRH         | 06:50          | EWG     | A319-100      | 150   | 116            |
| EW756         | VIE         | 06:50          | EWG     | B737-800      | 186   | 144            |
| FR1592        | MAN         | 06:55          | RYR     | B737-800      | 189   | 147            |
| EW520         | BCN         | 06:55          | EWG     | B737-800      | 186   | 144            |
| EW080         | MUC         | 07:00          | EWG     | A319-100      | 150   | 116            |
| EW032         | HAM         | 07:00          | EWG     | A319-100      | 150   | 116            |
| X32278        | FUE         | 07:00          | TUI     | B737-800      | 189   | 147            |
| EW354         | STN         | 07:05          | EWG     | A319-100      | 150   | 116            |
| EW788         | BUD         | 07:05          | EWG     | A319-100      | 150   | 116            |
| EW024         | TXL         | 07:15          | EWG     | A320-200      | 180   | 140            |
| EZY5912       | TXL         | 07:30          | EZY     | A320-200      | 180   | 140            |
| EW088         | MUC         | 07:50          | EWG     | A320-200 NEO  | 180   | 140            |
| FR8548        | BGY         | 08:10          | RYR     | B737-800      | 189   | 147            |
| EW8059        | TXL         | 08:15          | EWG     | A319-100      | 150   | 116            |
| EW1785        | MUC         | 08:20          | EWG     | A320-200      | 180   | 140            |
| EW460         | LHR         | 08:30          | EWG     | A319-100      | 150   | 116            |
| EZY5902       | TXL         | 08:35          | EZY     | A320-200      | 180   | 140            |
| LH1981        | MUC         | 08:35          | DLH     | A320-200      | 168   | 130            |
| EW7039        | HAM         | 08:45          | EWG     | A319-100      | 150   | 116            |
| EW8057        | TXL         | 08:50          | EWG     | A320-200      | 180   | 140            |
| LH1983        | MUC         | 09:20          | DLH     | A321-100/200  | 200   | 155            |
| FR3016        | MAD         | 09:25          | RYR     | B737-800      | 189   | 147            |
| OB6822        | IAS         | 09:30          | BMS     | B737-800      | 189   | 147            |
| OB122         | OTP         | 09:35          | BMS     | B737-500      | 126   | 98             |
| FR1355        | ALC         | 09:50          | RYR     | B737-800      | 189   | 147            |
| EW772         | PRG         | 09:50          | EWG     | A319-100      | 150   | 116            |
| EW014         | TXL         | 09:55          | EWG     | A320-200      | 180   | 140            |
| EW582         | PMI         | 09:55          | EWG     | A319-100      | 150   | 116            |

Table A.3: Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2

| Flight number | Destination | Departure Time | Airline | Aircraft Type | Seats | Seats Occupied |
|---------------|-------------|----------------|---------|---------------|-------|----------------|
| LH2207        | MUC         | 09:55          | DLH     | CL 600 RJ-900 | 90    | 70             |
| FR184         | SXF         | 10:00          | RYP     | B737-800      | 189   | 147            |
| EZY5904       | TXL         | 10:15          | EZY     | A320-200      | 180   | 140            |
| FR3018        | CIA         | 10:15          | RYP     | B737-800      | 189   | 147            |
| LH1985        | MUC         | 10:15          | DLH     | A320-200 NEO  | 180   | 140            |
| OS192         | VIE         | 10:25          | AUA     | A320-200      | 174   | 135            |
| EW284         | KLU         | 10:30          | EWG     | A319-100      | 150   | 116            |
| EW036         | HAM         | 10:30          | EWG     | A319-100      | 150   | 116            |
| FR130         | OPO         | 10:35          | RYP     | B737-800      | 189   | 147            |
| EW602         | LIS         | 10:40          | EWG     | A320-200      | 180   | 140            |
| EW082         | MUC         | 10:45          | EWG     | A319-100      | 150   | 116            |
| EW004         | TXL         | 10:55          | EWG     | A320-200      | 180   | 140            |
| EW766         | ZRH         | 10:55          | EWG     | A319-100      | 150   | 116            |
| FEG3082       | HRG         | 11:00          | FEG     | B737-800      | 189   | 147            |
| FR1590        | BRS         | 11:05          | RYP     | B737-800      | 189   | 147            |
| EW838         | BLQ         | 11:10          | EWG     | B737-800      | 186   | 144            |
| EW682         | ATH         | 11:20          | EWG     | A319-100      | 150   | 116            |
| 3O224         | NDR         | 11:25          | MAC     | A320-200      | 180   | 140            |
| EW972         | ZAG         | 11:30          | EWG     | A320-200 NEO  | 180   | 140            |
| PC1012        | SAW         | 11:35          | PGT     | B737-800      | 189   | 147            |
| BA2565        | LGW         | 11:45          | BAW     | A320-200      | 180   | 140            |
| TP587         | LIS         | 11:45          | TAP     | A320-200      | 180   | 140            |
| TK1672        | IST         | 11:55          | THY     | B737-900/ER   | 169   | 131            |
| EW7035        | HAM         | 12:15          | EWG     | A319-100      | 150   | 116            |
| FR6307        | SOF         | 12:25          | RYP     | B737-800      | 189   | 147            |
| EW8051        | TXL         | 12:30          | EWG     | A320-200      | 180   | 140            |
| EW886         | FCO         | 13:00          | EWG     | B737-800      | 186   | 144            |
| EW8067        | TXL         | 13:00          | EWG     | A319-100      | 150   | 116            |
| DP820         | VKO         | 13:10          | PBD     | B737-800      | 189   | 147            |
| LH1987        | MUC         | 13:15          | DLH     | A320-200 NEO  | 180   | 140            |
| EW752         | VIE         | 13:25          | EWG     | A319-100      | 150   | 116            |
| EW008         | TXL         | 13:35          | EWG     | A320-200      | 180   | 140            |
| FR7208        | PMI         | 13:40          | RYP     | B737-800      | 189   | 147            |
| XQ113         | AYT         | 13:40          | SXS     | B737-800      | 189   | 147            |
| EW034         | HAM         | 14:00          | EWG     | A319-100      | 150   | 116            |
| EZY5906       | TXL         | 14:00          | EZY     | A319-100      | 150   | 116            |
| FR8036        | DUB         | 14:00          | RYP     | B737-800      | 189   | 147            |

Table A.3: Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2

| Flight number | Destination | Departure Time | Airline | Aircraft Type     | Seats | Seats Occupied |
|---------------|-------------|----------------|---------|-------------------|-------|----------------|
| LH2199        | MUC         | 14:30          | DLH     | CL 600 RJ-900     | 90    | 70             |
| EW050         | TXL         | 14:35          | EWG     | A319-100          | 150   | 116            |
| EW464         | LHR         | 14:35          | EWG     | A319-100          | 150   | 116            |
| EW276         | SZG         | 14:50          | EWG     | A320-200          | 180   | 140            |
| TK1674        | IST         | 14:50          | THY     | B737-800          | 189   | 147            |
| PC1018        | SAW         | 15:05          | PGT     | B737-800          | 189   | 147            |
| DP874         | LED         | 15:10          | PBD     | B737-800          | 189   | 147            |
| EW768         | ZRH         | 15:15          | EWG     | A319-100          | 150   | 116            |
| EW084         | MUC         | 15:15          | EWG     | A319-100          | 150   | 116            |
| EW646         | FAO         | 15:30          | EWG     | B737-800          | 186   | 144            |
| EW8053        | TXL         | 15:35          | EWG     | A319-100          | 150   | 116            |
| EW7019        | HAM         | 15:45          | EWG     | A319-100          | 150   | 116            |
| W63988        | CRA         | 15:50          | WZZ     | A320-200          | 180   | 140            |
| EW584         | PMI         | 15:55          | EWG     | A320-200 NEO      | 180   | 140            |
| EW078         | LEJ         | 16:00          | EWG     | A319-100          | 150   | 116            |
| FR1596        | RAK         | 16:00          | RYP     | B737-800          | 189   | 147            |
| FR8518        | BGY         | 16:00          | RYP     | B737-800          | 189   | 147            |
| EW8071        | TXL         | 16:10          | EWG     | A320-200          | 180   | 140            |
| LH1989        | MUC         | 16:25          | DLH     | A320-200 NEO      | 180   | 140            |
| FR188         | SXF         | 17:05          | RYP     | B737-800          | 189   | 147            |
| EW006         | TXL         | 17:15          | EWG     | A320-200          | 180   | 140            |
| EW090         | MUC         | 17:15          | EWG     | A319-100          | 150   | 116            |
| EW030         | HAM         | 17:30          | EWG     | A319-100          | 150   | 116            |
| LH1991        | MUC         | 17:30          | DLH     | Embraer 195 - 200 | 120   | 93             |
| TK1676        | IST         | 17:35          | THY     | A320-200 NEO      | 159   | 123            |
| EZY5908       | TXL         | 18:10          | EZY     | A320-200          | 180   | 140            |
| FR2817        | STN         | 18:15          | RYP     | B737-800          | 189   | 147            |
| EW754         | VIE         | 18:15          | EWG     | A319-100          | 150   | 116            |
| EW020         | TXL         | 18:15          | EWG     | A319-100          | 150   | 116            |
| EW826         | MLP         | 18:20          | EWG     | A320-200          | 180   | 140            |
| EW468         | LHR         | 18:30          | EWG     | A320-200          | 180   | 140            |
| FR2658        | FAO         | 18:45          | RYP     | B737-800          | 189   | 147            |
| EW814         | VCE         | 18:45          | EWG     | B737-800          | 186   | 144            |
| EW086         | MUC         | 18:50          | EWG     | A319-100          | 150   | 116            |
| FR1602        | BLQ         | 18:55          | RYP     | B737-800          | 189   | 147            |
| EW762         | ZRH         | 19:00          | EWG     | A319-100          | 150   | 116            |
| EW356         | STN         | 19:05          | EWG     | A319-100          | 150   | 116            |

Table A.3: Scheduled flights for November 19, 2018 used as input for the Simulation of Cologne-Bonn Airport in Subsection 5.3.2

| Flight number | Destination | Departure Time | Airline | Aircraft Type       | Seats | Seats Occupied |
|---------------|-------------|----------------|---------|---------------------|-------|----------------|
| EW7033        | HAM         | 19:15          | EWG     | A319-100            | 150   | 116            |
| EW028         | DRS         | 19:15          | EWG     | A319-100            | 150   | 116            |
| TP589         | LIS         | 19:30          | TAP     | Embraer 195 - 200   | 118   | 92             |
| LH2205        | MUC         | 19:45          | DLH     | A319-100            | 138   | 107            |
| EW8055        | TXL         | 19:50          | EWG     | A320-200            | 180   | 140            |
| OS196         | VIE         | 19:55          | AUA     | Embraer 195 - 200   | 120   | 93             |
| FR1404        | WMI         | 19:55          | RYP     | B737-800            | 189   | 147            |
| LH1993        | MUC         | 20:30          | DLH     | A320-200            | 168   | 130            |
| XR194         | HRG         | 20:30          | CXI     | B737-800            | 189   | 147            |
| EZY5910       | TXL         | 20:45          | EZY     | A319-100            | 150   | 116            |
| LH1995        | MUC         | 21:15          | DLH     | A319-100            | 138   | 107            |
| FR2508        | BCN         | 21:25          | RYP     | B737-800            | 189   | 147            |
| FR2815        | STN         | 21:50          | RYP     | B737-800            | 189   | 147            |
| W67724        | SKP         | 22:10          | WZZ     | A321-100/200<br>NEO | 200   | 155            |

## A.4 AnyLogic Implementation Details

The Agent-based approach is implemented using the predefined blocks from the Process Modeling Library<sup>1</sup>, which is designed for agent-based and system dynamics models of complex systems. A detailed visualization of the implementation is given in Figure A.4.

Agents are generated from a *Source* block depending on time stamps given from a database. Delay blocks are used to model the walking time between the process steps with one *Delay* block placed between the process groups and the delay time calculated according to Equation 5.27. *SelectOutput* blocks are placed at each decision in the process tree, as they separate the agents path due to predefined conditions. At arrival a *SelectOutput* is used to check whether passengers are already late on arrival and if they are count them as missed using a *Sink* block. Analogously, these checks are done on arrival at each process step to count passengers who missed their flight. Before Check-In two other *SelectOutput* Blocks are used to split passengers who already checked in (first block) and therefore can skip the Check-In, if they have only carry-on luggage (second block). Another *SelectOutput* block

<sup>1</sup>Documentation of the Process Modeling Library: <https://www.anylogic.com/features/libraries/process-modeling-library/>

---

distributes the passengers to the Check-In counters that are assigned to their flight and checks, if the counter is still open. If the Check-In is already closed, the passengers are counted as missed using another *Sink* block. If they arrive too early, they are kept in a loop.

Each Process step is modeled using *Queue* blocks and *Service* blocks. The *Queue* blocks use the First-In-First-Out (FIFO) principle to dispatch the agents to the *Service* blocks. The *Service* blocks themselves pick a process time from the distribution functions given in Table 5.10 using the AnyLogic internal *normal* or *triangular* function, respectively. The number of available service stations is defined using resource parameters containing time-series for the availability of the resources assigned to the *Service* blocks. For the boarding process resources are defined representing the flights and aircraft availability at the gate. As *SelectOutput* blocks are only able to check for 4 possibilities, *SelectOutput* blocks are nested to distribute passengers to the corresponding gate before boarding. Directly before boarding further checks are conducted to determine whether the passengers arrive on time, boarding already opened, will open soon or boarding is already completed using several *Service* blocks. The number of passengers that miss their flights and time-series for the waiting times are written into output files for each process (determined using the *Queue* blocks).

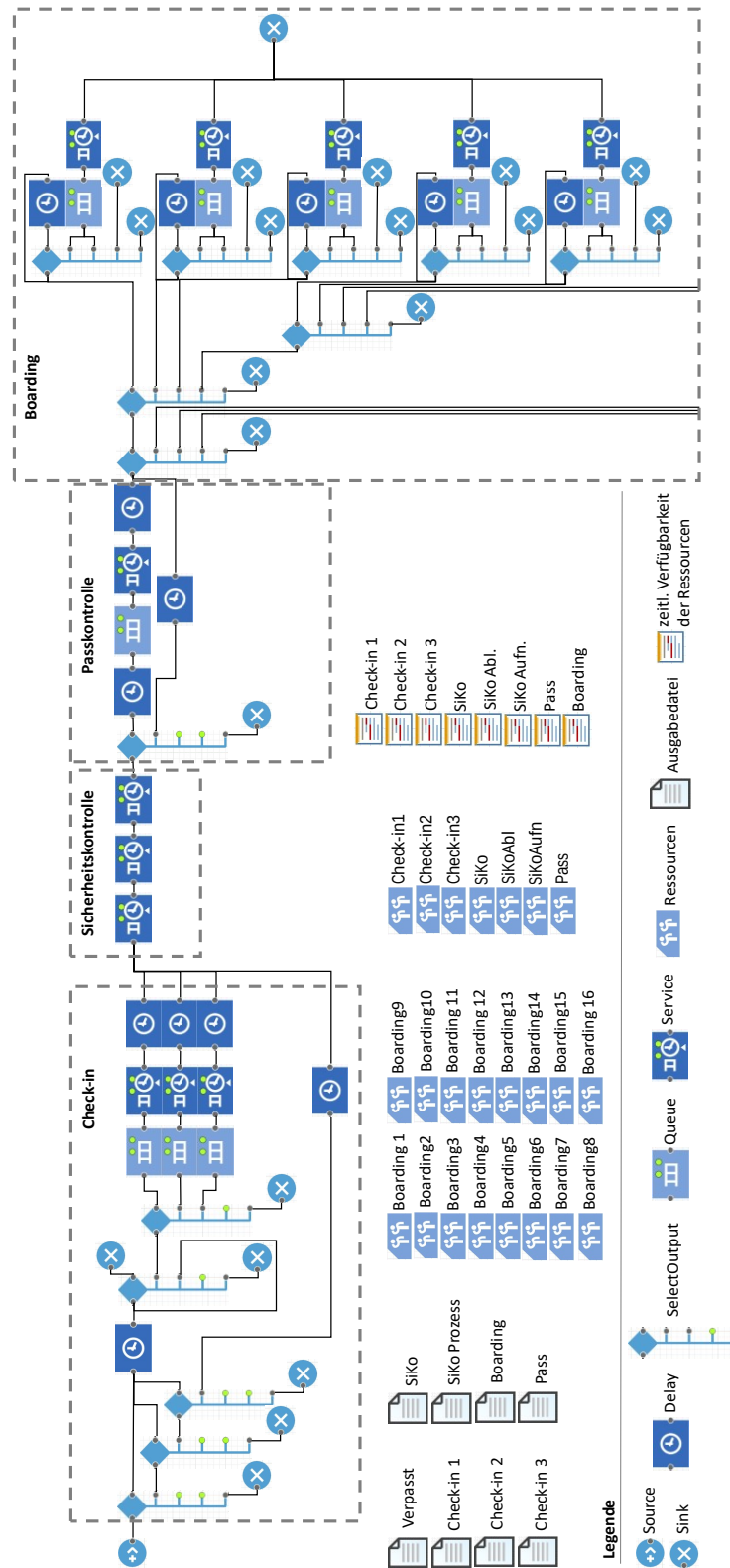


Figure A.4: Implementation scheme of the simulation using AnyLogic.

---

## References

---

- ABRAMS, M. AND WEISS, J., 2008. Malicious Control System Cyber Security Attack Case Study - Maroochy Water Services, Australia. Technical report, The MITRE Corporation Applied Control Solutions.
- ADV, 2018. Airport Travel Survey 2018: Zahlen, Fakten. trends. Technical report, Arbeitsgemeinschaft Deutscher Verkehrsflughäfen. [https://www.adv.aero/wp-content/uploads/2016/02/Airport-Travel-Survey-2018\\_Brosch~A\T1\OEre.pdf](https://www.adv.aero/wp-content/uploads/2016/02/Airport-Travel-Survey-2018_Brosch~A\T1\OEre.pdf).
- AEHNELT, R., 2011. Wikimedia Commons. [https://commons.wikimedia.org/wiki/File:Airport\\_infrastructure.png](https://commons.wikimedia.org/wiki/File:Airport_infrastructure.png).
- AHUJA, R. K.; MAGNANTI, T. L.; AND ORLIN, J. B., 1999. *Network Flows - Theory, Algorithms, and Applications*. Prentice Hall.
- AKINTADE, A., 2024. Blackout in UK Airport: 90,000 passengers affected, several flights cancelled. Peoples Gazette. <https://gazettengr.com/blackout-in-uk-airport-90000-passengers-affected-several-flights-cancelled/>.
- ANWAR, A. AND MAHMOOD, A. N., 2014. *Cyber Security of Smart Grid Infrastructure*, 103–132. Auerbach Publications. ISBN 9780429090578. doi:10.1201/b16390-9.
- ASAM, S., 2018. Wie viel zeit muss ich am flughafen einplanen? Merkur.de. <https://www.merkur.de/reise/viel-zeit-muss-eigentlich-flughafen-einplanen-zr-8697182.html>.
- ASMER, L.; POPA, A.; KOCH, T.; DEUTSCHMANN, A.; AND HELLMANN, M., 2019. Secure rail station - Research on the effect of security checks on passenger flow. *Journal of Rail Transport Planning & Management*, 10 (2019), 9–22. doi:10.1016/j.jrtpm.2019.04.002. <https://www.sciencedirect.com/science/article/pii/S2210970618301240>.
- AVEN, T., 2011. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Analysis*, 31, 4 (2011), 515–522. doi:10.1111/j.1539-6924.2010.01528.x. <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2010.01528.x>.
- AVJOBS, 2010. Airline Economics. Avjobs.com. <https://www.avjobs.com/history/airline-economics.asp>.
- BATTISTON, E; NICOSIA, V; AND LATORA, V., 2017. The new challenges of multiplex networks: Measures and models. *The European Physical Journal Special Topics*, 226, 3 (Feb. 2017), 401–416. doi:10.1140/epjst/e2016-60274-8.

- 
- BATTY, M.; AXHAUSEN, K. W.; GIANNOTTI, F.; POZDNOUKHOV, A.; BAZZANI, A.; WACHOWICZ, M.; OUZOUNIS, G.; AND PORTUGALI, Y., 2012. Smart cities of the future. *The European Physical Journal Special Topics*, 214, 1 (Nov 2012), 481–518. doi:10.1140/epjst/e2012-01703-3. <https://doi.org/10.1140/epjst/e2012-01703-3>.
- BEA, 2012. On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris. Technical report, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA).
- BIEDER, C. AND PETTERSEN GOULD, K., 2020. *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Springer International Publishing. ISBN 9783030472290. doi:10.1007/978-3-030-47229-0.
- BRAUSE, L.-M.; POPA, A.; KOCH, T.; DEUTSCHMANN, A.; AND HELLMANN, M., 2020. Optimization of resource demand for passenger services at airports during system failures such as blackouts. *European Transport Research Review*, 12 (2020), 1–13. doi:10.1186/s12544-020-00446-2. <https://api.semanticscholar.org/CorpusID:222143606>.
- BRUCHERSEIFER, E.; WINTER, H.; MENTGES, A.; MÜHLHÄUSER, M.; AND HELLMANN, M., 2021. Digital twin conceptual framework for improving critical infrastructure resilience. *at - Automatisierungstechnik*, 69, 12 (Nov. 2021), 1062–1080. doi:10.1515/auto-2021-0104.
- BSI, 2021. BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958). Technical report, Bundesamt für Sicherheit in der Informationstechnik.
- BUNDESAMT FÜR BEVÖLKERUNGSSCHUTZ UND KATASTROPHENHILFE, 2021a. Kritische Infrastrukturen - Sektoren- und Brancheneinteilung.
- BUNDESAMT FÜR BEVÖLKERUNGSSCHUTZ UND KATASTROPHENHILFE, 2021b. Living Guideline (01-2021) - Identifizierung im Kontext Kritischer Infrastrukturen.
- BUTLER, G. F. AND KELLER, M. R., 2001. *Handbook of airline strategy*. Aviation Week, New York, NY. ISBN 9780079823939.
- CBS NEWS, 2025. London's heathrow airport resumes some flights after fire causes "significant power outage". <https://www.cbsnews.com/news/heathrow-airport-london-closes-power-outage/>.
- CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE, 2012. Cyber Security in Civil Aviation. Technical report, Centre for the Protection of National Infrastructure.
- CHEN, L.-C. AND CARLEY, K. M., 2001. A Computational Model of Computer Virus Propagation. [http://www.casos.cs.cmu.edu/publications/papers/chen\\_2001\\_computationalmodel.pdf](http://www.casos.cs.cmu.edu/publications/papers/chen_2001_computationalmodel.pdf).
- CIVIL AVIATION AUTHORITY, 2018. CAP 642 - Airside Safety Management. Technical report, Civil Aviation Authority, United Kingdom. [https://publicapps.caa.co.uk/docs/33/CAP642Issue3\(11-2018\).pdf](https://publicapps.caa.co.uk/docs/33/CAP642Issue3(11-2018).pdf).

- 
- CIVIL AVIATION REGULATORY COMMISSION (CARC), 2018. Guidance Material: Airport Electrical System (34 GM-ADES). Technical report, The Hashemite Kingdom of Jordan. [https://carc.gov.jo/sites/default/files/inline-files/Airport\\_Electrical\\_System\(34GM-ADES\)222-compressed.pdf](https://carc.gov.jo/sites/default/files/inline-files/Airport_Electrical_System(34GM-ADES)222-compressed.pdf).
- CLEMENT, J., 2019. Most popular mobile social networking apps in the United States as of March 2019, by monthly users (in millions). Statista. <https://www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/>.
- COHEN, F., 1987. Computer viruses. *Computers & Security*, 6, 1 (Feb. 1987), 22–35. doi:10.1016/0167-4048(87)90122-2.
- COPPOLA, D. P., 2020. *Hazards*, 47–176. Elsevier. ISBN 9780128173688. doi:10.1016/b978-0-12-817368-8.00002-6.
- CORMEN, T. H.; LEISERSON, C. E.; RIVEST, R. L.; AND STEIN, C., 2001. *Introduction to Algorithms*. MIT Press, second edn. ISBN 0-262-03293-7.
- CURCIO, D.; LONGO, F.; MIRABELLI, G.; AND PAPPOFF, E., 2007. Passengers' Flow Analysis And Security Issues In Airport Terminals Using Modeling & Simulation. In *ECMS 2007 Proceedings edited by: I. Zelinka, Z. Oplatkova, A. Orsoni*. ECMS. doi:10.7148/2007-0374. <https://api.semanticscholar.org/CorpusID:106253>.
- CZERNIAWSKI, T. AND LEITE, F., 2020. Automated digital modeling of existing buildings: A review of visual object recognition methods. *Automation in Construction*, 113 (May 2020), 103131. doi:10.1016/j.autcon.2020.103131.
- DERRIBLE, S., 2012. Network Centrality of Metro Systems. *PLOS ONE*, 7, 7 (07 2012), 1–10. doi:10.1371/journal.pone.0040575. <https://doi.org/10.1371/journal.pone.0040575>.
- DEUTSCHMANN, A.; STROOT, S.; AND SCHIELE, M., 2011. Zivile Sicherheit: Abschlussbericht "Critical Parts - Simulation der Critical Parts". Technical report, German Aerospace Center, Institute for Air Transport and Airport Research.
- DFS, 2017. Luftverkehr in Deutschland - Mobilitätsbericht 2017. Technical report, DFS Deutsche Flugsicherung. <https://www.dfs.de/homepage/de/medien/publikationen/mobilitaetsbericht2017-web.pdf?cid=7m>.
- DIJKSTRA, E. W., 1959. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1, 1 (1959), 269–271. doi:10.1007/BF01386390.
- DISTEFANO, N. AND LEONARDI, S., 2014. Risk assessment procedure for civil airport. *International Journal for Traffic and Transport Engineering*, 4 (Mar. 2014). doi:10.7708/ijtte.2014.4(1).05.
- DOING BUSINESS, 2016. Getting electricity - Measuring reliability, prices and transparency. Technical report, The World Bank. <https://www.doingbusiness.org/content/dam/doingBusiness/media/Annual-Reports/English/DB16-Chapters/DB16-CS-GE.pdf>.

- 
- DPA, 2018. Nur Handgepäck dabei? Darum sollten Sie sich beim Boarding schnell anstellen. Merkur.de. <https://www.merkur.de/reise/fliegen-nur-mit-handgepaeck-zr-8422049.html>.
- DY LIACCO, T., 1967. The adaptive reliability control system. *IEEE Transactions on Power Apparatus and Systems*, PAS-86, 5 (May 1967), 517–531. doi:10.1109/tpas.1967.291728.
- ECKERT, C. AND KRAUSS, C., 2011. Sicherheit im Smart Grid: Herausforderungen und Handlungsempfehlungen. *Datenschutz und Datensicherheit - DuD*, 35, 8 (Aug. 2011), 535–541. doi:10.1007/s11623-011-0133-8.
- EFTIMOVA, E.; NELLINGER, C.; AND KOCH, T., 2024. Data-Driven Reconstruction of Processes From Pedestrian Trajectories. In *2024 Annual Modeling and Simulation Conference (ANNSIM)*, 1–13. IEEE. doi:10.23919/annsim61499.2024.10732881.
- EISAC, 2016. Analysis of the Cyber Attack on the Ukrainian Power Grid. Technical report, Electricity Information Sharing and Analysis Center. <https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf>.
- EISELIN, S., 2018. Warum Passagiere noch immer Schalter nutzen. Aerotelegraph.com. <https://www.aerotelegraph.com/check-in-warum-passagiere-noch-immer-schalter-nutzen>.
- EUROPEAN COMMISSION, 2006. Commission Decision of 28 March 2006 concerning the technical specification for interoperability relating to the control-command and signalling subsystem of the trans-European conventional rail system. Official Journal of the European Union. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:284:0001:0176:EN:PDF>.
- EUROPEAN COMMISSION, 2008a. COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32008L0114>.
- EUROPEAN COMMISSION, 2008b. REGULATION (EC) No 300/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Official Journal of the European Union. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:284:0001:0176:EN:PDF>.
- EUROPEAN COMMISSION, 2013. On a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure.
- EUROPEAN COMMISSION, 2015. Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R1998>.
- EUROPEAN COMMISSION, 2017. Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and

their oversight. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0373>.

EUROPEAN COMMISSION, 2019. Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures. Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R1583>.

EUROPEAN COMMISSION, 2022. DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=en>.

EUROPEAN COMMISSION, D. G. E. R. P., 2011. Cities of tomorrow - Challenges, visions, ways forward. Technical report, European Union. doi:10.2776/41803. [http://ec.europa.eu/regional\\_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow\\_final.pdf](http://ec.europa.eu/regional_policy/sources/docgener/studies/pdf/citiesoftomorrow/citiesoftomorrow_final.pdf).

EUROPEAN UNION AVIATION SAFETY AGENCY, 2023. Easy Access Rules for the Basic Regulation (Regulation (EU) 2018/1139). Technical report, European Union Aviation Safety Agency. <https://www.easa.europa.eu/en/downloads/107247/en>.

FEDERAL AVIATION ADMINISTRATION, 2010. Technical Guidance for Evaluating Selected Solar Technologies on Airports. Technical report, Federal Aviation Administration. <https://www.faa.gov/sites/faa.gov/files/airports/environmental/FAA-Airport-Solar-Guide-2018.pdf>.

FEDERAL AVIATION ADMINISTRATION, 2018. Advisory circular 150/5360-13 - planning and design guidelines for airport terminal facilities. Technical report, Federal Aviation Administration. [https://www.faa.gov/documentLibrary/media/Advisory\\_Circular/AC-150-5360-13A-Airport-Terminal-Planning.pdf](https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC-150-5360-13A-Airport-Terminal-Planning.pdf).

FINK, L. H. AND CARLSEN, K., 1978. Operating under stress and strain [electrical power systems control under emergency conditions]. *IEEE Spectrum*, 15, 3 (1978), 48–53. doi:10.1109/MSPEC.1978.6369445.

FLOYD, R. W., 1962. Algorithm 97: Shortest path. *Communications of the ACM*, 5, 6 (Jun. 1962), 345–345. doi:10.1145/367766.368168.

FRANKE, K.; STÜRMER, J. M.; AND KOCH, T., 2023. Automated Simulation and Virtual Reality Coupling for Interactive Digital Twins. In *2023 Winter Simulation Conference (WSC)*, 2615–2626. IEEE. doi:10.1109/wsc60868.2023.10407185.

FREEMAN, L. C., 1977. A Set of Measures of Centrality Based on Betweenness. *Sociometry*, 40, 1 (1977), 35–41. doi:10.2307/3033543. <http://www.jstor.org/stable/3033543>.

GEISBERGER, E.; BROY, M.; CENGARLE, M. V.; KEIL, P.; NIEHAUS, J.; THIEL, C.; AND THÖNNISSEN-FRIES, H.-J., 2015. *Living in a networked world. Integrated research agenda*

---

*Cyber-Physical Systems (agendaCPS)*. acatech - NATIONAL ACADEMY OF SCIENCE AND ENGINEERING.

GHASEMI, M.; SEIDKHANI, H.; TAMIMI, F.; RAHGOZAR, M.; AND MASOUDI-NEJAD, A., 2014. Centrality measures in biological networks. *Current Bioinformatics*, 9, 4 (Aug. 2014), 426–441. doi:10.2174/15748936113086660013.

GRAINGER, J. J. AND STEVENSON JR., W. D., 1994. *Power System Analysis*. Electrical and Computer Engineering. McGraw-Hill Education, 1st edn.

GUERRA, L.; MURINO, T.; AND ROMANO, E., 2008. Airport risk assessment: a probabilistic approach. *International Journal of Systems Applications, Engineering & Development*, 2, 2 (01 2008), 359–369.

HAASE, C. AND KIEFER, S., 2016. The complexity of the kth largest subset problem and related problems. *Information Processing Letters*, 116, 2 (Feb. 2016), 111–115. doi:10.1016/j.ipl.2015.09.015.

HAGBERG, A. A.; SCHULT, D. A.; AND SWART, P. J., 2008. Exploring network structure, dynamics, and function using networkx. In *Proceedings of the 7th Python in Science Conference*, 11–15. SciPy. doi:10.25080/tcww9851.

HAGE, P. AND HARARY, F., 1995. Eccentricity and centrality in networks. *Social Networks*, 17, 1 (Jan. 1995), 57–63. doi:10.1016/0378-8733(94)00248-9.

HAMZEH, M.; KARIMI, H.; AND MOKHTARI, H., 2012. A New Control Strategy for a Multi-Bus MV Microgrid Under Unbalanced Conditions. *IEEE Transactions on Power Systems*, 27, 4 (Nov 2012), 2225–2232. doi:10.1109/TPWRS.2012.2193906.

HANCOCK, D., 2003. Virus Disrupts Train Signals. The Associated Press. <https://www.cbsnews.com/news/virus-disrupts-train-signals/>.

HATZIARGYRIOU, N.; ASANO, H.; IRAVANI, R.; AND MARNAY, C., 2007. Microgrids. *IEEE Power and Energy Magazine*, 5, 4 (Jul. 2007), 78–94. doi:10.1109/mpae.2007.376583.

HERMANN, M.; PENTEK, T.; AND OTTO, B., 2016. Design Principles for Industrie 4.0 Scenarios. In *49th Hawaii International Conference on System Sciences (HICSS)*. IEEE. doi:10.1109/HICSS.2016.488.

HIDDEN, A., 1989. Investigation into the Clapham Junction Railway Accident. Technical report, Department of Transport, London. [https://www.railwaysarchive.co.uk/documents/DoT\\_Hidden001.pdf](https://www.railwaysarchive.co.uk/documents/DoT_Hidden001.pdf).

HOLLNAGEL, E., 1996. Reliability analysis and operator modelling. *Reliability Engineering & System Safety*, 52, 3 (1996), 327–337. doi:https://doi.org/10.1016/0951-8320(95)00143-3. <https://www.sciencedirect.com/science/article/pii/S0951832095001433>.

IBERIA, 2024. Zeitvorgaben. <https://www.iberia.com/de/annahme-schlusszeiten/>.

- 
- ILIĆ, M. D. AND ZABORSKY, J., 2000. *Dynamics and Control of Large Electric Power Systems*. Wiley Interscience. ISBN 978-0471298588.
- INTERGOVERNMENTAL PANEL ON CLIMATE CHANGE, 2022. Climate Change 2022 - Impacts, Adaption and Vulnerability. Technical report, IPCC. [https://www.ipcc.ch/report/ar6/wg2/downloads/report/IPCC\\_AR6\\_WGII\\_FinalDraft\\_FullReport.pdf](https://www.ipcc.ch/report/ar6/wg2/downloads/report/IPCC_AR6_WGII_FinalDraft_FullReport.pdf).
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 1983. Doc 9137 - Airport Services Manual - Part 8: Airport Operational Services. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 1991. Doc 9137 - Airport Services Manual, Part 7: Airport Emergency Planning. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2006. Doc 7300 - Convention on International Aviation. Technical report, ICAO. [https://www.icao.int/publications/Documents/7300\\_cons.pdf](https://www.icao.int/publications/Documents/7300_cons.pdf).
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2011. Annex 17 - Security. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2012. Doc 9859 - Safety Management Manual (SMM). Technical report, ICAO. [https://www.icao.int/SAM/Documents/RST-SMSSP-13/SMM\\_3rd\\_Ed\\_Advance.pdf](https://www.icao.int/SAM/Documents/RST-SMSSP-13/SMM_3rd_Ed_Advance.pdf).
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2017. Doc 9157 - Aerodrome Design Manual, Part 5: Electrical Systems. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2018. Annex 14 - Aerodromes, Volume I - Aerodrome Design and Operations. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2020. Doc 8973 - Aviation Security Manual. Technical report, ICAO.
- INTERNATIONAL CIVIL AVIATION ORGANIZATION, 2022. Annex 9 - Facilitation. Technical report.
- JIN, S.; LIU, Q.; ZHANG, W.; HE, Z.; HE, Y.; ZHANG, L.; LIU, Y.; XU, P.; ZHANG, X.; AND HE, Y., 2023. Data-driven methods for situation awareness and operational adjustment of sustainable energy integration into power systems. *Frontiers in Energy Research*, 11 (Aug. 2023). doi:10.3389/fenrg.2023.1253206.
- JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2012. Information Security - Guide for Conducting Risk Assessments. Technical Report 800-30, National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.
- JOYCE, K. E.; LAURIENTI, P. J.; BURDETTE, J. H.; AND HAYASAKA, S., 2010. A New Measure of Centrality for Brain Networks. *PLOS ONE*, 5, 8 (08 2010), 1–13. doi:10.1371/journal.pone.0012200. <https://doi.org/10.1371/journal.pone.0012200>.

- 
- KACHLÍKOVÁ, M., 2011. Selbstbedienung bei Passkontrolle - neues E-Gate auf Prager Flughafen. Radio Prague International. <https://deutsch.radio.cz/selbstbedienung-bei-passkontrolle-neues-e-gate-auf-prager-flughafen-8557865>.
- KANKI, B. G., 2018. Chapter 2 - Cognitive functions and human error. In *Space Safety and Human Performance* (Eds. T. SGOBBA; B. KANKI; J.-F. CLERVOY; AND G. M. SANDAL), 17–52. Butterworth-Heinemann. ISBN 978-0-08-101869-9. doi:10.1016/B978-0-08-101869-9.00002-9. <https://www.sciencedirect.com/science/article/pii/B9780081018699000029>.
- KAPPENMAN, J. G. AND ZANETTI, L. J. AND RADASKY, W. A., 1997. Geomagnetic storms can threaten electric power grids. *Earth in Space*, 9, 7 (Mar. 1997), 9,11.
- KARABASZ, I.; LOUVEN, S.; AND KERKMANN, C., 2017. Germans don't WannaCry. <https://global.handelsblatt.com/companies/germans-dont-wannacry-765291>.
- KEAN, T. H.; HAMILTON, L. H.; BEN-VENISTE, R.; KERREY, B.; FIELDING, F. F.; LEHMAN, J. F.; GORELICK, J. S.; ROEMER, T. J.; GORTON, S.; AND THOMPSON, J. R., 2004. The 9/11 Commission Report. Technical report, 9/11 Commission. <https://www.9-11commission.gov/report/911Report.pdf>.
- KEPHART, JEFFREY O. AND WHITE, STEVE R., 1993. Measuring and Modeling Computer Virus Prevalences. In *IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE. doi:10.1109/RISP.1993.287647.
- KESLER, B., 2011. The Vulnerability of Nuclear Facilities to Cyber Attack. Technical report, Strategic Insights. [http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-l1\\_Kesler.pdf](http://large.stanford.edu/courses/2017/ph241/bunner2/docs/SI-v10-l1_Kesler.pdf).
- KLEINMEIER, B.; ZÖNNCHEN, B.; GÖDEL, M.; AND KÖSTER, G., 2019. Vadere: An open-source simulation framework to promote interdisciplinary understanding. *Collective Dynamics*, 4 (Sep. 2019). doi:10.17815/cd.2019.21.
- KLM ROYAL DUTCH AIRLINES, 2024. Boarding times. <https://www.klm.at/information/airport/boarding-times>.
- KNEIDL, A., 2013. *Methoden zur Abbildung menschlichen Navigationsverhaltens bei der Modellierung von Fußgängerströmen*. Ph.D. thesis, Technische Universität München. <https://mediatum.ub.tum.de/1131501>.
- KOCH, T., 2025. Risk and impact analysis for blackouts at airports. doi:10.5281/ZENODO.14628507.
- KOCH, T.; BONARI, J.; VON DANWITZ, M.; AND POPP, A., 2024. Automatic Generation of Simulation Models for Digital Twins from State-of-the-Art Simulation Frameworks. In *2024 28th International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*. doi:10.1109/DS-RT62209.2024.00031.

- 
- KOCH, T.; DEUTSCHMANN, A.; AND MÖLLER, D. P. F., 2019a. Using process-oriented-grouping and linear algebra to optimize resource management. In *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE. doi:10.1109/icnsurv.2019.8735110.
- KOCH, T.; MÖLLER, D. P. F.; AND DEUTSCHMANN, A., 2017. Model-based airport security analysis in case of blackouts or cyber-attacks. In *16th IEEE Conference on Electro Information Technology*. doi:10.1109/EIT.2017.8053346.
- KOCH, T.; MÖLLER, D. P. F.; AND DEUTSCHMANN, A., 2018. A Python-based Simulation Software for monitoring the Operability State of Critical Infrastructures under Emergency Conditions. In *17th IEEE Conference on Electro Information Technology*. doi:10.1109/EIT.2018.8500219.
- KOCH, T.; MÖLLER, D. P. F.; AND DEUTSCHMANN, A., 2019b. *Smart Technologies as a Thread for Critical Infrastructures*, 275–289. Springer Singapore. ISBN 9789811371394. doi:10.1007/978-981-13-7139-4\_21. <https://api.semanticscholar.org/CorpusID:203327138>.
- KOTHARI, D. AND NAGRATH, I., 2003. *Modern Power System Analysis*. Tata McGraw-Hill Publishing Company. ISBN 9780070494893. <https://books.google.de/books?id=zfxQFM3RkkEC>.
- KRUSE, J.; SCHÄFER, B.; AND WITTHAUT, D., 2021. Revealing drivers and risks for power grid frequency stability with explainable AI. *Patterns*, 2, 11 (Nov. 2021), 100365. doi:10.1016/j.patter.2021.100365.
- LAMBERT, L. AND ADLER, L., 2014. Fitch cuts puerto rico electricity authority's rating again. <https://www.reuters.com/article/usa-puertorico-electricity/update-1-fitch-cuts-puerto-rico-electricity-authoritys-rating-again-idUSL2N0OS1PS20140611>.
- LAWRENCE, R. D.; HONG, S. J.; AND CHERRIER, J., 2003. Passenger-based predictive modeling of airline no-show rates. In *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD03. ACM. doi:10.1145/956750.956796.
- LEVESON, N. G., 2012. *Engineering a Safer World Systems Thinking Applied to Safety*. The MIT Press. ISBN 9780262298247. doi:10.7551/mitpress/8179.001.0001. <https://doi.org/10.7551/mitpress/8179.001.0001>.
- LIM, B., 2014. Emerging Threats from Cyber Security in Aviation - Challenges and Mitigations. *Journal of Aviation Management*, (2014).
- LLOYD, A. L. AND VALEIKA, S., 2007. *Complex population dynamics: nonlinear modeling in ecology, epidemiology and genetics*, chap. Network Models In Epidemiology: An Overview. doi:10.1142/9789812771582\_0008.

- 
- LYKOU, G.; ANAGNOSTOPOULOU, A.; AND GRITZALIS, D., 2018. Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. *Sensors*, 19, 1 (Dec. 2018), 19. doi:10.3390/s19010019.
- LYKOU, G.; MOUSTAKAS, D.; AND GRITZALIS, D., 2020. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors*, 20, 12 (Jun. 2020), 3537. doi:10.3390/s20123537.
- MARTCHEVA, M., 2015. *An Introduction to Mathematical Epidemiology*, chap. Introduction to Epidemic Modeling, 9,31. Texts in Applied Mathematics. Springer. ISBN 978-1-4899-7612-3. doi:10.1007/978-1-4899-7612-3\_2.
- MCCARTHY, J. AND MAHONEY, W., 2013. SCADA Threats in the Modern Airport. *International Journal of Cyber Warfare and Terrorism*, 3 (2013). doi:10.4018/ijcwt.2013100104.
- MCDONALD, H., 2024. Major cyber attack disrupts holiday season flights at Japan Airlines . Euronews.com. <https://www.euronews.com/business/2024/12/26/major-cyber-attack-disrupts-holiday-season-flights-at-japan-airlines>.
- MCMILLAN, R., 2007. Two charged with hacking LA traffic lights. IDG News Service. <https://www.computerworld.com/article/2817827/two-charged-with-hacking-la-traffic-lights.html>.
- MENEZES, A. C.; CRIPPS, A.; BUSWELL, R. A.; AND BOUCLAGHEM, D., 2013. Benchmarking small power energy consumption in office buildings in the United Kingdom: A review of data published in CIBSE Guide F. *Building Services Engineering Research and Technology*, 34, 1 (2013), 73–86. doi:10.1177/0143624412465092.
- MENG, Q.; ZHONG, K.; AND SUN, M., 2023. Dynamic response analysis of airport pavement under impact loading. *Applied Sciences*, 13, 9 (May 2023), 5723. doi:10.3390/app13095723.
- MENTGES, A.; HALEKOTTE, L.; SCHNEIDER, M.; DEMMER, T.; AND LICHTHE, D., 2023. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, 96 (07 2023), 103893. doi:10.1016/j.ijdrr.2023.103893.
- MITRE CORPORATION, 2014. CAPEC-1000: Mechanism of Attack, Common Attack Pattern Enumeration and Classification. <https://capec.mitre.org/data/definitions/1000.html>.
- MOHAMMADPOUR, H. AND DASHTI, R., 2011. Localization of short circuit faults in transformers using harmonic analysis and pattern recognition. *APAP 2011 - Proceedings: 2011 International Conference on Advanced Power System Automation and Protection*, 2 (10 2011). doi:10.1109/APAP2011.6180735.
- MÖLLER, D. P. F., 2016. *Guide to Computing Fundamentals in Cyber-Physical Systems*. Springer Publ. doi:10.1007/978-3-319-25178-3.

- 
- MÖLLER, D. P. F. AND VAKILZADIAN, H., 2014. Ubiquitous Networks: Power Line Communication and Internet of Things in Smart Home Environments. In *IEEE International Conference on Electro/Information Technology*, 596–601. IEEE. doi:10.1109/EIT.2014.6871832.
- MORLEY, J.; WIDDICKS, K.; AND HAZAS, M., 2018. Digitalisation, energy and data demand: The impact of internet traffic on overall and peak electricity consumption. *Energy Research & Social Science*, 38 (2018). doi:10.1016/j.erss.2018.01.018.
- MURPHY, R. J.; SUKKARIEH, M.; HAASS, J.; AND HRILJIAC, P., 2015. Guidebook on Best Practices for Airport Cybersecurity. Technical Report 140, Airport Cooperative Research Program.
- NEUBAUER, K.; FLEET, D.; AND AYRES JR., M., 2015. A Guidebook for Safety Risk Management for Airports. Technical Report 131, Airport Cooperative Research Program.
- NIGGEMANN, O.; BISWAS, G.; S., K. J.; KHORASGANI, H.; VOLGMANN, S.; AND BUNTE, A., 2015. Data-Driven Monitoring of Cyber-Physical Systems Leveraging on Big Data and the Internet-of-Things for Diagnosis and Control. In *Proceedings of the 26th International Workshop on Principles of Diagnosis*. <https://ceur-ws.org/Vol-1507/dx15paper24.pdf>.
- ORTEGA ALBA, S. AND MANANA, M., 2016. Energy Research in Airports: A Review. *Energies*, 9, 5 (2016). doi:10.3390/en9050349. <https://www.mdpi.com/1996-1073/9/5/349>.
- PALENSKY, P. AND DIETRICH, D., 2011. Demand Side Management: Demand Response, Intelligent Energy Systems, and Smart Loads. *IEEE Transactions on Industrial Informatics*, 7, 3 (2011). doi:10.1109/TII.2011.2158841.
- PARTHA SARATHY, P. R., 2018. *Analysis and Optimization of Medium Voltage Line Voltage Regulators*. Master's thesis, Norwegian University of Science and Technology. <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2560795>.
- PELFREY, W. V., 2005. The cycle of preparedness: Establishing a framework to prepare for terrorist threats. *Journal of Homeland Security and Emergency Management*, 2 (Jan. 2005). doi:10.2202/1547-7355.1081.
- PETERS, L., 2025. Chaos at Spanish and Portuguese airports following mass power outage . AeroTime. <https://www.aerotime.aero/articles/breaking-chaos-at-spanish-and-portuguese-airports-following-mass-power-outage>.
- PETTERSEN GOULD, K. AND BIEDER, C., 2020. *Safety and Security: The Challenges of Bringing Them Together*, 1–8. Springer International Publishing, Cham. ISBN 978-3-030-47229-0. doi:10.1007/978-3-030-47229-0\_1.
- POUDYAL, S.; AKHTAR, Z.; DASGUPTA, D.; AND GUPTA, K. D., 2019. Malware analytics: Review of data mining, machine learning and big data perspectives. In *2019 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE. doi:10.1109/ssci44817.2019.9002996.

- 
- PRICE, J. C. AND FORREST, J. S., 2016. *The threat matrix*, 461–513. Elsevier. doi:10.1016/B978-0-12-804293-9.00011-4.
- PRICEWATERHOUSE COOPERS INTERNATIONAL, 2014. Managing cyber risks in an interconnected world - Key findings from The Global State of Information Security Survey 2015. Technical report, Pricewaterhouse Coopers International.
- PRIYADARSHINI, I., 2019. *Introduction on Cybersecurity*, chap. 1, 1–37. Wiley. ISBN 9781119488330. doi:10.1002/9781119488330.ch1.
- PYRGIES, J., 2019. The uavs threat to airport security: risk analysis and mitigation. *Journal of Airline and Airport Management*, 9, 2 (Oct. 2019), 63. doi:10.3926/jairm.127.
- RAISSI, M.; PERDIKARIS, P; AND KARNIADAKIS, G. E., 2017. Physics informed deep learning (part i): Data-driven solutions of nonlinear partial differential equations. doi:10.48550/ARXIV.1711.10561.
- REAMS, R., 1999. Hadamard inverses, square roots and products of almost semidefinite matrices. *Linear Algebra and its Applications*, 288 (1999), 35 – 43. doi:[https://doi.org/10.1016/S0024-3795\(98\)10162-3](https://doi.org/10.1016/S0024-3795(98)10162-3). <http://www.sciencedirect.com/science/article/pii/S0024379598101623>.
- REISEN-EXPERTEN.DE, 2022. Check-In und Vorabend-Check-In am Flughafen Köln/Bonn. Online. <https://www.reisen-experten.de/reiseinformationen/flughafeninfos/flughafen-kolnbonn/check-in-682/>.
- SAYAMA, H., 2015. *Introduction to the modeling and analysis of complex systems*. Open SUNY Textbooks. ISBN 9781942341062. <https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=233>.
- SCHILDERS, W., 2008. *Introduction to Model Order Reduction*, 3–32. Springer Berlin Heidelberg. ISBN 9783540788416. doi:10.1007/978-3-540-78841-6\_1.
- SCHULTZ, M., 2010. *Entwicklung eines individuenbasierten Modells zur Abbildung des Bewegungsverhaltens von Passagieren im Flughafenterminal*. Ph.D. thesis, TU Dresden. <https://www.researchgate.net/publication/235926236>.
- SHIMBEL, A., 1953. Structural parameters of communication networks. *The bulletin of mathematical biophysics*, 15, 4 (Dec 1953), 501–507. doi:10.1007/BF02476438. <https://doi.org/10.1007/BF02476438>.
- SHIREY, R., 2000. *Internet Security Glossary*. doi:10.17487/RFC2828.
- SIEMENS, 2018. Resilient by design: Enhanced reliability and resiliency for puerto rico's electric grid. Technical report, Siemens. <https://assets.new.siemens.com/siemens/assets/public/1532100326.ece862442ca24d0cfce7ff0a9a0f94ac1b3cb9de.puertoricoresiliency-wp-fprint.pdf>.

- 
- SPRIGGS, J., 2002. Airport risk assessment: Examples, models and mitigations. In *Components of System Safety*, 183–195. Springer London, London. doi:10.1007/978-1-4471-0173-4\_11.
- STACHOWIAK, H., 2012. *Allgemeine Modelltheorie*. Springer Vienna. ISBN 9783709183281. <https://books.google.de/books?id=cjPxnQEACAAJ>.
- STAMP, J.; MCINTYRE, A.; AND RICARDSON, B., 2009a. Reliability Impacts from Cyber Attack on Electric Power Systems. In *2009 IEEE/PES Power Systems Conference and Exposition*, 1–8. IEEE. doi:10.1109/PSCE.2009.4840054.
- STAMP, J. E.; LAVIOLETTE, R. A.; PHILLIPS, L. R.; AND RICHARDSON, B. T., 2009b. Final Report: Impacts Analysis for Cyber Attack on Electric Power Systems (National SCADA Test Bed FY08). Technical report, Sandia National Laboratories. doi:10.2172/983693.
- STORY, R., 2013. Folium - A Python visualization package. Github. <https://github.com/python-visualization/folium>.
- STÜRMER, J. M.; GRAUMANN, M.; AND KOCH, T., 2023. Demonstrating Automated Generation of Simulation Models from Engineering Diagrams. In *2023 International Conference on Machine Learning and Applications (ICMLA)*, 1156–1162. IEEE. doi:10.1109/icmla58977.2023.00173.
- SURESH, V.; KACZOROWSKA, D.; JANIK, P.; AND REZMER, J., 2019. Load Flow Analysis in local microgrid with storage. *Przegląd Elektrotechniczny*, 1, 9 (Sep. 2019), 100–104. doi:10.15199/48.2019.09.19.
- TAGESSCHAU.DE, 2018. Am Flughafen Hamburg geht nichts mehr. <https://www.tagesschau.de/inland/flughafen-hamburg-stromausfall-101.html>.
- THE ANYLOGIC COMPANY, 2024. AnyLogic. <https://www.anylogic.de/>.
- THE GUARDIAN, 2011. Mass blackout hits california, arizona and mexico. <https://www.theguardian.com/world/2011/sep/09/blackout-california-arizona-mexico-san-diego>.
- TINNEY, W. F. AND HART, C. E., 1967. Power Flow Solution by Newton's Method. *IEEE Transactions on Power Apparatus and Systems*, (1967). doi:10.1109/TPAS.1967.291823.
- TRANSPORTATION RESEARCH BOARD AND NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, 2012. *Information Technology Systems at Airports—A Primer*. The National Academies Press, Washington, DC. doi:10.17226/14622. <https://nap.nationalacademies.org/catalog/14622/information-technology-systems-at-airports-a-primer>.
- URLAINIS, A.; SHOHEI, I.; LEVY, R.; ORNAI, D.; AND VILNAY, O., 2014. Damage in Critical Infrastructures Due to Natural and Man-made Extreme Events - A Critical Review. *Procedia Engineering*, 85 (12 2014). doi:10.1016/j.proeng.2014.10.580.

- 
- U.S. EIA, 2018. Annual Electric Power Industry Report. Technical report, U.S. Energy Information Administration. <https://www.eia.gov/todayinenergy/detail.php?id=35652>.
- U.S. GAO, 2004. Critical Infrastructure Protection - Challenges and Efforts to Secure Control Systems. Technical report, U.S. Government Accountability Office. <https://www.gao.gov/assets/gao-04-628t.pdf>.
- U.S. GAO, 2018. Critical Infrastructure Protection - Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption. Technical report. <https://www.gao.gov/assets/d18211.pdf>.
- USTUN, T. S.; OZANSOY, C.; AND ZAYEGH, A., 2011. Implementation of Dijkstra's algorithm in a dynamic microgrid for relay hierarchy detection. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE. doi:10.1109/smartgridcomm.2011.6102370.
- VON MEIER, A., 2006. *Electric Power Systems: A Conceptual Introduction*. Wiley. ISBN 9780470036426. doi:10.1002/0470036427.
- VOSKAKI, A.; BUDD, T.; AND MASON, K., 2023. The impact of climate hazards to airport systems: a synthesis of the implications and risk mitigation trends. *Transport Reviews*, 43, 4 (Jan. 2023), 652–675. doi:10.1080/01441647.2022.2163319.
- ŠIMKEVIČIŪTĖ, S., 2020. How the world's first cyber attack looked 200 years ago. NordVPN.com. <https://nordvpn.com/de/blog/semaphore-attack-mitm/>.
- WEIDMANN, ULRICH, 1992. Transporttechnik der Fußgänger: Transporttechnische Eigenschaften des Fußgängerverkehrs, Literaturlauswertung. Technical Report 90, ETH Zürich, Institut für Verkehrsplanung und Transporttechnik, Strassen- und Eisenbahnbau. doi:10.3929/ETHZ-A-000687810.
- WIDEMANN, M. AND MÖLLER, D. P. F., 2013. Using Model Pipelines to Simulate the Processes in and around an Airport through a Web-Interface. In *Proceedings of the 2013 Grand Challenges on Modeling and Simulation Conference, GCMS'13* (Toronto, Ontario, Canada, 2013). Society for Modeling & Simulation International, Vista, CA. doi:10.5555/2557668.2557693.
- WIKIPEDIA, 2022. List of battles and other violent events by death toll. [https://en.wikipedia.org/wiki/List\\_of\\_battles\\_and\\_other\\_violent\\_events\\_by\\_death\\_toll#Non-state\\_\(terrorist\)\\_attacks](https://en.wikipedia.org/wiki/List_of_battles_and_other_violent_events_by_death_toll#Non-state_(terrorist)_attacks).
- WILD, G.; MURRAY, J.; AND BAXTER, G., 2016. Exploring Civil Drone Accidents and Incidents to Help Prevent Potential Air Disasters. *Aerospace*, 3, 3 (Jul. 2016), 22. doi:10.3390/aerospace3030022.
- WINSBERG, E., 2003. Simulated Experiments: Methodology for a Virtual World. *Philosophy of Science*, 70, 1 (2003), 105–125. doi:10.1086/367872.

- 
- WITTE, J., 2018. Ursache für Stromausfall am Flughafen steht fest. WELT. <https://www.welt.de/regionales/hamburg/article176979597/Ursache-fuer-Stromausfall-am-Hamburger-Flughafen-steht-fest.html>.
- WORLD HEALTH ORGANIZATION, 2005. INTERNATIONAL HEALTH REGULATIONS. Technical report, World Health Organization. <https://iris.who.int/bitstream/handle/10665/246107/9789241580496-eng.pdf?sequence=1>.
- WXPYTHON, 2022. wxpython - the gui toolkit for python. <https://wxpython.org/>.
- YUNWEI LI; VILATHGAMUWA, D. M.; AND POH CHIANG LOH, 2004. Design, analysis, and real-time testing of a controller for multibus microgrid system. *IEEE Transactions on Power Electronics*, 19, 5 (Sep. 2004), 1195–1204. doi:10.1109/TPEL.2004.833456.
- YUSUFE, A. A.; MOSETLHE, T. C.; AND AYODELE, T. R., 2021. Allocation of active power losses to generators in electric power networks. *International Journal of Emerging Electric Power Systems*, 23, 1 (Apr. 2021), 73–88. doi:10.1515/ijeeps-2021-0014.
- ZABORSZKY, J.; PRASAD, K.; AND WHANG, K.-w., 1980. Operation of the Large Interconnected Power System by Decision and Control. *IEEE Transactions on Power Apparatus and Systems*, PAS-99, 1 (1980), 37–45. doi:10.1109/TPAS.1980.319606.
- ZHOU, J.; AYHAN, B.; KWAN, C.; D. LIMAYE, O.; AND LEE, W., 2011. Locating short-circuit faults in underground networks. 1–7. doi:10.1109/IAS.2011.6074404.
- ZIMMERMAN, R. D. AND MURILLO-SÁNCHEZ, C. E., 2024. MATPOWER User's Manual - Version 8.0. Technical report, Power Systems Engineering Research Center (PSerc). <https://matpower.org/docs/MATPOWER-manual-8.0.pdf>.
- ZIMMERMAN, R. D.; MURILLO-SÁNCHEZ, C. E.; AND THOMAS, R. J., 2011. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Transactions on Power Systems*, 26, 1 (2011), 12–19. doi:10.1109/TPWRS.2010.2051168.
- ZOLI, C.; STEINBERG, L. J.; GRABOWSKI, M.; AND HERMANN, M., 2018. Terrorist critical infrastructures, organizational capacity and security risk. *Safety Science*, (Jun. 2018). doi:10.1016/j.ssci.2018.05.021. <http://www.sciencedirect.com/science/article/pii/S0925753517305994>.



---

# Danksagung

---

Seit ich das Buch Blackout von Marc Elsberg gelesen habe, hat mich die Fragestellung, wie die tatsächlichen Auswirkungen eines solchen Stromausfalls auf die Gesellschaft aussehen würden, fasziniert. Mich freut es daher, dass ich mich am Deutschen Zentrum für Luft- und Raumfahrt mit dem Thema auseinandersetzen konnte und hoffe, dass meine Arbeit dabei hilft, unsere Infrastruktur zukünftig sicherer zu machen.

Dafür danke ich insbesondere Prof. Dr. rer. nat. Andreas Deutschmann, der mir die Arbeit an diesem wichtigen Thema ermöglicht und über die gesamte Dauer begleitet hat. Er hat mich auch in schwierigen Zeiten dazu motiviert die Arbeit zu finalisieren und damit, sowie mit zahlreichen inspirierenden Gesprächen, nachhaltig zur Fertigstellung beigetragen.

Zudem danke ich Prof. Dr.-Ing. Dietmar P. F. Möller, der meine Arbeit bis zu seinem wohlverdienten Ruhestand an der TU Clausthal betreut hat und mit vielen Impulsen zur Konzeption der Methodik beigetragen hat.

Mein aufrichtiger Dank gilt Univ.-Prof. Dr.-Ing. Alexander Popp, der zu einem späteren Zeitraum die Betreuung der Arbeit übernommen hat und ohne dessen Motivation die Fertigstellung dieser Arbeit unmöglich gewesen wäre. Ich danke ihm, dass er mir diesen Neustart ermöglicht und durch regelmäßige Gespräche und konstruktives Feedback maßgeblich zu dieser Arbeit beigetragen hat.

Ebenso danke ich meinen ehemaligen Bürokollegen Andrei Popa und Lukas Asmer, die stets für eine gute Arbeitsatmosphäre gesorgt haben und durch inspirierende Gespräche zur Konzeption der Methoden beigetragen haben. Im Rahmen ihrer Werkstudententätigkeit und zweier Abschlussarbeiten hat Lisa-Marie Brause maßgeblich zur Datenerhebung im Rahmen der Risikoanalyse und Implementierung Teile dieser Arbeit beigetragen, wofür ich ihr meinen aufrichtigen Dank aussprechen möchte.

Abschließend danke ich meiner Familie und meiner Freundin, die mich während der gesamten Zeit unterstützt und es mir damit ermöglicht haben die notwendige Zeit für die Anfertigung der Dissertation zu finden.