13th International Defense and Homeland Security Simulation Workshop
20th International Multidisciplinary Modeling & Simulation Multiconference

2724-0363 © 2023 The Authors.
doi: xx.xxxx/xxxx

Container terminal simulation for vulnerability assessment

Stefanie Gote[1,*], Alexander Gabriel[1] and Frank Sill Torres[1]

[1]German Aerospace Center - Institute for the Protection of Maritime Infrastructure, Fischkai 1, Bremerhaven, 27572, Germany

[*]Corresponding author. Email address: stefanie.gote@dlr.de

Abstract

Threat and risk scenarios, which could led to disruptions at ports, are manifold. To understand the behavior of the port under disruptions, simulations are used by port operators and researchers. This leads to the need of a simulation of the container terminal which could include disruptions and look at process performance for a vulnerability assessment. The paper describes this development of a port simulation for the flexible integration of disruptions. First, a graphical process model is established, the main processes of the process model are transferred into a simulation model and then the influence from disruptions in sub-processes on the main process are examined. The consideration of disruptions in the main and sub-processes, leads to a variety of multilayered models. To reduce complexity and for more transparency and overview, a concentration on single scenarios is expedient. The paper provides first insight in how the models could be designed.

Keywords: container terminal; port simulation; port disruption; process modelling

1. Introduction

There are manifold threat and risk scenarios, which could led to disruptions at ports. For climate changes there are for example rising water levels and earthquakes. To understand the behavior of the port under disruptions, simulations are used by port operators and researchers.

An example for the impact on a port through disruption is the fictive scenario described in the Cyber Risk Management (CyRiM) project. The project CyRiM project show the great impact of a small attack on the complete supply chain. Hackers attack a ship management company and get access to the system. They infiltrate a cargo document with a virus. The company had not recognised the attack. With departure at the origin port, they send the documents to the next port. Someone in the port open the document, through the opening the virus goes into the port cargo management network. It scrambled the database of the container content. So the port is interrupted in the processes and have to manually verify the containers. To prevent a spreading of the virus as a cascade through the supply chain, the port shut down the system completely, because they cannot identify the document through which the virus came into the system. This shutdown takes several days. (Daffron et al., 2019)

Another example, where the shutdown of a port has a huge influence on the supply chain, is the shutdown of the Shezhen-Yantian port during the corona-pandemic. The shutdown leads to delays in the supply chain and supply bottlenecks, especially in the technology and electronics sector. (Wurzel, 2021)

These are two examples, where the disruption of a port, is followed by disruptions in the supply chain. Some disruptions result in a complete shutdown of the port or terminal, others only influence parts of the port or terminal. The impacts and cascading effects differ depending on the

Table 1. Threat and risk scenarios for wind parks

natural hazards	anthropogenic threat
storm tide	accidents and working accidents
flood/ wash of the waves	theft and wilful destruction
extreme weather	unauthorized access and sabotage
lightning	cyber-physical attacks
aging	terrorism
seaquake	...
...	

(Gabriel, 2023)

port or scenario. For the vulnerability assessment, the understanding of the ports behavior is essential and simulations of scenarios helps there. The goal of the paper is to describe the implementation of a simulation model for the vulnerability assessment, at the example of a container terminal. Whereby a focus was placed on the modeling of the disruptions.

The paper continues with description of actual scenarios and simulation. Then, in Section 3, an overview of the procedure and modelling methods is given. Afterwards, the implementation of the simulation is described. In Section 5, the results are discussed. Finally, an outlook for further use of the model is given.

2. Threat and risk scenarios in the port and how to simulate them for vulnerability assessment

In this section are first some threat and risk scenarios of the port described, then the past work on port simulations is reviewed and in the last part gives some examples for simulations in vulnerability and resilience assessment.

2.1. Threat and risk scenarios in the port

To get an overview over possible threat and risk scenarios the examples from wind farms listed in Table 1 were taken, as they could nearly all be transferred on ports. Seaquakes could be submitted trough earthquakes, as it happened for example in February at the port of Iskenderun (Paone, 2023). The earthquake led to fall over of the containers in the yard and through the destruction of the containers there started a fire in the container terminal (Paone, 2023).

In the introduction there were two scenarios described which lead to a complete shut down of the port for some time. When considering scenarios occurring through the climate change there are also scenarios which impact the performance of the port or terminal, but do not lead to a completely fail out. A scenario where the intensity could be varied is the rising of the water level. *Blanco Torell* (2022) used a flood simulations model to show the impacted areas in a port for two case studies. Depending on the rising level only small areas or nearly the complete port could be flooded.

2.2. Port simulation

There exist different simulation models of ports in general and container terminals (Dragović et al., 2017). Some models focus only on parts of the services, for example the rail terminal of a container terminal or the towage and pilote services (Caballini et al., 2012; Nikghadam et al., 2023; Sadeghi et al., 2021). Other models are more general reproductions of a port with a container terminal (Kotachi et al., 2013). The used methods and tools also differ. There are for example system dynamics methodology, discrete event simulation and multi-agent discrete event simulation (Caballini et al., 2012; Kotachi et al., 2013). Tools for the simulations were general programming languages like C, simulation languages like AweSim or simulation software like Powersim Studio (Hayuth et al., 1994; Demirci, 2003; Caballini et al., 2012). There are different simulation tools for ports and terminals on the market, for example from anylogic and Arena Simulation. The anylogic simulation uses a multi method approach to model business processes or make the container yard planning (anylogic, 2023). The Arena Simulation tool is a discrete event simulation (Rockwell Automation, 2023). Simulations pursue different goals, for example the comparison of alternative terminal layouts (Clausen et al., 2012) or to find an investment strategy for resource adding to relieve bottlenecks (Demirci, 2003). This shows the diversity of port simulations.

2.3. Examples for models in vulnerability and resilience assessment

Vulnerability could be described as the weakness for the disruption of the functionality (Lenz, 2009). An application for the vulnerability assessment in the maritime context is the use of a disruption simulation to show impacts of a port fail out for a shipping network and analyse the network vulnerability (Liu et al., 2022). *Macdonald et al.* (2018) show the importance of simulations for the supply chain resilience management, as it is used to study system behavior under disruptions. A supply chain is a complex system and some scenarios had not occurred yet, so the simulation helps to get a better understanding of the systems behavior (Macdonald et al., 2018). The port is also a complex system, sometimes modelled as system of systems (Caballini et al., 2012), so it could be assumed that simulation is there also an important tool for the resilience management. In another work the authors provide a framework for the assessment of port resilience with use of dependency analysis methodology for the system modelling and Bayesian networks for the modelling of the risk events (Smith et al., 2021). In a follow up work they apply the models on a case study of container terminal operation (Smith et al., 2022). *Bruzzone et al.* (2022) describe a simulator for different accidents and other scenarios in the port. Used scenarios are the spoil of material, e.g. oil, and the dispersion of gas (Bruzzone et al., 2022). The simulation includes impacts on port infrastructure and people in

the port and effects of countermeasures (Bruzzone et al., 2022).

As pointed out in the section before simulations for ports are different depending on the goal of the simulation. And the scenarios for disruptions are diverse. This paper should answer the question how to built a simulation for a vulnerability assessment at the example of a container terminal, with the focus on the disruptions of the processes.

3. From the process model under normal behavior to the behavior under disruptions

This section describes the procedure from a modelling of the normal processes to processes with disruptions. To show the functionality of a vulnerability assessment through the productivity, a simulation model is needed to calculate the productivity's for varying scenarios. As the vulnerability is used to measure functionality during disruptions, the scenarios for the simulation should be disruption events. The first step is the creation of business process models, to understand what happens in the port. The chosen notation for the process description is the Business Process Modeling and Notation (BPMN). Next step is bringing all the processes together in one model, to describe all connections for the simulation. This model of the system is then transferred into a simulation model. The simulation model is implemented in Python. The next step is to describe the impact disruptions from sub-processes have on the main process through the functional resonance analysis method (FRAM). FRAM is often used for the understanding of what happens during accidents in complex socio-technical systems (Hollnagel, 2012). For that it looks first at what goes right in the system and then why things went wrong (Hollnagel, 2012).

4. Implementation of a port simulation for vulnerability assessment

Section 4 first describes how the process productivity is used in the vulnerability assessment, then the building of the process model and the simulation model. In the last subsection it is described how sub-processes could be included in the process model.

4.1. Process productivity for vulnerability assessment

The functionality of a process is a statement how far the process fulfills the process task. A process is defined so that it always has an input (Herrmann and Fritz, 2016) and the fulfillment of a process could be described through the generated output. As the productivity degree describes how good a process task is fulfilled it could be used to make a statement about the functionality. (Gote, 2022) So the process productivity, needed for the calculation of the productivity degree, is part of the vulnerability assessment.

The main task of a container terminal is the transshipment of containers (Speer, 2017). That means that the processes of the container handling are main processes. To handle a container, there is always container handling equipment (CHE) used, which need a driver, when not automatic operating. The CHE and their drivers are the resources of the process, as shown in Figure 1. The container is the In- and Output of the process.

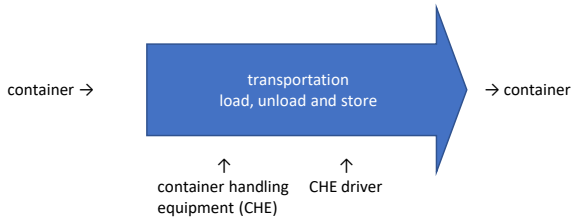

Figure 1. General process design (Gote, 2022)

The productivity of the CHE could be used for all processes. It is calculated trough the following equation

$$Productivity_{CHE} = \frac{number\ of\ cycles_{CHE}}{work\ time_{CHE}}. \quad (1)$$

A cycle starts with the pick up of the container, including the empty run to the container position, and finishes with the set down of the container when the connection to the CHE is released (Terminal Industry Committee 4.0, 2021a). The work time is the time for the cycle, this exclude times where for example the quay crane (QC) waits for a straddle carrier (SC) to bring a container (Gote, 2022).

4.2. Process model of a container terminal

The modelled terminal is an import-export terminal, which means that the focus is on the transshipment between ships and trains or trucks (Speer, 2017). The type of an import-export terminal was chosen with regard to the terminals in Bremerhaven and Hamburg. The container terminals in Bremerhaven and Hamburg are capable of handling the large deep-sea vessels (bremenports, 2023; Port of Hamburg, 2023). But there exists also feeder vessel traffic (bremenports, 2023). There are QCs for the load and unload from the ships, rail mounted gantry cranes (RMGs) for train load and unload and SC to store the containers and load and unload the trucks. The structure of the container terminal is shown in Figure 2. The main processes during the container handling are the load and unload of ships, trains and trucks, the transportation of the containers and the storage and take out of the yard (Carlo et al., 2013).

As starting point of the processes, the arriving of a ship, train, or truck is chosen. Then the containers are unload from the transport medium. Afterwards, new containers are loaded, while the unloaded containers are stored in the yard. The process for the movement of the containers are broke apart in several process steps. For example the ship unloading process in Figure 3 has four steps for the unloading of a container with the QC. The processes for

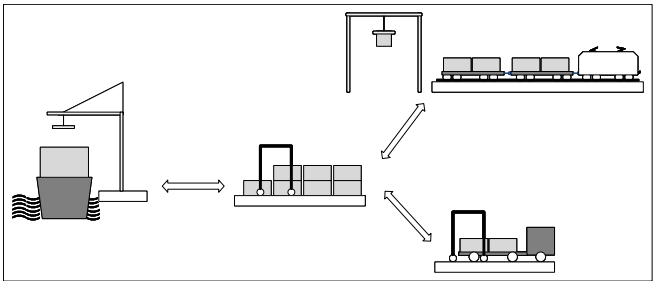

Figure 2. Design of the container terminal

the ships and trains are then extended, so that they start with the incoming of the arrival information and then go over the planning and the allocation of berth and rail to the arriving. The three processes for the different transportation modes are included into one model, as preparation for the simulation model.

As shown in Figure 1 the process steps for the movement of the containers require the resources CHE and driver. The arriving and departure of the workers, together with the starting of the CHE, are own processes which also have to be modelled. The shift start is an own process part. With start of the shift the drivers arrive and start there CHE, which is then ready for work (compare Figure 4). The CHE with the driver is then in the status idle, which is defined as the status where the CHE is on and not receiving or executing any order (Terminal Industry Committee 4.0, 2021b). The idle CHE waits to get an order to start moving a container. After the container is moved, the CHE goes back in the idle status or when the shift ends the driver turns off the CHE and leaves work.

4.3. From the process model to the simulation

The next step is the transfer from the process model into a simulation model. The goal of the simulation is to describe the behavior of the terminal with disruptions. To affect the general process described in Figure 1, there are two possibilities. The first option is that the resource CHE or CHE driver is not available for the process step, this leads to waiting time. The second option is, that the process steps needs more time, for example the QC has to slow down because of the weather conditions. The model is created with Python. To set up a simulation environment, the SimPy package is used. The simulation environment provides a simulation time and control the runtime of the simulation (SimPy, 2023). Furthermore, it provides classes for events and with this definition the possibility to let a process wait for a certain time (SimPy, 2023). The load and unload processes are mainly executed in the class *order* with subclasses for all three transport modes, ship, train, and truck. The process steps, like "QC moves to pick up position", "QC take up ct" and "remove twistlocks" (compare Figure 3), are summarized and described as one timeout in the function. The main focus of the function is the resource allocation. To create a disruption, it is important to have the possibility of varying the number of CHE and the CHE drivers. To reach that, there is one list for every CHE and one for there drivers. This lists are connected into one list in the class *shift*. The connected list is called *idle CHE* and from this list the elements are taken for use in the order processes. When the process finishes the resources are put back into the list. For a disruption, the resources could be transferred into another list, where the order working processes have no access. The simulation calculates the performance of the CHE for every hour. With the information about the performance it is possible to discover disruptions early. For that there are ranges defined (compare Figure 5). The first one describe the normal variation of the performance. If the performance is lower then this range, it is a signal that there is something happening. When the performance drops down significant, it is a failure. With the simulation, it is possible to forecast the performance. Signals for a disruptions and a drop down of the performance could be detected early and so with an early intervention the performance will drop less.

4.4. Disruption of container handling through subprocesses

Starting with the in subsection 4.2 described main processes, other processes are inserted to the model. The process of charging or refilling the SC for example has an direct impact on the functionality of the SC. So it is important that for example the fuel procurement is in time. During the charging or refilling process or when it runs out of energy the SC is not available for the container movement. That could lead to waiting times, when it happens during a peak time. Another example is the functionality of the terminal operating system (TOS). The processes needed for the functionality of the TOS are not looked at in detail. But when the TOS does not work, it had a huge impact on the main process. To demonstrate this, a FRAM model from the container handling, with focus on the TOS processes, is shown in Figure 6. The functions provided with support of the TOS are highlighted. To visualize the impact on the container handling functions, the control is highlighted with different colours. That shows that the control information from the TOS are needed for a majority of the functions.

An example, where the connection is not so directly given, is the payment of the workers. When the payment for example have often a delay, the motivation of the workers goes down and they work slower. This could be seen as impact in increasing process times.

5. Lessons learned from building the models

The creation of the process model, points out the importance of the resources CHE and CHE-Drivers for the container handling processes. Consequently, the numbers of CHE and CHE-Drivers are possible points for variations in the simulation as well as the time needed for a process

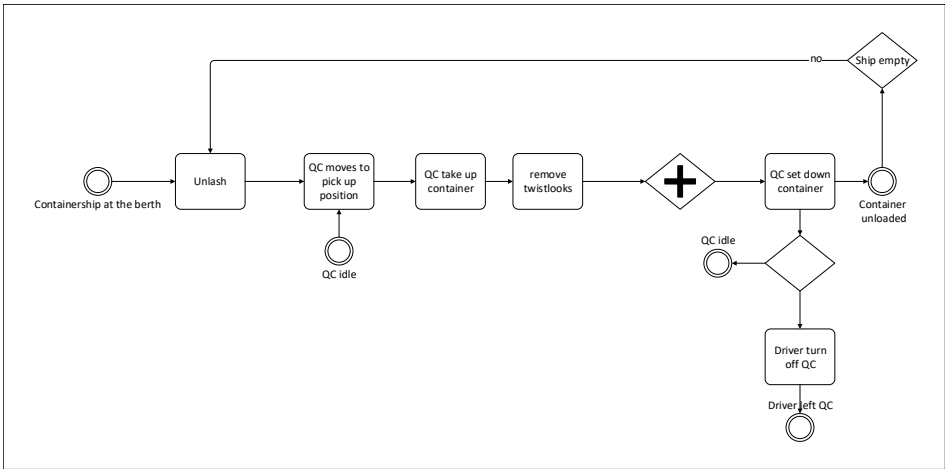

Figure 3. Cut out of the process container ship load.

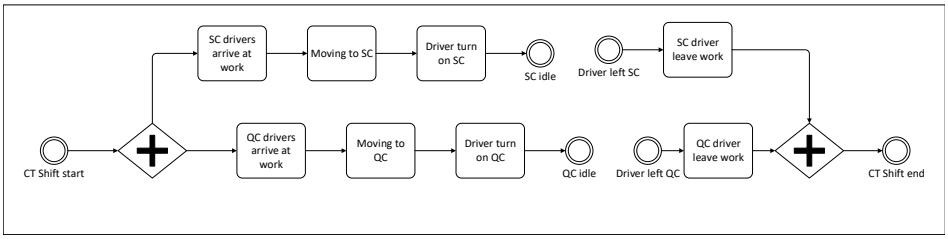

Figure 4. Cut out of the shift process.

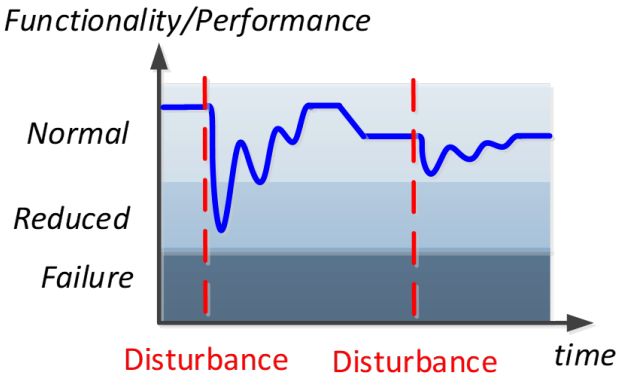

Figure 5. Relation between performance and resilience (Gabriel, 2023)

step. Including sub-processes with the FRAM to the process model shows that disruptions could all be modelled as waiting times, longer process times, or reduced number of resources. So the waiting time on resources is another important key performance indicator (KPI) for the performance of the terminal. The idea of a general model where all disruptions could be included get quite complex considering the sub-processes. The examples of the loading process of the SC and the FRAM model for the TOS have different risk and threat scenarios where the sub-processes get disrupted. Another point is that the influence on the main process parts differ widely. To reduce the complexity, scenarios could be simulated different with only taking into account the most relevant sub-processes.

As the container terminal is a complex system, the complexity has to be reduced. It depends on the user where the model goes more in detail. For the beginning, the model depth is so, that all changes of resources, like driver and container handling equipment (CHE), are modeled. With this modeling depth, an influence of the CHE on the productivity could be shown, but not which functionality of the CHE has the influence. It is for example possible to identify a straddle carrier as cause of a productivity decrease, but whether that occurs because the driver is tired or the SC need some repair cannot be said. If the user want to have a picture of the complete terminal, this depth is good to not get too much information. If it is important to get a deeper look at some parts of the process, this is also possible, as the simulation could be built up modular. The modularity of the simulation is created through the implementation in classes and functions. The modularity also allows the addition of other processes and also of other terminal parts or for example a lock with the lock processes.

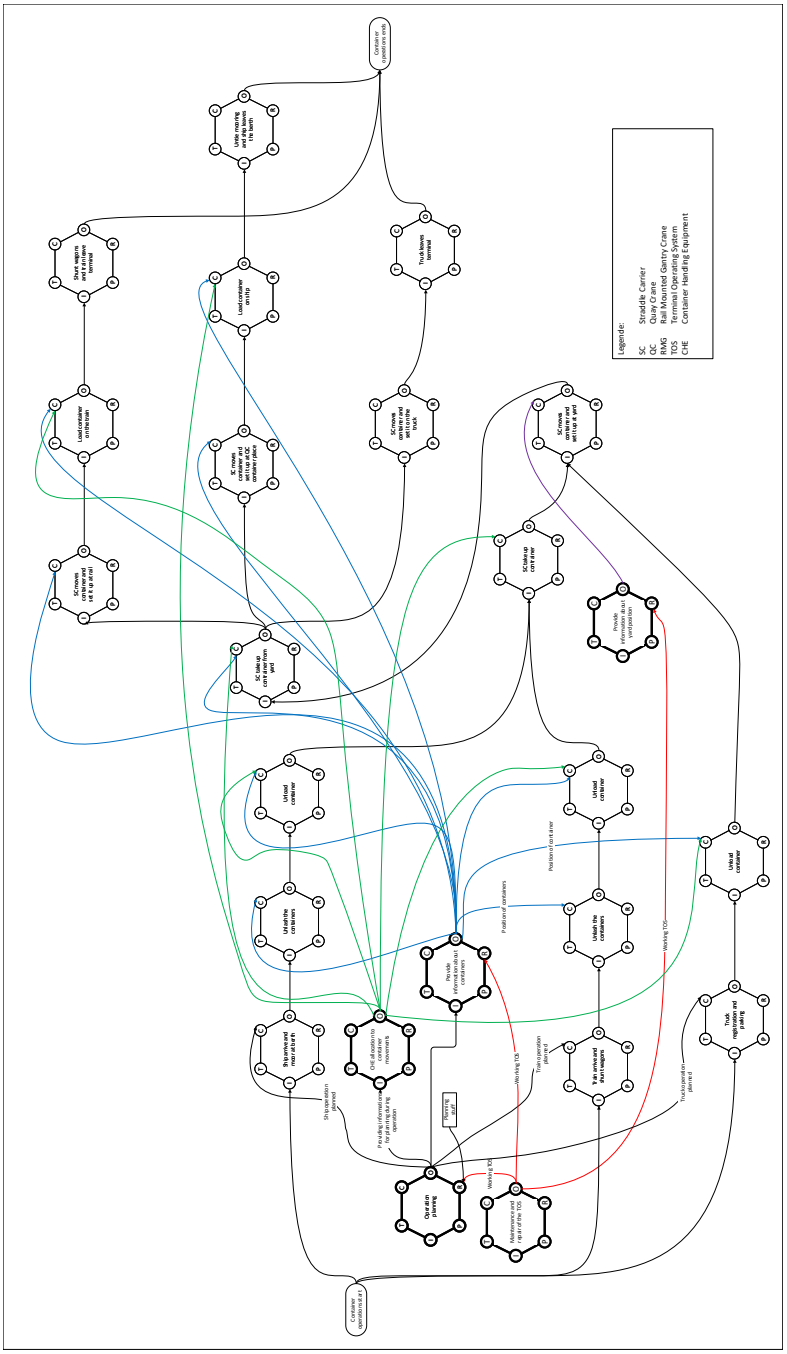

Figure 6. FRAM model of the container handling process with focus on the terminal operating system.

6. Conclusion

This paper showed first steps of building a simulation of a container terminal with disruptions for the vulnerability assessment.

The models have to be extended and the importance of different disruptions for the implementation have to be discussed with stakeholders, like terminal operators. A important next step is the validation of the models. For the normal behavior of the port there are average values in the literature. To collect more detailed information about the container terminal processes and behavior of the processes under disruption, terminal operators should be interviewed. For disruptions like accidents, there exist probabilities for the occurrence, which could be used. As the FRAM model show only, the connections of the processes regarding disruptions have to be transferred into the Python simulation. The described simulation from behavior under disruption is a starting point for a larger simulation model of the terminal and of a complete port with more then one terminal, e.g. a container and a ro-ro-terminal.

References

anylogic (2023). Port and Terminal Simulation Software.

Blanco Torell, A. E. (2022). Comparative Assessment of the Resilience of Harbors and Surrounding Regions against Water-related Hazards. Case Study: Durban & Bremerhaven. Bremerhaven.

bremenports (2023). A hub for goods flows from all over the world.

Bruzzone, A., Massei, M., Sinelshchikov, K., Giovannetti, A., Ferrari, R., de Paoli, A., Gadupuri, B., Reverberi, A., Fancello, G., Frosolini, M., Vairo, T., Piroddi, G., Gaborit, F., and Paoli, J. (2022). Innovative Virtual Lab for Improving Safety and Port Operations. In *Proceedings of the International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation, HMS*. CAL-TEK srl.

Caballini, C., Sacone, S., and Siri, S. (2012). The port as a system of systems: A System Dynamics simulation approach. In *Proceedings - 2012 7th International Conference on System of Systems Engineering, SoSE 2012*, pages 191–196.

Carlo, H. J., Vis, I. F. A., and Roodbergen, K. J. (2013). Seaside operations in container terminals: literature overview, trends, and research directions. *Flexible Services and Manufacturing Journal*, 27(2-3):224–262.

Clausen, U., Kaffka, J., and Meier, F. (2012). CONTSIM–Container Terminal Management with Simulation. *Procedia - Social and Behavioral Sciences*, 54:332–340. Proceedings of EWGT2012 - 15th Meeting of the EURO Working Group on Transportation, September 2012, Paris.

Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K., Leveretta, E., and Cambridge Centre for Risk Studies (2019). Shen attack: Cyber risk in Asia Pacific Ports. *CyRiM Report*.

Demirci, E. (2003). Simulation Modelling and Analysis of a Port Investment. *Simulation*, 79:94–105.

Dragović, B., Tzannatos, E., and Park, N. K. (2017). Simulation modelling in ports and container terminals: literature overview and analysis by research field, application area and tool. *Flexible Services and Manufacturing Journal*, 29(1):4–34.

Gabriel, A. (2023). Schutz maritimer Infrastrukturen. Bremerhaven, 19.06.2023.

Gote, S. (2022). Fuzzy-Logik basierte Methodik zur Vulnerabilitätsbewertung eines Containerterminals. Bremerhaven.

Hayuth, Y., Pollatschek, M. A., and Roll, Y. (1994). Building A Port Simulator. *SIMULATION*, 63(3):179–189.

Herrmann, J. and Fritz, H. (2016). *Qualitaätsmanagement Lehrbuch fur Studium und Praxis*. Hanser, Munchen.

Hollnagel, E. (2012). *FRAM, the frequency resonance analysis method*. Ashgate.

Kotachi, M., Rabadi, G., and Obeid, M. F. (2013). Simulation Modeling and Analysis of Complex Port Operations with Multimodal Transportation. *Procedia Computer Science*, 20:229–234. Complex Adaptive Systems.

Lenz, S. (2009). *Vulnerabilität Kritischer Infrastrukturen*. Bundesamt fur Bevölkerungsschutz und Katastrophenhilfe, Bonn.

Liu, X., Li, J., Yang, Y., and Xu, B. (2022). Vulnerability change of container shipping network on Maritime Silk Road under simulation disruption. In *2022 International Symposium on Sensing and Instrumentation in 5G and IoT Era (ISSI)*. IEEE.

Macdonald, J., Zobel, C., Melnyk, S., and Griffis, S. (2018). Supply chain risk and resilience: theory building through structured experiments and simulation. *International Journal of Production Research*, pages 1–19.

Nikghadam, S., Vanga, R., Rezaei, J., and Tavasszy, L. (2023). Cooperation between vessel service providers in ports: An impact analysis using simulation for the Port of Rotterdam. *Maritime Transport Research*, 4:100083.

Paone, A. (2023). Fire at Turkey's Iskenderun Port extinguished -defence ministry.

Port of Hamburg (2023). Germany's largest container port. https://www.hafen-hamburg.de/en/terminals/containerterminals.

Rockwell Automation (2023). Arena Simulation Software in Port & Terminal. https://www.rockwellautomation.com/en-us/products/software/arena-simulation/discrete-event-modeling/port-terminal.html.

Sadeghi, M., Bagheri, M., and Pishvaee, M. S. (2021). Evaluation of rail terminals in container ports using simulation: A case study. *SIMULATION*, 97(12):809–820.

SimPy (2023). Environments. https://simpy.readthedocs.io/en/latest/topical_ guides/environments.html.

Smith, Diaz, Shen, and Longo (2021). Conceptual devel-

opment of a probabilistic graphical framework for assessing port resilience. In *Proceedings of the 23rd International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation*. CAL-TEK srl.

Smith, K., Diaz, R., Shen, Y., and Longo, F. (2022). Definition and Detection of Hypervulnerabilities using a Framework for Assessing Port Resilience. In *Proceedings of the International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation, HMS*. CAL-TEK srl.

Speer, U. (2017). *Optimierung von automatischen Lagerkransystemen auf Containerterminals*. Springer Fachmedien Wiesbaden.

Terminal Industry Committee 4.0 (2021a). Cycle 2021.002. https://tic40.atlassian.net/wiki/spaces/TIC40Definitions/pages/444923978/Cycle 2021.002.

Terminal Industry Committee 4.0 (2021b). Idle. https://tic40.atlassian.net/wiki/spaces/TIC40Definitions/pages/37650433/Idle.

Wurzel, S. (2021). Belastung für Welthandel: Frachter stauen sich vor Südchina. *tagesschau.de*.