An Information Flow Modelling Approach for Critical Infrastructure Simulation

Denise Gall, Christian Luidold, Gregor Langner, Thomas Schaberreiter, Gerald Quirchmayr
Faculty of Computer Science,
University of Vienna
Vienna, Austria
email: denise.gall@univie.ac.at, christian.luidold@univie.ac.at, gregor.langner@univie.ac.at,
thomas.schaberreiter@univie.ac.at, gerald.quirchmayr@univie.ac.at

***Abstract*—Building a realistic environment for simulating cascading effects in critical infrastructures depends heavily on information received from experts, as well as on an accurate representation of processes and assets related to critical infrastructures. The approach introduced in this paper provides the conceptualization and implementation of an information flow model as a foundation for the subsequent development of a multi-layered risk model. The designed models represent both a process view, with the focus on procedures carried out by critical infrastructures, and a more technical object view, by defining objects and parameters representing assets and interactions. Starting with an analysis of relevant threats and affected infrastructures, use case scenarios are prepared in textual form and subsequently evaluated together with critical infrastructure representatives in end-user workshops. Based on the respective use case, a process view is established in form of an activity diagram including information flows, displaying processes of critical infrastructures during a threat. The activity diagram supports the evaluation and collection of information during subsequent end-user workshops with the aim to review and substantiate the model. The object diagram provides technical aspects of the use cases, for supporting the realization of a simulation and a corresponding risk model. The approach was developed in the context of a national research project for analyzing cascading effects in and between critical supply networks. The resulting diagrams demonstrate how cascading effects can be modelled in a structured form to support discussions with and between experts of critical infrastructures and emergency services, and how such models can serve as a foundation for subsequent simulation.**

Index Terms*—Information Flow Modelling; Critical Infrastructure; Infrastructure Simulation; Cascading Effects.

I. Introduction

In times of advanced automation in critical supply networks, critical infrastructures (CIs) need to be resilient against a multitude of threats in order to maintain public interests. Regarding the protection against threats against their own infrastructure, providers are in many cases well prepared. However, when facing cascading effects due to failures in other CIs due to intentional or unintentional causes, protection measures are harder to establish as possible cascading effects are often unknown. Therefore, it is an essential step to assist CI providers in identifying cascading failures in scenarios that are not part of the daily processes within the CI's own ecosystem, but pose relevant and potentially devastating threat scenarios. Historic examples underlining the gravity of cascading effects provide exceptional insights regarding the importance of resilience against external events, e.g., as shown in Oslo, Norway in 2007. This incident affected public transportation and underlying systems for around 20 hours. In addition, network systems were also affected by disruptions for around 10 hours and the central train station had to be evacuated due to a fire, triggered by a short circuit caused by a destroyed high-voltage cable [1].

In order to facilitate the mitigation of risks, an additional focus on the aspect of communication and collaboration among dependent CIs should be considered. Collaboration among CIs supports identifying dependencies between the infrastructures and thus enables them to prepare themselves specifically for impacts of cascading failures. Furthermore, sharing this information with external stakeholders like emergency services can lead to more efficient strategies for emergency services in case of large-scale incidents that require close coordination between first responders. An effective approach lies in the implementation of an adapted information flow model, which provides a framework that helps to organize how specific types of information are to be communicated.

In this paper, we present an approach for supporting CI providers and emergency services by creating an instantiated information flow model, composed of an activity diagram and an object diagram, based on a textual description of a threat scenario. The information flow model offers a new way to represent cascading effects of incidents in interdependent CIs in a structured form. The aim of this model is to facilitate discussions on the feasibility of cascading threat scenarios, and to encourage CI stakeholders to contribute to the shared knowledge represented by the information flow model. Simulations based on this shared understanding of threat scenarios will be able to optimize response to incidents based on those threat scenarios and help to coordinate first response with external actors like emergency services. In the context of CI networks, information flow does not only represent the digital information that is exchanged between CIs, but follows the broader definition of goods and services that are exchanged between infrastructures.

Our approach for information flow modelling is based on activity and object diagrams established from a textual description of a threat scenario. The information flow model includes an activity diagram for providing a process view and a technical view implemented by an object diagram, which provides a definition of objects and their parameters. The information sources utilized to derive the diagrams included multiple workshops with experts from CIs and emergency services. We evaluate the results in a case study derived from results carried out in the ongoing ODYSSEUS project [2].

Section II provides an overview of related work and the applied methodologies. The subsequent Section III describes the modelling approach including the modelling prerequisites, the activity and object diagram definitions, and iterative refinements of the models. In Section IV, we present a case study within the scope of the ODYSSEUS project [2] and evaluate the findings in Section V. Section VI provides a conclusion and an outlook on future work.

II. Related Work

The methodology used for the presented modelling approach was greatly influenced by the design-science methodology described by Hevner et al. [3], as well as initially by the Soft Systems Methodology (SSM) described by Checkland [4]. The design-science research methodology consists of seven guidelines, from which an in-depth understanding of a given design problem and potential solutions can be gained. We utilize the design-science principles to create a design artifact in the form of a conceptual information flow model. The refinement and evaluation of the resulting artifact is conducted by multiple workshops with experts applying the world cafe methodology [5] described below, as well as technical evaluations conducted by project partners for further refinement. The principles of design-science were applied in the iterative refinement of the modelling results in all phases of the process.

Regarding the execution and the results of the workshops, the adopted world cafe process consists of seven design principles, which offers the participants to share their expertise in small groups [5]:

1) Set the Context
2) Create Hospitable Space
3) Explore Questions that Matter
4) Encourage Everyone's Contribution
5) Connect Diverse Perspectives
6) Listen Together for Patterns and Insights
7) Share Collective Discoveries

In terms of information flow modelling, Kupfersberger et al. [6] propose an approach for defining a conceptual security-driven information flow model for international software integration projects that was evaluated in a case study regarding an EU cybersecurity project CS-AWARE [7]. The authors focus on the representation of internal processes, what relevant data is used and how the communication with other components is realized in order to derive the framework conditions of their model [6]. Considering the comparable environments between Kupfersberger et al. [6] and this work, a similar approach was chosen with a set of adaptions regarding a broader field of stakeholders, and the goal of creating a multi-layered risk model, as well as to satisfy the requirements mentioned above.

For establishing a model representing activities as well as information flows, a lot of available approaches exist, including UML (Unified Modeling Language) activity diagrams, Business Process Model and Notation (BPMN) or Data Flow Diagrams (DFD). In our context, activity diagrams based on BPMN [8] were identified as most suitable, since BPMN is an established standard for representing business processes and workflows, and is not restricted to a certain domain or organization. Additionally, BPMN is a suitable instrument for presenting processes to different user groups, and provides a notation for message flows between layers [9].

Regarding modelling a more technical view, UML class diagrams [10] were selected as this technique allows to develop a representation of objects and parameters. However, the model had to be slightly expanded to support information flows and to suit our domain by adding modelling entities for representing information flows including shared information.

III. Modelling Approach

Identifying dependencies and potential risks caused by cascading effects between CIs is a complex issue. CIs are in many cases highly dependent on the services provided by other CIs, and failures in both the physical and cyber systems of one CI may cause service disruptions or failures in other CIs. Another major concern for interdependency risks is caused by geographical proximity of CIs, since a catastrophic event in an area can cause major disruptions in CI services, with potentially high impacts on the population [11]. The model presented in this paper is specifically designed for dealing with such sophisticated multi-stakeholder domains by applying the design-science method [3] as well as the SSM [4]. These methodologies offer procedures and guidelines on how to retrieve information and model highly complex environments such as CIs and how to reveal unknown problematic issues.

Following the design-science method introduced by Hevner et al. [3], we pursue an iterative approach, including:

- Analyzing the modelling prerequisites, which includes defining threat scenarios in textual form, based on an analysis of possible threats affecting CI networks.
- Based on the previously defined use cases, activity diagrams are established including the most important information flows between CIs and emergency services.
- For obtaining a more technical view of the use cases, relevant objects and parameters necessary for simulation are identified and modelled in an object diagram.
- Both the activity diagram and the object diagram are further refined in multiple workshop settings, as described in Section III-D.

The goal of the modelling approach is to create a structured activity diagram from the textual threat scenarios, to be able to model cascading effects and message flows between CIs and emergency services. The model forms the foundation for later simulations of the critical networks and serve as a basis for CIs and emergency services to get more insights into cascading effects and their impacts.

A. Modelling Prerequisite

The basis for the modelling efforts described in this work are textually composed threat scenarios that describe procedures and cascading effects in CIs during threats. In order to create realistic scenarios, the first step is to gather more information on threats affecting CIs and their dependencies. Therefore, possible dangers in urban areas were analyzed by creating a catalog of various threats, based on static and dynamic sources dealing with disasters and emergencies. These data sources include the Swiss catalog of threats, disasters and emergencies [12], newspaper articles and reports from authorities and other relevant organizations, dealing with incidents and threats. The identified threats were evaluated in terms of likelihood and impact in combination with national and international historical data and current developments, which resulted in a first set of use case scenarios. The main categories of threats identified were social threats, natural disasters and technological threats, according to the Swiss catalog of threats, disasters and emergencies [12].

The first drafts of threat scenarios were validated and refined in a workshop with security and business continuity experts from multiple CIs. The workshop's goal was to receive as much information from end-users for establishing realistic use cases and for the subsequent modelling activity.

In line with the principles of the SSM [4], the end-user workshops were composed of a large variety of stakeholder groups, in order to be able to obtain their views and expertise, and to gain a holistic understanding of the dynamics caused by an incident as modelled by the threat scenarios.

In the context of the project, the main stakeholders are an interdependent network of CI providers and emergency services, who are an integral part of the threat scenarios in the incident response. They were deeply involved in establishing realistic threat scenarios, as the goal of the project is to support the stakeholders by providing simulations on cascading effects. Furthermore, security experts are part of the stakeholder group, as the introduced method allows to identify information flows and dependencies between CIs, in order to gain an additional perspective on the potential ramifications of cascading incidents. Similarly, simulation experts are part of the stakeholder group in order to ensure that the translation of real-world incidents into simulation is viable and realistic. Furthermore, the perspective of first responders is crucial in understanding the dynamics of large-scale cascading incidents. Therefore, the input of emergency services and other first responders as part of the stakeholder group is important

In order to facilitate information collection in end-user workshops, the SSM [4] offers an approach that supports gathering information from experts by enforcing participants to model a big picture of the domain. However, due to limited possibilities in the context of the project, the world cafe process [5] was chosen for data gathering from the stakeholder groups. In the context of the project, the setting of a world cafe offered every end-user the possibility to reveal their expertise and estimation of relevance for each defined event and the associated impacts.

The information gathered during the workshop was used as basis for the resulting updated textual description of the use cases, comprising threats, impacts and the threat response by individual CIs. An especially interesting area of discussion in those stakeholder groups are the cascading failures that affect more than one CI. While failures contained within their own infrastructures are usually well understood and managed, there is great potential in better understanding the dynamics of cascading failures affecting multiple CIs. CI operators rarely have the opportunity to discuss cascading effects in a broad multi-stakeholder set-up, leading to valuable information to be uncovered and incorporated into the threat scenarios and subsequent models.

B. Modelling Scenario Behavior in Activity Diagrams

The activity diagram presented in this section represents a process view of events, including cause and impact on dependent infrastructures, extracted from the textual description of the threat scenarios. This is an important basis for the subsequent scenario simulation, as it transforms all the events defined in textual form in the threat scenario description into structured sequences, including information flows between infrastructures.

Additionally, visual models facilitate the evaluation and adaptation of end-user provided content, since the visual representation and grouping of information facilitates comprehension of sequences of events and cause and impact relationships [13].

The transformation of textual information to the representation in the activity diagram starts by identifying all involved CIs and other relevant stakeholder assets, followed by the identification of tasks and activities that are performed by those assets during the threat scenario. Those tasks and activities that change the state of an asset during a threat scenario need to be considered for modelling. The identified activities are to be sorted logically and chronologically, as that may not be necessarily preset in textual form.

After identifying CIs and tasks, the most essential step of the process, identifying information flows according to activities, is conducted. These information flows are of such importance, as they affect other CIs' states due to cascading effects. For example, if there is an area-wide power outage, which may lead to traffic accidents due to failures in traffic lights, emergency services have to secure these accidents sites, which in turn affects the capacity of available emergency response units. In case of another emergency, there might be bottlenecks.

Identifying information flows between stakeholders includes thoroughly reading the given textual use case and extracting all information flows predefined in the description. Additionally, information flows can be identified by perusing every identified task and deepen the knowledge relating to each task by conducting background research or seek for additional input from the stakeholder group, as suggested by [6] and [1]. This is especially relevant in the case of cascading failures, where only the perspective of some elements of the failure chain has been initially captured, and additional input from potentially affected stakeholders is required. Other information flows may have been revealed by end-users intentionally or unintentionally during the conducted workshop. Once all information from the textual form is extracted, the actual model can be built.

In order to ensure the practical relevance of the constructed activity diagram, established notations, such as BPMN, were applied. BPMN allows to demonstrate process sequences within one layer as well as information exchange between different layers. For facilitating the activity diagram, a layered design is recommended, where one infrastructure is visualized by a pool corresponding to the BPMN standard. Within one pool, the sequence flow of processes is modelled for one infrastructure. Tasks can be either activities that do not impact other infrastructures, or activities that send information to other infrastructures. To emphasize the differentiation between the two forms of tasks, we suggest using different coloring, as presented in Figure 1.

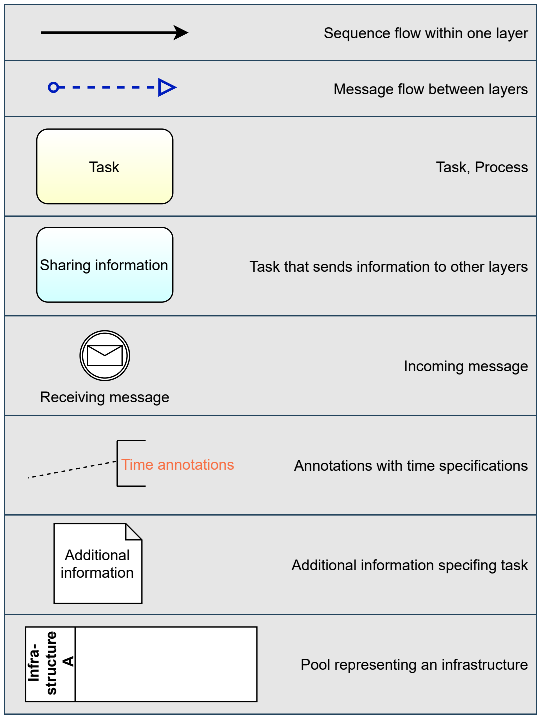
Sequence flow within one layer
Message flow between layers
Task
Task, Process
Sharing information
Task that sends information to other layers
Receiving message
Incoming message
Time annotations
Annotations with time specifications
Additional information
Additional information specifing task
Infra-structure A
Pool representing an infrastructure

Fig. 1. Notation for Activity Diagram

Receiving information from other infrastructures is demonstrated by Intermediate Message Events, according to the BPMN concepts. Information flows are demonstrated by dashed blue lines with an arrow, which demonstrates information exchange from one infrastructure to another one. Information flows included in the model are unidirectional, which means that information is exchanged only in one way, namely from the sending to the receiving infrastructure. If information should be shared in both ways, it is necessary to model information flows separately, by utilizing an individual information flow in each direction. Sequence flows within one infrastructure are represented by a black line with an arrow at one end. Furthermore, we would emphasize to use different coloring for information and sequence flows, to distinctly differentiate those two flows. Additionally, the modelling entities provide the option to add time annotations and other additional information, if required.

C. *Modelling Scenario Parameters in Object Diagrams*

The designed activity diagram allows to develop an advanced information flow model and to identify objects and parameters needed for simulating behaviors and information flows in CIs in the context of the described threat scenarios. This step requires close cooperation with simulation experts, as they offer input regarding requirements and limitations of simulation environments.

The first step of developing an object diagram is to identify and specify the objects that are relevant for the specified threat scenario. This requires a closer look at the CIs and other assets identified in the context of the activity diagram, and extract the objects that are actually affected by it. When considering the scenario of a blackout, which results in failure of traffic lights, traffic light represents an object of the transport CI. For consistency and simple representation, a layered design is suggested, where all objects of one infrastructure are combined in one layer.

Necessary objects that describe the use case can be revealed by considering questions like ”Which objects present the infrastructure in general?”, ”Which objects are necessary for processing the tasks presented in the activity diagram?” or ”Which objects are required for processing information flows from other infrastructures?”.

Once the objects are identified, parameters for each item are defined, whereby only descriptive parameters are considered, as values will be assigned in another phase of the project. Distinguishing between descriptive parameters and their values is important, as the value changes depending on the simulation environment, while the descriptive parameter remains the same. However, it can be helpful to consider values at this point for determining descriptive parameters [14]. Declaring parameters can be facilitated by dividing them into the following subcategories:

- Private: Parameters that are predefined
- Public: Parameters that are set during simulation
- Derived: Parameters derived from other parameters’ values

The suggested categories are based on the UML standard attribute categories, but their meaning is adapted to the needs of the domain. After considering all parameters, relationships between objects are specified by considering relations between objects within a layer and information flows between objects of different layers, according to the activity diagram. For completing the technical view, parameters that are shared between infrastructures need to be identified, for allowing correct simulation of information flows.

For visualizing the object diagram, we suggest UML class diagram representation, since it offers entities relevant for our method. Small adaptions were made to support the domain’s requirements, as presented in Figure 2. As UML class diagrams do not provide modelling entities for representing information flows, a notation for this concern was added. Through this notation it is possible to represent information shared between infrastructures involved in the use case, which is especially required for simulation purposes. In this context, UML also does not have a notation for representing parameters that are shared between entities according to information flows. A notation to represent shared parameters within a blue rectangle as an annotation to the information flows was added.

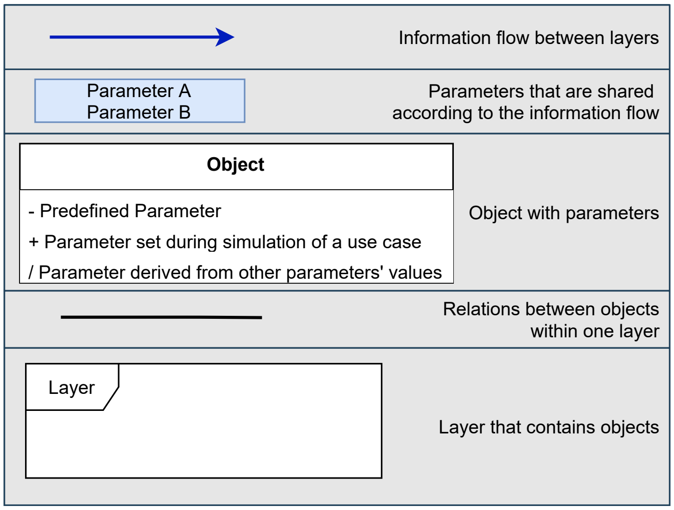
Information flow between layers
Parameter A
Parameter B
Parameters that are shared according to the information flow
Object
- Predefined Parameter
+ Parameter set during simulation of a use case
/ Parameter derived from other parameters' values
Object with parameters
Relations between objects within one layer
Layer
Layer that contains objects

Fig. 2. Notation for Object Diagram

Similar to the activity diagram, we recommend to use layers for representing infrastructures. An object is represented by the UML entity of a class and contains parameters presented according to their characteristics. For specifying the type of the parameter, the standard notation from UML was used but semantically adapted to the domain's needs. According to UML, the symbol ”-” preceding the name of an attribute classifies the visibility as private and ”+” defines it as public [10]. For the presented domain the semantics of the symbols are adapted. The symbol ”-” before the parameter classifies that the parameter's value is specified prior to the simulation start, ”+” however classifies parameter values that are initiated during the simulation and ”/” specifies a value that is derived from other parameters' values.

Relations between objects can either represent relations within one infrastructure, or information flows between objects owned by different stakeholders. Information flows in this context are only unidirectional, with the arrow on one end indicating the receiving object. For an easy distinction between the two types of relations, it is also suggested to use different coloring.

D. Iterative Refinement of Modelling Results

Once the diagrams are established, it is vital to hold additional workshops in the stakeholder group in order to gather additional feedback from domain experts and evaluate information captured in the diagrams. This is in line with the design-science methodology [3] as well as the SSM [4] presented in Section II, which both include iterative refinement of the established models of the studied domain as a core principle of the methodology. Reviewing the results together with the stakeholders allows to identify inaccuracies or wrong representation of events and allows to refine modelled information flows between CIs. Furthermore, it enables to substantiate specific aspects of objects or behaviors with more detail, until the desired level of detail is reached to derive a meaningful and realistic simulation.

The goal of further workshops is to reveal information regarding every-day processes, threats which can lead to failures in the CI's services, how such a failure would affect other infrastructures, how the CI can be affected by failures of other stakeholders and to assign realistic values to identified parameters in the context of the threat scenarios. Workshops should support revealing such dependencies, which can be further analyzed within the simulations. Additionally, information on communication and collaboration with other stakeholders can be revealed.

After such workshops the activity diagrams and possibly also the textual description can be adapted to obtain realistic use cases that capture all relevant information for modelling processes during a threat. The visual models enforce feedback and discussion in workshops as information is presented more clearly and organized than it is in a purely textual representation.

IV. Case Study

In the context of the ODYSSEUS project [2], a case study was conducted with domain experts ranging from research partners to employees from various CIs including experts from the field of cyber security, operations, and business continuity. The following section provides an in-depth overview of the case study and the evaluation process.

The project's goal is to identify and simulate cascading effects between CIs in an urban area to improve procedures and reactions in case of a threat scenario. Therefore, main end-users in this context are CI providers and emergency services, who participated in multiple workshops and offered insights into the procedures of their domain.

According to the approach introduced in this paper, use cases representing threat scenarios in urban areas were designed and evaluated in the context of end-user workshops. The workshops were held in form of a world cafe, where use cases were evaluated by the relevance for providers of CIs. Due to their profound feedback, only three out of four initially defined use cases were considered as relevant enough to be further elaborated.

Once the newly gained information was applied to adapt the use cases, the textual form was converted into an activity diagram. Figure 3 shows an excerpt of the created activity model with information flows between CIs. The activity diagram shows the case of a power failure. The CIs involved and presented in the diagram are power supply, private transport and police forces represented as pools. The yellow tasks are activities within the CI with no influence on other ones. The blue tasks represent activities that send information to other CIs. For instance, activity P2.3 ”Serious traffic accidents” sends a message to police forces, as they receive emergency calls due to these accidents. In consequence of these received emergency calls, police forces have to secure accident sites as stated in task P3.2, sending a message flow to private traffic indicating that traffic will be regulated.

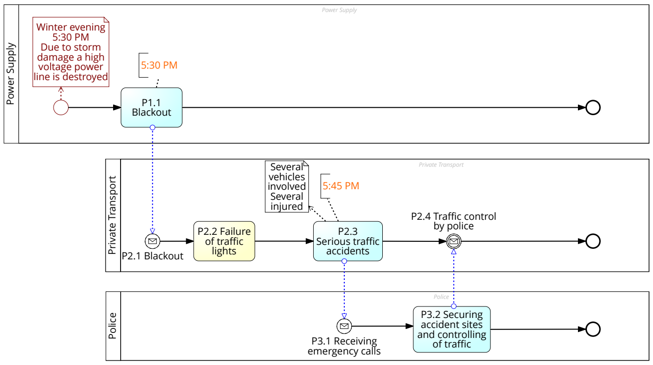
Power Supply
Power Supply
Winter evening
5:30 PM
Due to storm damage a high voltage power line is destroyed
5:30 PM
P1.1 Blackout
Private Transport
Private Transport
Several vehicles involved
Several injured
5:45 PM
P2.1 Blackout
P2.2 Failure of traffic lights
P2.3 Serious traffic accidents
P2.4 Traffic control by police
Police
Police
P3.1 Receiving emergency calls
P3.2 Securing accident sites and controlling of traffic

Fig. 3. ODYSSEUS Activity Diagram - Snapshot

Additional information that is not part of the actual information flow, but can provide useful annotations for the scenario or the users of the scenario, can be annotated to each node via a comment, as can be seen in the context of node P2.3.

Figure 4 presents an excerpt of the resulting object diagram in the project's context, created according to Section III-C.

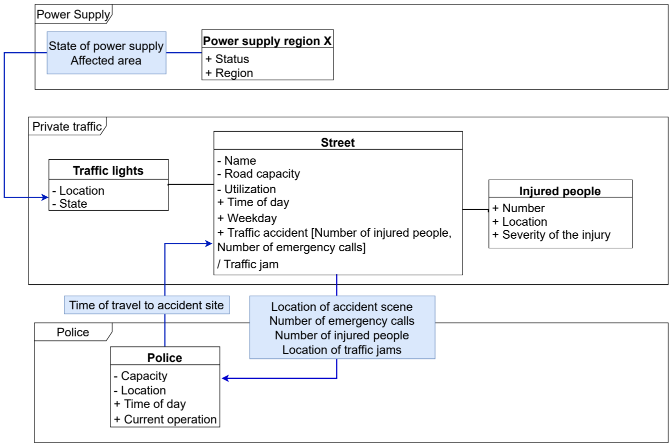

Fig. 4. ODYSSEUS Object Diagram - Snapshot

The model presents each CI and its main objects relevant for simulating the defined use cases. Each object includes parameters that are necessary for presenting the infrastructure and indicating its actual state, e.g., infrastructure private traffic is presented by the objects traffic lights, street and injured people. Each object is further depicted by parameters that are additionally classified due to their behavior. The object ”Police” for example is presented by the predefined parameters ”Capacity” and ”Location”, which indicates that these parameters do not change during simulation. ”Time of day” and ”Current operation” on the other hand are parameters, which change during simulation, according to inputs from other infrastructures or the simulation environment itself. Most of the objects include a parameter “Capacity” to capture whether the object should change its state, if the maximum capacity is reached.

The first draft of the diagram included objects, parameters and information flows, but after evaluation with project partners, it was decided to additionally include parameters exchanged by information flows. Information flows are presented by blue lines, where the arrow states the receiving infrastructure. Parameters exchanged during an information flow are represented by blue rectangles including the parameter names. For instance, there is an information flow from ”Power supply region X” to ”traffic lights”. Information shared in this example is the state of the power supply and which area is served by the power supply.

The aim of the created models is to present processes and information flows between CIs executed during a given threat event and to provide a basic model for simulation. In line with the modelling approach presented in Section III-D, for evaluating the current state of the use cases and according models, workshops with experts of each area of CIs individually were performed. The main goals of these workshops were to gain more insight regarding the general processes of the infrastructure, as well as processes happening during our defined threats. With each workshop, we obtained important feedback from participating domain experts, which was used to adapt the use cases and activity diagrams, to provide a more realistic view of behaviors during a threat.

V. Discussion of Results

The paper presents an information flow modelling approach to support simulating cascading effects in CIs by achieving the following objectives:

- *Modelling cascading effects through CIs in a structured form*
  The resulting activity diagram demonstrates how cascading effects and information flows through CIs during threat scenarios can be transformed from a textual description into a structured visual form. The output is able to adequately model the activities depicted in the threat scenarios, and is especially helpful in outlining the potential cause and effect relationships of cascading failures. Additionally, the created model supports evaluating the realistic representation of events and information flows with experts during information gathering workshops.
- *Establishing a basis for subsequent simulation*
  The model has shown to be a valid basis for subsequent simulation, as it provides a process view of the threat scenarios including information flows and the objects needed for establishing a simulation environment. The activity diagram represents the process view of behaviors and events, while the object diagram provides the technical view including assets and parameters needed for simulation.
- *Supporting discussion with and between CI providers and emergency services*
  During the expert workshops, we observed that the activity diagram supported stakeholders in easier following our intention of providing scenario based CI interdependency models, and the activities observed in the involved CIs

during those scenarios. The subsequent discussions with stakeholders in the context of iterative refinement of the model have shown that many of the relationships presented in the activity diagram were not adequately considered and understood by CI operators. In this sense, the activity diagram has proven to add value in adding to the holistic understanding of threat scenarios for CI providers. The stakeholders have shown particular interest in those findings during our workshop sessions.

- *Supporting emergency services to prepare emergency plans*
  The activity diagram and subsequent simulation outputs should support emergency services for establishing emergency plans in case such threat scenarios occur. At this point we are not yet able to provide an evaluation of this aspect, since the validation will be part of a later phase of the currently ongoing ODYSSEUS project. Thus, a final conclusion regarding the aspect of communication and collaboration between CIs and emergency services cannot yet be made.

VI. Conclusion and Future Work

The presented modelling approach demonstrates how textual descriptions of threat scenarios can be transformed into a process view and a technical view to support simulating cascading effects in CIs. With this method cascading effects through CIs can be modelled in a structured form, to support discussions in workshops with stakeholders and to provide a comprehensible basis for establishing communication and collaboration between CIs and emergency services. The modelling approach consists of multiple steps from analyzing the requirements on threat scenarios, reviewing the defined scenarios in end-user workshops on the basis of established activity diagrams and finally designing a technical view by creating object diagrams. The textual descriptions and the constructed diagrams serve as a core enabler for specifying an environment for simulation of the scenarios, which can be to a large extent directly based on this model. The modelling approach was used in the context of the ODYSSEUS project, where the method has proven to be quite helpful in building a common understanding of the basic foundations for all partners involved in the project, especially for the simulation experts. Additionally, the designed activity diagrams supported the evaluation of the defined threat scenarios in the end-user workshops, which resulted in substantial feedback based on the realistic representation of behaviors in threat scenarios. Future work on this approach within the ODYSSEUS project includes obtaining values for identified objects' parameters and further evaluation with end-users.

Acknowledgments

This work was partially funded by the Austrian FFG research program KIRAS in course of the project ODYSSEUS ("Simulation und Analyse kritischer Netzwerk-Infrastrukturen in Städten") under Grant No. 873539.

References

[1] I. B. Utne, P. Hokstad, and J. Vatn, "A method for risk modeling of interdependencies in critical infrastructures," *Reliability Engineering & System Safety*, vol. 96, no. 6, pp. 671–678, 2011.

[2] KIRAS Sicherheitsforschung, "ODYSSEUS - simulation and analysis of critical network infrastructures in cities," [retrieved: October, 2020]. [Online]. Available: https://www.kiras.at/en/financed-proposals/detail/d/odysseus-simulation-und-analyse-kritischer-netzwerk-infrastrukturen-in-staedten/

[3] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *Management Information Systems Quarterly*, vol. 28, pp. 75–, 03 2004.

[4] P. Checkland, *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective*. Chichester, England, UK: Wiley, Jun 1981.

[5] The World Café Community Foundation, "The World Cafe," [retrieved: October, 2020]. [Online]. Available: http://www.theworldcafe.com

[6] V. Kupfersberger, T. Schaberreiter, and G. Quirchmayr, "Security-driven information flow modelling for component integration in complex environments," in *Proceedings of the 10th International Conference on Advances in Information Technology, IAIT 2018, Bangkok, Thailand, December 10-13, 2018*. ACM, 2018, pp. 19:1–19:8. [Online]. Available: https://doi.org/10.1145/3291280.3291797

[7] "A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis CS-AWARE," Sep 2020, [retrieved: October, 2020]. [Online]. Available: https://cordis.europa.eu/project/id/740723

[8] OMG, "Business process model and notation (bpmn)-version 2.0.2," 2013, [retrieved November, 2020]. [Online]. Available: http://www.omg.org/spec/BPMN/2.0.2/

[9] M. Chinosi and A. Trombetta, "Bpmn: An introduction to the standard," *Computer Standards & Interfaces*, vol. 34, no. 1, pp. 124–134, 2012.

[10] OMG, "Unified modeling language (uml 2.5.1.)," 2017, [retrieved: October, 2020]. [Online]. Available: https://www.omg.org/spec/UML/2.5.1

[11] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE control systems magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[12] Bundesamt für Bevölkerungsschutz (BABS), "Catalog of threats. disasters and emergencies Switzerland," 2019, [retrieved: October, 2020]. [Online]. Available: https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrdkatalog.html

[13] B. C. Hungerford, A. R. Hevner, and R. W. Collins, "Reviewing software diagrams: A cognitive study," *IEEE Transactions on Software Engineering*, vol. 30, no. 2, pp. 82–96, 2004.

[14] J. Sokolowski, C. Turnitsa, and S. Diallo, "A conceptual modeling method for critical infrastructure modeling," in *41st Annual Simulation Symposium (anss-41 2008)*. IEEE, 2008, pp. 203–211.