RESili8

Resilience for Cyber-Physical Energy Systems

Deliverable D4.1

Knowledge Representation for Existing Modeling Approaches

Version 1.1

Deliverable

Arlena Wellßow (OFFIS)
Julian Kohlisch (OFFIS),
Eric Veith (Universität Oldenburg),
Paul Smith (Lancaster University),
Edmund Widl, Francesca Soro, F. Pröstl Andrén (AIT),
Andreas Theil, Roland Zoll (Wiener Netze),
Malte Puhan (SOL)

2023-11-30

This project has received funding in the framework of the joint programming initiative ERA-Net Smart Energy Systems' focus initiative Digital Transformation for the Energy Transition, with support from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883973.

Smart Energy Systems ERA-Net

DOCUMENT INFORMATION

• **Deliverable No.:**	D4.1
• **Deliverable Name:**	Knowledge Representation for Existing Modeling Approaches
• **Work Package:**	WP4 – Concept and Architecture for Resilient Planning and Operation
• **Lead Partner:**	OFFIS
• **Submission Date:**	2023-11-30
• **Status:**	□ draft, □ final, ☒ submitted

DISSEMINATION LEVEL

☒	**Public**	Publicly available
□	**Programme Participants**	Restricted to other programme participants (including ERA-Net and national funding organizations)
□	**Restricted**	Restricted to a group specified by the Consortium (including ERA-Net and national funding organizations)
□	**Confidential**	Confidential, only for members of the Consortium (including ERA-Net and national funding organizations)

CHANGE LOG

Date	Version	Author/Editor	Summary of Changes Made
2022-09-15	v0.1	F. Pröstl Andrén (AIT)	Initial document structure
2023-09-19	v0.2	Arlena Wellßow (OFFIS)	Adapting structure to Deliverable 4.1
2023-11-02	v0.3	Arlena Wellßow (OFFIS)	Adding background texts.
2023-11-30	v1.0	Arlena Wellßow (OFFIS)	Completing the document for a first version
2023-12-22	v1.1	Arlena Wellßow (OFFIS)	Resolve comments

TABLE OF CONTENTS

1 Executive Summary

Over-provision and usage of the n-1 rule will not be sufficient to achieve resilience in future energy systems. The grid converges to a Cyber-Physical System (CPS); therefore, complexity rises, and problems in the digital transition occur. Also, over-providing would only be sustainable without using traditional power generation. Therefore, considering resilience theory and developing practice usages for energy systems is imperative.

RESili8 contributes to this development by adding new approaches for the resilient operation of energy systems as well as optimal and sustainable planning, AI-based analysis of resilient architectures, and continuous implementation and validation of resilient applications.

This deliverable covers the concepts developed in WP4.1 that target the refactoring of knowledge representation to make use of it in AI experiments and offline data generation.

In this work package, we focus on developing fundamental methods that are essential for using threat and hazard analysis to improve the learning capability of AI-based models. This comprehensive effort includes developing and refining a specialized analysis tool based on Deep Reinforcement Learning (DRL). The planned outcomes of this project will manifest themselves in the form of carefully crafted formats suitable for human understanding and machine interpretation. These formats will play a central role in facilitating model training processes and enable seamless integration with the intricate nuances of AI-based learning methods. Another critical aspect of the planned deliverables concerns the provision of datasets that serve as a robust training and testing environment and thus contribute significantly to the iterative refinement and validation of the developed AI models. Essentially, this work package is intended to contribute to the convergence of threat and hazard analysis with state-of-the-art AI technologies and create a symbiotic relationship between analytical findings and machine intelligence.

Here, we present a novel approach by combining System Theoretic Process Analysis (STPA) with Misuse Case (MUC) templates as well as Holistic Test Descriptions (HTD) to accomplish a toolchain that, with reinforcement learning embedding, analyses possible threat situations even further and in more detail. This allows faster test case generation for lab-based testing, as the output of this toolchain are lab specifications of explicit test cases. While STPA and MUCs enable expert knowledge input into reinforcement learning experiments, the machine learning part in this toolchain allows checking multiple parameters and set-ups faster than possible in a real-time lab. The situations labeled as especially critical after training and testing the reinforcement learning agents are then described in HTD to allow a reproducible lab test.

Once implemented, this concept aims to simplify and speed up test case definition and provide higher test coverage through the agents' exploration.

Therefore, the future work following this conceptualization is the implementation of the proposed toolchain in an at least partially automated way. In an even further view, this toolchain could then be added to a CiI/CD Pipeline that includes lab testing. In this context, the toolchain proposed here would continuously add new lab-testing specifications to be covered whenever there are new findings by the STPA or through exploration of the machine learning agents.

2 Introduction

Resilience for future energy systems cannot be ensured by over-provisioning, as is done today. It is not socially sustainable and cannot address the complexity and challenges of the digital transformation that energy systems are undergoing. Resilience thinking and practice for energy systems needs to be reinvented. *RESili8* does this through a novel resilience solution package for Cyber-Physical Energy Systems (CPESs), including optimal and sustainable planning and AI-based analysis of resilient architectures, continuous implementation and validation of resilient applications, and new solutions for resilient operation of energy systems. This innovative solution package will advance the green energy transition by ensuring security of supply and facilitates the further integration of green energy technologies. *RESili8* is executed by leading European research institutes, industry, and need-owners, working together to develop and test the *RESili8* solution in lab and pilot demonstrations [10].

2.1 Introduction to Knowledge Representation

The convergence of the energy grid, a critical national infrastructure known as the smart grid, from both IT and OT perspectives necessitates the inclusion of expertise from grid operators and ICT specialists. This is crucial due to the implementation of ICT-based control systems, which are integrated into the grid to manage volatile generation and prosumers efficiently. While enhancing usability, this integration also introduces a heightened risk of errors and potential cyber attacks, consequently increasing the likelihood of system failure [17, 34, 42].

Traditionally, the risk of failure within the energy system was mitigated by the redundancy of the physical system (following the N-1 rule) [17]. However, with the growing need for highly efficient power grid operation, driven by extensive ICT integration, this approach is no longer sufficient. The integration of ICT introduces its own set of risks, where the failure of physical systems can lead to the failure of ICT systems and vice versa. Redundancy remains important, but it alone cannot address these risks; new technologies such as secure communication protocols and encryption must be employed for mitigation [34, 42].

The power grid is transforming, rendering it highly non-deterministic as an overall system. The complexity arises from the introduction of machine learning systems for optimization, the proliferation of prosumer roles, the emergence of localized energy markets, and the significant contribution of distributed renewable energy sources (DERs) in achieving efficiency goals. Extensive simulations are required to develop mitigations in response to these challenges [50, 51].

However, this development demands a substantial investment in terms of time and financial resources, as the time spent on development must be accounted for [50, 51]. Consequently, previous approaches have turned to agent-based systems, often leveraging Deep Reinforcement Learning (DRL), to generate effective mitigation strategies for unforeseen scenarios [19].

Nevertheless, there exists a plethora of expert knowledge in energy systems that AI agents typically lack. To perform as effectively as or even better than human operators, all this knowledge must be acquired through training. This is particularly crucial in critical situations that occur infrequently and are not well-represented in historical data used for training. Addressing these scenarios requires the incorporation of additional scenario data or the infusion of expert knowledge [19].

3 Methodology

The necessary concepts and ideas for this were developed in a workshop that was split into several distinct meetings with people from Wiener Netze, AIT, and OFFIS who possess specialized knowledge relevant to the subject matter under consideration.

Iteratively the different ideas were discussed and criteria such as importance and feasibility were considered.

The results were documented during these sessions and are summarized in this document.

4 Known Concepts and Own Adaption

Expert knowledge modeling is a dynamic field situated at the intersection of human expertise, human learning, and artificial intelligence. Its importance is profound in the fields of electrical engineering and sustainable energy systems, and it promises transformative applications for the way we understand, manage, and optimize smart power grids. This discipline embodies a continuous pursuit of methodologies and techniques that harmonize human insight, empirical knowledge, and the computational prowess of machines. By transforming complex human expertise into computer models, we seek to unlock a wide range of applications, from improving grid resilience to optimizing demand-side management strategies in smart energy systems. In this deliverable, we embark on a comprehensive exploration of the foundational principles that underlie expert knowledge modeling and introduce a concept that aims to connect the fields of human expertise and machine learning in a novel way.

4.1 Use Cases and Misuse Cases

4.1.1 Use Cases

The IEC 62559 standard outlines the use case methodology as a systematic procedure for collecting and describing use cases. According to this standard, IEC 62559-2 provides a standardized and organized template for use case descriptions. The information contained in this template encompasses the use case's name and identifier, along with its scope, objectives, conditions, and narrative in natural language. It also encompasses supplementary details, such as its relationship to other use cases, prioritization, and a set of associated KPIs. The diagrams associated with the use case are displayed in the template's second section. Following this, there is a breakdown of technical information, including a roster of all active components and a step-by-step analysis for each scenario related to this use case. Lists of exchanged information and requirements, which are also integral components of the template, are linked to these processes. Common terminology and specific details are placed at the end.

IEC 62559 is a series of standards with widespread application across various fields [23]. The works of Trefke et al. [49] and Clausen et al. [11] demonstrate the application of the use case technique in a significant European smart grid project. In the DISCERN project, Santodomingo et al. [41] presents approaches for analysis based on the use case standard. Building on these approaches, Schütz et al. [43] incorporates related strategies from [36], [1], and [2]. The use case methodology, adapted from the results of the DISCERN project, was subsequently employed in later projects within the SINTEG framework [42].

4.1.2 Misuse Cases

Misuse cases serve as a method for conducting threat modeling, specifically allowing experts to articulate undesirable behaviors within their system.

The misuse case approach builds upon the use case methodology outlined in IEC 62559. Consequently, describing unwanted behavior as misuse cases for systems already defined in IEC 62559 becomes a more straightforward task. Thereby, a misuse case encapsulates a scenario that is recognized but explicitly undesirable. This encompasses both cyber-physical attacks and inappropriate system behaviors.

The work of Sindre and Opdahl [44] applied the need for misuse cases, as discussed in the later publication by Sindre and Opdahl [45], to a template rooted in the "use case" template introduced by Cockburn [12]. Sindre and Opdahl [45] introduces concepts and notation for misuse instances, textual specifications and illustrative examples for working with misuse cases.

The misuse case template encompasses information concerning misactors and the general actor details outlined in the template according to IEC 62559-2, which are situated within the same section as the actors in the standard.

The section about scenarios is tailored to failure scenarios that necessitate additional specifics, such as the worst-case threat or the likelihood of occurrence [3].

An overview of a misuse case is given in Figure 1.

There are two possible methods for collecting data in MUCs: Elicitation of templates supported by use cases and elicitation of templates supported by domain knowledge. In the first method, a ready-made use case template is examined to identify undesirable (system) behavior or attacks that could affect the respective use case. The data of the MITRE ATT&CK dataset identified as suitable is systematically checked.

The second method relies on known attacks that represent known undesirable behavior in a general form without a specific use case. In this scenario, the template for the misuse case is completed based on information about known attacks and their corresponding remediation measures.

By applying one of these methods, a professional can create an abuse case tailored to the desired scenario. It is then advisable to ensure consistency with other domain experts and review different modeling formats such as the Smart Grid Architecture Model (SGAM) from the IEC SRD 63200 standard for the energy domain or the STIX data to eliminate potential ambiguities and uncertainties resulting from the use of natural language.

For the approach presented in this paper, an almost complete template for an abuse case is crucial as a basis for the subsequent steps. Errors at this stage can carry over to later stages, affecting data quality and the validity of the conclusions drawn from the method.

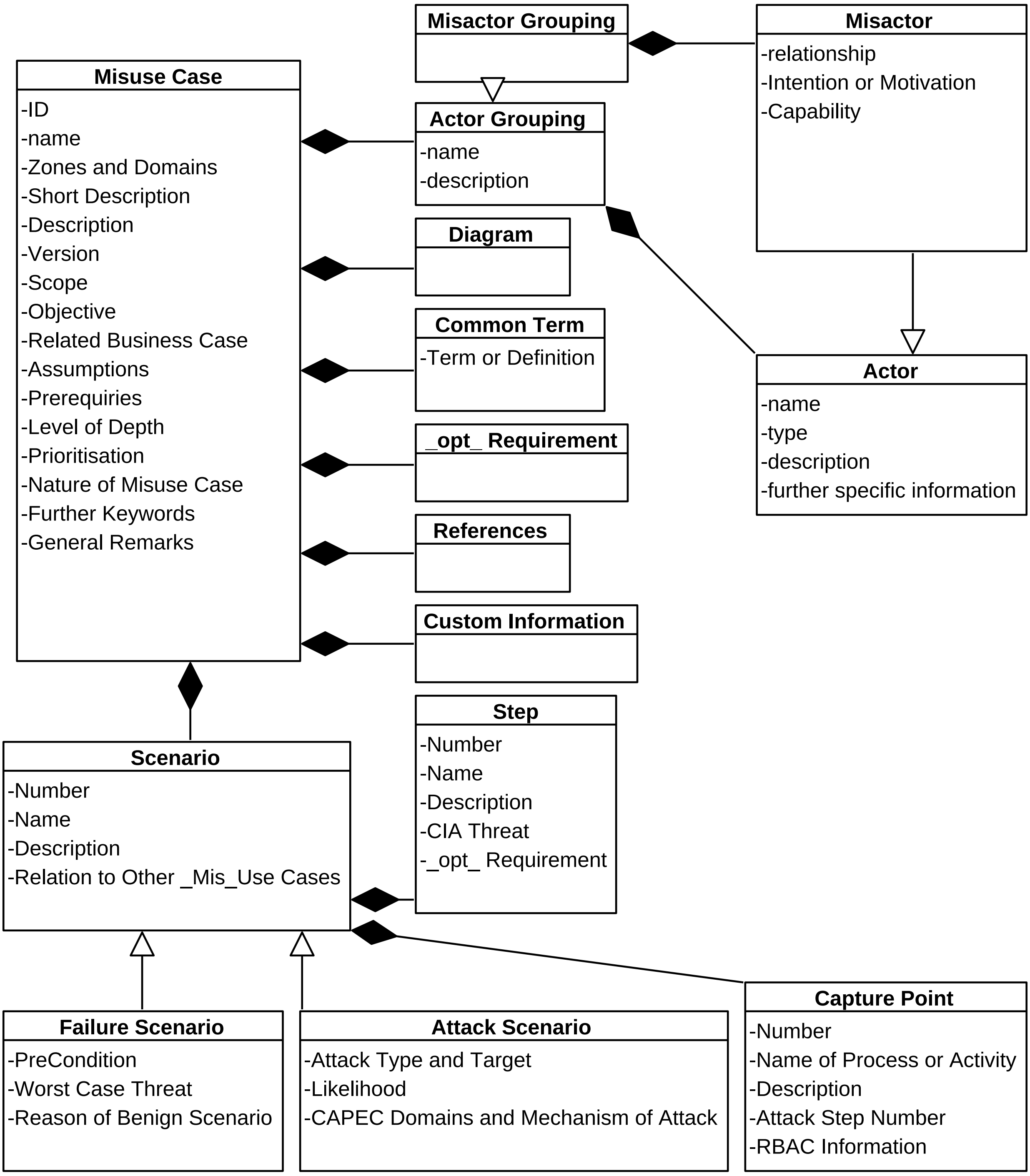


Figure 1: Information contained in an Misuse Case (MUC) structured as an UML class diagram [54]

4.2 Holistic Testing Description

For the purpose of identifying and defining the critical parameters and procedures for performing a test, the *Holistic Testing Description* (HTD) approach seeks to assist domain experts in documenting their objectives and creating configurations [28]. It includes a collection of textual templates, a visual notation, and partial procedures that an expert may use to organize, improve, and document a test effort.

The *System under Test* (SuT) in HTD establishes the abstract, categorical, system boundaries of the test system that includes all relevant subsystems and interactions (domains) required for the study. The *Object under Investigation* (OuI) – which is a subset of the SuT – comprises the component(s) that are to be characterized or validated. The functions relevant for the operation of the SuT are described as the *Functions under Test* (FuT), whereas the *Function(s) under Investigation* (FuI) – which are a subset of the FuT – refer to the functions specifically used (operationalized) by the OuI. The *Purpose of Investigation* (PoI) defines the test objective and specifies if it is for characterization, validation, or verification. Together, the items listed above can be used to define the *Test Criteria*, which formalize the test metrics into target criteria, variability attributes, and quality attributes.

The HTD defines three levels of detail for test definitions, each of which refers to the preceding level, resulting in incremental scoping of an actual test/experiment:

- A *Test Case* (TC) is a set of conditions under which a test can establish whether or not a system, component, or one of its features is functioning as planned.
- A *Test Specification* (TS) outlines the test system (i.e. how the OuI will be embedded in a specific SuT), which system characteristics will be adjusted and observed for the evaluation of the test objective, and how the test will be carried out (test design).
- The *Experiment Specification* (ES) specifies how a specific TS is to be realized in a specific laboratory infrastructure or simulation implementation.

A TC defines the essential objectives and context of a test, whereas the TS and ES define the concrete test execution.

Both STPA and HTD employ a deductive top-down approach, with the detailed results from STPA guiding the formulation of specific test and experiment specifications in the HTD [46].

4.3 System Theoretic Process Analysis (STPA)

System Theoretic Process Analysis (STPA) is a top-down deductive hazard analysis approach that has been developed by Leveson and Thomas [32]. It has been used extensively to determine the system weaknesses or deficiencies that could lead to an accident or loss. The STPA approach can be summarized, as follows.

Initially, after performing a scoping exercise, the high-level accidents or *losses* of concern are identified. For example, for an energy distribution system, this could include safety-related accidents (injury, loss of life) and power quality issues. Ultimately, these are the losses that should not occur. The next step is to identify *hazard scenarios* that could result in a loss. A hazard scenario can be described as a worst case scenario (or system state) that could result in a loss. For example, a circuit breaker not opening in an over-voltage situation (a hazard) could result in electrocution or equipment damage (a loss). The next task is to identify the *hazardous (or unsafe) control actions* that could lead to a hazard scenario. To achieve this, it is necessary to understand the high-level control schema for a system that is being analyzed. This involves examining the control actions that can be performed and determining whether they could result in a hazard by considering a control action in relation to a set of keywords. These keywords relate to the control action being applied too late or early (temporal concerns) or not at all, for example. The outcome of this task is a set of control actions (e.g., open breaker) and conditions under which the application of that control (e.g., too late) could result in a hazard scenario. These hazardous control actions can be transformed into *safety constraints*, which express control behaviours that must not be violated to ensure that a hazard does not manifest. Following on from this analysis, the final step is to determine shortcomings (or deficiencies) in control that could result in hazardous control. This task is performed using a high-level annotated diagram of the control systems that are being evaluated. The annotations describe deficiencies (also known as causal factors) that *could* result in hazardous control. For example, deficiencies in the controller or systems model may result in hazardous control actions. Similarly, incorrect or delayed feedback from the system may result in a control action being applied too late – a hazardous control and violation of a safety constraint. An example control diagram, showing deficiencies, for a scenario that includes a Building Energy Management System (BEMS) controller is presented in Figure 2.

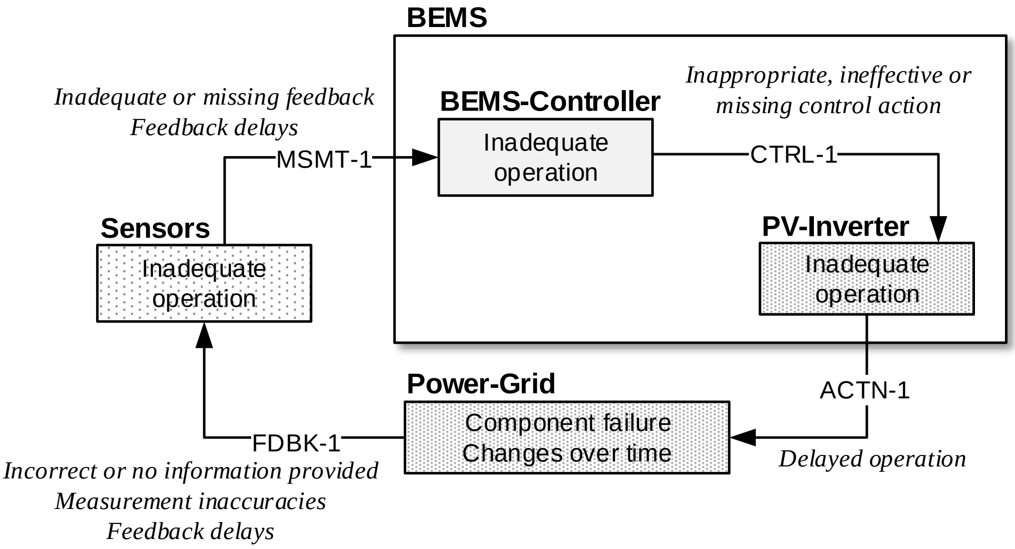


Figure 2: An example control schema showing potential deficiencies (also referred to as causal factors) that could result in hazardous control. [46]

Several important items are understood at the conclusion of this analysis: *(i)* the losses of concern; *(ii)* the hazard scenarios that could result in those losses; *(iii)* the control actions that may result in a hazard (which can be reformulated as safety constraints); and *(iv)* the deficiencies that may result in hazardous control. The analysis is not concerned, necessarily, with the cause of the deficiencies that may result in safety constraints being violated – they could be caused by component failure or a cyber-attack, for example. To identify the potential cyber security causes of control deficiencies, Friedberg *et al.* [20] extended STPA with steps, called STPA-SafeSec. In summary, the extension includes steps to map the high-level control schema that is used for STPA onto its system implementation, and then determine which security objectives (confidentiality, integrity, and availability) can be violated in order to cause a deficiency. For example, a deficiency could be missing feedback to a controller (see Figure 2; in this case, a lack of *availability* of the communications network that provides the feedback can result in the delay. A further step would then be to identify the attacks, e.g., a Denial of Service (DoS) attack, and security vulnerabilities, which may result in a lack of availability. In this way, there is a deductively determined relationship between a high-level loss and a threat or vulnerability. This information can the be used to support risk-informed decision making regarding how to mitigate threats and vulnerabilities in a running system or alter its design.

As mentioned at the outset of this deliverable, energy systems are becoming increasingly non-deterministic. Formulated another way, it is difficult to determine whether the violation of a safety constraint (or potentially unsafe control action) can result in a loss. Several factors are contributing to this, including the use of distributed control schemes, applications of machine learning and artificial intelligence (in the future), and the stochastic behaviour of generation and loads – the system and its behaviour is complex, complicated, and – in some cases – opaque. There are several variables to consider to determine whether a *candidate* hazardous control action will result in a hazard scenario, and a loss. Moreover, STPA encourages the analyst to consider the worst case scenario; determining the characteristics of this scenario may not be straightforward for distributed energy systems (smart grids), and it can be desirable to not consider the worst case, for some classes of loss (e.g., when losses are related to financial penalties, rather than loss of life). Therefore, what is needed is a means to explore the dimensions of potential hazard scenarios to better understand the risk and affirm the circumstances (system states) and presence of candidate unsafe control actions. One way to achieve this is via lab-based experimentation. To this end, Smith *et al.* [46] proposed a scheme that integrates the activities and outcomes that are associated with an STPA analysis with the Holistic Test Description (HTD) approach for refining and documenting experiments. In short, the integrated approach proposed takes findings from an STPA analysis and uses them to populate increasingly specific test descriptions using HTD. The outcome is a set of detailed lab-based experiment descriptions, which can be used to examine the characteristics of scenarios that could result in high-level losses. Absent from this approach is a means to characterize and model the behaviour of intelligent adversaries (and defenders) when considering cyber security-related scenarios. This is important as it forms an important input to experiments regarding the likely and worst-case adversarial behaviour that could result in a loss.

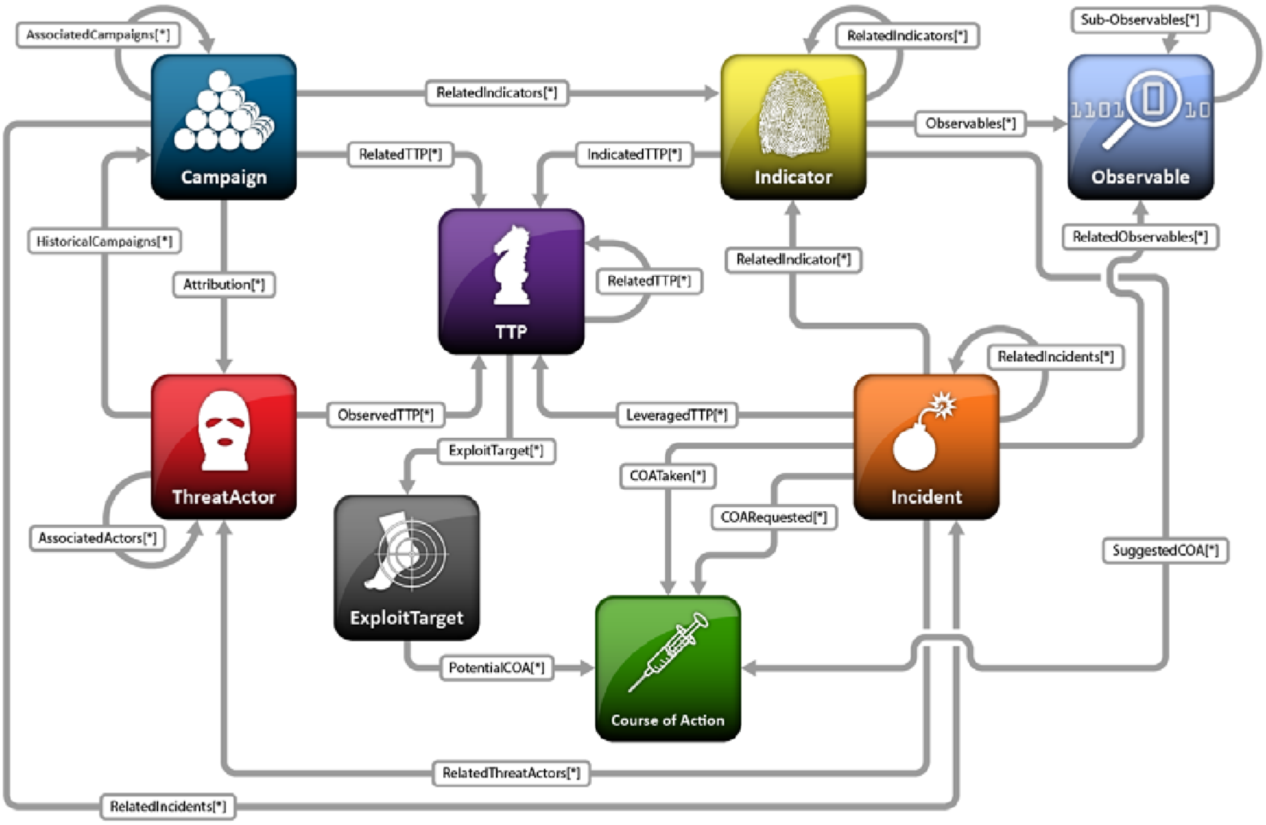


Figure 3: Concept for STIX v1.0 structure by Barnum [5]

4.4 STIX™ and TAXII™

4.4.1 Structured Threat Information eXpression (STIX™)

As organizations increasingly recognize the need to collect cyber threat intelligence, the key to success lies in effective information sharing with trusted partners and peers. Cyber threat intelligence and information sharing is invaluable for focus and prioritization in today's complex cybersecurity landscape, but there is a fundamental need for standardized, structured representations of this information. This structured exchange is critical to making the overwhelming amount of complex cybersecurity data more manageable and actionable. With Structured Threat Information eXpression (STIX™) the Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence Technical Committee developed a standardized language [7]. Data in the form of *Structured Threat Information eXpressions* (short: STIX data) gives structured information about cyber attacks [6]. STIX data is stored in a graph-based information model and OASIS defines eighteen such called *STIX Domain Objects* for entity nodes, which are connected via two defined *STIX Relationship Objects* [37]. Some of these entity node types are referred to as tactics, techniques, and procedures written as TTP, which can be traced back to the military origin of this abbreviation. The whole structure of STIX v1.0 is shown in Figure 3 and discussed by Barnum [5]. This was later extended in STIX v2.0 and v2.1.

4.4.2 Trusted Automated Exchange of Intelligence Information (TAXII™)

The Trusted Automated Exchange of Intelligence Information (TAXII™), which is also developed by the OASIS Cyber Threat Intelligence Technical Committee, describes the way, STIX data is meant to be exchanged. Therefore TAXII is an application layer protocol with a RESTful API. OASIS also

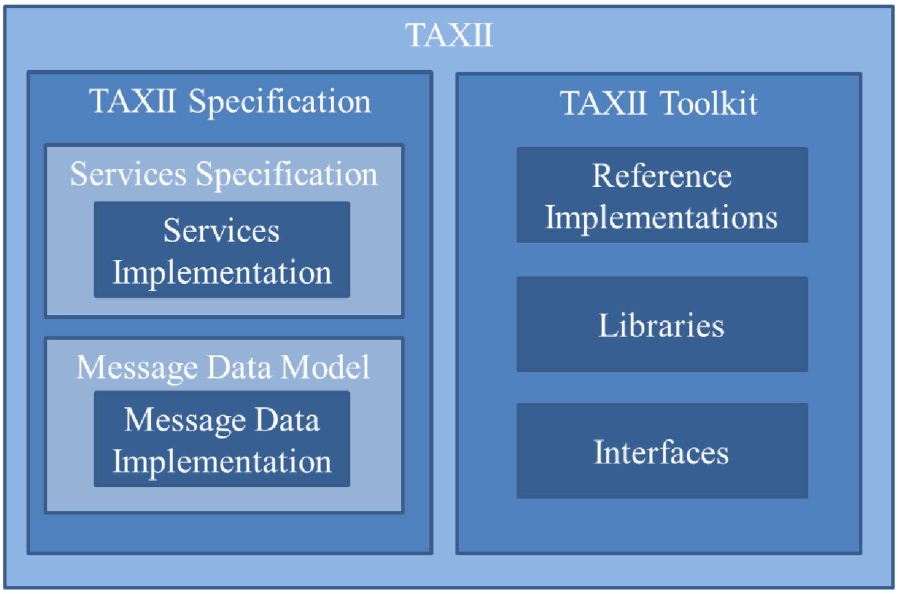


Figure 4: Visual Representation of TAXII by Connolly, Davidson, and Schmidt [14]

provides requirements for TAXII clients and servers. By development, TAXII is meant to be simple and scalable to make sharing STIX data as easy as possible [13]. A visual representation in shown in Figure 4

As stated in the work of Connolly, Davidson, and Schmidt [14] the main goal of TAXII is to enable the timely and secure sharing of threat intelligence within and between cyber defense communities. The goal is to use common standards for sharing indicators and more across organizations and products/services. In addition, TAXII aims to expand the sharing of indicators to support robust, secure and comprehensive sharing of more meaningful cyber threat information. The framework is designed to cover a broad range of use cases and practices common across cyber threat intelligence sharing communities.

TAXII leverages existing mature standards where appropriate and ultimately seeks adoption by one or more international standards organizations. It is important to note that TAXII is not building a sharing community itself, but rather acting as a facilitator that enables communities to engage in sharing activities.

To address the current shortcomings in cyber threat intelligence sharing, TAXII provides common, open specifications for the transmission of cyber threat intelligence. These specifications cover essential functions such as encryption, authentication, addressing, alerting and querying between systems, ensuring a comprehensive and secure approach to cyber threat intelligence sharing.

4.4.3 MITRE ATT&CK® STIX Data

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) collects and provides cyber attack data. It targets the missing communication between communities dealing with the same attacks [48].

4.5 Ontologies

To work with ontologies, one has to define the term of *ontology*.

- Ontology:An ontology is a formalism that enables the formal representation of concepts underlying a certain term and their interconnections [25]. In computer science, ontologies are considered information and knowledge systems, represented as a combination of A-Box and T-Box.

The following definitions of T-Box and A-Box, both integral components of an ontology as outlined in the preceding definition, are provided. To adequately define the concept of a T-Box, it is necessary to first clarify the notion of a definition in the context of ontologies.

- Definition: A definition of a concept specifies the properties and concepts an individual must satisfy to be assigned to that concept [4].

- T-Box: A terminology (or T-Box) T refers to a finite set of definitions where, for every atomic concept A within T, there exists at most one axiom within T whose left-hand side is A [4].

The T-Box encompasses a terminology that conveys intensional knowledge. This terminology is built through declarations describing the general properties of concepts, implying a hierarchical relationship among individual components, suggesting a representation of T-Boxes as a lattice-like structure [4].

Example A T-Box may contain the following concepts:

- Prosumer := Consumer $\sqcap \exists \texttt{hasFeedIn}.\top$
- Consumer := $\exists \texttt{consumesEnergy}.\top$

- A-Box: An A-Box contains statements of membership by individuals, establishing relationships between the concepts of the description logic and concrete individuals. Thus, an A-Box encompasses enhanced knowledge about the domain of interest [4].

In contrast, an A-Box contains "membership statements" that apply the knowledge of concepts to the level of individuals. Membership statements represent facts about individual entities associated with the terminological concepts of the T-Box [4].

Example Examples of statements within the A-Box include:

- that a concrete entity belongs to the class Prosumer (e.g., $\texttt{Prosumer}(\texttt{HouseholdX})$) or
- that the consumer on the third household in line consumes no energy at this moment.

Once an abstraction level is established, ideally all factors can be classified within the ontology.

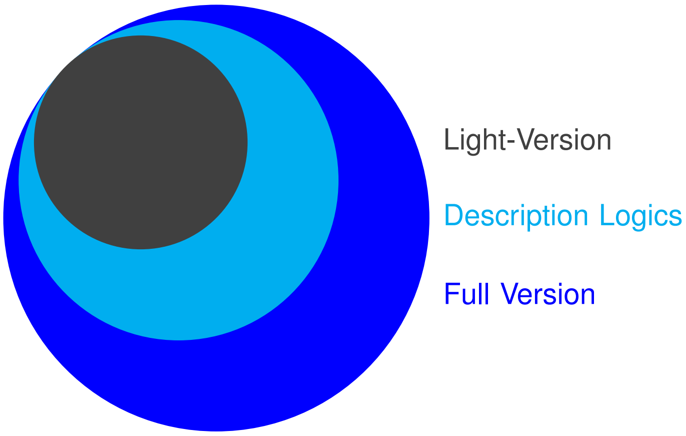


Figure 5: Hierarchy of OWL Versions [24]. Graphic from "Semantic Web Technologies" (Dr. Harald Sack, Hasso-Plattner-Institut, Universität Potsdam) in [53]

4.5.1 OWL

One way to represent ontologies in a machine-readable format is through the Web Ontology Language (OWL) 2. It was developed after ontologies in RDF Schema no longer provided sufficient expressiveness to represent the desired relationships [30]. For this purpose, a working group was established by the World Wide Web Consortium (W3C) to develop OWL, and in 2004, the W3C released a recommendation for this language.

OWL is available in several versions. The hierarchy of these versions is depicted in Figure 5.

From OWL Light to the full version, there is an increase in expressiveness [24] along with a decrease in possible (and decidable) analysis procedures [24]. Although the first version, OWL 1, already includes many functions and embedded inference tools like RACER [26], there are still issues such as faulty syntax analysis of its syntax [24]. These were addressed with the release of OWL 2.

OWL 2 was split in the same way as OWL 1. Its hierarchy is therefore also shown in Figure 5.

4.5.2 Protégé

Protégé is a development environment for OWL 2 that includes many special features. For example, it offers the possibility to directly use description logic inference tools like HermiT and Pellet within the application, as Protégé includes a direct memory connection.

These inference tools allow for the analysis of ontologies created in Protégé. For example, the consistency of the ontology can be checked. Additionally, using these tools allows for specific queries to the ontology, such as querying subclasses of a subset of classes.

Protégé was developed as an environment for the development of knowledge-based systems and has been continuously improved since its release in 1983. It was originally conceived to alleviate a bottleneck in knowledge acquisition. The first version of Protégé was an application that provided structured knowledge to simplify the knowledge acquisition process [21]. Since its release in 2015, Protégé has evolved into the most widely used platform for creating ontologies [35].

Protégé is available as both a local program and a web application called Protégé-Web. Both options have advantages and disadvantages. While the local program does not require an internet connection, the web version allows for easy sharing of developed ontologies with others who can collaborate without the need for external versioning. Protégé-Web can also be used locally, allowing for work within one's network without external access. However, Protégé-Web does not include the inference tools available in the desktop version.

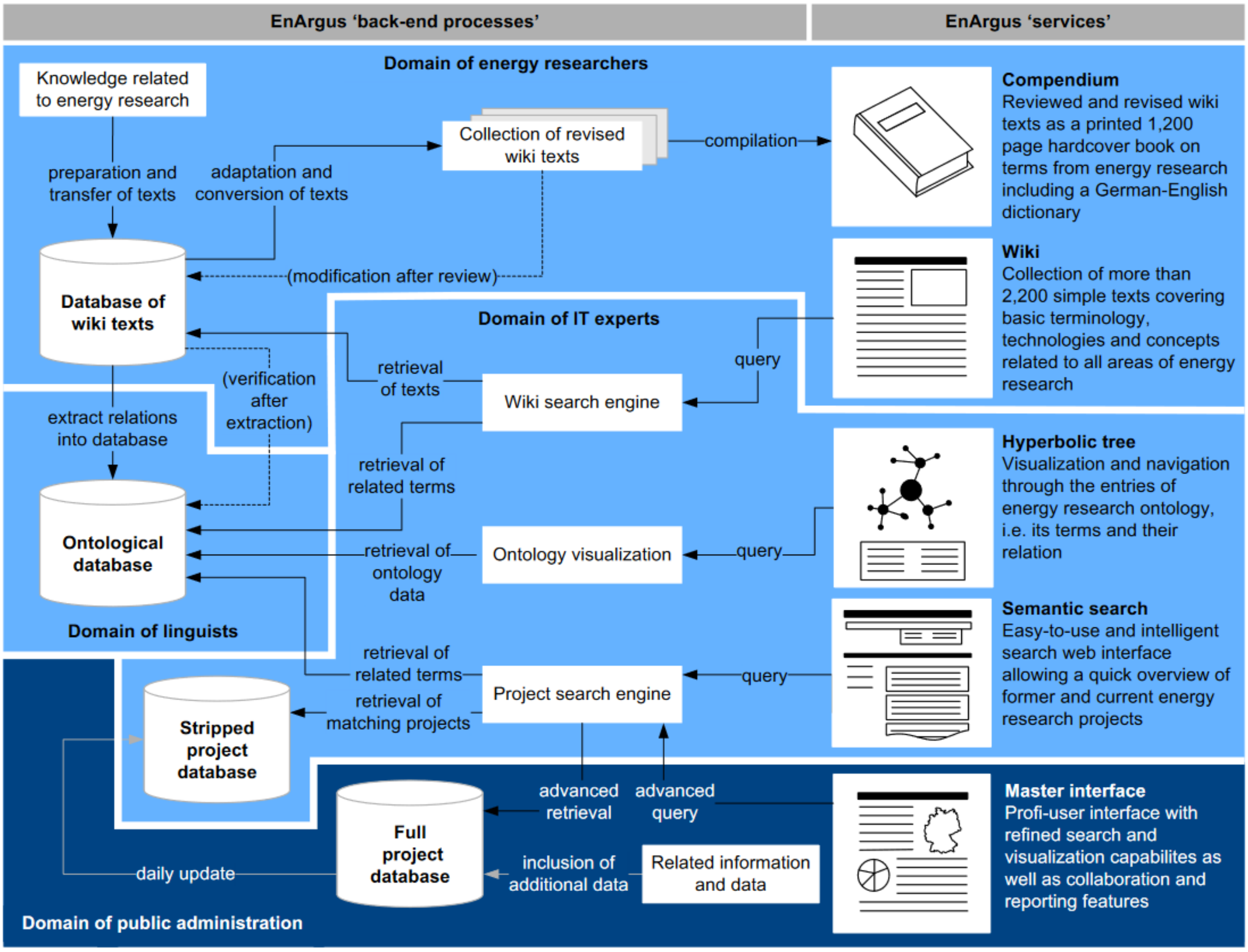

EnArgus 'back-end processes'
EnArgus 'services'
Domain of energy researchers
Knowledge related to energy research
preparation and transfer of texts
adaptation and conversion of texts
Collection of revised wiki texts
compilation
Compendium
Reviewed and revised wiki texts as a printed 1,200 page hardcover book on terms from energy research including a German-English dictionary
Database of wiki texts
(modification after review)
Wiki
Collection of more than 2,200 simple texts covering basic terminology, technologies and concepts related to all areas of energy research
Domain of IT experts
query
retrieval of texts
Wiki search engine
(verification after extraction)
extract relations into database
retrieval of related terms
Hyperbolic tree
Visualization and navigation through the entries of energy research ontology, i.e. its terms and their relation
Ontological database
retrieval of ontology data
Ontology visualization
query
Domain of linguists
Semantic search
Easy-to-use and intelligent search web interface allowing a quick overview of former and current energy research projects
retrieval of related terms
Project search engine
query
Stripped project database
retrieval of matching projects
advanced retrieval
advanced query
Full project database
Master interface
Profi-user interface with refined search and visualization capabilites as well as collaboration and reporting features
daily update
inclusion of additional data
Related information and data
Domain of public administration

Figure 6: Simplified overview over EnArgus from [29]

4.5.3 Ontologies in the Energy Domain

There is a sum of existing ontologies in the energy domain to mention.

In their work Booshehri et al. [8] show the concept for the Open Energy Ontology (OEO) which includes domain terminologies from certain categories. It includes geography, meteorology, math and computer science, economic and engineering terms. The OEO is part of a toolbox called *Open Energy Family*.

A well-known ontology in the energy domain is EnArgus, which was initiated by the German Federal Ministry for Economic Affairs and Energy (BMWi). Oppermann et al. [38] present this ontology stating that EnArgus "contributes to making the energy sector more transparent and offers clear advantages for professional use compared to similar systems" [38]. A simplified overview from Hirzel et al. [29] is shown in Figure 6.

SARGON is a smart grid ontology combining classes shown in Figure 7. It was presented by Haghgoo et al. [27] and extends the smart appliance reference ontology (SAREF) which was developed for the interconnection of smart devices in the context of IoT.

As Ontology for Energy Management Applications (OEMA) focuses on Energy Management terminologies and aims for one unified ontology in this sector. [15] state that there are already existing ontologies like BOnSAI [47] or ThinkHome [39] but representation of different energy domains with different levels of detail and different terminology raises an interoperability problem.

In a later publication Cuenca, Larrinaga, and Curry [16] again address this problem considering even more ontologies to combine in the sectors of smart home energy management applications, build-

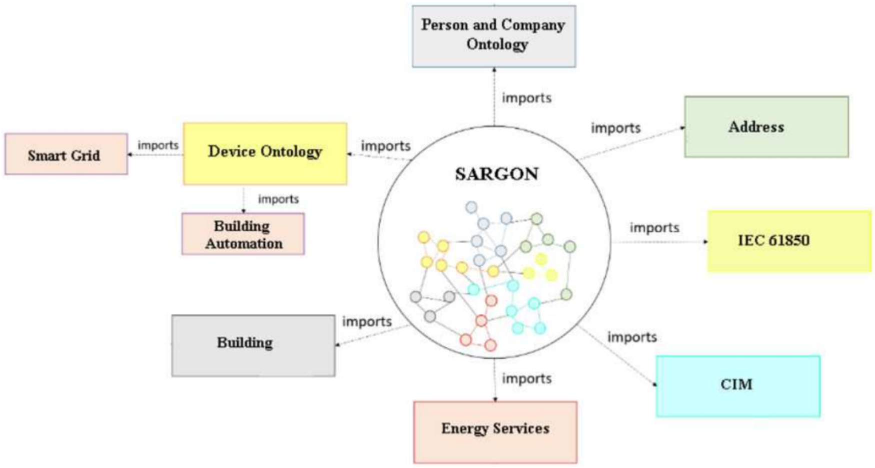


Figure 7: Conceptional view of SARGON in Protégé. From [27]

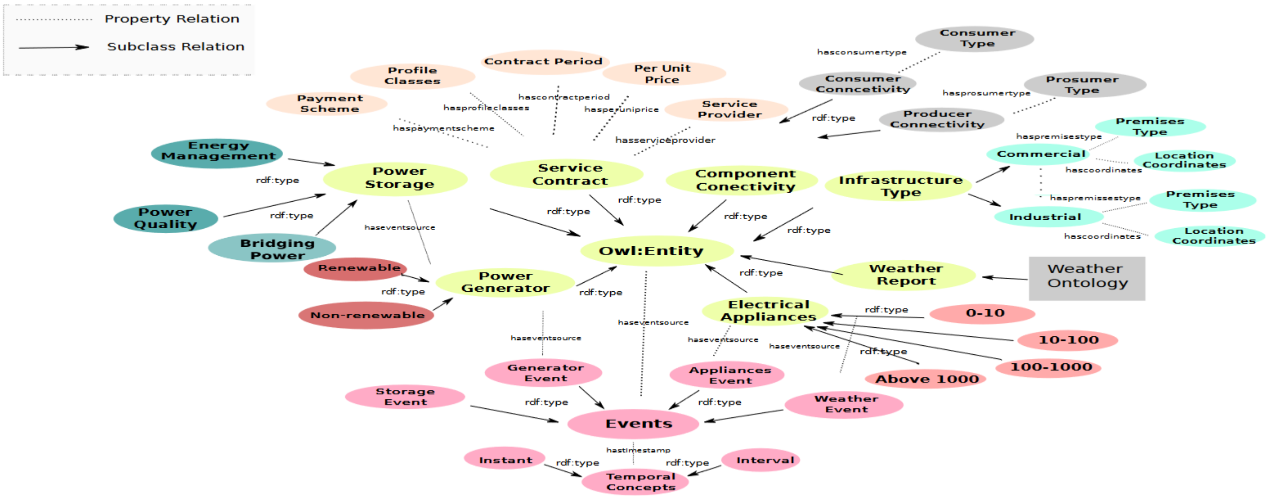


Figure 8: Design of the prosumer oriented ontology approach. From [22]

ing/district/city energy management applications, organization energy management applications, and smart grid demand response management applications.

One of the considered ontologies is SEMANCO. Madrazo, Sicilia, and Gamboa [33] aim to inform stakeholders in urban planning concerning CO_2 reduction. Therefore they link ontologies from different domains to include already existing knowledge.

Gillani, Laforest, Picard, et al. [22] propose a prosumer-centered ontology for the energy domain. Its design is shown in Figure 8. The focus is on the complexity of entities that serve several purposes as prosumers do with consumption and generation.

Burel, Piccolo, and Alani [9] focus on creating awareness. Therefore, the proposed ontology *EnergyUse* pivots around the terms of energy consumption. This is thought to enable users to view and compare energy consumption and discuss through a common terminology.

In 2017 the European Telecommunications Standards Institute (ETSI) voted for an extension of SAREF called SEAS. SEAS is a modularized and versioned ontology with core modules containing ProcessExecution, Evaluation, System, and FeatureOfInterest. Linked with these core modules are vertical and alignment modules as well as external ontologies. Lefrançois [31] points out contributions regarding this ontology and shows its structure as seen in Figure 9.

OnoPowSys is a very specific ontology used in a Knowledge Management System for controlling a virtual Eco-Industrial Park. There are two studies shown by Devanand et al. [18]: Application of

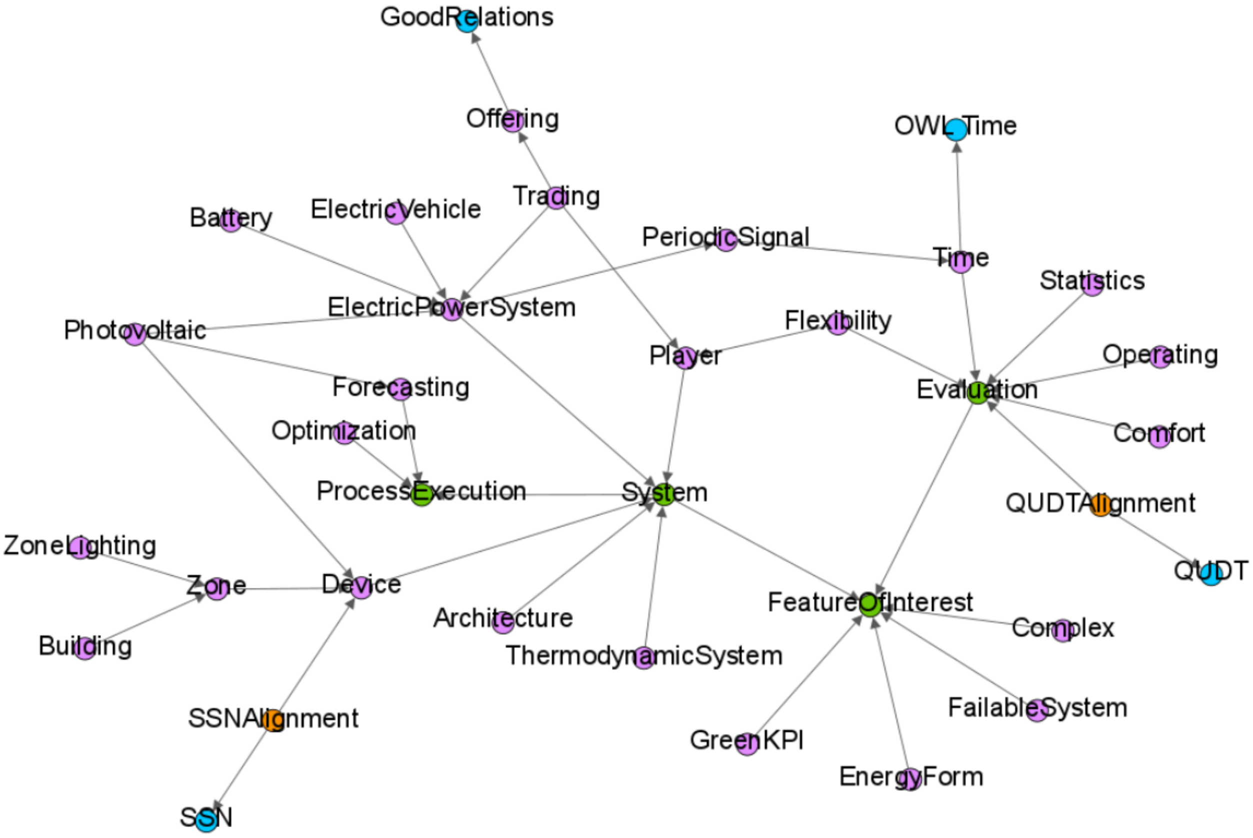


Figure 9: Structure of SEAS. Core modules are shown in green, vertical modules in pink, alignment modules in yellow, and external ontologies in blue. From [31]

optimal power flow to the connected Eco-Industrial Park and cross-domain interaction in the case of knowledge exchange in a diesel power plant making use of chemical and electrical engineering.

Another specific ontology is OntoMG, which is tailored to microgrids. Salameh et al. [40] aim to solve two problems in microgrids: semantic interoperability and multi-objective aspects of the microgrid. Hence, OntoMG shall be able to make components in the grid semantically able to communicate with each other through defined standards and model all aspects of the microgrid to fulfill all objectives.

5 Concepts for Machine-Readable Knowledge Representation

In the RESili8 project we designed a concept for knowledge representation as well as additional techniques needed to make efficient usage of it. These are described in the following sections.

Our focus in the RESili8 project is to make expert knowledge usable for AI applications (more specifically: reinforcement learning). Therefore the concept provides features that are especially useful in this context.

5.1 Sample Misuse Case: Usage of Electronic Vehicles as Movable Batteries

The first step in concept development was finding a scenario that is fitting to the project scope and can be used as a common discussion base.

In multiple meetings, a scenario was elaborated that has relevance in grid operation and is interesting for experiment development. The scenario was then transferred into a MUC.

The main focus of this MUC is the usage of Electric Vehicles (EVs) as so-called moving batteries. This means, that the EVs batteries are also used as a feed-in source instead of just loading them for usage.

This is valuable in situations in which the grid operator can decide between load or feed-in. However, when the EV is connected on private property without control-contract the grid operator is left with the owner or company deciding about the schedules. If one of those wants to get compensation for lowering its energy consumption it might be a valid strategy to first increase the load by connecting all available vehicles. The arising bottleneck then might force the grid operator to pay money to lower the load. Therefore, a constant money flow would arise. Not paying the owners of the properties the load was raised might help in the first instance but one has to take in mind that property owners can cooperate in this instance.

The same is the case for feed-in. Feeding in on bad timing might be beneficial, as the price for consumed energy might drop while there is no real over-production.

The MUC contains two sub-scenarios: One in which Electric Vehicle (EV) batteries capacities are loaded and fed-in with bad timing and one in which it is done position-wise. Position-wise refers to a setup with at least two feeders in which one has a high load and one has a low load. While intuitive it would be beneficial to charge the EVs at the feeder with a low load, it is vice versa. EVs are charged at the feeder with a high load and feed-in at the feeder with a lower load. This creates a power flow in a direction that might become critical for the grid operator.

We chose this scenario, as it might happen in a grid with specific market setups, and it's a scenario with a lot of tuneable parameters, which are to be analyzed by reinforcement learning experiments during the RESili8 project.

The whole MUC can be found in the appendix subsection A.1.

5.2 Designed Concept: Embed MUCs in STPA Analysis and Describe Lab-Testcases through HTD

The first concept we came up with is the combination of MUC, Systems Theoretic Process Analysis (STPA), and Holistic Test Description (HTD) in a hierarchical order. At the first level STPA is applied to the topic of interest. As mentioned, the outcome will include hazard scenarios found for the topic of interest.

Using this STPA output, MUCs are defined. They will be extended through specific expert knowledge and therefore describe the situation in more detail. From this MUC then experiments can be defined.

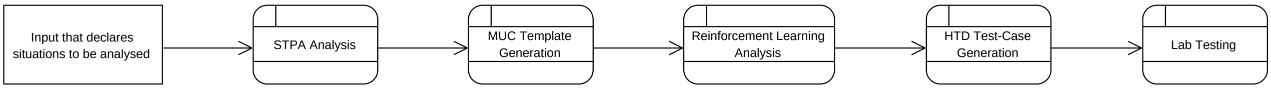

Input that declares situations to be analysed
STPA Analysis
MUC Template Generation
Reinforcement Learning Analysis
HTD Test-Case Generation
Lab Testing

Figure 10: Information flow for the proposed concept.

This can be done either directly from the MUC data that can be extended if needed (see section 5.2) or from a combination of data formats.

In our concept we figured that one way to do so is by extending the MUC-STPA toolchain by HTD for test definition. This is especially useful with lab testing. This is also a beneficial addition to the STPA-MUC-RL toolchain, as scenarios marked as critical by the reinforcement learning experiments can then be evaluated in the lab with real-time operating components.

As an addition to this concept, STIX and TAXII can be included to achieve a easy to share knowledge database, that can be extended after analysis results are given.

Extension of Misuse Cases If you want to use MUCs for experiment generation, extensions have to be made. The following part was already covered in a publication ([54]) coming from the project context in collaboration with the University of Oldenburg. It describes the extension for the generation of palaestrAI experiment files. palaestrAI is a tool developed at the University of Oldenburg and in OFFIS and is used as a tool for AI analysis in RESili8. Figure 11 shows the database export of an experiment in palaestrAI.

In order to create a comprehensive experiment file for use with palaestrAI using misuse case data, certain modifications need to be incorporated into the template.

As illustrated in figures 11 and 1, both formats contain a significant amount of data. In the approach presented here, where the experiment file is generated from the MUC, the data from the MUC is considered as given, while the data from the experiment needs to be generated based on the provided data.

We anticipate that actor groupings will represent a single AI agent. All actors associated with the actor grouping must be assets usable and/or controllable by the agent.

Certain data can be correlated (refer to figure 12 and detailed listing in table 1).

For instance, the "Actorgrouping Name" from the MUC can be linked to the "Agent name" in the experiment description. This is feasible because the defending Actorgroupings can be treated as a "Defender-Agent," and the attacking Misactorgroupings can be treated as an "Attacker-Agent."

Additionally, the "Actor Name" in the corresponding table can be aligned with "Simulation Component Name," describing assets that the agent (actor grouping) can use and/or control. This correlation extends to "Actor Type," which maps to "Simulation Component Type," indicating the type of asset (e.g., sensor, PV, ...). The same applies to "Misactor Intentions" and Objectives, which can be mapped to general "Agent Objectives" or, in the case of "Misactor Intentions," to "Attack Agent Objectives."

Initially, there is no designated input space for experiment-specific identifiers such as the seed, the number of repetitions, the maximum number of generated runs, or the palaestrAI version. Additionally, there is no provision for environmental declarations, resulting in the absence of sensor and actuator declarations in the misuse case, as well as grid declarations (buses, power plants, etc.). Consequently, no mapping between agents and sensors or actuators can be derived from the MUC at this point.

Moreover, all the necessary definitions for the simulation environment are absent in the MUC. Although, if filled out with strict constraints, one can extract component names and types from the misuse case, there is no further declaration in a machine-readable format. Accommodating this data

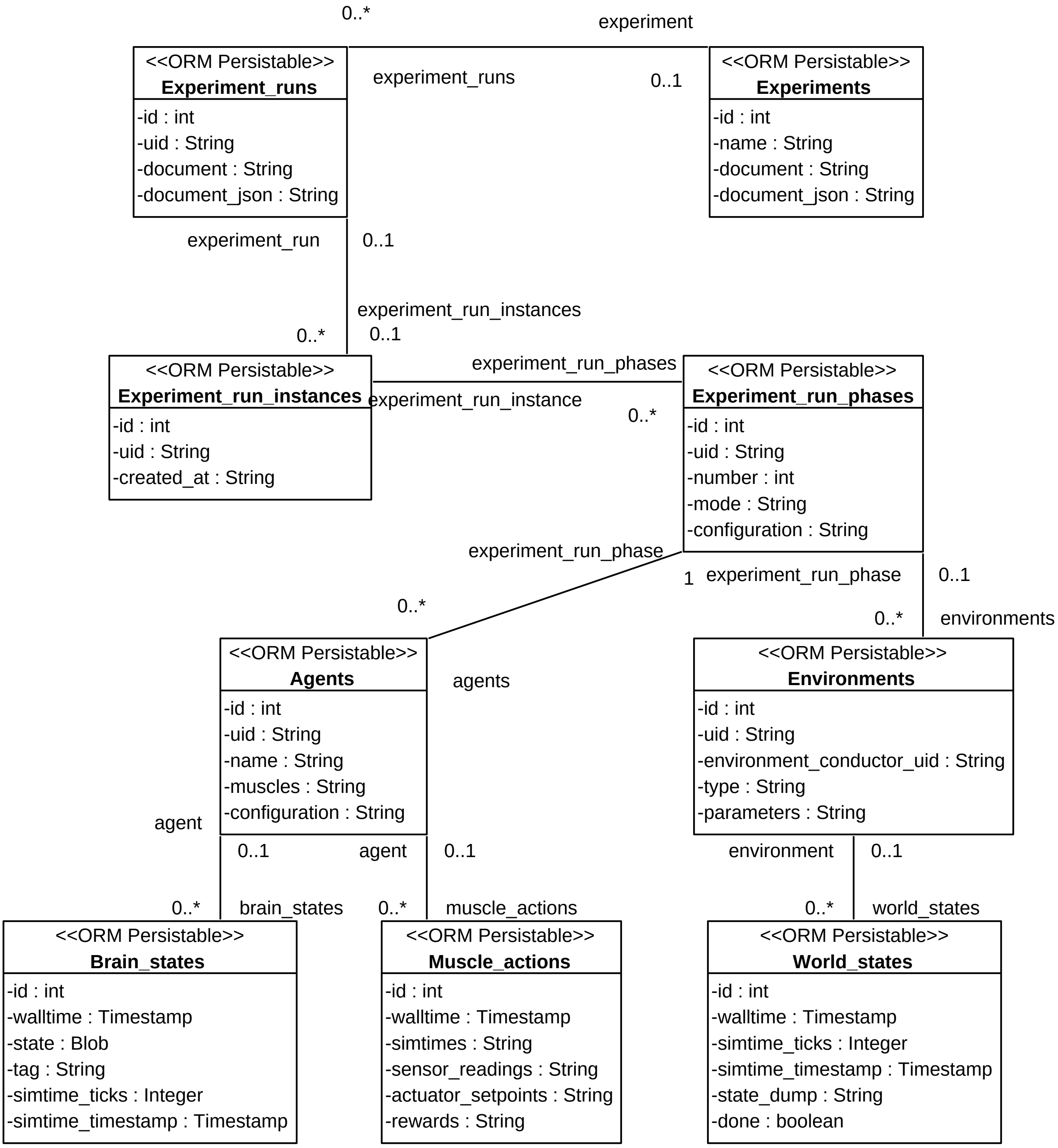


Figure 11: Experiment Design schema in palaestrAI [54]

MUC Information	**Experiment Information**
Actorgrouping Name	Agent Name
Misactor Intentions	Attack Agent Objectives
Objectives	Agents Objectives
Actor Name	Simulation Component Name
Actor Type	Simulation Component Type

Table 1: Current maximal mapping of MUC and Experiment Information

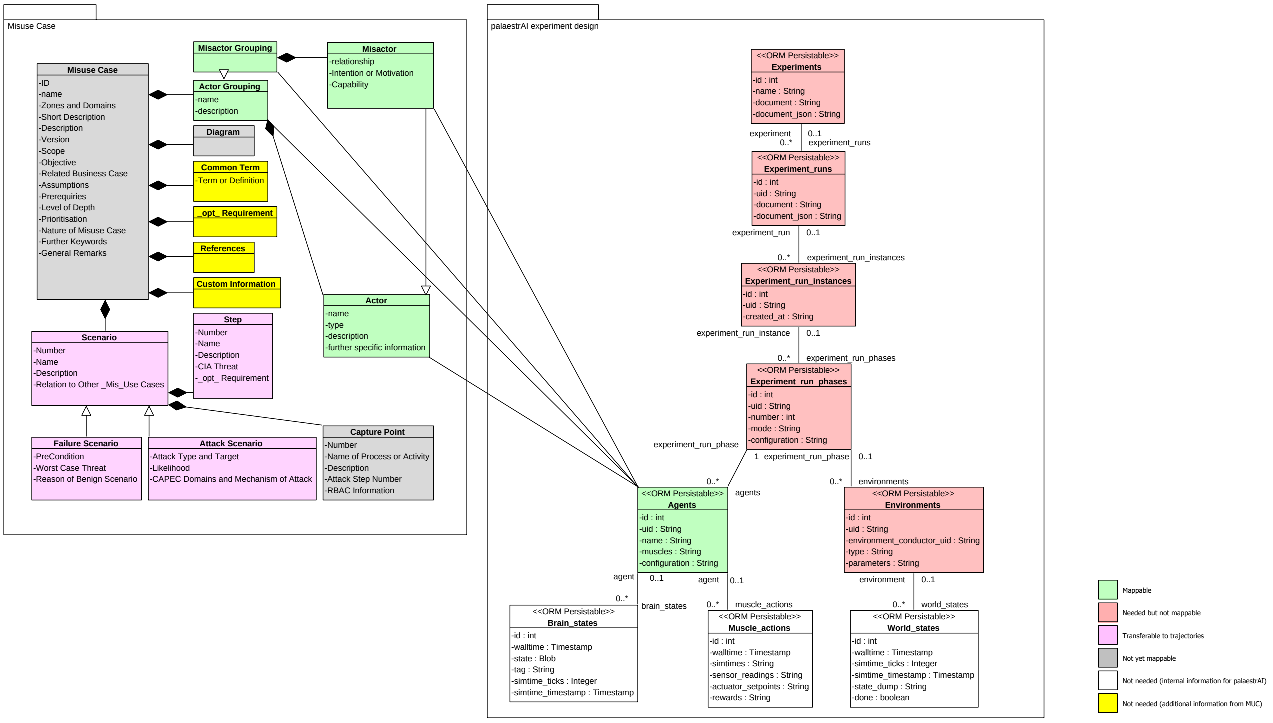


Figure 12: MUC and palaestrAI data formats compared and mapped [54].

in a structured machine-readable way would be less complex and less prone to errors, assuming the information is entered correctly, as with unstructured text.

The next missing element in the misuse case template, when attempting to extract an experiment file for use with palaestrAI, is phase configurations. The MUC provides only a general overview of the scenario, unrelated to an AI training or test phase. Including this information in a separate block or document could be beneficial for expedited parameter tuning.

For the experiment file, a definition of the agent's brain and muscle is also necessary. These factors influence the actions taken (muscle) as well as the memory of the last actions and the learning process (brain). Integrating these parameters in a readily accessible location is considered advantageous.

Finally, the absence of information in a misuse case used for palaestrAI experiment file generation includes the combination of agents, assets, and parameters for designing different experiment run files. Since misuse cases are not typically tailored to different experiments, this information is lacking. A fitting approach to address this is the use of multiple (mis)-actor groupings for different agents, along with multiple generations of assets for tuning. The details for combining these elements would then be added to the other tune-able parameters.

In summary, there is a gap when transitioning from MUC to a palaestrAI experiment design. This can be seen in Figure 12, where both data formats are compared against each other.

With this approach, we propose a toolchain as seen in Figure 10, where an STPA-analyzed situation is further investigated by transformation through MUC templates, experiment file generation, and reinforcement learning. The specific, problematic situations and their hyperparameters e.g. grid structure, number of EVs in the grid, or location of wall boxes, can then be described in HTD and taken into lab tests, where e.g. new algorithms or control schemes can be developed and tested against these specific setups.

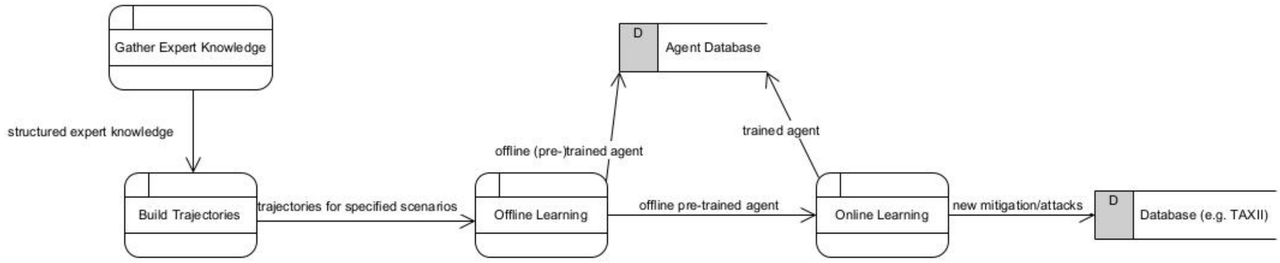


Figure 13: Proposed dataflow for generated trajectories from expert data

5.3 Document Read-out and General Experiment File Generation

For automated template processing to generate experiment files, a document read-out is needed. Like the MUC extension, the following was already covered by a paper ([52]) in project context and collaboration with the University of Oldenburg.

After the MUC template is filled out, the diagrams and the tables of the MUC are exported as serialized and standardized XML Metadata Interchange (XMI)/XML files based on IEC 62559-3. Therefore, the diagrams are exported as an XMI from a tool like visual paradigm, while the MUC DOCX file is exported as an XML file via Microsoft Word. These files are then read into a script that generates an experiment file based on the information from the MUC and commonly known information such as the structure. The simplified version of this algorithm is presented as pseudocode in algorithm 1. For the presentation of this approach, only a limited set of information is taken from the MUC. The remaining needed information e.g. the environment and the mapped, distinct sensors in this environment are derived from a previously created experiment file.

For receiving the agent data the exported diagram is scanned for entities with the «agent» stereotype, if a MUC export is used to generate the experiment file, the XML is scanned for the actor table. From these sources, the agent's name and its objectives are taken. Afterwards, the YAML output file is generated. Therefore the setup information from an already created experiment is taken. The information taken from the input is then merged with the additional information and put together into a complete experiment file.

5.4 Trajectory Generation from Expert Knowledge

When a data readout from MUCs is accomplished, the next step in the RESili8 will be trajectory generation for offline learning. Offline learning enables machine learning agents to make use of predefined strategies and therefore expert knowledge. As the machine learning agents we aim to use are not able to understand natural language, it is imperative to generate data to learn from.

We aim to do this based on the specified scenarios in the MUC template. A general overview of the dataflow is depicted in Figure 13.

Algorithm 1 Pseudocode: Simplified Generation of an Experiment File from XML Data [52]

```
Open XML input file                                  ▷ MUC XML and/or diagram XML export
name_list = empty list
objective_list = empty list
for actor in MUC do ▷ either from UML actor definition or by scanning the actor tables in the MUC
    Add name of agent to name_list
    Add objective to objective_list
end for
Close XML input file
Open YAML output file
Write experiment setup data to the output file     ▷ This is simplified for a first presentation of this approach
for agent_name in name_list do
    Write agent description to the output file ▷ This data is a mixture of already created experiment definitions and the agent description from the input.
    Map agent objective from objective_list
    Write mapped objective to the output file
end for                      ▷ The following is well simplified for a first presentation of this approach
Write sensor and actor information to the output file
Define phases according to actor information in the output file
Close YAML output file
Output the generated YAML file
```

6 Conclusion and Future Work

In this work, we presented an innovative approach that combines STPA with MUC templates and HTD. The integration of reinforcement learning improves the toolchain's ability to analyze potential threat situations in more detail. This speeds up the generation of lab-specific test cases, as the toolchain outputs explicit test case specifications. The use of STPA and MUCs facilitates the inclusion of expert knowledge in reinforcement learning experiments, while the machine learning component accelerates the evaluation of multiple parameters and setups, which exceeds the capabilities of the real-time lab. In particular, situations identified as critical after training and testing reinforcement learning agents will be documented in HTD for reproducible laboratory testing.

In our opinion, the implementation of this concept aims to achieve two things: streamlining the processes for defining test cases and increasing test coverage through comprehensive agent exploration.

The natural progression in the case of future work is the implementation of the proposed toolchain, aiming for at least partial automation. A broader perspective involves integrating this toolchain into a Continuous Integration/Continuous Deployment (CI/CD) pipeline that includes lab testing. This would enable the toolchain to continuously update the lab test specifications based on new insights from STPA or discoveries from research with machine learning agents. The overall goal is to create a dynamic and adaptable testing framework that increases the robustness and efficiency of cybersecurity measures.

Appendix A Appendix

A.1 MUC Template: Electric Vehicles as Movable Batteries

1.1.1 1 Description of the Misuse Case

1.1 Name of the Misuse Case

Misuse Case Identification		
ID	Area Domain(s)/ Zone(s)	Name of Misuse Case
R8-EV1	Distribution / Operation	Usage of EV to create a bottleneck in the grid

1.2 Version Management

Version Management				
Version No.	Date	Name of Author(s)	Changes	Approval Status
0.1	08.06.2023	Arlena Wellßow	First Draft	Draft
0.2	10.08.2023	Arlena Wellßow	Filled in Scenarios	Draft

1.3 Scope and Objectives of Misuse Case

Scope and Objectives of Misuse Case	
Scope	This misuse case describes unwanted or hostile behavior when using EVs in a way so that a bottleneck is created
Objective(s)	Defender: Keep the grid stable Attacker: Move and charge/decharge EVs in order to create bottlenecks
Related Business Case(s)	Grid maintenance, Higher EV coverage

1.4 Narrative of Misuse Case

Narrative of Misuse Case

Short Description

In order to harm the grid, the here described attacker will use EVs in order to create bottlenecks in the grid, which could lead to failures or the need to insert money into local markets.

Complete Description

Narrative of Misuse Case
In recent years, electric vehicles (EVs) have gained popularity as a cleaner and more sustainable mode of transportation. However, as with any technological advancement, there is potential for misuse. This includes the concept of deliberately causing harm to the power grid by creating bottlenecks and utilizing EVs as mobile batteries in a hostile manner. Harm to the Grid: The power grid is a complex network that delivers electricity from power plants to consumers. Disrupting this system can have severe consequences, affecting not only daily life but also critical services that rely on a continuous power supply. By intentionally damaging or impairing the grid's infrastructure, individuals can cause widespread chaos and societal disruption. One potential strategy to harm the grid is by creating bottlenecks in the electricity distribution process. EVs, with their ability to store and discharge large amounts of electrical energy, can be used as mobile batteries to manipulate the demand and supply dynamics. By coordinating the charging and discharging of a fleet of EVs strategically, it is possible to overwhelm the grid's capacity at specific points, causing localized power outages and cascading effects throughout the system. EVs are equipped with advanced battery systems capable of storing significant amounts of electricity. In a hostile scenario, these vehicles can be leveraged as mobile power sources, moving in a manner that disrupts the stability of the grid. This strategy involves charging EVs during periods of high demand and subsequently discharging them rapidly when the demand is low, overwhelming the grid's capacity and potentially causing power fluctuations or blackouts. To maximize the impact on the grid, hostile actors may deploy sophisticated algorithms, technologies and techniques to optimize the charging, decharging, and movement of EVs. By coordinating these actions to coincide with peak demand periods or specific areas of the grid, they can amplify the disruptions caused. Such tactics could be used as a form of targeted attack, aiming to paralyze specific regions or critical infrastructure.

1.5 Misuse Case Conditions

Misuse Case Conditions
Assumptions
The grid is in a stable state before the attack. The attacker has controllable EVs in the grid.
Prerequisites
EVs are charged enough to be moved/ can be charged enough.

1.6 Further Information to the Misuse Case for Classification/ Mapping

Classification Information
Relation to other Use Cases and Misuse Cases Grid Operation
Level of Depth SMUC
Prioritisation high
Generic, Regional or National Relation Most likely national
Nature of the Misuse Case Technical / security

Classification Information
Further Keywords for Classification EVs, Attack on grid, create bottlenecks

1.7 General Remarks

General Remarks

1.1.2 2 Diagrams of Misuse Case

Diagram of Misuse Case

1.1.3 3 Technical details

3.1 Actor and Misactor Profiles

Actors			
Grouping		Defender	
Group Description		Actor (Agent) who protects the grid against the attacking actors.	
Actor Name	Actor Type	Actor Description	Further Specific Information
Defender	Defender	Defends the voltage band by controlling the not impacted assets and regulating the charging schedule	

Misactors						
Grouping		Harmful Actor in the Grid				
Group Description		Misactors who want to harm the grid				
Misactor Name	Misactor Type	Misactor Description	Relationship	Intention/ Motivation	Capability	Further Specific Information
EVAttacker	Unknown	Wants to harm the grid by creating bottlenecks using EVs	Has access to controllable EVs in the smart grid	Generate bottlenecks using EVs	Is able to control EVs in the grid	

3.2 References

References						
No.	References Type	Reference	Status	Impact on Misuse Case	Originator / Organisation	Link

1.1.4 4 Step by Step Analysis of Misuse Case

4.1 Overview of Failure Scenarios

4.2 General/Specific attack scenarios

Attack Scenario Conditions						
Attack Scenario # No.	Attack Type	Attack Target	CAPEC Domains and Mechanisms of Attack	Relevant Scenario No.	Likelihood	Relation to other (Mis-)Use Case
EV_1	Unwanted Behavior (to many EVs charging)	Power Grid			High	
Step No.	Name of Process/ Activity	Event	Description	Step of the Attack Scenario	CIA Threat	Requirements R-ID
1	First EV starts charging	Charging started	A first EV is charging on a bus			
2	Second EV starts charging	Charging started	A second EV starts charging on a bus. This can be several timesteps after step 1. If one of the EVs is disconnected, SC transfers to step 1.			
3..n; n>=3	Nth EV start charging	Charging started	A nth EV starts charging on a bus. This can be several timesteps after step n-1. If one of the EVs is disconnected, SC transfers to step n-1			

Attack Scenario Conditions						
n+1	Capacity reached	Capacity reached	The maximal capacity for charging is reached			
N+2	(N+1)th EV starts charging	Charging started, Capacity to low	A new EV is charging. However, capacity is to low to allow charging in this timestep. Unwanted behavior occurs.			

Attack Scenario Conditions						
Attack Scenario # No.	Attack Type	Attack Target	CAPEC Domains and Mechanisms of Attack	Relevant Scenario No.	Likelihood	Relation to other (Mis-)Use Case
EV_2	Moving of EVs in order to gain money from markets	Power Grid			High	
Step No.	Name of Process/ Activity	Event	Description	Step of the Attack Scenario	CIA Threat	Requirements R-ID
1	EVs are charged	Charging started	EVs are charged anywhere			
2	Prices are low in a specific station	Price notification at A	A price notification is sent for substation / charging station A			
3	EVs get charged there	Charging started at A	EVs are moved and charged at substation / charging station A			
Time passing	...	...	This might be due to a price set at a later point in time or because of EV movement	...	...	...
4	Sell prices high	Price notification at B	A price notification is sent for substation / charging station B			

Attack Scenario Conditions

5	EVs feed in	Feed in started at B	EVs are moved and feed in at substation / charging station B			

Attack Scenario Conditions

Attack Scenario # No.	Attack Type	Attack Target	CAPEC Domains and Mechanisms of Attack	Relevant Scenario No.	Likelihood	Relation to other (Mis-)Use Case
EV_3	2 Feeder: 1 charging 1 decharging	Power Grid			Unknown	
Step No.	Name of Process/ Activity	Event	Description	Step of the Attack Scenario	CIA Threat	Requirements R-ID
1..n	n (n>=1) vehicles charging at feeder A	Charging started	n (n>=1) vehicles charging at feeder A			
Time pass	. . .	. . .	This might be due to the plan of feeding in at bad timing (time based attack) or because of EV movement (spacial attack)	. . .	. . .	. . .
n+1 . . . 2n	n vehicles feeding in at feeder B	Feed in started	n vehicles feeding in at feeder B			

4.3 Overview of Capture point (optional)

Capture Points (optional)

Step No.	Description of the Capture Point	Attack Step No.	RBAC Information

1.1.5 5 Requirements

Requirements(optional)

Categories ID	Category Name for Requirements	Category description

Requirements(optional)

Requirement ID	Requirement Name	Requirement Description

1.1.6 6 Common Terms and Definitions

Common Terms and Definitions

Term	Definition

1.1.7 7 Custom information(optional)

Custom Information (optional)

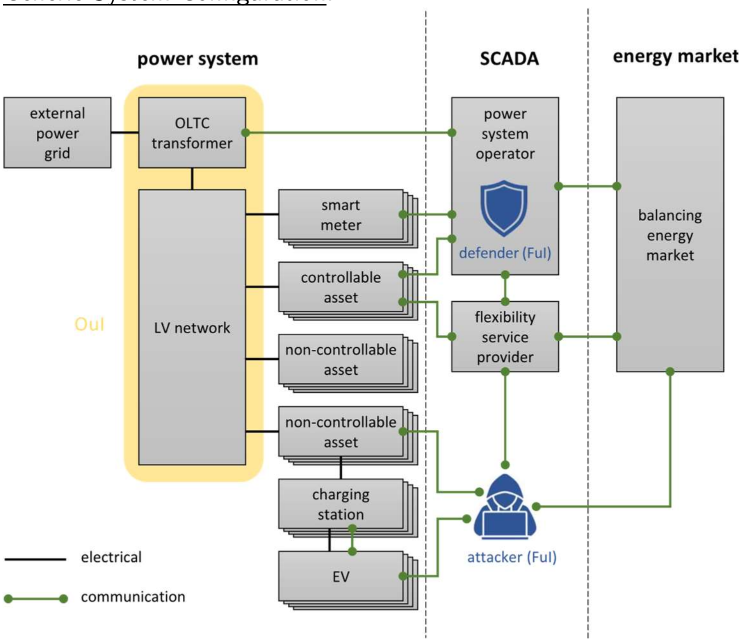
Key	Value	Refers to subsubsection

HTD Template: Electric Vehicles as Movable Batteries

1 Test Case EV-Misuse

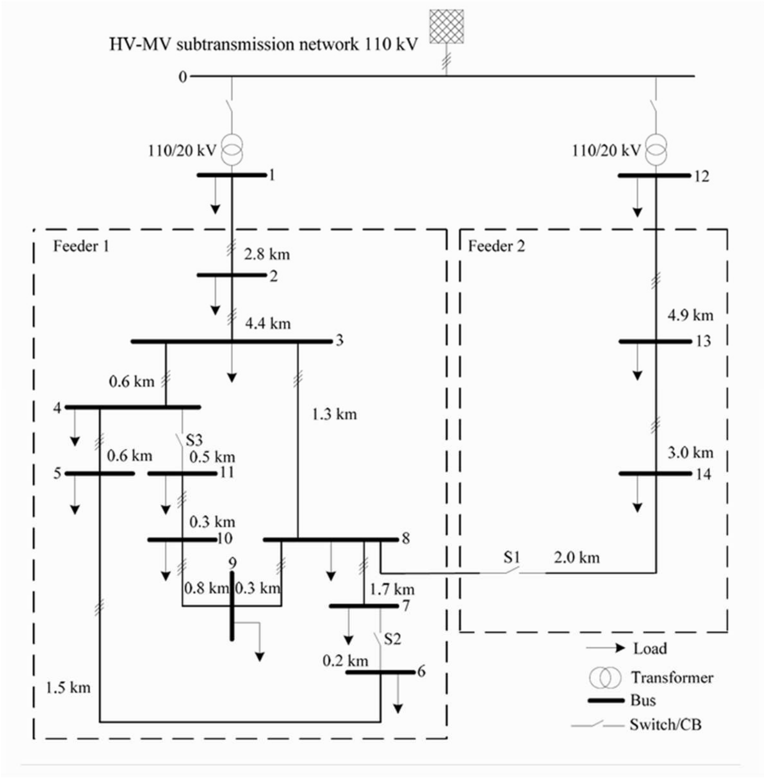
Authors A. Wellßow, E. Veith, A. Theil, E. Widl Version 1.0
Project Resili8, Task 4.4 Date 28.11.2023

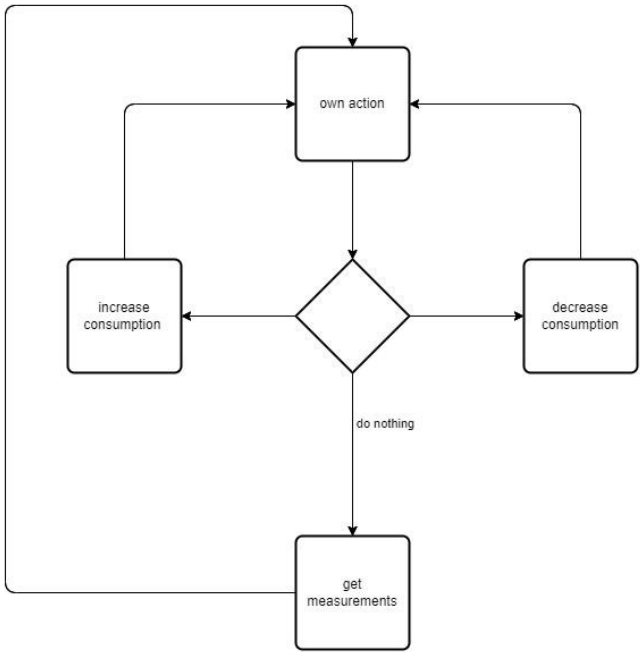
Title of the Test Case	Misuse of an EV fleet for attacks on the power system
Narrative	To cause harm to the grid, a potential attacker may employ electric vehicles (EVs) to create grid bottlenecks, which could result in grid failures or the need to inject money into local markets. EVs have grown in popularity in recent years as a cleaner and more sustainable means of transportation. However, like with every technical advancement, there is the possibility of abuse. This involves the idea of purposefully inflicting damage to the power system by creating bottlenecks though the deployment of EVs in an adversarial way. The large amounts of electrical energy that EVs can store and discharge makes them ideal for use as mobile batteries to shift demand and supply dynamics. This test case assesses potential attack strategies and their respective countermeasures. The objective is to identify underlying systemic vulnerabilities and estimate the likelihood of the emergence of worst-case environment conditions.
Function(s) under Investigation (*FuI*)	Strategic coordination of charging and discharging of an electric vehicle fleet with peak demand periods can cause localized power disruptions and cascading failures across the system by exceeding the grid's capacity in those places. This test case investigates algorithms, technologies, and strategies of hostile actors to maximize damage to the power system through charging, discharging, and movement of EVs.
Object under Investigation (*OuI*)	• LV network • OLTC transformer
Domain under Investigation (*DuI*)	• power system • control / ICT • EVSE infrastructure
Purpose of Investigation (*PoI*)	Characterization: • assess impact on power system • determine most effective attack and defense strategies

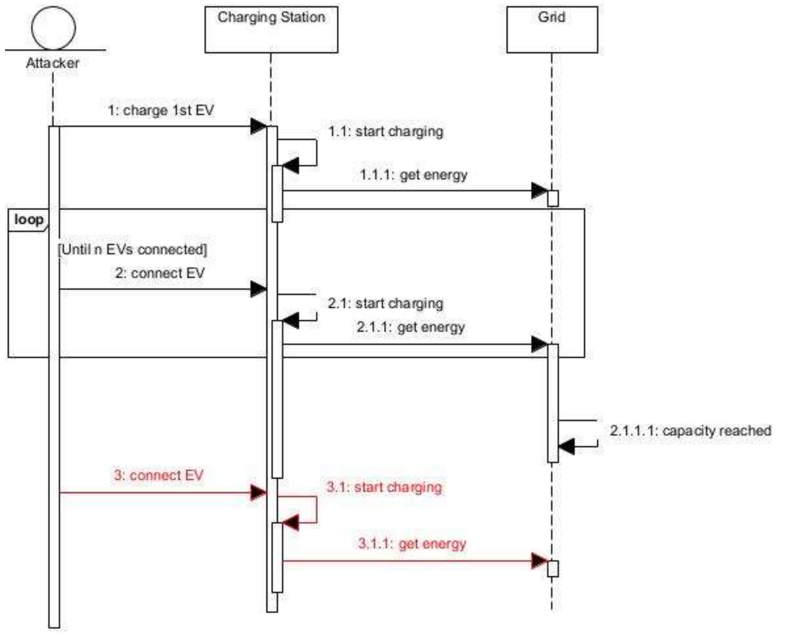
System under Test (*SuT*)	Generic System Configuration:  power system SCADA energy market external power grid OLTC transformer OuI LV network smart meter controllable asset non-controllable asset non-controllable asset charging station EV power system operator defender (FuI) flexibility service provider balancing energy market attacker (FuI) electrical communication Controllable assets: • assets whose power consumption and / or generation can be controlled • actuated either by the power system operator or a flexibility service provider Charging stations: • located on private premises • not supervised / controlled by an EVSE operator
Functions under Test (*FuT*)	• OLTC transformer control • local control of controllable assets for flexibility provision • EV fleet management (by attacker)
Test criteria *(TCR)*	Characterization of LV network stability under attack
Target Metrics *(TM)*	voltage band stability
Variability Attributes *(VA)*	Controllable test factors: • EV fleet charging / dis-charging schedule • market signals • flexibility provision (power consumption of controllable assets) Uncontrollable test factors: • power consumption of loads (base load)
Quality Attributes *(QA)*	voltage band deviation: 1.00 ± 0.07 p.u.

2 Qualification Strategy

2.1 Test Specification EV-Misuse.TS1

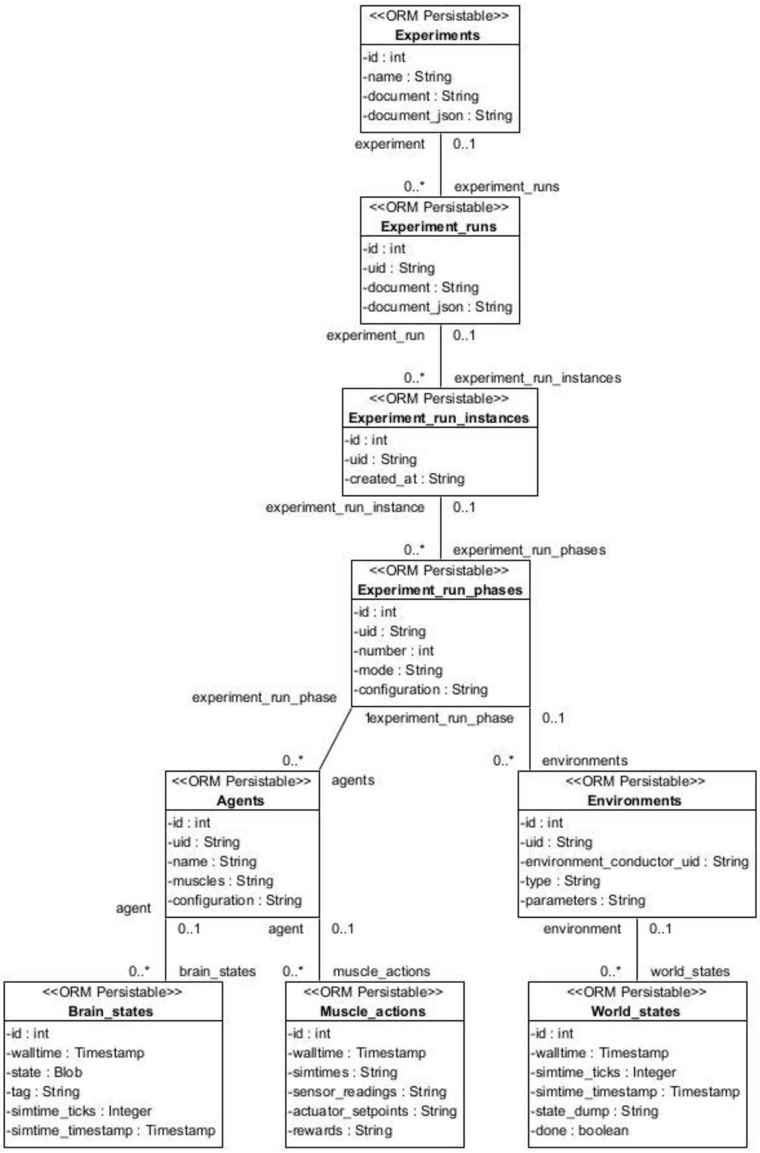
Reference to Test Case	EV-Misuse
Title of Test	Single Feeder Overload
Test Rationale	• excessive EVs charging on private premises strains the power grid • EV charging stations are not controllable by power system operator or flexibility provider
Specific Test System	Power grid:  HV-MV subtransmission network 110 kV 0 110/20 kV 1 110/20 kV 12 Feeder 1 2.8 km 2 4.4 km 3 0.6 km 4 S3 0.6 km 0.5 km 5 11 1.3 km 0.3 km 10 9 8 0.8 km 0.3 km 1.7 km 7 S2 0.2 km 6 1.5 km Feeder 2 4.9 km 13 3.0 km 14 S1 2.0 km Load Transformer Bus Switch/CB
Target measures	• grid voltages at all network nodes • grid voltages at OLTC transformer
Input and output parameters	Controllable input parameters: • tap position of OLTC transformer (1.25% per step) • power consumption / feed-in of charging stations • power consumption of controllable assets Uncontrollable input parameters: • power consumption of loads (base load) Output parameters: • voltages at all busses • active / reactive power at all busses

	• line loadings
Test Design	 own action increase consumption decrease consumption do nothing get measurements Attacker: • start charging • stop charging • increase other consumption (own asset) • decrease other consumption (own asset) • ask for neighborhood connections Defender: • change tap position when voltage band violation reaches ± 0.1 p.u. (delay / dead time: 30 seconds) • increase generation • decrease generation Attack-Pattern:

	 Attacker Charging Station Grid 1: charge 1st EV 1.1: start charging 1.1.1: get energy loop [Until n EVs connected] 2: connect EV 2.1: start charging 2.1.1: get energy 2.1.1.1: capacity reached 3: connect EV 3.1: start charging 3.1.1: get energy
Initial system state	• The grid is in a stable state before the attack. • EVs are sufficiently charged to be moved.
Evolution of system state and test signals	• EV #1 starts charging on a bus. • EV #2 starts charging on a bus. This can be several timesteps after step 1. … • EV #N starts charging on a bus. This can be several timesteps after step N-1. • The maximal capacity for charging is reached. • EV #(N+1) starts charging. However, capacity is too low to allow charging at this timestep.
Other parameters	N/A
Temporal resolution	15 minutes
Source of uncertainty	adaptive behavior of attacker and defender
Suspension criteria / Stopping criteria	stop after predefined period of time (1 day)

3 Mapping to Research Infrastructure

3.1 Experiment Specification EV-Misuse.TS1. palaestrAI

Reference to Test Specification	EV-Misuse.TS1
Title of Experiment	Adversarial Resilience Learning for Single Feeder Overloading
Research Infrastructure	OFFIS
Experiment Realisation	 <<ORM Persistable>> Experiments -id : int -name : String -document : String -document_json : String experiment 0..1 0..* experiment_runs <<ORM Persistable>> Experiment_runs -id : int -uid : String -document : String -document_json : String experiment_run 0..1 0..* experiment_run_instances <<ORM Persistable>> Experiment_run_instances -id : int -uid : String -created_at : String experiment_run_instance 0..1 0..* experiment_run_phases <<ORM Persistable>> Experiment_run_phases -id : int -uid : String -number : int -mode : String -configuration : String experiment_run_phase 1experiment_run_phase 0..1 0..* agents 0..* environments <<ORM Persistable>> Agents -id : int -uid : String -name : String -muscles : String -configuration : String <<ORM Persistable>> Environments -id : int -uid : String -environment_conductor_uid : String -type : String -parameters : String agent 0..1 agent 0..1 environment 0..1 0..* brain_states 0..* muscle_actions 0..* world_states <<ORM Persistable>> Brain_states -id : int -walltime : Timestamp -state : Blob -tag : String -simtime_ticks : Integer -simtime_timestamp : Timestamp <<ORM Persistable>> Muscle_actions -id : int -walltime : Timestamp -simtimes : String -sensor_readings : String -actuator_setpoints : String -rewards : String <<ORM Persistable>> World_states -id : int -walltime : Timestamp -simtime_ticks : Integer -simtime_timestamp : Timestamp -state_dump : String -done : boolean
Experiment Setup	• palaestrAI: train and test attacker and defender as autonomous agents • mosaik: training / testing environment for palaestrAI
Experimental Design and Justification	palaestrAI is the framework for the Adversarial Resilience Learning (ARL) reference implementation. The ARL core concept consists of two agents, attacker and defender agents, working on a common model of a cyber-

	physical system (CPS). The attacker's goal is to de-stabilize the CPS, whereas the defender works to keep the system in a stable and operational state. Both agents do not perceive their opponent's actions directly, but only the state of the CPS itself.
Precision of equipment and measurement uncertainty	N/A
Storage of experiment data	Metadata and results from all simulation runs will be stored in a dedicated database (SQLite) for further processing.

Abbreviations

CPES	Cyber-Physical Energy System
CPS	Cyber-Physical System
EV	Electric Vehicle
EVs	Electric Vehicles
HTD	Holistic Test Description
MUC	Misuse Case
OEMA	Ontology for Energy Management Applications
OEO	Open Energy Ontology
STPA	Systems Theoretic Process Analysis
XMI	XML Metadata Interchange

References

[1] Marie van Amelsvoort, Christina Delfs, and Mathias Uslar. “Application of the interoperability score in the smart grid domain”. In: *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*. IEEE. 2015, pp. 442–447.

[2] Marie Antoinette van Amelsvoort. “SG-rating–Putting values on smart grid architectures”. In: *it-Information Technology* 58.1 (2016), pp. 29–36.

[3] Mana Azamat, Johann Schütz, and Mathias Uslar. “Use Cases Also Exist for Attackers – How to Foster the Concept of Misuse Cases”. In: *12. (Hybrid) Symposium Communications for Energy Systems (ComForEn)*. 2023.

[4] Franz Baader et al. *The description logic handbook: Theory, implementation and applications*. Cambridge university press, 2003.

[5] Sean Barnum. “Information with the Structured Threat Information eXpression (STIX™)”. In: (2013).

[6] Sean Barnum. “Standardizing cyber threat intelligence information with the structured threat information expression (STIX)”. In: *Mitre Corporation* 11 (2012), pp. 1–22.

[7] Sean Barnum. “Standardizing cyber threat intelligence information with the structured threat information expression (stix)”. In: *Mitre Corporation* 11 (2012), pp. 1–22.

[8] Meisam Booshehri et al. “Introducing the Open Energy Ontology: Enhancing data interpretation and interfacing in energy systems analysis”. In: *Energy and AI* 5 (2021), p. 100074. ISSN: 2666-5468. DOI: https://doi.org/10.1016/j.egyai.2021.100074. URL: https://www.sciencedirect.com/science/article/pii/S2666546821000288.

[9] Grégoire Burel, Lara SG Piccolo, and Harith Alani. “Energyuse-a collective semantic platform for monitoring and discussing energy consumption”. In: *The Semantic Web–ISWC 2016: 15th International Semantic Web Conference, Kobe, Japan, October 17–21, 2016, Proceedings, Part II 15*. Springer. 2016, pp. 257–272.

[10] S. Cejka, R. Mosshammer, and A. Einfalt. “Java embedded storage for time series and meta data in Smart Grids”. In: *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. Nov. 2015, pp. 434–439. DOI: 10.1109/SmartGridComm.2015.7436339.

[11] Marie Clausen et al. “Use Case methodology: A progress report”. In: *Energy Informatics* 1.1 (2018), pp. 273–283.

[12] Alistair Cockburn. *Writing effective use cases*. Pearson Education, 2001.

[13] Julie Connolly, Mark Davidson, and Charles Schmidt. “The trusted automated exchange of indicator information (TAXII)”. In: *The MITRE Corporation* (2014), pp. 1–20.

[14] Julie Connolly, Mark Davidson, and Charles Schmidt. “The trusted automated exchange of indicator information (taxii)”. In: *The MITRE Corporation* (2014), pp. 1–20.

[15] Javier Cuenca, Felix Larrinaga, and Edward Curry. “A Unified Semantic Ontology for Energy Management Applications.” In: *WSP/WOMoCoE@ ISWC*. 2017, pp. 86–97.

[16] Javier Cuenca, Felix Larrinaga, and Edward Curry. “DABGEO: A reusable and usable global energy ontology for the energy domain”. In: *Journal of Web Semantics* 61 (2020), p. 100550.

[17] Michiel De Nooij et al. “Development and application of a cost–benefit framework for energy reliability: Using probabilistic methods in network planning and regulation to enhance social welfare: The N-1 rule”. In: *Energy Economics* 32.6 (2010), pp. 1277–1282.

[18] Aravind Devanand et al. “OntoPowSys: A power system ontology for cross domain interactions in an eco industrial park”. In: *Energy and AI* 1 (2020), p. 100008.

[19] Lars Fischer et al. “Adversarial Resilience Learning—Towards systemic vulnerability analysis for large and complex systems”. In: *ENERGY 2019, The Ninth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies*. 9. Athens, Greece: IARIA XPS Press, 2019, pp. 24–32. ISBN: 978-1-61208-713-9. arXiv: 1811.06447.

[20] Ivo Friedberg et al. “STPA-SafeSec: Safety and security analysis for cyber-physical systems”. In: *Journal of Information Security and Applications* 34 (2017), pp. 183–196. ISSN: 2214-2126.

[21] John H Gennari et al. “The evolution of Protégé: an environment for knowledge-based systems development”. In: *International Journal of Human-computer studies* 58.1 (2003), pp. 89–123.

[22] Syed Gillani, Frederique Laforest, Gauthier Picard, et al. “A Generic Ontology for Prosumer-Oriented Smart Grid.” In: *EDBT/ICDT Workshops*. Vol. 1133. 2014, pp. 134–139.

[23] Marion Gottschalk, Mathias Uslar, and Christina Delfs. *The use case and smart grid architecture model approach: the IEC 62559-2 use case template and the SGAM applied in various domains*. Springer, 2017.

[24] Bernardo Cuenca Grau et al. “OWL 2: The next step for OWL”. In: *Journal of Web Semantics* 6.4 (2008), pp. 309–322.

[25] Tom Gruber. “Ontology.” In: *Encyclopedia of database systems* 1 (2009), pp. 1963–1965.

[26] V Haarslev and R Möller. *RACER system description, in ‘IJCAR’01: Proceedings of the First International Joint Conference on Automated Reasoning’*. 2001.

[27] Maliheh Haghgoo et al. “SARGON–Smart energy domain ontology”. In: *IET Smart Cities* 2.4 (2020), pp. 191–198.

[28] Kai Heussen et al. “ERIGrid Holistic Test Description for Validating Cyber-Physical Energy Systems”. In: *Energies* 12.14 (2019). DOI: 10.3390/en12142722.

[29] Simon Hirzel et al. “What’s going on in energy efficiency research? A platform to enhance the transparency of energy research funding in Germany”. In: (2017).

[30] Ian Horrocks, Peter F Patel-Schneider, and Frank Van Harmelen. “From SHIQ and RDF to OWL: The making of a web ontology language”. In: *Journal of web semantics* 1.1 (2003), pp. 7–26.

[31] Maxime Lefrançois. “Planned ETSI SAREF extensions based on the W3C&OGC SOSA/SSN-compatible SEAS ontology paaerns”. In: *Workshop on semantic interoperability and standardization in the IoT, SIS-IoT*. 2017, 11p.

[32] Nancy G. Levenson and John P. Thomas. *STPA Handbook*. Tech. rep. MIT, 2018.

[33] Leandro Madrazo, Alvaro Sicilia, and Gonzalo Gamboa. “SEMANCO: Semantic tools for carbon reduction in urban planning”. In: *Proceedings of the 9th European Conference on Product and Process Modelling*. 2012.

[34] Christoph Mayer et al. “Resilienz digitalisierter Energiesysteme”. In: *Blackout-Risiken Verstehen, Stromversorgung Sicher Gestalten* (2020).

[35] Mark A Musen. “The protégé project: a look back and a look forward”. In: *AI matters* 1.4 (2015), pp. 4–12.

[36] Christian Neureiter et al. “Towards consistent smart grid architecture tool support: From use cases to visualization”. In: *IEEE PES Innovative Smart Grid Technologies, Europe*. IEEE. 2014, pp. 1–6.

[37] OASIS Open Cyber Threat Intelligence Committee. *Introduction to STIX*. [Online; accessed 2023-02-01]. 2022.

[38] Leif Oppermann et al. “Finding and analysing energy research funding data: The EnArgus system”. In: *Energy and AI* 5 (2021), p. 100070.

[39] Christian Reinisch et al. “Thinkhome energy efficiency in future smart homes”. In: *EURASIP Journal on Embedded Systems* 2011 (2011), pp. 1–18.

[40] Khouloud Salameh et al. “A generic ontology-based information model for better management of microgrids”. In: *Artificial Intelligence Applications and Innovations: 11th IFIP WG 12.5 International Conference, AIAI 2015, Bayonne, France, September 14-17, 2015, Proceedings 11*. Springer. 2015, pp. 451–466.

[41] R Santodomingo et al. “SGAM-based methodology to analyse Smart Grid solutions in DISCERN European research project”. In: *2014 IEEE International Energy Conference (ENERGYCON)*. IEEE. 2014, pp. 751–758.

[42] Johann Schütz, Mathias Uslar, and Marie Clausen. *Digitalisierung. Synthesebericht 3 des SINTEG Förderprogramms, Studie im Auftrag des BMWK, Berlin*. Berlin, May 2022.

[43] Johann Schütz et al. “IEC 62559-2 USE CASE TEMPLATE-BASED SMART GRID ARCHITECTURE ANALYTICS”. In: *CIRED 2021-The 26th International Conference and Exhibition on Electricity Distribution*. Vol. 2021. IET. 2021, pp. 2935–2939.

[44] Guttorm Sindre and Andreas L Opdahl. “Templates for misuse case description”. In: *Proceedings of the 7th International Workshop on Requirements Engineering, Foundation for Software Quality (REFSQ'2001), Switzerland*. 2001.

[45] Guttorm Sindre and Andreas L. Opdahl. “Eliciting security requirements with misuse cases”. In: *Requirements Engineering* 10.1 (Jan. 1, 2005), pp. 34–44. ISSN: 1432-010X. DOI: 10.1007/s00766-004-0194-4. URL: https://doi.org/10.1007/s00766-004-0194-4 (visited on 12/15/2022).

[46] Paul Smith et al. “Towards a Systematic Approach for Smart Grid Hazard Analysis and Experiment Specification”. In: *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)*. Vol. 1. IEEE. 2020, pp. 333–339.

[47] Thanos G Stavropoulos et al. “BOnSAI: a smart building ontology for ambient intelligence”. In: *Proceedings of the 2nd international conference on web intelligence, mining and semantics*. 2012, pp. 1–12.

[48] The MITRE Corporation. *MITRE ATT&CK®*. [Online; accessed 2023-02-01]. 2022.

[49] Jörn Trefke et al. “Smart Grid Architecture Model use case management in a large European Smart Grid project”. In: *IEEE PES ISGT Europe 2013*. IEEE. 2013, pp. 1–5.

[50] Mathias Uslar. “Energy Informatics: Definition, State-of-the-art and new horizons”. In: *Proceedings der ComForEn 2015 Vienna*. Ed. by Friederich Kupzog. TU Wien. Wien: OVE Verlag, 2015.

[51] Mathias Uslar et al. “Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A European perspective”. In: *Energies* 12.2 (2019), p. 258.

[52] Eric Veith, Arlena Wellßow, and Mathias Uslar. “Learning new attack vectors from misuse cases with deep reinforcement learning”. In: *Frontiers in Energy Research* 11 (2023), p. 1138446.

[53] Arlena Wellßow. “Entwurf eines Prozesses zur Formalisierung sicherheitsrelevanter Phänomene für das automatisierte Fahren”. Carl von Ossietzky Universität Oldenburg, 2022.

[54] Arlena Wellßow et al. “Threat Modeling for AI Analysis: Towards the Usage of Misuse Case Templates and UML Diagrams for AI Experiment Description and Trajectory Generation”. In: *Proceedings of the 2024 The 13th International Conference on Informatics, Environment, Energy and Applications*. IEEA '24. New York, NY, USA: Association for Computing Machinery, 2024, accepted, to be published.

CONSORTIUM

DISCLAIMER

All information provided reflects the status of the RESili8 project at the time of writing and may be subject to change.

Neither the RESili8 Consortium as a whole, nor any single party within the RESili8 Consortium warrant that the information contained in this document is capable of use, nor that the use of such information is free from risk. Neither the RESili8 Consortium as a whole, nor any single party within the RESili8 Consortium accepts any liability for loss or damage suffered by any person using the information.

The content and views expressed in this material are those of the authors and do not necessarily reflect the views or opinion of the ERA-Net SES initiative. Any reference given does not necessarily imply the endorsement by ERA-Net SES.

COPYRIGHT

This project has received funding in the framework of the joint programming initiative ERA-Net Smart Energy Systems' focus initiative Digital Transformation for the Energy Transition, with support from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883973.