NFDI4Energy Conference

1. NFDI4Energy Conference

10.5281/zenodo.10655835

Published: 2024-02-22

Machine-Readable Expert Knowledge Representation Concept

Towards Autonomous Scenario Analysis

Arlena Wellßow[1,2], Paul Smith[4], Edmund Widl[3], Eric Veith[1], Julian Kohlisch-Posega[2], Francesca Soro[3], Malte Puhan[6], Andreas Theil[5], Mathias Uslar[2], and Roland Zoll[5]

[1]Carl-von-Ossietzky Universität Oldenburg, Germany
[2]OFFIS e.V., Germany
[3]Austrian Institute of Technology, Austria
[4]Lancaster University, UK
[5]Wiener Netze, Austria
[6]Solandeo, Germany

Keywords: Knowledge Representation, Misuse Case, HTD, STPA, Reinforcement Learning

1 Introduction

The convergence of Information and Communications Technology (ICT) and the energy grid, known as the smart grid, requires expertise from both grid operators and ICT specialists due to the integration of ICT-based control systems. This integration, while enhancing efficiency, also increases the risk of errors and cyber attacks, leading to potential system failures [1]–[3].

Traditionally, the energy system's risk of failure was mitigated by physical system redundancy. However, with extensive ICT integration, this approach is no longer sufficient, necessitating the use of e.g. secure communication protocols and encryption alongside redundancy for effective risk mitigation [2], [3].

The evolving power grid, driven by machine learning, prosumer roles, localized energy markets, and distributed renewable energy sources, increases the complexity of the system, and therefore requirements for simulations also become higher for mitigation development [4], [5]. However, this demands significant time and financial investment, prompting the use of agent-based systems for effective mitigation strategy generation in unforeseen scenarios [6].

Agents based on Deep Reinforcement Learning (DRL) can equally find attack vectors and mitigations, but require training in a simulated environment to derive their policy. A DRL agent learns from its reward signal, which is a way to describe an ideal state in terms of a single scalar. Training can be expensive, requiring up to several billion samples to train a sensible policy in complex environments. It would be desirable to train from existing data, known as Offline Learning in the DRL domain. This existing

data is export knowledge. However, expert knowledge is usually expressed in an non-machine-readable, more informal way, such as use cases. We propose an algorithm to query modelled data, represented in semi-structured form, e. g., as UML diagrams. We propose an approach to use this semi-structured formats as source for offline learning, leveraging extensive research data management facilities as backbone.

2 Background

In the following subsections, we briefly introduce some background work that forms the basis of our contribution.

2.1 Misuse Cases

Building on the well-established `IEC 62559` standard in energy informatics, Misuse Cases (MUCs) serve as a valuable tool for threat modeling by detailing undesirable behaviors. These scenarios encompass explicit instances of recognized undesirable behavior, including cyber-physical attacks and inappropriate system behaviors. Derived from the `IEC 62559-2` template, MUCs include misactors and provide specific details, such as worst-case threats and likelihood of occurrence. To enhance the robustness of MUCs, consistency checks with domain experts and compatibility with modeling formats are recommended. A well-structured MUC template is crucial for maintaining data quality and validity in subsequent steps [7], [8].

2.2 Systems Theoretic Process Analysis (STPA)

STPA is a top-down systems-oriented hazard analysis approach that has been proposed by Leveson and Thomas for hazard analysis [9]. It focuses on identifying losses and their causes due to system flaws, leading to the formulation of hazard scenarios. In previous work [10], we have sought to extend STPA to determine how the compromise of security properties that are associated with a system implementation can result in hazard scenarios and accidents that can be determined using STPA.

2.3 Holistic Test Description (HTD)

HTD is a structured approach to the specification of laboratory-based experiments for power systems, which was developed in the EU-funded ERIGrid project[1]. In a similar fashion to STPA, a top-down approach is taken to defining the objectives of experiments (tests) through to detailed specifications of laboratory environments and experiment specifications. In previous work, we have proposed combining STPA and HTD to support the specification of experiments that can be used to evaluate the robustness of smart grids to failures that are induced by cyber-attacks [11].

3 Proposed Concept: Embed MUCs in STPA Analysis and Describe Testcases through HTD

The proposed concept is a combination of MUC, STPA, and HTD in a hierarchical order. At the first level, STPA is applied to the topic of interest. The results of this analysis will contain specific hazard scenarios.

[1] The ERIGrid project: https://erigrid.eu/

Using this STPA output, MUCs are defined for all of these scenarios. They will be extended through expert knowledge, extend the hazardous situations to scenarios, and therefore describe the situation in more detail. From this, MUC experiments can be defined. This can be done either directly from the MUC data that can be extended if needed (see subsection 4.1) or from a combination of data formats.

In our concept, we propose 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 an easy-to-share knowledge database, that can be extended after analysis results are given.

4 Needed Additions

4.1 MUC Extension

To apply MUCs for experiment generation, modifications are needed as outlined in [8] from collaborative work with the University of Oldenburg. This extends MUCs for generating palaestrAI experiment files in the RESili8 project.

Creating a comprehensive palaestrAI-compatible experiment file from misuse case data requires template adjustments. The misuse case provides data, but the experiment data must be generated. Actor groupings represent a single AI agent, with correlations between various data elements.

The misuse case lacks experiment-specific identifiers, environmental declarations, and simulation details. Notably, phase configurations, agent brain and muscle definitions, and information for designing different experiment run files are absent. To address these gaps, an extension for experiment generation is necessary.

4.2 Document-Read out

To automate MUC-based experiment file generation, a document read-out [12] is employed. Completed MUC templates, diagrams, and tables are exported. A script extracts a limited MUC information set for presentation. Additional details, like environment specifics and mapped sensors, come from an existing experiment file. Agent data is obtained by scanning the exported files for entities with specific stereotypes, resulting in a YAML output file. This process combines setup information with additional details for a comprehensive experiment file.

4.3 Trajectory Generation

When a data readout from MUCs is accomplished, the next step 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.

Author contributions

All authors participated in the discussion of the concept and its creation. AW, EW, PS, EV, and FS contributed their gathered knowledge to the toolchain proposal using MUCs, STPA, RL and HTD. AW wrote this abstract with additional help from PS and authorial feedback from EV and MU.

Competing interests

The authors declare that they have no competing interests.

Funding

This work has been funded by the German Federal Ministry for Economic Affairs and Climate Action under the project grant *RESili8* (03EI4051A).

References

[1] M. De Nooij, B. Baarsma, G. Bloemhof, H. Slootweg, and H. Dijk, "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," *Energy Economics*, vol. 32, no. 6, pp. 1277–1282, 2010.

[2] C. Mayer, G. Brunekreeft, M. Blank-Babazadeh, S. Stark, M. Buchmann, M. Dalheimer, *et al.*, "Resilienz digitalisierter energiesysteme," *Blackout-Risiken Verstehen, Stromversorgung Sicher Gestalten*, 2020.

[3] J. Schütz, M. Uslar, and M. Clausen, *Digitalisierung. Synthesebericht 3 des SINTEG Förderprogramms, Studie im Auftrag des BMWK, Berlin*. Berlin, May 2022.

[4] M. Uslar, "Energy Informatics: Definition, State-of-the-art and new horizons," in *Proceedings der ComForEn 2015 Vienna*, F. Kupzog, Ed., TU Wien, Wien: OVE Verlag, 2015.

[5] M. Uslar, S. Rohjans, C. Neureiter, *et al.*, "Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A european perspective," *Energies*, vol. 12, no. 2, p. 258, 2019.

[6] L. Fischer, J. M. Memmen, E. M. Veith, and M. Tröschel, "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*, Athens, Greece: IARIA XPS Press, 2019, pp. 24–32, ISBN: 978-1-61208-713-9. arXiv: 1811.06447.

[7] M. Azamat, J. Schütz, and M. 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.

[8] A. Wellßow, J. Kohlisch-Posega, E. Veith, and M. Uslar, "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*, ser. IEEA '24, New York, NY, USA: Association for Computing Machinery, 2024, accepted, to be published.

[9] N. G. Levenson and J. P. Thomas, "STPA Handbook," MIT, Tech. Rep., 2018.

[10] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications*, vol. 34, pp. 183–196, 2017, ISSN: 2214-2126.

[11] P. Smith, E. Piatkowska, E. Widl, F. P. Andrén, and T. I. Strasser, “Towards a systematic approach for smart grid hazard analysis and experiment specification,” in *2020 IEEE 18th International Conference on Industrial Informatics (INDIN)*, IEEE, vol. 1, 2020, pp. 333–339.

[12] E. Veith, A. Wellßow, and M. Uslar, “Learning new attack vectors from misuse cases with deep reinforcement learning,” *Frontiers in Energy Research*, vol. 11, p. 1 138 446, 2023.