Elektrotech. Inftech. (2023) 140:419–424
https://doi.org/10.1007/s00502-023-01151-3

e+i elektrotechnik und informationstechnik

Use cases also exist for attackers—how to foster the concept of misuse cases

Mana Azamat · Johann Schütz · Mathias Uslar

Received: 16 May 2023 / Accepted: 16 June 2023 / Published online: 28 July 2023

Abstract Due to the new digital control structures of cyber-physical energy systems (CPES), where the control interventions no longer take place physically on site but are triggered, released, executed and acknowledged remotely by automated control systems, there is not only the risk of incorrect actions by plants or operators, but also of possible attacks or misuses. In this contribution, we propose an integrated security-by-design approach (on a conceptual level) for testing the interoperability of various heterogeneous systems (e.g., TSO-DSO communications) by combining multiple, but yet separated, state-of-the-art approaches. With the objective of eliminating or minimizing the impact of cyber incidents, best practices from various sectors have been adapted and integrated with well-established methods and standards from the energy sector, such as the IEC 62559-2 use case template.

Keywords Interoperability testing · Testbed architecture · Misuse case · STIX2.0 · IHE Gazelle

Use Cases existieren auch für Angreifer – Vom Konzept der Misuse Cases profitieren

Zusammenfassung Aufgrund der neuen digitalen Steuerungsstrukturen von cyber-physischen Energiesystemen (CPES), bei denen die Steuerungseingriffe nicht mehr physisch vor Ort stattfinden, sondern von automatisierten Steuerungssystemen aus der Ferne ausgelöst, freigegeben, ausgeführt und quittiert werden, besteht nicht nur die Gefahr von Fehlhandlungen durch Anlagen oder Betreiber, sondern auch durch mögliche Angriffe oder Missbrauch. In diesem Beitrag wird ein integrierter Security-by-Design-Ansatz (auf konzeptioneller Ebene) für die Prüfung der Interoperabilität verschiedener heterogener Systeme (z. B. TSO-DSO-Kommunikation) vorgeschlagen, indem mehrere, aber bisher unabhängige, Ansätze des State-of-the-Art kombiniert werden. Mit dem Ziel, die Auswirkungen von Cyber-Zwischenfällen zu eliminieren oder zu minimieren, wurden bewährte Verfahren aus verschiedenen Sektoren herangezogen, angepasst und mit etablierten Methoden und Standards aus dem Energiesektor, wie z. B. dem IEC 62559-2 Use Case Template, integriert.

Schlüsselwörter Interoperabilitätstests · Testbed-Architektur · Misuse Case · STIX2.0 · IHE Gazelle

1 Introduction

In numerous emergent domains, we have to deal with the interconnection and combination of various heterogeneous systems from different manufacturers using different communication protocols and data models, which need to exchange their messages in order to realize collaborative business models and joint objectives. For this purpose, interoperability has to be considered as a fundamental enabler and requirement, which aims to certify whether the required end-to-end communication process between the various ICT systems is appropriately fulfilled on all needed levels and the entire system is implemented and performing according to requirements and expectations for performance, security vulnerability and data integrity [9]. Hence, as a non-functional requirement, it becomes crucial that the actors and respective system owners agree on a standardized method, e.g., via the *Common Information Model* (CIM, IEC 61970 data model and protocol stack), thereby all actors are able

M. Azamat (✉) · J. Schütz · M. Uslar
Energy, Standardized Systems Engineering and Assessment, OFFIS – Institute for Information Technology, Escherweg 2, 26121 Oldenburg, Germany
mana.azamat@offis.de

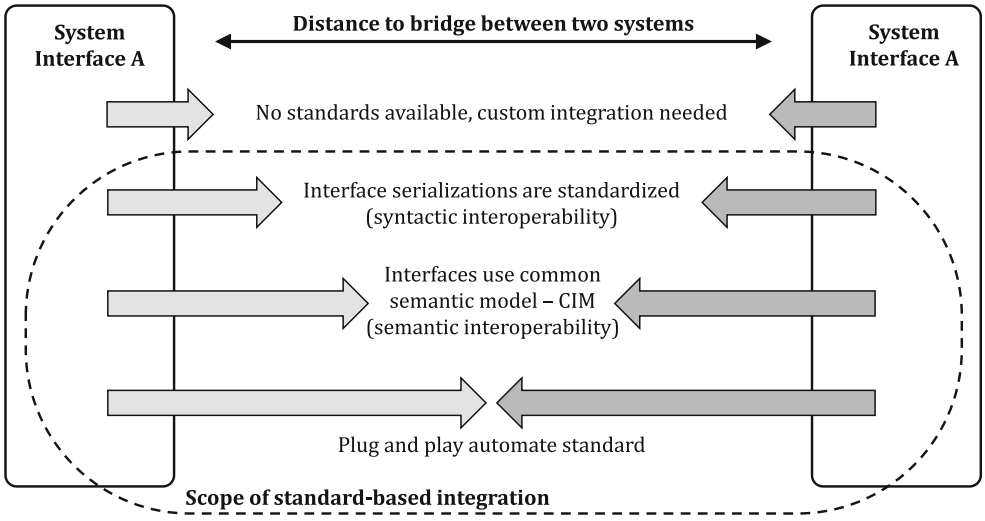

Fig. 1 Integration distance between two systems (based on [1])

to receive, process, and send each other messages in a secure, efficient, and traceable manner [17]. Otherwise, as depicted in Fig. 1, the so-called *distance to integrate* increases, whereby the lack of interoperability creates unnecessarily high integration costs and additional risks over time.

The distance and thus the costs of integration decrease with the degree of standardization, as these creates well-defined integration points that enable a composability between the interacting systems with a reasonable amount of effort [15]. However, the challenge of plug-and-play capability in a smart grid as a system of systems is that the heterogeneous actors across the energy value chain cannot know their communicating partners or their respective (technical) systems in advance. Although a number of standards have already been established to promote a seamless integration or interoperability in the energy sector (e.g., CIM or 61850), these standards alone cannot guarantee the practical interoperability between two systems implemented by independent vendors. Since standards are usually written in natural language, they can be ambiguous, contain gaps or even errors and contradictions. This poses the issue of different interpretations and, consequently, different implementations of the same standard. As a result, it is not uncommon that even if several systems implement the same standard, they are not necessarily fully interoperable with each other [14]. Thus, to ensure interoperability, corresponding interoperability tests need to be realised and certificates need to be issued, which provide evidence that the interoperability has been tested and can be ensured [12]. In order to close this last gap, the main objectives of interoperability testing are [2]:

- Providing a guarantee of seamless end-to-end communication between two systems and a certain level of security.
- Increasing the reliability of the systems connectivity.
- Validate the technical compatibility between the two systems.
- Minimizing compatibility issues during data transferring between two systems.
- Using a uniform data structure (type and format) between connected systems.

To achieve the above-mentioned objectives, the test management system or so-called test bed system IHE (*Integrating the Healthcare Enterprise*)-Gazelle [6] was able to successfully establish itself as a comprehensive and widely recognized interoperability testing tool in the healthcare area. In compliance to the requirements of the ISO/IEC 17025 standard [7], Gazelle substantially focuses on the syntactic and semantic validation of the exchanged information and, therefore, can be used for interoperability as well as conformance tests [3]. Moreover, the suitability of the use of Gazelle within the energy sector has already been successfully demonstrated within the research project "*IES Austria – Integrating the Energy System*", which adapted the IHE methodology to the energy sector, under consideration of the domain-specific requirements [14]. However, interoperability testing requires rigorous test specifications, as they are a critical influencing factor that must precisely define the scenarios derived from the use cases to maximize the opportunities, leading to the identification of inconsistencies and errors in an explicit and structured procedure (Fig. 2).

This contribution is organized as follows. Sect. 2 will provide the background on the building blocks for the method developed which will be covered in Sect. 3. Sect. 4 will conclude with preliminary results and draw a pathway for future research.

2 Background and Related Work

In addition to the previously introduced testing tool (IHE Gazelle), this contribution is based on four com-

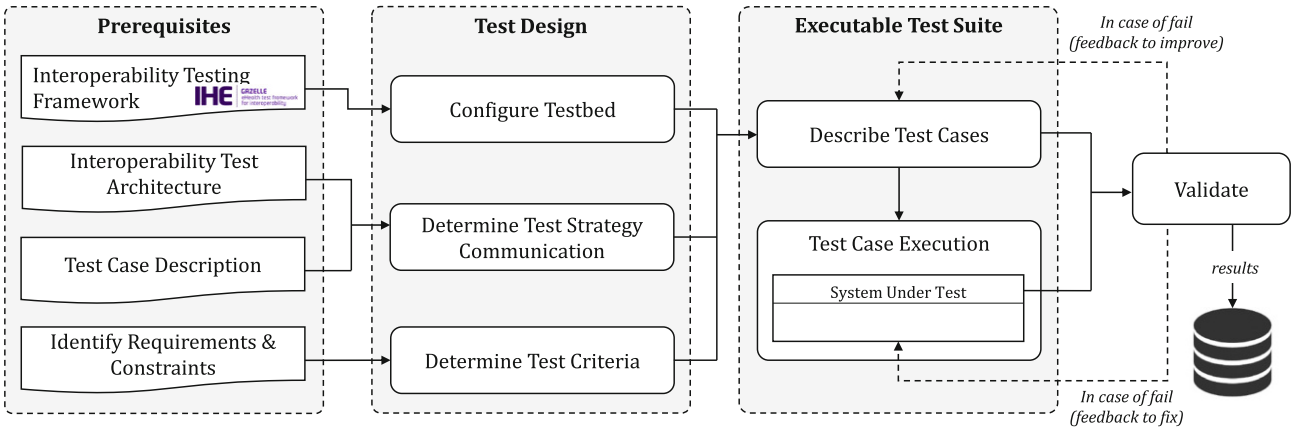

Fig. 2 Interoperability testing architecture (based on [2])

plementary key approaches from different domains combined. The next pargraphs will shortly outline the individual building blocks used and put them in context how we use them in the scope of this very contribution.

Use Case-Template. The standard IEC 62559 is an international standard entitled "Use Case Methodology" and deals with the documentation and specification of use cases. With this standard, use cases are systematically recorded and documented. The template [4] supports the gathering elicitation and analysis of the (interoperability) requirements between decentralized, communicating systems and it has included eight sections and different subsections, which provide a holistic overview of the whole use case, the actors involved, the information exchanged, and the technical process.

Misuse Case-Template. The misuse case follows the outline of the standardized IEC 62559-2 template, with the aim of addressing possible attacking scenarios due to unintended behavior and documenting the context of abusive behavior alongside system threats from the attacker's point of view in more detail. Enabling an early identification and analysis of cyber threats and developing proper mitigation strategies to reduce the risk to an appropriate level during the design phase is the main aim of the misuse case-template which focuses primarily on non-functional requirements and in particular safety requirements.

MITRE ATT&CK Framework. The *MITRE Adversarial Tactics, Techniques, and Common Knowledge* (ATT&CK) framework [16] is used to document and track various adversarial techniques and coordinate cyber-attack responses consistent with that.

STIX2. *Structured Threat Information Expression* (STIX™) [11], which is developed by the *Organization for the Advancement of Structured Information Standards (OASIS)* Cyber Threat Intelligence Technical Committee, is a standardized language and serialization format regarded as an effective threat information-sharing tool. It is also a graph-based informational model, which *standardized cyber threat intelligence* (CTI) data in a machine-readable format [10, 13]. It contains 18 *domain objects* (SDOs), represented as "nodes", and *STIX Relationship Objects* (SROs), represented as "edges", to establish a link between the objects [18]. The STIX information in version 2.0, is stored as a *JavaScript Object Notation (JSON)*, a machine-readable data format which is derived from the JavaScript programming language to represent the objects and their properties.

The use case-template focuses on providing the needed and desired functionality of a system which shall be provided with *Quality of Service* (QoS) requirements as well and uninterrupted procedural behaviour. The misuse case introduces the notion of interrupted behaviour, thus, an error. This error typically has a cause with might be unintentional but also intentional – thus, an attack. This attack might be part of already existing documented threats and could be mitigated against – if structured information on how the threat works could be brought into the process. This is done utilizing STIX.

3 Proposed Integration of the Tooling

In this section, we describe the high-level overview of the proposed interoperability and security test setup, which serves mainly as a test bed solution for the overall testing process and covers the newly introduced (mis-)use case without considerable engineering effort. This model is designed in a standardized generic way, allowing its adaption in a more appropriate / customized way, particularly for organizations that have deviating requirements as, for instance, the need in a grid lab to model and simulate the use cases themselves. In addition, from the perspective of scalability, it allows the testing of small and medium, sized scenarios. An overview of the model is depicted below in Fig. 3.

As a first step, we focus mainly on ensuring the interoperability of two or more systems. For this purpose, we derive the relevant information from the existing use case-template, which also contains

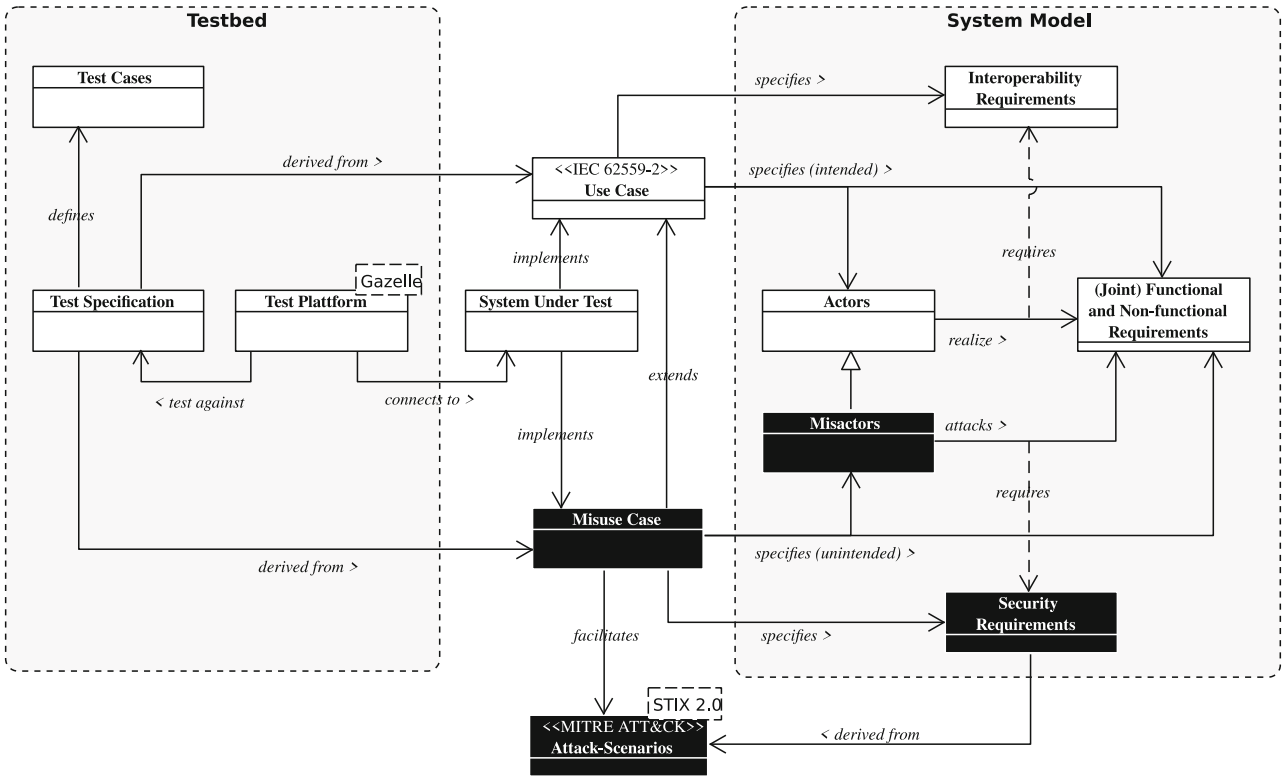

Fig. 3 The proposed conceptual model for interoperability testing taking attackers into account (own representation)

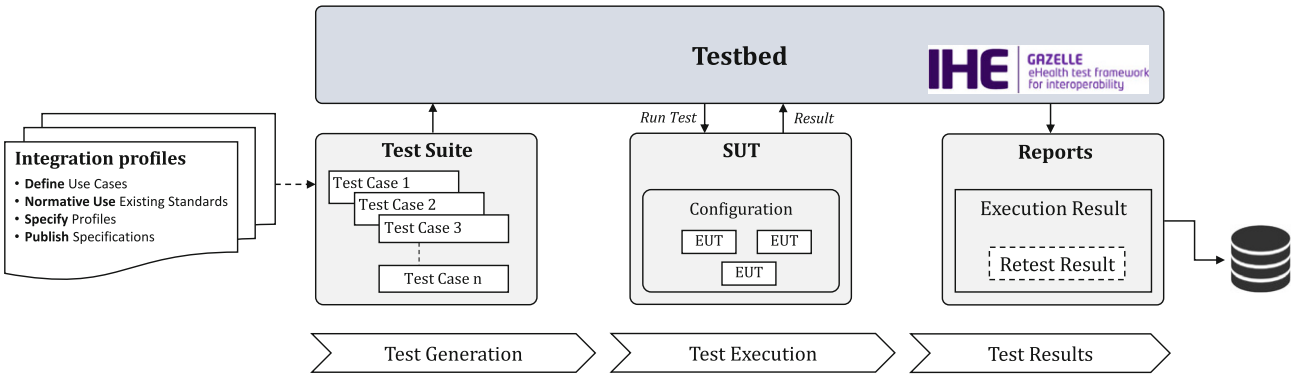

Fig. 4 Schematic overview of the test process (based on [19])

functional as well as non-functional requirements to specify and model the system of interest and its corresponding behaviour. It also can serve as a basis for a simulation that represents how the components communicate with each other, whereby the different actors or mis-actors can be simulated as digital twins in order to run the use case scenarios without the actual components. The results can provide insights into the systems behavior under various scenarios and conditions (e.g. attacks). By the additional analysis of the behavior of the communicating systems under different (misuse case) scenarios, it is possible to assess how they behave, (e.g.) if they receive syntactically and semantically valid data, but with (intentional or unintentional) manipulated values that would enforce unreasonable reactions. This allows the system behavior to be understood and validated before it is actually implemented and put operational. The configuration of a simulation setup should incorporate all the components required in the envisioned use cases, as well as the matching communication infrastructure between these components, and provide a realistic emulation and model. To ensure a *System Under Test* (SUT) meets all the functional as well as non-functional requirements, we need to generate a set of test cases from the use cases to check whether the behavior of the system under test achieves needed interoperability. The test cases to run in the simulation are created in the generation phase.

Once the generation phase is over, the testbed platform (IHE Gazelle) receives the test instruction to process the test on SUT. The test response will be send back to the Gazelle to analyze the result set. In the test results phase, we need to analyze the test results and try to resolve the probable failure (Fig. 4), whereby the integration profiles provide the concrete technical specifications for the concrete interfaces that need to be tested [5].

In a second step, we aim to enrich the STIX-based modeling concept in the context of interoperability testing by the IHE Gazelle platform. In this direction, the information derived from the misuse case-template could be used to interact with the MITRE ATT&CK *Knowledge Base* (KB) toward improving cyber defences [8] and exchange data between different MISP (*Malware Information Sharing Databases*) instances.

4 Conclusion

In this contribution, we presented an integrated formal approach for interoperability testing based on a standardized testing tool which has been put into practice in the healthcare domain and a process. Then, we introduced the conceptual approach for interoperability testing by applying a STIX2.0-based modeling to test various (smart grid) communication protocols and standards against the intended and unintended behavior of communication between systems. First results proved that the non-domain specific approach can be transferred with benefits to the energy domain. The IHE Gazelle as well as the procedural approach included proves useful in different domains and scenarios – not just for testing for intended functions, but also for non-intended observable behaviour.

However, one current drawback is that the different attack scenarios provided by the MITRE ATT&CK KB have to be implemented within the testbed in a modular and re-configurable way. Thus, future work will focus on the technical integration of misuse cases and applying automated testing methods in order to use STIX-based semantics as security testing scenarios in daily operations.

Acknowledgements This research work has been funded by the European Commission grants IDUNN (grant no. 101021911).

References

1. Bleiker R, Specht M (2013) Testing in the Smart Grid: Compliance, Conformance and Interoperability, Springer Berlin Heidelberg, Berlin, Heidelberg, pp 147–161. https://doi.org/10.1007/978-3-642-34916-4_9
2. ETSI EG 202 810 (2010) Methods for Testing and Specification (MTS); Automated Interoper-ability Testing; Methodology and Framework (Ver. 1.1.1)
3. Frohner M, Gottschalk M, Franzl G, Pasteka R, Uslar M, Sauermann S (2017) Smart grid interoperability profiles development. In: 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp 189–194, https://doi.org/10.1109/SmartGridComm.2017.8340674
4. Gottschalk M, Uslar M, Delfs C (2017) The use case and smart grid architecture model approach: The iec 62559-2 use case template and the sgam applied in various domains. Springer Nature, 6330 Cham, Switzerland, SpringerBriefs in Energy, vol 1, p 93
5. Gottschalk M, Franzl G, Frohner M, Pasteka R, Uslar M (2018) From integration profiles to interoperability testing for smart energy systems at connectathon energy. Energies 11(12), https://doi.org/10.3390/en11123375
6. IHE International (2023) Gazelle – eHealth Test Framework for Interoperability. https://gazelle.ihe.net. Accessed 26 Mar 2023
7. ISO/IEC 17025:2017 (2017) General Requirements For the Competence of Testing and Calibration Laboratories
8. Kim JH, Kim IK (2019) ITU-T X.ucstix – Use Cases for Structured Threat Information Expression (STIX™). https://handle.itu.int/11.1002/1000/13849. Accessed 26 Mar 2023
9. Mondorf A, Wimmer MA, Reiser D (2013) A framework for interoperability testing in pan-european public service provision. In: Wimmer MA, Janssen M, Scholl HJ (eds) Electronic Government, Springer Berlin Heidelberg, Berlin, Heidelberg, pp 188–199
10. OASIS Open (2021) STIX Version 2.1. https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html. Accessed 26 Mar 2023
11. OASIS Open (2023) STIX—Structured Threat Information Expression. https://oasis-open.github.io/cti-documentation/stix/intro.html. Accessed 26 Mar 2023
12. Reif, V et al (2023) Towards an interoperability roadmap for the energy transition. In: 12. (Hybrid) Symposium Communications for Energy Systems (ComForEn)
13. Sadique F, Cheung S, Vakilinia I, Badsha S, Sengupta S (2018) Automated structured threat information expression (stix) document generation with privacy preservation. In: 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp 847–853, https://doi.org/10.1109/UEMCON.2018.8796822
14. Schütz J, Uslar M, Meister J (2021) A case study research on interoperability improvement in smart grids: State-of-the-art and further opportunities. Open Research Europe 1(33), https://doi.org/10.12688/openreseurope.13313.1
15. The GridWise Architecture Council (2008) GridWise® Interoperability Context-Setting Framework v1.1. https://gridwiseac.org/pdfs/GridWise_Interoperability_Context_Setting_Framework.pdf. Accessed 26 Mar 2023

16. The MITRE Corporation (2023) MITRE ATT&CK®. https://attack.mitre.org. Accessed 26 Mar 2023
17. Uslar M, Specht M, Rohjans S, Trefke J, Gonzalez JMV (2012) The Common Information Model CIM – IEC 61968/61970 and 62325 – A Practical Introduction to the CIM. Springer Berlin, Heidelberg, https://doi.org/10.1007/978-3-642-25215-0
18. Wilhoit K, Opacki J (2022) Operationalizing Threat Intelligence: A Guide to Developing and Operationalizing Cyber Threat Intelligence Programs. Packt Publishing, Birmingham
19. Winkler D, Hametner R, Biffl S (2009) Automation component aspects for efficient unit testing. In: 2009 IEEE Conference on Emerging Technologies & Factory Automation, pp 1–8, https://doi.org/10.1109/ETFA.2009.5347022

Mana Azamat, holds a B.Sc. degree in Computer Engineering (Hardware Engineering) from Shiraz University, Iran and a Master degree (M.Sc.) in Media-Informatics from University of RWTH-Aachen, Germany. She joined the OFFIS – Institute for Information Technology (in Oldenburg, Germany) in 2018 as researcher in security analysis of smart grids and later she has been contributing to smart grid and energy-related re-search projects as consultant / internal project manager.

Johann Schütz, is a researcher in the field of Energy Informatics at OFFIS – Institute for Information Technology in Oldenburg, Germany. He received his Bachelor and Masters Degree in Business Informatics at the University of Applied Sciences of Osnabrück in 2014 and the University of Oldenburg in 2017, respectively. Since graduation, he has been working at OFFIS with a focus on energy systems as systems-of-systems.

Mathias Uslar, is member for the German NC in the IEC SyC Smart Energy WG 5 as well as in the various national German mirrors. He is senior principal scientist as well as Group Manager at the OFFIS – Institute for Information Technology in Oldenburg, Germany. His work focuses on the topic of Systems Engineering and Assessment, mainly focusing on the aspects of System-of-systems interoperability as well as IT security.