Report from Dagstuhl Seminar 21451

Managing Industrial Control Systems Security Risks for Cyber Insurance

Edited by

Simon Dejung[1], Mingyan Liu[2], Arndt Lüder[3], and Edgar Weippl[4]

1 **SCOR – Zürich, CH,** sdejung@scor.com
2 **University of Michigan – Ann Arbor, US,** mingyan@umich.edu
3 **Otto-von-Guericke-Universität Magdeburg, DE,** arndt.lueder@ovgu.de
4 **University of Vienna & SBA Research – Wien, AT,** edgar.weippl@univie.ac.at

Abstract

Industrial control systems (ICSs), such as production systems or critical infrastructures, are an attractive target for cybercriminals, since attacks against these systems may cause severe physical damages/material damages (PD/MD), resulting in business interruption (BI) and loss of profit (LOP). Besides financial loss, cyber-attacks against ICSs can also harm human health or the environment or even be used as a kind of weapon. Thus, it is of utmost importance to manage cyber risks throughout the ICS's lifecycle (i.e., engineering, operation, decommissioning), especially in light of the ever-increasing threat level that is accompanied by the progressive digitization of industrial processes. However, asset owners may not be able to address security risks sufficiently, nor adequately quantify them in terms of their potential impact (physical and non-physical) and likelihood. A self-deceptive solution might be using insurance to transfer these risks and offload them from their balance sheet since the underlying problem remains unsolved. The reason for this is that the exposure for asset owners remains and mitigation measures may still not be implemented adequately while the insurance industry is onboarding unassessed risks and covering it often without premium and without managing the potential exposure of accumulated events. The Dagstuhl Seminar 21451 "Managing Industrial Control Systems Security Risks for Cyber Insurance" aimed to provide an interdisciplinary forum to analyze and discuss open questions and current topics of research in this area in order to gain in-depth insights into the security risks of ICSs and the quantification thereof.

Seminar November 7–12, 2021 – http://www.dagstuhl.de/21451
2012 ACM Subject Classification Security and privacy → Economics of security and privacy; Social and professional topics → Information system economics
Keywords and phrases industrial control systems, security, cyber insurance, cyber risk quantification, production systems engineering, risk engineering, SCADA, Industry 4.0
Digital Object Identifier 10.4230/DagRep.11.10.36
Edited in cooperation with Eckhart, Matthias

Managing Industrial Control Systems Security Risks for Cyber Insurance, *Dagstuhl Reports*, Vol. 11, Issue 10, pp. 36–56
Editors: Simon Dejung, Mingyan Liu, Arndt Lüder, and Edgar Weippl

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Matthias Eckhart (SBA Research – Wien, AT, meckhart@sba-research.org)
Simon Dejung (SCOR – Zürich, CH, sdejung@scor.com)
Mingyan Liu (University of Michigan – Ann Arbor, US, mingyan@umich.edu)
Arndt Lüder (Otto-von-Guericke-Universität Magdeburg, DE, arndt.lueder@ovgu.de)
Edgar Weippl (University of Vienna & SBA Research – Wien, AT, edgar.weippl@univie.ac.at)

The security economics community has an ambivalent position on quantifying cyber risk: on the one hand, there is a long-standing interest in establishing cyber risk measurement, while on the other hand, relevant publications report contradictory results [7] or present models with insufficient evidence of validity [6]. As researchers remain cautious about the interpretation of modeling results, the insurance industry's need for gaining a quantitative understanding of cyber risk is more critical than ever. A serious concern for insurers is that a large-scale cyber-attack could result in significant claims arising from transferred security risks. Considering the adverse business implications of cyber-related high-impact, low-frequency events, it is necessary to estimate and control the potential exposure to such losses. Previous industry studies attempted to address this issue by proposing hypothetical worst-case scenarios involving power grids [8], ports [9], and other industrial applications [4]. Furthermore, several industry-led working groups conducted workshops to assess the plausibility, impact, and claim implications of potential ICS-related catastrophic loss events (cf., for instance, [10, 11, 5, 12]). However, it is still not fully understood how the peculiarities of ICSs, technological change in light of strategic initiatives (e.g., Industry 4.0 [3]), and the increasingly sophisticated nature of cyber-physical attacks influence the loss frequency and loss severity [1]. Moreover, a holistic consideration of cyber-physical risk featuring the complete ICS lifecycle calls for an interdisciplinary research approach [2].

Thus, the aim of this Dagstuhl seminar was to bring together different communities to foster research activities that advance the understanding of cyber risks pertaining to ICSs and associated insurance aspects. The concepts developed as part of this seminar are a result of interdisciplinary work conducted by academics and industry professionals, both junior and senior, from the fields of

(i) computer science,
(ii) automation engineering,
(iii) actuarial science, and
(iv) economics.

To address the issues outlined above, the purpose of the seminar was to make the first steps toward a probabilistic cyber catastrophe model that is tailored to the ICS domain. In particular, we planned to achieve the basis of an economic loss model that builds upon worst-case scenarios in which globally and simultaneously many industrial processes in critical infrastructure sectors (e.g., power, petrochemical, transport, logistics) are affected by cyber-attacks. Figure 1 visualizes possible components of such a model, which were discussed and challenged during the seminar. In the first phase, the scenario is formulated, fundamental assumptions are specified, and the theoretical basis of the statistical model is formed. After that, the model is calibrated with data obtained from various sources, such as loss databases or subject-matter experts. Finally, the model and its underlying assumptions are validated.

To set the frame for the seminar, the organizers defined four topics that were covered in plenary sessions and breakout sessions. In each plenary session, lightning talks were held that motivated the collaborative work in the breakout sessions. The working groups studied

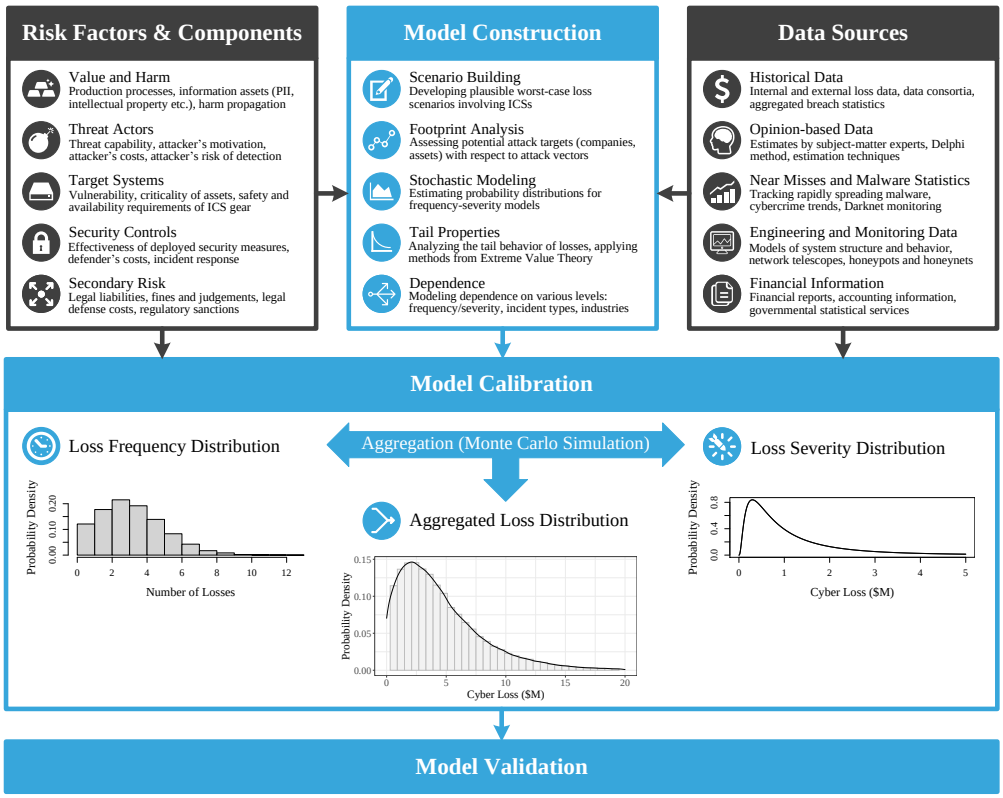

Figure 1 Potential components of a probabilistic cyber catastrophe model for the ICS domain (adapted from materials provided by SCOR SE).

the same overarching topic of the breakout session (yet each with a different focus) in order to strengthen interdisciplinary exchange.

Overall, the following topics and motivating research questions were addressed:

1. *ICS Threat Landscape*: How have cyber attacks against ICSs evolved and what should we expect in terms of attack sophistication, persistence, and impact in the future?
2. *Cyber-Physical Risk Quantification*: How can we quantitatively model economic losses caused by ICS-focused cyber risks (i.e., probabilistic cyber catastrophe model)?
3. *Insurance*: What are the opportunities and limitations of transferring ICS-focused cyber risks to insurers?
4. *Management of Security Risks*: Which hard (e.g., technological security measures) and soft (e.g., information sharing, regulations, funding) factors increase or reduce the attack likelihood and severity?

The seminar started with a welcome session to bridge the disciplinary gap. In this session, the organizers presented the seminar program, explained key terms, and discussed core concepts to familiarize attendees with the terminologies used by different communities. Over the following days, several participants gave lightning talks that focused on the following topics:

- cyber-physical systems, security-relevant aspects within their lifecycle, and procurement considerations,

- current ICS security challenges with an emphasis on technological trends (e.g., Industry 4.0, smart manufacturing, Industrial Internet of Things),
- cyber-physical risk assessments, where special attention was given to analysis and quantification methods,
- various aspects of (cyber) insurance (e.g., cyber cat modeling, underwriting, economic problems, regulations), and
- security economics, featuring studies on cybercrime analysis and vulnerability forecasting.

The lightning talks gave participants the opportunity to present new perspectives and challenges, which led to lively discussions that shaped the group sessions. Unfortunately, the restrictions caused by the SARS-CoV-2 pandemic made it not possible to conduct the estimation exercises with all participants, which would have been required for achieving the cyber cat model. However, conducting the seminar in a hybrid format still enabled the participants both on-site and remote to work together on challenging open questions, contribute to group discussions, and forge new research collaborations.

The organizers thank all participants for their valuable contribution. Furthermore, this seminar would not have been possible without the great technical support provided by the Schloss Dagstuhl staff and the considerable effort made by the video conferencing assistants Sejdefa Ibisevic, Markus Maier, and Sara Tajik.

References

1 Matthias Eckhart, Bernhard Brenner, Andreas Ekelhart, and Edgar Weippl. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges. *Journal of Internet Services and Information Security (JISIS)*, 9(3):52–73, August 2019.

2 Gregory Falco, Martin Eling, Danielle Jablanski, Matthias Weber, Virginia Miller, Lawrence A. Gordon, Shaun Shuxun Wang, Joan Schmit, Russell Thomas, Mauro Elvedi, Thomas Maillart, Emy Donavan, Simon Dejung, Eric Durand, Franklin Nutter, Uzi Scheffer, Gil Arazi, Gilbert Ohana, and Herbert Lin. Cyber risk research impeded by disciplinary barriers. *Science*, 366(6469):1066–1069, 2019.

3 Henning Kagermann, Johannes Helbig, Ariane Hellinger, and Wolfgang Wahlster. Recommendations for implementing the strategic initiative INDUSTRIE 4.0 – securing the future of german manufacturing industry. Final report of the Industrie 4.0 working group, acatech – National Academy of Science and Engineering, München, April 2013.

4 Lloyd's of London, Guy Carpenter, and CyberCube Analytics. Cyber risk: The emerging cyber threat to industrial control systems. Technical report, Lloyd's of London, Guy Carpenter, and CyberCube Analytics, February 2021.

5 Lobo, Francis. Upstream oil & gas cyber risk: Insurance technical review. Technical report, Joint Rig Committee, May 2018. A Joint Rig Committee Report.

6 Vilhelm Verendel. Quantified security is a weak hypothesis: A critical survey of results and assumptions. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, NSPW '09, pages 37–50, New York, NY, USA, 2009. ACM.

7 Daniel W. Woods and Rainer Böhme. SoK: Quantifying cyber risk. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 211–228, May 2021.

8 Lloyd's of London and Cambridge Centre for Risk Studies. Business blackout: The insurance implications of a cyber attack on the us power grid. Technical report, Lloyd's of London and Cambridge Centre for Risk Studies, July 2015.

9 Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University. Shen attack: Cyber risk in asia pacific ports. Technical report, Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University, 2019.

10 Dejung, Simon. Economic impact of cyber accumulation scenarios. Technical report, SCOR Global P&C, 2017.

11 Dejung, Simon. Newsletter – risk assessment for ICS/SCADA security in industrial property, engineering, power, oil & gas. Technical report, SCOR Global P&C, March 2018. A joint workshop in March 2018 by LMA, IMIA & OPERA at SCOR (Zurich).

12 IMIA Working Group. Cyber risks: Engineering insurers perspective. Technical Report 98 (16), September 2016. IMIA Annual Conference 2016 – Doha, Qatar.

2 Table of Contents

3 Overview of Talks

3.1 Malware Economics for ICS Risk

Luca Allodi (TU Eindhoven, NL)

Joint work of Luca Allodi, Michele Campobasso, Fabio Massacci
Main reference Michele Campobasso, Luca Allodi: "Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale", in Proc. of the CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020, pp. 1665–1680, ACM, 2020.
URL http://dx.doi.org/10.1145/3372297.3417892

I bring into focus the relevance of attacker and cybercrime capabilities in the ICS threat scenario. I propose a two-dimensional space to map past ICS incidents over the IT/OT/"logic" knowledge and the process knowledge the attacker needs to engineer and deliver a successful attack. I identify an area of attacks where common cybercriminals ("Dimitry") can operate (and are operating), supported by the underground markets. I discuss implications in terms of attack surface stability, and shared attacker capabilities that together characterize a "baseline risk" for ICS. As such, I argue this baseline risk is systemic to all ICS scenarios, can be quantified, and should be used to identify the gap between what any attacker can achieve, and what sophisticated, resourceful, nation-state level attackers can: how far away from "Dimitry" an attacker has to move to achieve what type of impact?

3.2 Twin-based Continuous Countermeasure Deployment

Fabrizio Baiardi (University of Pisa, IT)

Joint work of Fabrizio Baiardi, Federico Tonelli
Main reference Fabrizio Baiardi, Federico Tonelli: "Twin Based Continuous ICT Risk Management" in Proc. of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Venice, Italy, November 1-5, 2020, pp. 2012–2019, Singapore: Research Publishing, 2020.
URL https://www.rpsonline.com.sg/proceedings/esrel2020/html/5003.xml

Digital twins are virtual replicas that simulate the behavior of physical devices before they are built and to support their maintenance. We extend this technology to cybersecurity and integrate it with adversary emulation to define a policy to remediate the vulnerabilities of an ICT before threat actors can exploit them. Distinct twins model, respectively, the infrastructure and threat actors. A twin describes the infrastructure modules, their vulnerabilities, and the elementary attacks actors can implement. The twin of a threat actor describes its attack surface, its goals, how it selects attacks, and it handles attack failures. The Haruspex software platform builds the infrastructure twin and those of the threat actors, and it automates the emulation. In this way, it can discover the attack paths the actor implements without disturbing the infrastructure. In each path, the actor composes elementary attacks to reach its goal. Multiple emulations can discover all the actor paths by covering stochastic factors such as attack success or failure. The knowledge of the paths enables the remediation policy to minimize the countermeasures to deploy. A twin-based approach supports a continuous remediation process to handle changes in the infrastructure, new vulnerabilities, and new threat actors because the platform can update the twins and run adversary emulations. If new attack paths exist, the platform applies the remediation policy. Experimental data confirm the effectiveness of this approach.

References

1. Andy Applebaum, Doug Miller, Blake Strom, Henry Foster, and Cody Thomas. Analysis of automated adversary emulation techniques. In *Proceedings of the Summer Simulation Multi-Conference*, SummerSim '17, San Diego, CA, USA, 2017. Society for Computer Simulation International.
2. Andy Applebaum, Doug Miller, Blake Strom, Chris Korban, and Ross Wolf. Intelligent, automated red team emulation. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, ACSAC '16, pages 363–373, New York, NY, USA, 2016. Association for Computing Machinery.
3. Fabrizio Baiardi. Avoiding the weaknesses of a penetration test. *Computer Fraud & Security*, 2019(4):11–15, 2019.
4. Fabrizio Baiardi and Daniele Sgandurra. Assessing ICT risk through a Monte Carlo method. *Environment Systems and Decisions*, 33(4):486–499, Dec 2013.
5. Fabrizio Baiardi and Federico Tonelli. Twin based continuous ICT risk management. In Piero Baraldi, Francesco Di Maio, and Enrico Zio, editors, *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, pages 2012–2019, Singapore, 2020. Research Publishing.
6. Fabrizio Baiardi, Federico Tonelli, and Alessandro Bertolini. CyVar: Extending Var-At-Risk to ICT. In Fredrik Seehusen, Michael Felderer, Jürgen Großmann, and Marc-Florian Wendland, editors, *Risk Assessment and Risk-Driven Testing*, pages 49–62, Cham, 2015. Springer International Publishing.
7. Sean Barnum. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX^{TM}). techreport, The MITRE Corporation, February 2014.
8. Sarah Brown, Joep Gommers, and Oscar Serrano. From cyber security information sharing to threat management. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, WISCS '15, pages 43–49, New York, NY, USA, 2015. Association for Computing Machinery.
9. Matthias Eckhart and Andreas Ekelhart. *Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook*, chapter 14, pages 383–412. Springer International Publishing, Cham, 2019.
10. Bob Martin. Common Vulnerabilities Enumeration (CVE), Common Weakness Enumeration (CWE), and Common Quality Enumeration (CQE): Attempting to systematically catalog the safety and security challenges for modern, networked, software-intensive systems. *Ada Lett.*, 38(2):9–42, December 2019.
11. Peter Mell, Karen Scarfone, and Sasha Romanosky. The Common Vulnerability Scoring System (CVSS) and its applicability to federal agency systems. *NIST Interagency Report*, 7435, August 2007.
12. Stephen Moskal, Shanchieh Jay Yang, and Michael E. Kuhl. Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach. *The Journal of Defense Modeling and Simulation*, 15(1):13–29, 2018.
13. Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, and Cody B. Thomas. MITRE ATT&CK®: Design and philosophy. *MITRE Product*, (10AOH08A-JC), March 2020.
14. Fei Tao, He Zhang, Ang Liu, and A. Y. C. Nee. Digital twin in industry: State-of-the-art. *IEEE Transactions on Industrial Informatics*, 15(4):2405–2415, April 2019.

3.3 Quantifying Cyber Risk

Rainer Böhme (Universität Innsbruck, AT)

Joint work of Rainer Böhme, Daniel Woods
Main reference Daniel W. Woods, Rainer Böhme: "SoK: Quantifying Cyber Risk", in Proc. of the 42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021, pp. 211–228, IEEE, 2021.
URL http://dx.doi.org/10.1109/SP40001.2021.00053

This talk introduces a causal model inspired by structural equation modeling that explains cyber risk outcomes in terms of latent factors measured using reflexive indicators. First, we use the model to classify empirical cyber harm studies. We discover cyber harms are not exceptional in terms of typical or extreme losses. The increasing frequency of data breaches is contested and stock market reactions to cyber incidents are becoming less negative over time. Focusing on harms alone breeds fatalism; the causal model is most useful in evaluating the effectiveness of security interventions, which are surveyed in the second half of the talk.

3.4 Are ICS Scenarios Scalable? Ingredients of an Economic Loss Model

Simon Dejung (SCOR – Zürich, CH)

Main reference Simon Dejung: "Newsletter – risk assessment for ICS/SCADA security in industrial property, engineering, power, oil & gas," SCOR Global P&C, Tech. Rep., Mar. 2018, A joint workshop in March 2018 by LMA, IMIA & OPERA at SCOR (Zurich).
URL https://www.imia.com/wp-content/uploads/2021/07/Economic_impact_Cyber_loss_accumulation_scenarios_SVV.pdf

Are scenarios like Industroyer, Havex, Triton/Trisis, Stuxnet scalable? Cyber attacks are the new normal and are correlated with increasing digitalization and interconnectivity. If these attacks are single incidents, they are mainly affecting the attacked victim and companies and/or individuals being linked to these companies having suffered such hostile acts. What we observe more and more is scalability by automation and/or recycling with or without manual adaption of the used malware. Currently we see most incidents in the IT environment and even attacks on critical infrastructures like Colonial pipeline were triggered by office IT ransomware. What if ICS/SCADA/OT scenarios become scalable and e.g., Stuxnet derivatives are more widely used damaging not only non-physical assets, but also physical assets? Current cyber loss models focus on IT damages and its consequences, which are mainly non-physical. Economic loss models breaching the gap to the physical word, considering the probability of material damages and the likelihood of scalability are in its infancy. Interdependencies and interactions of risk factors like e.g., attackers' capabilities, resources, motivation, political and macro-economic environment are not yet sufficiently addressed. Economic loss models properly addressing these factors will serve decision makers on various levels.

References

1 Dejung, Simon. Economic impact of cyber accumulation scenarios. Technical report, SCOR Global P&C, 2017.
2 Dejung, Simon. Newsletter – risk assessment for ICS/SCADA security in industrial property, engineering, power, oil & gas. Technical report, SCOR Global P&C, March 2018. A joint workshop in March 2018 by LMA, IMIA & OPERA at SCOR (Zurich).
3 Ben Hobby and Matthew Hogg. Cyber insurance & business interruption. Technical report, The International Underwriting Association of London Limited and RGL Forensics, July 2018. A report from the IUA's Cyber Underwriting Group in association with RGL Forensics.
4 Matthew Honea, Yoshifumi Yamamoto, Jonathan Laux, Craig Guiliano, and Megan Hart. Silent cyber scenario: Opening the flood gates. Technical report, Aon and Guidewire – Cyence Risk Analytics, October 2018.
5 IMIA Working Group. Cyber risks: Engineering insurers perspective. Technical Report 98 (16), September 2016. IMIA Annual Conference 2016 – Doha, Qatar.
6 Lloyd's of London and Cambridge Centre for Risk Studies. Business blackout: The insurance implications of a cyber attack on the us power grid. Technical report, Lloyd's of London and Cambridge Centre for Risk Studies, July 2015.
7 Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University. Shen attack: Cyber risk in asia pacific ports. Technical report, Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University, 2019.

3.5 Building Blocks of a Cyber Cat Model

Téodore Iazykoff (SCOR – Paris, FR)

This talk explains basic concepts of cat modeling to build cyber models. A step by step guide provides key principles to enable participants to use a scenario-based approach. Both deterministic and stochastic approaches are compared, and detailed examples for each methodology are presented using a Cloud outage scenario. Participants were given the opportunity to discuss similarities and differences with natural catastrophe models.

3.6 Towards Joined Cyber Insurance Exercises

Helge Janicke (Cyber Security CRS – Joondalup, AU)

Joint work of Helge Janicke, Richard Smith, Allan Cook, Leandros Maglaras, Bil Hallaq
Main reference Richard Smith, Helge Janicke, Ying He, Fenia Ferra, Adham Albakri: "The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework", Comput. Secur., Vol. 109, p. 102398, 2021.
URL http://dx.doi.org/10.1016/j.cose.2021.102398

Insurers need to understand the residual risk and potential consequences of a cyber attack on the businesses they insure. Evaluating documentation of compliance, controls and checklists only goes so far and may not provide a proper picture of an organization's cyber security posture. Many large organizations undertake table-top exercises and have defined incident response plans, but the proof is often in the management of an incident and in the proficiency of the staff responding, that is ultimately responsible for mitigating the consequences. There is

an opportunity for cyber insurers to provide training simulations (similar to those mandated for nuclear facilities) as an additional service line to their business, helping inform risk assessments not solely based on controls, policies and plans but also to take into account and organization's cyber capability, capacity and proficiency. The research challenges here are significant, as it is unclear how simulations are co-developed and how capability, capacity and proficiency can be effectively assessed. There are also technical challenges that require more realistic scenarios for ICS. Commercial ICS cyberranges are emerging, but may be underdeveloped, expensive to operate and are not easily adapted to changing technologies. This presentation will incorporate direct experiences in running ICS-specific incident response training from the UK's NCSC funded Agile Incident Response for ICS (AIR4ICS) project. It will also set out some of the challenges to motive the following breakout session.

References

1 Allan Cook, Helge Janicke, Richard Smith, and Leandros Maglaras. The industrial control system cyber defence triage process. *Computers & Security*, 70:467–481, 2017.
2 Bil Hallaq, Andrew Nicholson, Richard Smith, Leandros Maglaras, Allan Cook, Helge Janicke, and Kevin Jones. A novel hybrid cyber range for security exercises on cyber-physical systems. *International Journal of Smart Security Technologies*, 8(1):16–34, January 2021.
3 Richard Smith, Helge Janicke, Ying He, Fenia Ferra, and Adham Albakri. The agile incident response for industrial control systems (AIR4ICS) framework. *Computers & Security*, 109:102398, 2021.

3.7 Race-to-the-Bottom: Evolution of Threat Landscape to Industrial Control Systems

Marina Krotofil (Maersk – Aarhus, DK)

Industrial Control Systems (ICS) threat landscape has changed dramatically over the past years. New threats have emerged to challenge the shock created by Stuxnet. This talk will present the evolution of the ICS exploits and tactics to picture ongoing "race-to-the-bottom" trend between ICS threat actors and defenders. This trend refers to the tendency of the attackers to move their exploits one layer down as soon as security controls are introduced at some layer of the computer or network architecture. While OT asset owners begin to harden operator consoles and embrace ICS network monitoring solutions, the attackers are already moving their exploits into the controllers at the regulatory layer of network architecture. The reason for this strategy is the lack of exploit mitigation and detection capabilities in most of the embedded systems components deployed within ICS and a lack of tools to support compromise assessment and forensic analysis of these systems. This talk will outline the ICS exploitation trends and briefly discuss their implication on defensibility and evaluating risks to ICS environments.

3.8 Vulnerability Forecasting: Theory and Practice

Éireann Leverett (University of Cambridge, GB)

Joint work of Éireann Leverett, Matilda Rhode, Adam Wedgbury
Main reference Éireann Leverett, Matilda Rhode, Adam Wedgbury: "Vulnerability Forecasting: In theory and practice", CoRR, Vol. abs/2012.03814, 2020.
URL https://arxiv.org/abs/2012.03814

It is possible to forecast the volume of CVEs released within a time frame with a given prediction interval. For example, the number of CVEs published between now and a year from now can be forecast within 8% of the actual value. Different predictive algorithms perform well at different lookahead values other than 365 days, such as monthly, quarterly, and half year. It is also possible to estimate the proportions of that total volume belonging to specific vendors, software, CVSS scores, or vulnerability types. Some vendors and products can be predicted with accuracy, others with too much uncertainty to be practically useful. This paper documents which vendors are amenable to being forecasted. Strategic patch management should become much easier with these tools, and further uncertainty reductions can be built from the methodologies in this paper.

3.9 Risk Dependency and Cyber Insurance

Mingyan Liu (University of Michigan – Ann Arbor, US)

Joint work of Mingyan Liu, Mahdi Khalili, Parinaz Naghizadeh, Armin Sarabi, Tongxin Yin

Cyber risks are notoriously interdependent at a firm level: an insured's risk is a function of not only its own conditions, but also that of its vendors and suppliers. Insurers generally try to avoid this type of risk dependency. Within this context, I will discuss our research over the past 7–8 years on shifting the focus from the conventional view of using insurance as primarily a risk management mechanism to one of risk control and reduction by looking for ways to re-align the incentives of parties involved in an insurance contract and exploiting the unique properties of cyber risk. In particular, using a commonly practiced rate-schedule based policy framework, I will analyze and compare three different policy portfolios and make a case for why insurers should actually consider embracing risk dependency in their underwriting. I will also share our most recent work on underwriting ransomware insurance. In doing so, I will draw a number of parallels between ransomware attacks and the centuries-old crime, kidnapping for ransom, discuss how the latter has been an insurable risk, and highlight lessons we can learn in conceptualizing an effective framework around the design and governance of ransomware insurance.

References

1 Mohammad Mahdi Khalili, Mingyan Liu, and Sasha Romanosky. Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, 5(1), October 2019.
2 Mohammad Mahdi Khalili, Parinaz Naghizadeh, and Mingyan Liu. Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9):2226–2239, September 2018.

3 Mingyan Liu. *Embracing Risk: Cyber Insurance as an Incentive Mechanism for Cybersecurity*, volume 2. Morgan & Claypool Publishers LLC, June 2021.
4 Yang Liu, Armin Sarabi, Jing Zhang, Parinaz Naghizadeh, Manish Karir, Michael Bailey, and Mingyan Liu. Cloudy with a chance of breach: Forecasting cyber security incidents. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 1009–1024, Washington, D.C., August 2015. USENIX Association.
5 Armin Sarabi, Parinaz Naghizadeh, Yang Liu, and Mingyan Liu. Risky business: Fine-grained data breach prediction using business profiles. *Journal of Cybersecurity*, 2(1):15–28, December 2016.

3.10 Exploiting production system engineering data to evaluate attacks

Arndt Lüder (Otto-von-Guericke-Universität Magdeburg, DE)

Main reference Anna-Kristin Behnert, Felix Rinker, Arndt Lüder, Stefan Biffl: "Migrating Engineering Tools Towards an AutomationML-Based Engineering Pipeline", in Proc. of the 19th IEEE International Conference on Industrial Informatics, INDIN 2021, Palma de Mallorca, Spain, July 21-23, 2021, pp. 1–7, IEEE, 2021.
URL http://dx.doi.org/10.1109/INDIN45523.2021.9557517
Main reference Stefan Biffl, Arndt Lüder, Kristof Meixner, Felix Rinker, Matthias Eckhart, Dietmar Winkler: "Multi-view-Model Risk Assessment in Cyber-Physical Production Systems Engineering", in Proc. of the 9th International Conference on Model-Driven Engineering and Software Development, MODELSWARD 2021, Online Streaming, February 8-10, 2021, pp. 163–170, SCITEPRESS, 2021.
URL http://dx.doi.org/10.5220/0010224801630170
Main reference Arndt Lüder, Stefan Biffl, Felix Rinker, Anna-Kristin Behnert: "32 Engineering Data Logistics based on AML", pp. 579–602, De Gruyter Oldenbourg, 2021.
URL http://dx.doi.org/doi:10.1515/9783110745979-034
Main reference Kristof Meixner, Arndt Lüder, J. Herzog, Dietmar Winkler, Stefan Biffl: "Patterns for Reuse in Production Systems Engineering" in Proceedings of the 33th International Conference on Software Engineering and Knowledge Engineering (SEKE)", Pittsburgh, USA, July 1-10, 2021, IEEE, 2021.
URL http://dx.doi.org/10.18293/SEKE2021-150

Engineering data are a vital source of information applicable to evaluate security concerns within production systems.

To make them applicable at first an engineering data logistics is required resulting in an aggregated set of engineering information related to all assets within a production system and at second appropriate analysis methodologies for the collected engineering data treasure are required.

Relevant research question in this directions are the following: What are the right data sources to represent the required knowledge for a security evaluation? What is an appropriate data logistics? How to analyze the collected data?

Attention has to be put on the necessary effort and the potentials of reusing engineering data that can reduce effort significantly.

3.11 ICSs in the context of Industry 4.0 - A life cycle consideration

Arndt Lüder (Otto-von-Guericke-Universität Magdeburg, DE)

Production systems can be considered as a combination of resources intended to be used to execute production processes resulting in products exposint "the right" product properties for beeing valuable for customers. Hence a PPR based consideration of products can help to understand potential impacts on production systems resulting from security attacks.

Such attacks can disable, hamper or disturb production systems. Disable mean permanently prevent a functionality from being applied thus stoping production. Hamper means temporarily prevent a functionality from being applied. Finally disturb means changing function results without notice.

While currently disable and hamper are mainly considered within research disturb is less considered. But such attachs are much more effectfull to companies as they are more difficult to identify than the others by conventional production system quality management.

This leads to the following research questions:

- How to collect and classify assets and attacks to production systems?
- What are motivation, aim, effect, and required knowledge of different attacks?
- Are there similarities and differences?
- Will we find "same" assets?
- Will attacks at engineering time enable / enforce attacks at runtime?
- Which knowledge is required?

3.12 Dependency Model of a SCADA System for Goal-Oriented Risk Assessment

Simin Nadjm-Tehrani (Linköping University, SE)

In this talk I present some reflections from the past two days about how to do ICS risk analysis and relate to work done in my group and other colleagues. The insurance companies and policy makers want to know how to assess economic risks in relation to cyber incidents in ICS. They seem to want an "easy" approach that works without taking months/years to perform. At the other end of the spectrum we have the cybersecurity researchers who study risk in diverse ways and create multiple tools and methods that need feeding with a lot of information. Will these meet the requirements? The meeting has discussed relatively little the contrasts in stakeholders perspectives [3, 2]. I open the talk by some approaches for cyber risk analysis at different levels of granularity and embryos of some (digital) tools to support the analysis activities. I conclude with some recent work [1] that is based on a goal-directed approach to analysis risk in a SCADA context that may be transferable to other areas.

References

1 Yulia Cherdantseva, Pete Burnap, Simin Nadjm-Tehrani, and Kevin Jones. A configurable dependency model of a SCADA system for goal-oriented risk assessment (under submission). 2022.

2 Maria Vasilevskaya and Simin Nadjm-Tehrani. Quantifying risks to data assets using formal metrics in embedded system design. In Floor Koornneef and Coen van Gulijk, editors, *Computer Safety, Reliability, and Security*, pages 347–361, Cham, 2015. Springer International Publishing.

3 Maria Vasilevskaya and Simin Nadjm-Tehrani. Model-based security risk analysis for networked embedded systems. In Christos G. Panayiotou, Georgios Ellinas, Elias Kyriakides, and Marios M. Polycarpou, editors, *Critical Information Infrastructures Security*, pages 381–386, Cham, 2016. Springer International Publishing.

3.13 Cyber Insurance: ICS vs ITS

Galina Schwartz (Cyber Blocks Inc. – Berkeley, US)

Joint work of Galina Schwartz, Carlos Barreto, Alvaro A. Cardenas
Main reference Carlos Barreto, Galina Schwartz, Alvaro A. Cardenas: "Cyber-Risk: Cyber-Physical Systems Versus Information Technology Systems", pp. 319–345, Springer International Publishing, 2021.
URL http://dx.doi.org/10.1007/978-3-030-65048-3_14

This talk introduces a taxonomy of cyber risks for ICS (Industrial control systems) and ITS (information technology systems). Both, ICS and ITS are data rich environments, yet they are plagued by extreme information deficiencies, combined with a high level of information asymmetries. We outline the factors complicating the advancement of ICS cyber-insurance ecosystem, incl.: extreme information scarcity; risk assessment difficulties, exacerbated by the growing complexity of ICS and the intricacies of risk prorogation. We conclude that without improving security relevant information, the cyber-insurance market for ICS may stall. Market advancement requires overcoming data scarcity and lack of standardization. We call for further research in CPS risk management, and specifically design and evaluation of novel technical tools and policies / regulations improving incentives of the ICS decision-makers to collect and share security related data. This talk is loosely based on [2, 1].

References

1 Carlos Barreto, Galina Schwartz, and Alvaro A. Cardenas. *Cyber-Insurance*, pages 347–375. Springer International Publishing, Cham, 2021.
2 Carlos Barreto, Galina Schwartz, and Alvaro A. Cardenas. *Cyber-Risk: Cyber-Physical Systems Versus Information Technology Systems*, pages 319–345. Springer International Publishing, Cham, 2021.

3.14 Counterfactual Analysis of Cyber-Physical Risk

Gordon Woo (Risk Management Solutions – London, GB)

Whenever notable adverse events occur, effort is naturally focused on risk mitigation and disaster prevention. According to psychologists, the great majority of thoughts about the past focus on how things might have been better. These are upward counterfactuals. However, important lessons may also be learned from thoughts about how things might have been otherwise – in particular if they had been worse. These are downward counterfactuals [1]. Most cyber-physical attacks turn out to be near-misses; examples of what might happen, but has not yet happened.

In 2013, an Iranian hacker, working on behalf of the Iranian government, repeatedly obtained unauthorized access to the SCADA systems of the Bowman Dam, in Rye, N.Y.. Although SCADA system access would normally have permitted remote operation and manipulation of the Bowman Dam's sluice gate, by a stroke of good fortune, this had been manually disconnected for maintenance at the time of his intrusion. This was a near-miss. Counterfactually, manipulation of the sluice gate might have led to flooding.

The historical record of cyber attacks is brief, but there is a large database of cyber attacks and their loss impacts. This historical database can be supplemented by a downward counterfactual database, which is currently under development.

References

1 Gordon Woo. Downward counterfactual search for extreme events. *Frontiers in Earth Science*, 7, 2019.

3.15 How Insurance Shapes Incident Response

Daniel Woods (Universität Innsbruck, AT)

Joint work of Daniel Woods, Rainer Böhme
Main reference Daniel W Woods, Rainer Böhme: "How Cyber Insurance Shapes Incident Response: A Mixed Methods Study", 2021.
URL https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-woods.pdf

Cyber insurance policies commonly indemnify the cost of incident response services. This creates a multi-layered economic problem in that the policyholder hiring external firms incurs transaction costs and the insurer paying the bill creates a principal-agent problem. We adopted a multistage research design to understand how insurers address the problem. The talk explains how insurers have created a private ordering by controlling which firms are selected, negotiating prices ahead of time, and punishing low service quality by withholding future work. A minority of firms win the majority of work, thereby building trust through repeated interactions.

4 Working Groups

4.1 Analyzing the ICS Threat Landscape

Matthias Eckhart (SBA Research – Wien, AT)

Joint work of All Participants of the Seminar

The objective of this breakout session was to clarify the assumptions regarding ICS-targeting cyber-attacks that underlie loss scenarios. As a first step, the participants determined attributes of threat actors that influence the plausibility of a scenario. The considered attributes are in line with typical attacker properties that are assessed during profiling activities as part of threat modeling, which are often described in security textbooks. Examples include intent, motivation, skills, and resources. Given the evident focus on high-impact events, the participants concentrated on the following attacker archetypes:

(i) state-sponsored actors who want to gain a strategic advantage for their country of origin (e.g., in terms of political, military, and economic power),
(ii) terrorists who aim for maximum visibility to promote their ideologies and attract sponsors, and
(iii) organized cybercrime groups that are financially motivated.

Several assumptions were also made concerning the interactions between attackers and defenders. Most importantly, the participants agreed on an attacker model that considers rational and opportunistic decisions. In other words, adversaries have a limited budget available to execute cyber-physical attacks over a certain time period during which they can also adapt the attack strategy, seeking to minimize their costs while maximizing the defender's losses. Further aspects to consider when defining the attacker model relate to the strategic and tactical dimension, including the preparation phase and required resources (e.g., testbeds, exploits), techniques to gain a foothold, coordination of attack campaigns, and approaches to minimize the risk of detection. In this context, the following questions were discussed by participants:

- What are the resources and skills needed to execute large-scale cyber-attacks against ICSs?
- How does the level of difficulty change along the entire spectrum of ICS-targeting cyber-attacks?
- Which factors drive the scalability of a cyber-physical attack? How scalable is the considered cyber-physical threat?
- How likely are highly coordinated cyber-attacks launched against ICSs?
- Which trends (e.g., IT/OT convergence, Industrial Internet of Things, increasing redundancy in the supply chain) influence risk factors?
- Would such an attacker model have a reasonable stability? Would it be sensible to incorporate it in a loss scenario, considering that the threat landscape and technological trends change so rapidly?
- Which IT security measures have to be adapted to the requirements and characteristics of OT environments?
- How will the regulatory landscape pertaining to ICS security emerge in the next few years?
- How and to what extent is the state of ICS security improved by the standardization and implementation of reference architectures?
- What would be an attacker model that insurance will cover?

Naturally, the search for answers to these questions is guided by the idea that past observations are to a certain extent indicative of the future. Thus, prior ICS-related security incidents and near misses were intensively discussed. A recurring question among participants was why comparatively few noteworthy loss events involving ICSs are known. If the current state of ICS security is as alarming as is often portrayed, why do we not see *more* large-scale ICS-focused attacks that inflict significant damages? Obviously, the majority of successful attacks are promptly handled by incident response teams to limit their impact and even those that caused physical damages often go unreported or are not recognized as security incidents. However, it still seems that the (admittedly sparse) empirical data on cyber-physical attacks are not in line with what we would expect in terms of loss severity. One factor that may explain this discrepancy is the diversity in the context of hardware, software, and industrial processes, limiting the scalability of cyber-physical attacks.

Besides the discussions on how the threat landscape has evolved over the years, the participants also engaged in thought experiments about future attack trends. The groups came up with a set of observations and reflections suggesting that the overall state of ICS security will most likely not improve. Instead, the participants expect that malware will find its way into new generations of ICSs (e.g., renewable energy), cascading risks rise due to the proliferation of cloud-based industrial applications and the Industrial Internet of Things, and supply chain attacks become more sophisticated. Further, they expect that the

ICS threat landscape will be heavily shaped by the global political developments. As for non-state-sponsored threat actors, the participants anticipate that ICSs will become more profitable targets when terrorists and criminals acquire the expertise to scale up their attacks.

4.2 Developing Extreme Cyber-Physical Loss Scenarios

Matthias Eckhart (SBA Research – Wien, AT)

Following the discussions on the ICS threat landscape, the subsequent breakout sessions focused on developing loss scenarios for the ICS-specific cyber cat model. Ultimately, the objective was to describe and estimate extreme, but plausible cyber-physical attack scenarios featuring cascading effects, which increase the risk that losses could accumulate to a level that exceeds the (re)insurer's capacity to absorb it. The lightning talks given by Simon Dejung and Téodore Iazykoff served as a valuable introduction to catastrophe modeling and stimulated a fruitful exchange of ideas among participants about which approach to take. Two strategies emerged from these activities:

(i) The *top-down* approach seeks to estimate the impact of cyber-physical attacks at the macroeconomic level. Initially, the industry landscape is systematically analyzed to find chokepoints that could harm the global economy in the event of a large-scale attack. In particular, dependencies between companies need to be assessed to identify potential fragile economic conditions, which requires a broad understanding of supply chains and the market structure. Then, the overall problem is decomposed to reduce the complexity of estimating economic losses. An example for such a sub-problem would be the market share of victims in GDP terms. Once the skeleton of the scenario has been constructed, a further drill down to the factors that ultimately drive the frequency and severity can be carried out. The main task at this stage is to determine plausible cyber-physical attacks launched against the considered victims and the consequences that could push PD/MD, BI, and LOP to a realistic maximum.

(ii) The *bottom-up* approach seeks to approximate aggregate losses by using firm-level estimates. Thus, the initial focus lies on the technical and operational aspects from an asset owner's perspective when designing attack scenarios. In this context, the results of business impact analyses and risk assessments are central to understanding the potential consequences of loss of control and loss of safety. Furthermore, a retrospective view upon (non-)cyber-related ICS incidents may be used to identify and discard unrealistic scenarios. It should also be noted that scenarios with more advanced cyber-physical attacks may require careful consideration of the involvement of other roles (i.e., victims) within the ICS lifecycle, such as product suppliers, systems integrators, and service providers. After establishing a solid basis for the analysis, it is necessary to identify victim candidates that would be similarly affected (e.g., due to similarities in their IT/OT architectures) and to assess how the effects of the considered loss event could propagate across sectors.

Depending on the group members' background and confidence to start estimating the loss frequency and loss severity based on macro- or micro-factors, a mixed approach may be beneficial. In this way, complementary views can be incorporated to ensure that assessments coming from both directions meet in the middle. The experience we gained from the breakout

sessions was that the bottom-up approach more easily takes subject-matter experts on a journey further down the rabbit hole of cyber-physical attacks, especially if their expertise is predominantly technical.

One group proposed the notion of *proximity* as an indicator for correlated risk, which was well-received and deemed highly useful by other groups. Measures of proximity are relevant to both top-down and bottom-up approaches and take different forms:

- *Logical proximity:* Multiple independent systems that are prone to fail at once due to the use of the same type of components or architectures are considered to be in close logical proximity. Basic examples that may lead to closer logical proximity include shared libraries, (near) identical configurations, similar artifacts in model-driven development, or even common blueprints for engineered systems (e.g., Tesla's Gigafactory concept that heavily relies on similar plans and equipment to accelerate expansion).
- *Temporal proximity:* If this property is present, multiple systems are prone to fail in close succession due to coordinated attacks performed by adversaries to achieve a particular goal. For instance, close temporal proximity exists if a series of well-timed attacks target independent units, one after another, seeking to bring down critical infrastructure.
- *Causal proximity:* This measure reflects the susceptibility of systems caused by their strong dependencies to others. Basically, if an attack compromises an integral component of an infrastructure, the entire services built on top are affected as well. Typical examples that can inflict serious losses due to causal proximity are related to the supply chain (e.g., hardware trojans) and infrastructure (e.g., DNS service disruption that leads to a widespread outage of websites).

In this context, two central questions arise: First, how can we measure logical, temporal, and causal proximity? Second, what actions can be taken to mitigate these forms of proximity? While these questions remain important avenues for future research, the participants suggested that engineering data could enable proximity measurements (at least in greenfield projects) and that different techniques of software diversity may be applicable to the industrial domain. Since data for proximity measurements on a global scale is scarce, the participants attempted to gauge the level of technological heterogeneity in different industrial domains. From a purely anecdotal perspective, it has been suggested that there are few industrial processes relying on highly specialized equipment that can be sourced from just one or two suppliers.

When developing the extreme cyber-physical loss scenarios, the following key questions were considered by the participants:

- Which targets would be profitable for the considered attacker archetypes and which of them could incur significant losses?
- What are possible chokepoints?
- What kind of long-term damages may be incurred by victims of cyber-physical attacks?
- What mechanisms are typically in place that ensure a safe, ultimate shut-down of a plant in case the systems have been compromised and are out of operator control?
- How quickly can asset owners switch to manual operation in the event of an attack to recover the industrial processes?
- What would be an adequate balance of prevention and response measures?
- How will the supplier landscape emerge (e.g., mergers and acquisitions, standardization) and what would be the consequences in terms of correlated risk?
- How can the incident response capacity needed for a given cyber-physical cat event be quantified?
- What are the differences in cyber-physical risk perception from the asset owner's and insurer's perspective?

- How does the sophistication of security measures in ICSs change depending on the level of insurance cover?
- How do asset owners find a balance between risk mitigation and risk transfer? Can we observe regional or sectoral differences?
- Which requirements regarding the implementation of ICS security measures can be imposed by insurers?
- Which information on ICSs should systems integrators provide to support the insurability of cyber-physical risk?
- How can certifications of ICS components shape the insurance industry?

To kick-off scenario building, the organizers have asked the participants about their interest and expertise in answering the aforementioned questions. After establishing common ground, brainstorming sessions were conducted to identify and frame the scenarios, which involved the following domains:
(i) power transmission,
(ii) natural gas (pipelines),
(iii) rail transport, and
(iv) air traffic control.
The participants decided to prioritize loss severity over loss frequency as variables of the former were deemed more stable. Given the limited time available, the participants approached the estimation problem by decomposing it into parameters, rating the parameters per scenario relative to each other, and constructing arguments that support these standpoints. The following list provides on overview of the considered parameters.

- Infrastructure: logical proximity, geographical dispersion, and resilience (in the sense of fault tolerance)
- Adversary: required domain knowledge (with respect to the industrial processes operated by the victim), required knowledge of the victim's IT environment and organizational structure, required knowledge of the victim's OT environment and executed process, and required resources to perform the attack (e.g., testbeds, person hours)
- Impact: negative physical effects and financial losses

While the participants engaged in vivid discussions during parameter ranking that led to important insights into the underlying problems, it became apparent that a more domain-specific setting is needed. Many of the sketched worst-case scenarios portrayed disastrous consequences, but on second thought the impact seemed negligible. For instance, the impact of a gas pipeline outage can be buffered by the storage capacity of the network, allowing time for recovery. The breakout sessions showed that determining such factors requires specialized know-how and a greater focus on a specific scenario. Thus, we plan to intensify our efforts by mobilizing additional domain expertise and initiating follow-up projects. Nevertheless, conducting the scenario building exercises was a valuable experience and marks the first step toward an ICS-focused cyber cat model.

Participants

- Luca Allodi
TU Eindhoven, NL
- Gergely Biczók
Budapest University of Technology & Economics, HU
- Rainer Böhme
Universität Innsbruck, AT
- Carl Denis
Universität der Bundeswehr – München, DE
- Matthias Eckhart
SBA Research – Wien, AT
- Alexander Horch
HIMA – Brühl, DE
- Sejdefa Ibisevic
Universität Wien, AT
- Julia Kittel
FH Emden, DE
- Klaus Kursawe
GridSec – Geneva, CH
- Arndt Lüder
Otto-von-Guericke-Universität Magdeburg, DE
- Fabio Massacci
Vrije Universiteit Amsterdam, NL
- Thomas Steinhaus
Munich Re, DE
- Edgar Weippl
University of Vienna & SBA Research – Wien, AT
- Jens Wiesner
BSI – Bonn, DE
- Daniel Woods
Universität Innsbruck, AT

Remote Participants

- Fabrizio Baiardi
University of Pisa, IT
- Vivien Bilquez
Zurich Insurance Group, CH
- Achim D. Brucker
University of Exeter, GB
- Richard Clayton
University of Cambridge, GB
- Simon Dejung
SCOR – Zürich, CH
- Andreas Ekelhart
SBA Research – Wien, AT
- Barbara Fila
IRISA – Rennes, FR
- Peter Hacker
Distinction.Global – Uetikon am See, CH
- Teodore Iazikoff
SCOR – Paris, FR
- Helge Janicke
Cyber Security CRS – Joondalup, AU
- Ersin Kaplan
HDI Global SE – Hannover, DE
- Marina Krotofil
Maersk – Aarhus, DK
- Éireann Leverett
University of Cambridge, GB
- Mingyan Liu
University of Michigan – Ann Arbor, US
- Markus Maier
Universität Wien, AT
- Jürgen Musil
Netinsurer – Wien, AT
- Simin Nadjm-Tehrani
Linköping University, SE
- Ranjan Pal
University of Michigan – Ann Arbor, US
- Keyun Ruan
Empty Labs Ltd. – London, GB
- Galina Schwartz
Cyber Blocks Inc. – Berkeley, US
- Sara Tajik
SBA Research – Wien, AT
- Josephine Wolff
Tufts Universtity – Medford, US
- Gordon Woo
Risk Management Solutions – London, GB
- Quanyan Zhu
NYU – Brooklyn, US