Dagstuhl Seminar 21451: Managing Industrial Control Systems Security Risks for Cyber Insurance

November 07 – 12, 2021

Version 1.5

Organizers:
Simon Dejung (SCOR – Zürich, CH) sdejung@scor.com
Mingyan Liu (University of Michigan – Ann Arbor, US) mingyan@umich.edu
Arndt Lüder (Universität Magdeburg, DE) arndt.lueder@ovgu.de
Edgar Weippl (University of Vienna & SBA Research, AT) edgar.weippl@univie.ac.at

Collector:
Matthias Eckhart (University of Vienna & SBA Research, AT) meckhart@sba-research.org

Video Conferencing Assistants:
Sejdefa Ibisevic (University of Vienna – Wien, AT) sejdefa.ibisevic@univie.ac.at
Markus Maier (University of Vienna – Wien, AT) markus.maier@univie.ac.at
Sara Tajik (SBA Research – Wien, AT) stajik@sba-research.org

1 Objectives and Topics of the Seminar

This Dagstuhl seminar aims to advance the understanding of cyber risks pertaining to industrial control systems (ICSs) and associated insurance aspects. To this end, we intend to contribute to the transition from a qualitative to a quantitative cyber risk measurement approach. The developed concepts and models will be a result of interdisciplinary work conducted by academics and industry professionals from the fields of computer science, automation engineering, and actuarial science.

Expected Output The expected output is an economic loss model based on ICS worst-case scenarios, affecting globally and simultaneously many critical infrastructures (e.g., power, petrochemical, transport, logistics etc.). Ideally, this model will be refined by the participants after the seminar and published as a joint research work.

Research Topics To set the frame for this seminar, we identified four topics that will be covered in plenary sessions and breakout sessions. In each plenary session, three lightning talks will be held that should motivate the collaborative work in the breakout sessions. The working groups (à 5–7 participants) will study the same overarching topic of the breakout session (yet each with a different focus) in order to strengthen the interdisciplinary exchange.

To reach the expected output, the main topics and motivating research questions, are:

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 the severity?

2 General Information

SARS-CoV-2 Prevention Measures The seminar takes place under strict hygiene and preventive measures. We expect that all participants have read and adhere to the protection and hygiene concept of Schloss Dagstuhl.[1] If you have additional questions regarding this concept, please send an e-mail to `service@dagstuhl.de`.

Hybrid Mode Due to the travel restrictions caused by the SARS-CoV-2 pandemic, the organizers decided to host the seminar in hybrid mode, meaning that on-site participation is possible and remote participants can join via Zoom as well. The Zoom participation link will be posted on the Dagstuhl Wiki.[2] Three video conferencing assistants were nominated by the collector who operate the equipment and support the participants if technical difficulties arise. We recognize that time zone differences may hinder the ability of remote participants to join group sessions; hence, we allow reasonable adjustments to the agenda if needed.

Group Work The organizers have defined research questions (abbreviated as RQ) for the breakout sessions. These research questions should serve as entry points into the topics, facilitating and encouraging inter-disciplinary discussions. The organizers have split up the participants into groups for the breakout sessions I and II in advance, but participants are free to switch groups. Each group needs to nominate a chair who is responsible for moderating the group discussions, presenting and documenting the results.

Collaborative Work Please follow the Dagstuhl Wiki[3] for further information, which can be accessed using your personal DOOR credentials. The findings of breakout sessions and other key results should be documented in our shared Google Drive directory.[4] Furthermore, note that we have setup a group on Signal[5] to facilitate communication among participants. You can join this group via the link[6] or by using the QR code shown in Figure 1.

Figure 1: QR code to join the Signal group.

Lightning Talks Please avoid conference-style talks, do not (only) propose solutions but allow your talk to raise open research questions. Leave enough time at the end of your talk for an open discussion. Furthermore, take the highly interdisciplinary setting of this seminar into account; try to avoid acronyms and technical jargon. We kindly ask you to upload your slides to the seminar materials website[7], which can be accessed using your personal DOOR credentials.

3 Method

It is worth reiterating that the objective of this seminar is to make the first steps toward a probabilistic cyber catastrophe model that is tailored to the ICS domain. To provide a basis for discussions on the method to be used to develop this model, we have visualized a set of potentially useful method elements in Figure 2. Note that the components listed in Figure 2 are only a first draft that should be challenged.

[1] `https://www.dagstuhl.de/program/planning-your-visit/sars-cov-2-prevention`
[2] `https://angelina.dagstuhl.de/guestWiki/index.php/21451`
[3] `https://angelina.dagstuhl.de/guestWiki/index.php/21451`
[4] `https://drive.google.com/drive/folders/1TDhVvrXOBSz2_FPct7nbFXAV31AzemwG`
[5] `https://signal.org/`
[6] `https://signal.group/#CjQKIMER6gUit6SojuxZ-Y3Xka72gR2av_ak21CC2yoI3syoEhDqN6ZWHipQg3QMKGeAQC6O`
[7] `https://materials.dagstuhl.de/index.php?semnr=21451`

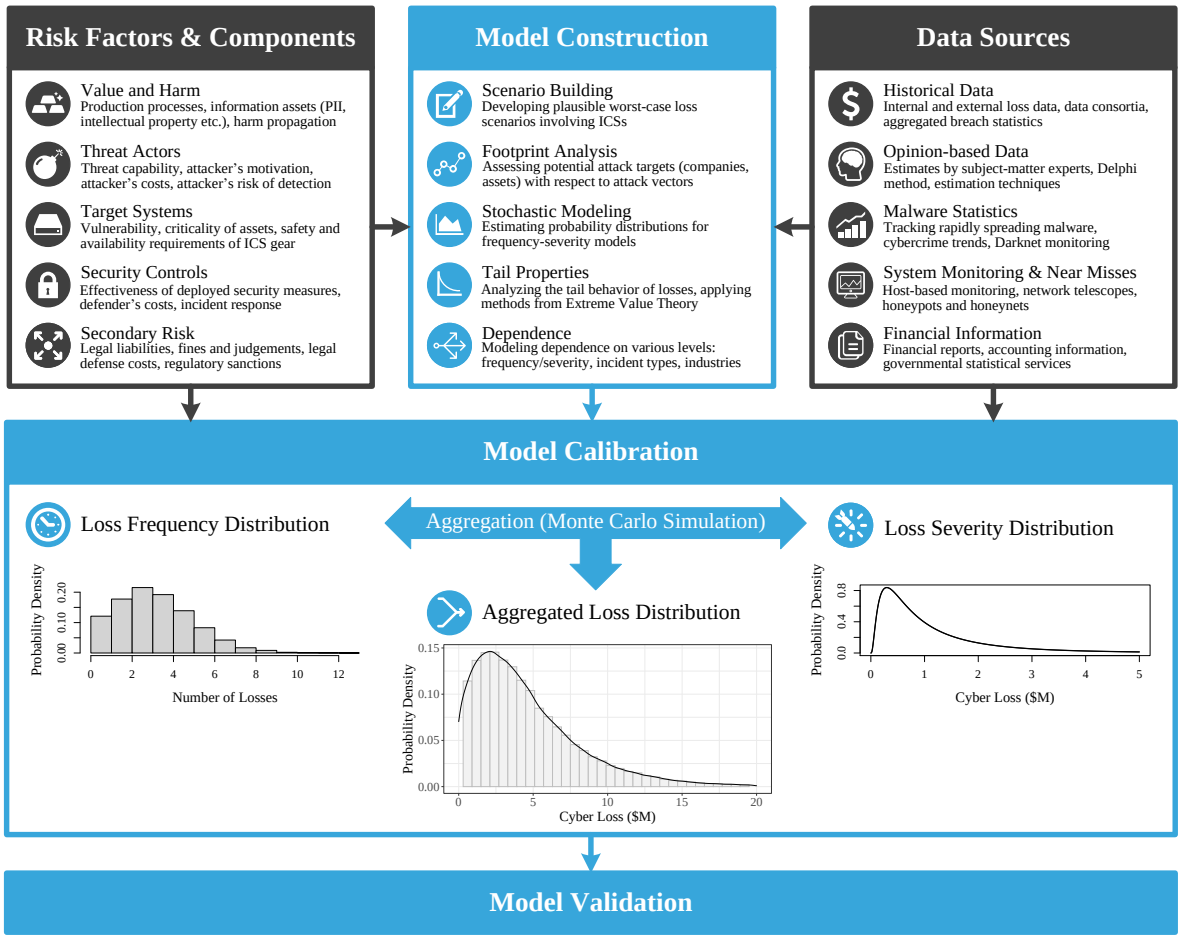

Figure 2: Potential components of a probabilistic catastrophe model for the ICS domain (adapted from materials provided by SCOR SE).

4 Supporting Literature

We kindly ask participants to skim the following articles in advance of the seminar:

[1] Dejung, Simon. *Newsletter — Risk Assessment for ICS/SCADA Security in Industrial Property, Engineering, Power, Oil & Gas*. Tech. rep. A joint workshop in March 2018 by LMA, IMIA & OPERA at SCOR (Zurich). SCOR Global P&C, Mar. 2018. URL: `https://www.imia.com/wp-content/uploads/2018/11/RISK-ASSESSMENT-ICS_SCADA-SECURITY-PROPERTY-ENGINEERING-POWER-ENERGY.pdf`.

[2] Gregory Falco et al. "A Research Agenda for Cyber Risk and Cyber Insurance". In: *18th Annual Workshop on the Economics of Information Security WEIS*. 2019. URL: `https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_35.pdf`.

[3] IMIA Working Group. *Cyber Risks Engineering Insurers Perspective*. Tech. rep. 98 (16). IMIA Annual Conference 2016 – Doha, Qatar. Sept. 2016. URL: `https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf`.

[4] Lloyd's of London and Cambridge Centre for Risk Studies. *Business Blackout: The insurance implications of a cyber attack on the US power grid*. Tech. rep. Lloyd's of London and Cambridge Centre for Risk Studies, July 2015. URL: https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf.

[5] Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University. *Shen Attack: Cyber risk in Asia Pacific ports*. Tech. rep. Lloyd's of London, Cambridge Centre for Risk Studies, and Nanyang Technological University, 2019. URL: https://www.msig-asia.com/sites/msig_asia/files/downloads/CyRiM_ShenAttack_FinalReport.pdf.

[6] Lloyd's of London, Guy Carpenter, and CyberCube Analytics. *Cyber risk: The emerging cyber threat to industrial control systems*. Tech. rep. Lloyd's of London, Guy Carpenter, and CyberCube Analytics, Feb. 2021. URL: https://www.lloyds.com/news-and-insights/risk-reports/library/icsreport.

[7] Lobo, Francis. *Upstream Oil & Gas Cyber Risk: Insurance Technical Review*. Tech. rep. A Joint Rig Committee Report. Joint Rig Committee, May 2018. URL: https://www.lmalloyds.com/lma/readfile.aspx?iDocumentStorageKey=92c60394-2d02-4732-b75f-e54a02fa384d&iFileTypeCode=PDF&iFileName=upstream%20cyber%20report.

[8] Daniel W. Woods and Rainer Böhme. "SoK: Quantifying Cyber Risk". In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2021.

5 Schedule

Monday, 8th November 2021

09:00 **Welcome Session**
Simon Dejung, Mingyan Liu, Edgar Weippl, and Arndt Lüder

10:15 **Coffee Break**

10:30 **Session: Bridging the disciplinary gap**
A research agenda for cyber risk and cyber insurance
Simon Dejung
Security improvements in the production systems life cycle
Edgar Weippl
ICSs in the context of Industry 4.0 - A life cycle consideration
Arndt Lüder
Building blocks of a cyber cat model
Téodore Iazykoff

12:15 **Lunch**

13:30 **Breakout Session I: Analyzing the ICS threat landscape**
Race-to-the-Bottom: Evolution of threat landscape to industrial control systems (10 min.)
Marina Krotofil
RQ: How has the threat landscape evolved and what may be future ICS-targeting attack trends?
All participants

14:30 **Break**

14:45 **Breakout Session II: Developing extreme cyber loss scenarios**
Introduction and methodology
Organizers
RQ: What can be extreme, but plausible cyber loss scenarios (i.e., global ICS attacks)?
All participants

15:30 **Short Coffee Break (Breakout Session II continues afterwards until 17:00)**

17:00 **Presentation of the developed scenarios**
Group Chairs

18:00 **Dinner**

20:00 **Selection of most relevant scenarios & further planning**
All participants

Tuesday, 9th November 2021

09:00 **Session: Cyber-physical risk quantification**
Quantifying cyber risk
Rainer Böhme
Counterfactual analysis of cyber-physical risk
Gordon Woo
Using the Haruspex platform to quantify and manage cyber risk
Fabrizio Baiardi

10:00 **Coffee Break**

10:30 **Breakout Session III: Developing extreme cyber loss scenarios**
Introduction and methodology
Organizers
RQ: How likely (frequency) are the defined cyber loss scenarios?
RQ: What is the effective economic damage & impact on society (severity)?
Link these probabilities with the associated maximum economic losses.
All participants

12:15 **Lunch**

14:15 **Session: Insurance**
How risk dependency impacts insurance: from risk transfer to risk reduction
Mingyan Liu
How insurance shapes incident response
Daniel Woods
Cyber-insurance considered harmful
Fabio Massacci

15:30 **Short Coffee Break**

15:45 **Breakout Session IV: Developing extreme cyber loss scenarios**
Introduction and methodology
Organizers
RQ: How long can attacks persist before they are stopped and damage has been repaired?
RQ: Which are the scenarios & vectors of concern? How much can they spread?
RQ: Which hard (e.g., security measures) and soft (e.g., regulations) factors increase or reduce the probability (frequency) and amount of damage (severity)?
All participants

17:00 **Presentations of initial results**

18:00 **Dinner**

Wednesday, 10th November 2021

09:00 **Session: Security economics & Cyber Insurance**
Malware economics for risk quantification
Luca Allodi
Towards joined cyber insurance exercises
Helge Janicke
Vulnerability forecasting
Éireann Leverett

10:00 **Coffee Break**

10:30 **Breakout Session V: Insurance**
RQ: What are the opportunities and limitations of (cyber) insurance in the context of ICSs?
All participants

12:15 **Lunch**

14:00 **Excursion to Völklingen Ironworks**

18:30 **Dinner, niche topics, and free time**

Thursday, 11th November 2021

09:00 **Session: Lightning talks pool**
Exploiting production system engineering data to evaluate attacks
Arndt Lüder
ICS vs ITS cyber insurance: Is there a need to regulate, and how to?
Galina A. Schwartz
Dependency model of a SCADA system for goal-oriented risk assessment
Simin Nadjm-Tehrani
Insurance and procurement in ICS security
Klaus Kursawe

10:00 **Coffee Break**

10:30 **Breakout Session VI: External incentives for managing cyber-physical risks**
RQ: How can the incentives (e.g., regulation, funding, increased liability) be improved?
All participants

12:15 **Lunch**

13:30 **Breakout Session VII: Deep dive into selected topics**
All participants

15:30 **Break**

16:15 **Breakout Session VIII: Deep dive into selected topics**
All participants

18:00 **Departing Reception**

Friday, 12th November 2021

09:00 **Presentations of final results**
Group Chairs

10:45 **Coffee Break**

11:00 **Closing Session**
Wrap-Up, Next Steps, and Feedback
Organizers

12:15 **Lunch**

14:00 **Departure**