NEWSLETTER – RISK ASSESSMENT FOR ICS/SCADA SECURITY IN

INDUSTRIAL PROPERTY, ENGINEERING, POWER, OIL & GAS

A joint workshop in March 2018 by LMA, IMIA & OPERA at SCOR (Zurich)

Corresponding author:
Simon Dejung,
SCOR Global P&C
General Guisan Quai 26
Zurich, Switzerland
sdejung@scor.com

2018

SCOR
The Art & Science of Risk

TABLE OF CONTENTS

Contents

Acknowledgment 3
Newsletter 4
Abstract 4
Risk Assessment Steps 4
Questionnaires & Check lists 6
Guidelines & Recommended Practices 7
Bibliography & Table of figures 8

Acknowledgment

THE FOLLOWING EXPERTS AND ORGANIZATIONS – IN ALPHABETIC ORDER, SUPPORTED THIS STUDY. WE ARE VERY GRATEFUL FOR THEIR CONTRIBUTION:

Adrian Koster, MELANI
Alexander Horch, HIMA Paul Hildebrandt GmbH
Andreas Muehlemann, Switch
Candid Wüest, Symantec
Daniel Caduff, Federal Office for National Economic Supply
Daniel Schirato, Axpo
Dario Walder, Federal Office for National Economic Supply
Edgar Weippl, SBA Research GmbH
Francesca De Gregorio, Swiss Re
Ivo Maritz, BKW
Jean-Christophe Crouzet, Liberty Global Group
Jens Mehrfeld, BSI
John Munnings-Tomes, Navigators
Lukas Ruf, Consecom
Markus Edel, VdS Schadenverhütung GmbH
Michael Hammer, Scor
Milos Sarbajic, Helvetia
Patrick Davison, LMA Lloyds
Robert Aikey, Department of Homeland Security
Silvan Schenker, Federal Office for National Economic Supply
Simon Steinrücken, Hannover Re
Stefan Lenzhofer, CERT Austria
Stephan Beirer, GAI NetConsult GmbH
Thomas Pache, RiskPoint
Tobias Gebhardt, Munich Re

Newsletter

Abstract

Several ICS makers for critical infrastructures and industrial property suffered hacks or experienced software flaws in the recent past or communicated vulnerabilities which were or could have been - individually or potentially also simultaneously – exploited, resulting in an accumulation of damages (physical and non-physical), economic & insurance losses and outages.

This newsletter is the outcome of a workshop held in March 2018 in Zurich, Switzerland with internationally respected OT/ICS security experts. The newsletter gives guidance how insurance professionals can assess ICS controlled property risks and critical infrastructure – e.g. engineering, power, oil and gas. Insurance professionals should focus on measures by the insured to bring the frequency down and to impede propagation of cyber incidents, attacks and malware across a company network.
Underwriter and risk engineer should request, and risk manager and brokers should at least provide information about the following nine cyber incident related capabilities of the insured with focus on *"detect, protect, respond"*:

- Detection measures in place for monitoring & attack campaigns
- Organization & countermeasures in place once a cyber incident occurred (BCM strategy)
- IT/OT inventory (hard-& software), incl. IoT's and WiFi enabled deviced
- Patch management & life cycle policy
- Topology, segregation and compartmentalization of the insured asset (firewall & password policy)
- Backup & recovery policy
- IT/OT security training concept
- Supplier management
- Documentation

Risk Assessment Steps

The OT/ICS cyber risk culture and awareness can be categorized as:

- unaware / ignoring the exposure
- aware of the exposure
- aware and actively managing the exposure by continuous risk assessment

The ultimate goal for the insurance industry is to reduce that way the non-affirmative cyber risk of industrial property lines, to quantify the - currently silent – cyber exposure and draw a clear line between non-physical and physical aspects and their consequences (BI).

To approach this problem from a technical insurance perspective, several excellent publications broke down this complex topic:

- Cyber Insurance & Business Interruption (International Underwriting Association of London , 2018)
- Upstream Oil & Gas Cyber Risk: Insurance – Technical Review (Lloyd's Market Association & International Underwriting Association, 2018)
- Cyber Security & Safety Considerations for Oil, Gas & Petrochemical Risk Assessment (Lloyd's Market Association, 2017)
- The Guidelines on Cyber Security Onboard Ships (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI, 2017)
- Cyber Risks - Engineering Insurers Perspective (IMIA, 2016)

These documents give an overview and recommendations how to deal with the cyber exposure in different lines of business. What is partially missing in these publications is an easy to implement approach to assess the cyber risk of industrial property lines.

A good starting point to get familiar with this task – although maybe to extensive for an insurance risk engineer or underwriter - is the NIST cyber framework which follows a risk-based logic: *"identify, protect, detect, respond, recover"*. The NIST framework refers to the most common standards ISO/IEC, COBIT, ISA among others. The 108 subcategories form a comprehensive questionnaire to each of the five framework functions *"identify, protect, detect, respond, recover"*.
https://www.nist.gov/cyberframework

Several questionnaires and checklist derive from the NIST framework and are handier in use as they are shorter. We list nine of them which we consider relevant and recommend insurance professionals building on this existing knowledge. Underwriters and risk engineering should pick from these documents the questions which they consider relevant for their particular risk assessments. The guidelines underneath give some more background if needed.

Systems and devices should never be connected to public networks and only reachable via virtual private network, e.g. for remote maintenance. The internet exposure of an industrial risks can be assessed with ICS/SCADA search engines like the ones below. This is a rough indicator about the IT/OT security maturity of a policyholder. Figure 1 (Dejung, 2017) shows ICS systems in Switzerland, connected to the internet mid-April 2017 with the following widely used protocols, s7, modbus, fox, dnp3, bacnet.:

- https://www.shodan.io/explore/category/industrial-control-systems
- https://www.scadacs.org/ and their corresponding search engine censys.io

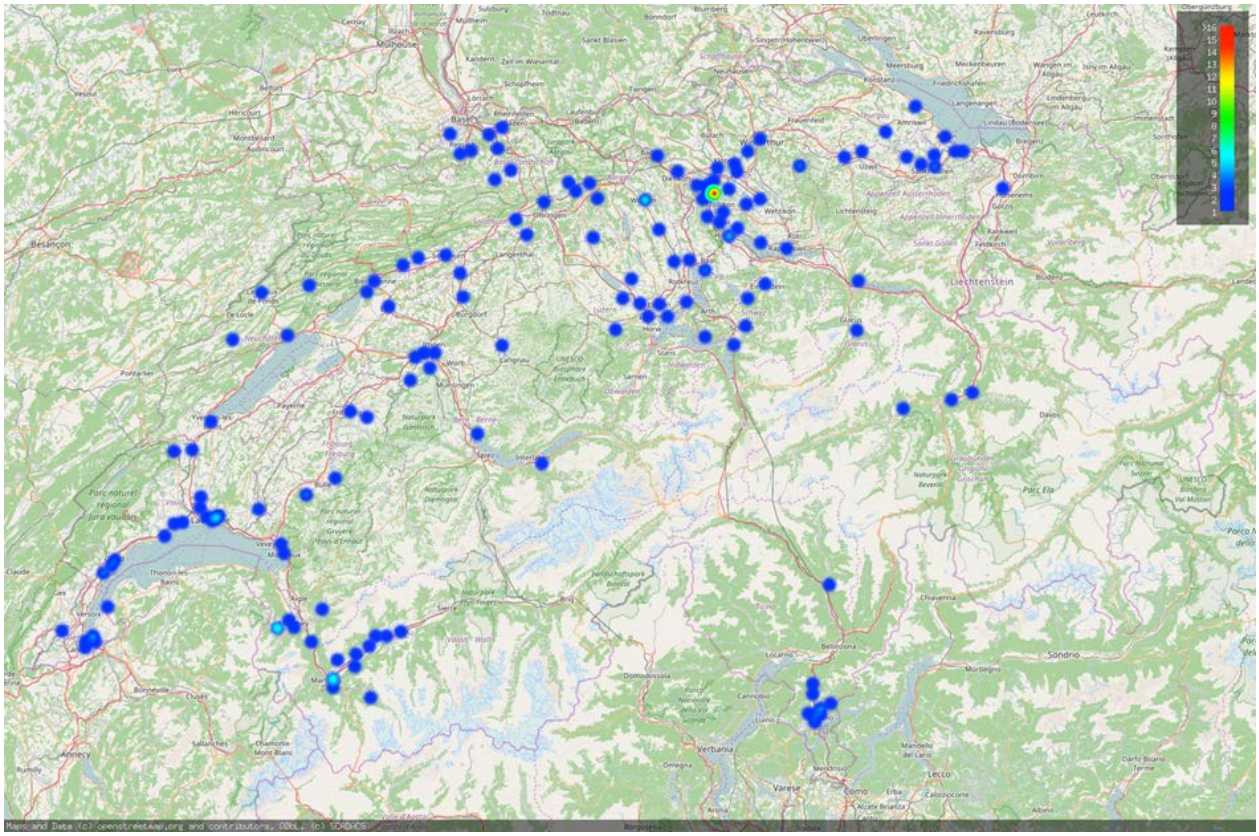

Figure 1: ICS systems in Switzerland, connected to internet mid-April 2017(protocols, s7, modbus, fox, dnp3, bacnet)

The Guide to Industrial Control Systems (ICS) Security (NIST, 2015) recommends the segregation of the insureds network as follows:

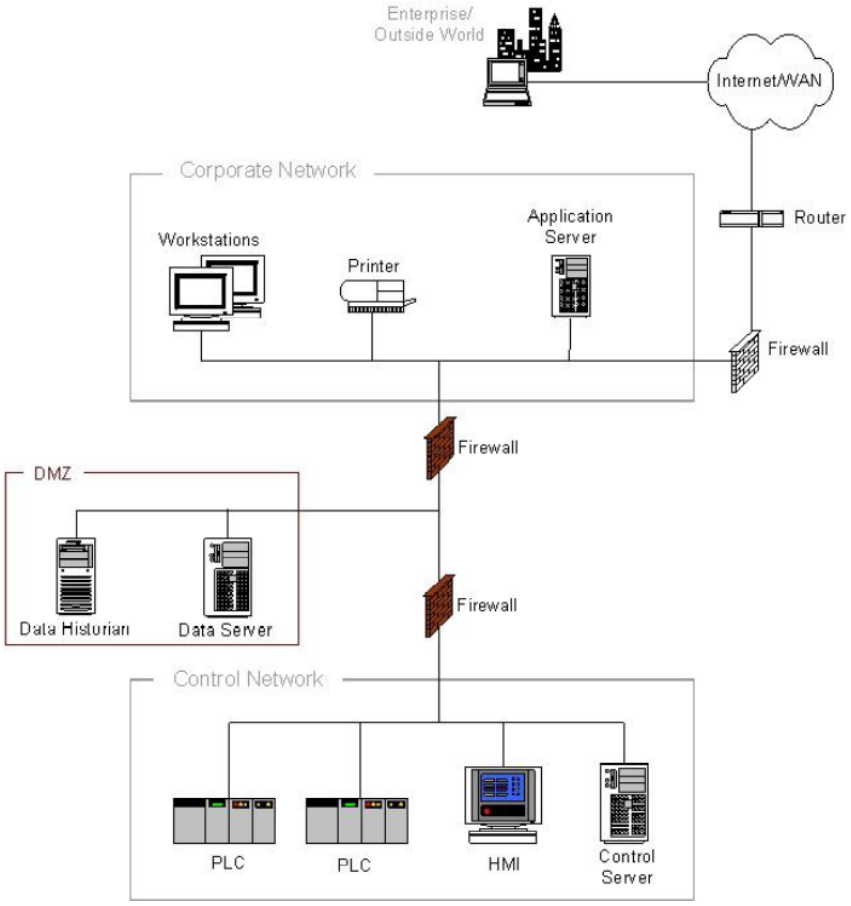

Figure 2: Recommended network segregation

Questionnaires & Check lists

- VdS Quick-Check for ICS (VdS Germany, 2018)
- Checklist security of ICS/SCADA systems (National Cyber Security Centre - Ministry of Security and Justice Netherlands, 2016)
- Top 10 Cyber Vulnerabilities for Control Systems (GE Oil & Gas, 2016)
- Measures for the protection of ICSs (Swiss Federal Reporting and Analysis Centre for Information Assurance MELANI, 2013)
- 10 Basic Cybersecurity Measures (Water Information Sharing and Analysis Center, 2015)
- ICS Cyber Security: Recommended Best Practices (Public Safety - Government of Canada, 2012)
- Hydro Cyber/SCADA Security Checklist (Federal Energy Regulatory Commission, 2016)
- 21 Steps to Improve Cyber Security of SCADA Network (Department of Energy United States of America, 2002)
- Audit protocols for industrial cyber security (Baybutt, 2003)

Guidelines & Recommended Practices

- Communication network dependencies for ICS/SCADA Systems (European Union Agency for Network and Information Security (ENISA), 2017)
- Managing Cybersecurity for ICS (ANSSI French Network and Security Agency, 2012)
- Improving ICS Cybersecurity with Defense-in-Depth Strategies (Department of Homeland Security & Industrial Control Systems Cyber Emergency Response Team, 2016)
- ICS Security Compendium, BSI (German Federal Office for Information Security, 2013)
- Minimum standard for improving ICT resilience (Swiss Federal Office for National Economic Supply FONES, 2018)
- Cybermaturity Platform (CMMI Institute - An ISACA Enterprise , 2018)

Bibliography & Table of figures

ANSSI French Network and Security Agency. (2012). *Managing Cybersecurity for Industrial Control Systems.* Retrieved from https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf

Baybutt, P. (2003). *Audit Protocol for Industrial Cyber Security.* Retrieved from http://www.primatech.com/images/docs/paper_audit_protocols_for_industrial_cyber_security.pdf

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI. (2017). *Cyber Security Onboard Ships.* Retrieved from http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16

CMMI Institute - An ISACA Enterprise . (2018). *Cybermaturity Platform*. Retrieved from https://cmmiinstitute.com/cmmi

Dejung, S. (2017). *Economic Impact of Cyber Accumulation Scenarios*.

Department of Energy United States of America. (2002). *21 Steps to Improve Cyber Security of SCADA Network.* Retrieved from https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Department of Homeland Security & Industrial Control Systems Cyber Emergency Response Team. (2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Retrieved from https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

European Union Agency for Network and Information Security (ENISA). (2017). *Communication network dependencies for ICS/SCADA Systems.* Retrieved from https://www.enisa.europa.eu/publications/ics-scada-dependencies

Federal Energy Regulatory Commission. (2016). *FERC Hydro Cyber/SCADA Security Checklist – Form 3*. Retrieved from https://www.ferc.gov/industries/hydropower/safety/guidelines/security/checklist.pdf

GE Oil & Gas. (2016). *Top 10 Cyber Vulnerabilities for Control Systems.* Retrieved from https://www.ge.com/digital/sites/default/files/Top-10-Cyber-Vulnerabilities-for-control-systems.pdf

German Federal Office for Information Security. (2013). Retrieved from ICS Security Compendium: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.pdf;jsessionid=A39EC848E2CFB1C6605E16482640182F.1_cid369?__blob=publicationFile&v=3

IMIA. (2016). *Cyber Risk - Engineering Insurers Perspective.* Retrieved from https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf

International Underwriting Association of London . (2018). *Cyber and Business Interruption.* Retrieved from https://www.iua.co.uk/IUA_Member/Document_Library/Circulars_2018/IUA_publishes_cyber_insurance_and_business_interruption_report.aspx

Lloyd's Market Association & International Underwriting Association. (2018). *Upstream Oil & Gas Cyber Risk: Insurance – Technical Review.* Retrieved from http://www.lmalloyds.com/LMA/publications/upstreamcyberreport.aspx

Lloyd's Market Association. (2017). *Cyber Security & Safety Consideration for Oil, Gas & Petrochemical Risk Assessment.* Retrieved from http://www.lmalloyds.com/LMA/News/LMA_bulletins/xLMA_bulletins/LMA17_033_PD.aspx

National Cyber Security Centre - Ministry of Security and Justice Netherlands. (2016). *Checklist security of ICS/SCADA systems.* Retrieved from https://www.ncsc.nl/english/current-topics/factsheets/checklist-security-of-ics-scada-systems.html

National Cyber Security Centre. (2015). *Security for ICS.* Retrieved from https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS%20-%20Executive%20Summary%20Final%20v1.0.pdf

NIST. (2015). Retrieved from Guide to Industrial Control Systems (ICS) Security: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Public Safety - Government of Canada. (2012). *Industrial Control System (ICS) Cyber Security: Recommended Best Practices*. Retrieved from Public Safety Canada: https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2012/tr12-002-en.aspx

Swiss Federal Office for National Economic Supply FONES. (2018). Retrieved from Minimum standard for improving ICT resilience: https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html

Swiss Federal Reporting and Analysis Centre for Information Assurance MELANI. (2013). *Measures for the protection of industrial control*

systems (ICSs). Retrieved from MELANI: https://www.melani.admin.ch/melani/en/home/dokumentation/checklists-and-instructions/measures-for-the-protection-of-industrial-control-systems--icss-.html

VdS Germany. (2018). *VdS Quick-Check for ICS* . Retrieved from VdS: https://www.vds-quick-check.de/en/vds-quick-check-for-ics-in-detail/

Water Information Sharing and Analysis Center. (2015). *10 Basic Cybersecurity Measures - Best Practices to Reduce Exploitable.* Retrieved from ICS US CERT: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Figure 1: ICS systems in Switzerland, connected to internet mid-April 2017(protocols, s7, modbus, fox, dnp3, bacnet) 5
Figure 2: Recommended network segregation 6