

# MAPPING INDICATORS OF RISK WITH ICS ATT&CK TTPs

Carolina Adaros

PhD Candidate, BCU, UK



Bosch PSIRT Analyst, Germany





# Carolina Adaros

Bosch PSIRT Product Security Incident Handler, since April 2019

PhD candidate in cybersecurity, since February 2017



## Studies

### Electronics Engineering

PUCV, Chile (Thesis in microcontrollers)

### MSc Analytics, Risk Analysis&OR

The University of Manchester, UK

### PhD Candidate

BCU, UK (Cyber-risks ICS/IloT)

## Work experience

### Chile

- Industrial Control & Automation
- Analytics /QA / Process improvement
- IT Consultancy
- Lecturer, Corporate Trainer

### UK

- Cybersecurity Risk Mngmt. Lecturer
- Cybersecurity tutor

### Germany

- Bosch Product Security handler



## Publications

- Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment (CRISiS, 2019)
- Understanding Cyberrisks in IoT: When Smart Things Turn Against You (BEP, 2019)
- Continuous Risk Management for Industrial IoT: A Methodological View (ISC, 2018)
- Collective responsibility and mutual coercion in IoT botnets A tragedy of the commons problem (BASS, 2018)

## Goals of the Bosch PSIRT

### Incident Response

Coordinating security incident response for all Bosch products.

### Vulnerability Management

Ensure effective management of security vulnerabilities in Bosch products.

### Security Community Work

Open to the global security community, to support research and encourage responsible disclosure of vulnerabilities.

MITRE CNA since 2019

[www.psirt.bosch.com](http://www.psirt.bosch.com)

# PhD research work:

## Continuous cyber-risk assessment for ICS & IIoT

### PhD project aim

**Define methodology to monitor cyber-risks during operation of Industrial Control Systems**

- Improve responsiveness to rapidly evolving threats
- Holistic approach (able to be adapted to a broad variety of contexts)

### Research questions

What information is needed in order to monitor security risks in ICS/IIoT?

How can that information be derived from what you can actually measure?

How can existing cyber-risk management frameworks be adapted for a more dynamic risk monitoring?

How can these modifications be introduced?

# PhD research work:

## Continuous cyber-risk assessment for ICS & IIoT

### PhD project aim

**Define methodology to monitor cyber-risks during operation of Industrial Control Systems**

- Improve responsiveness to rapidly evolving threats
- Holistic approach (able to be adapted to a broad variety of contexts)

### Research questions

**What information is needed in order to monitor security risks in ICS/IIoT?**

**How can that information be derived from what you can actually measure?**



**MITRE**  
**ATT&CK**

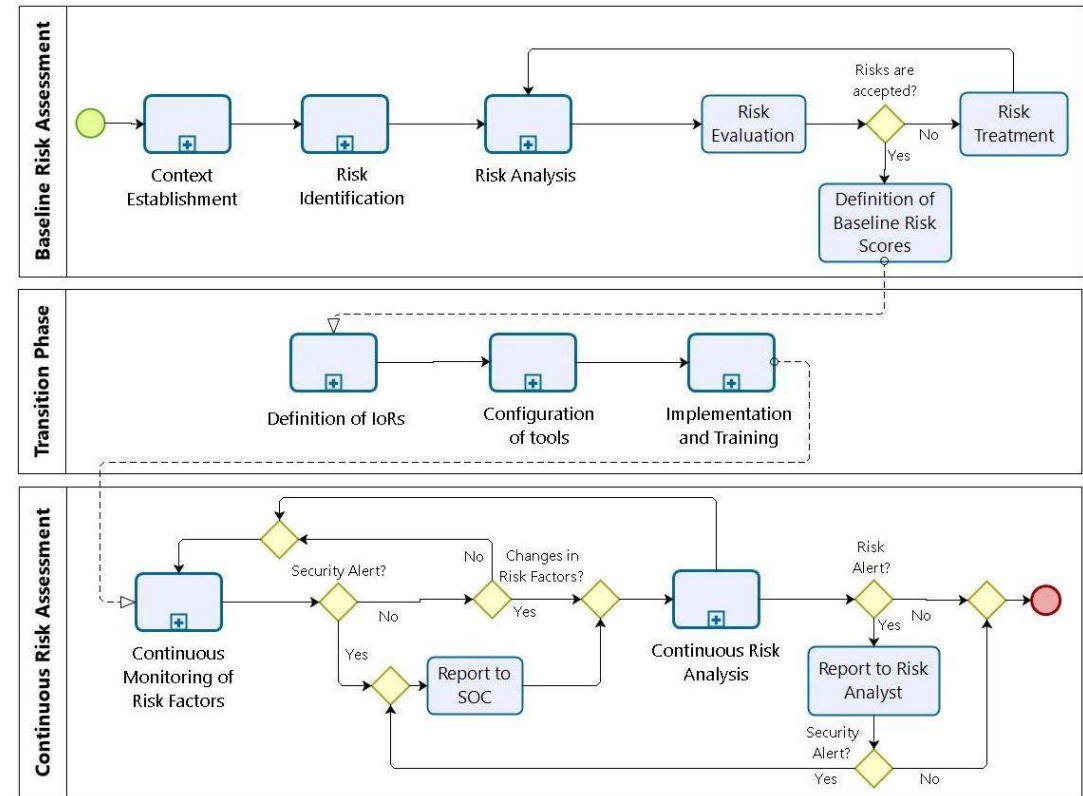
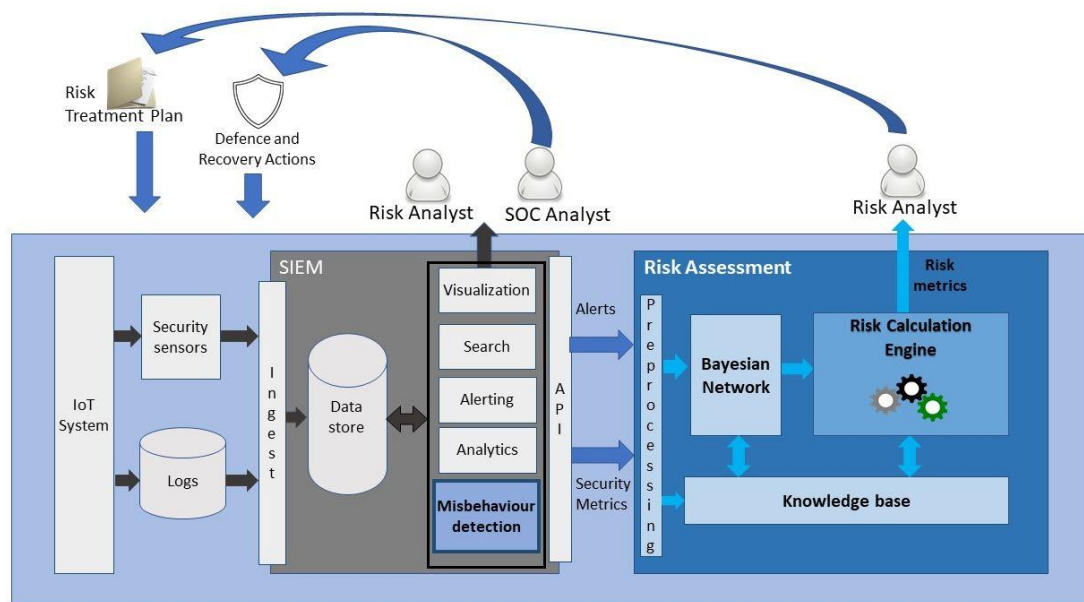
ICS adversary  
tactics,  
techniques &  
procedures

**How can existing cyber-risk management frameworks be adapted for a more dynamic risk monitoring?**

**How can these modifications be introduced?**

# PhD research work: Continuous cyber-risk assessment for ICS & IIoT

## *Architecture and Methodology for the Continuous Risk Assessment*



# PhD research work:

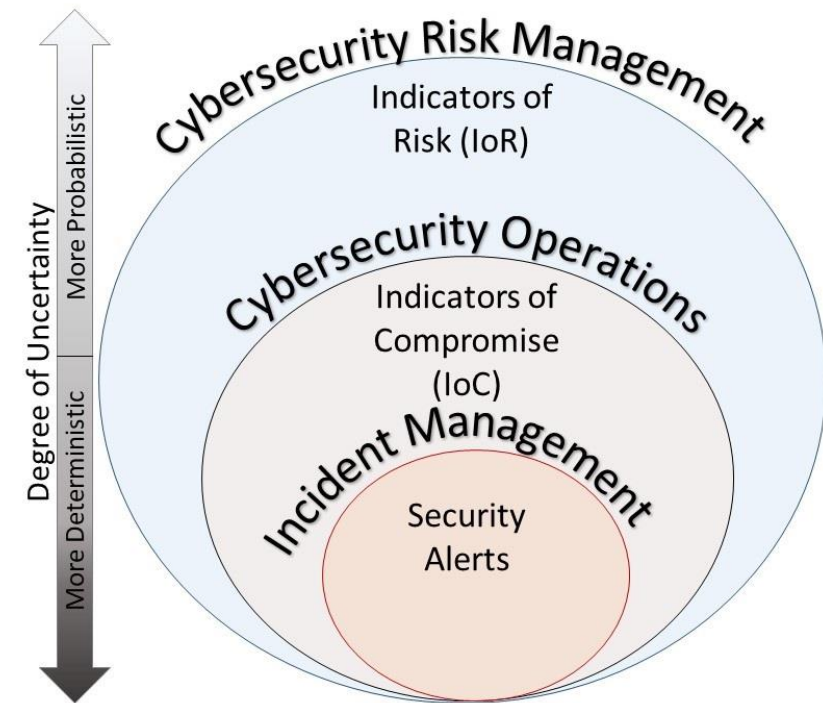
## Continuous cyber-risk assessment for ICS & IIoT

### *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

### What is an IoR?

An observation that can be associated with a higher probability of an unwanted event.

- ✓ IoRs are not deterministic
- ✓ A combination of IoRs provides more certainty and accuracy than a single IoR.





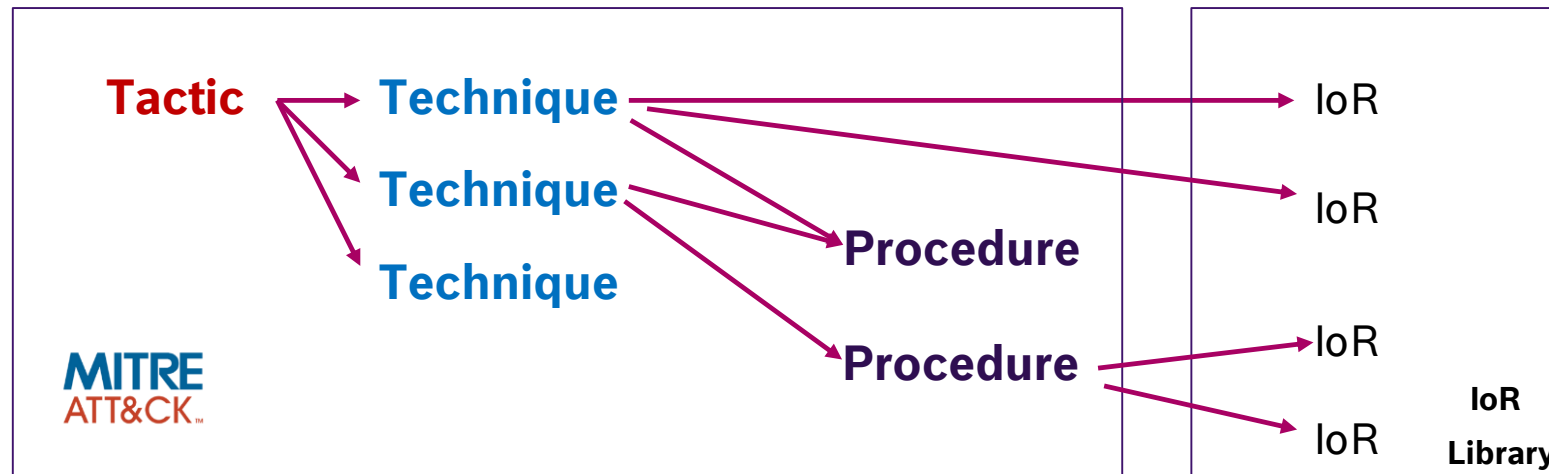
# PhD research work:

## Continuous cyber-risk assessment for ICS & IIoT

### *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

#### Research regarding IoRs:

- **Initial stage:** IoRs for an specific use case were derived
- **Current stage:** building a prototype IoR library based on ICS ATT&CK TTPs



# PhD research work: Continuous cyber-risk assessment for ICS & IIoT

## *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

### Probabilistic approach (conditional probabilities)

#### Forward inference:

$$\diamond P(\text{IoR} \mid \text{Technique})$$

#### Backward inference:

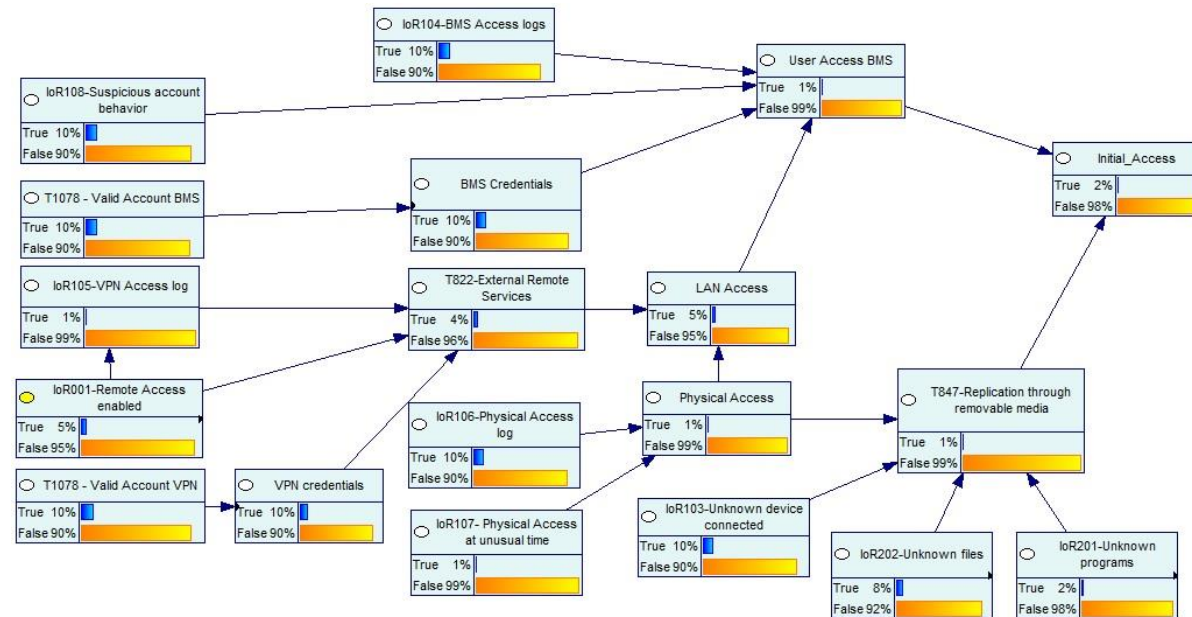
##### One IoR

$$\diamond P(\text{Technique} \mid \text{IoR})$$

##### Multiple IoRs

$$\diamond P(\text{Technique} \mid (\text{IoR}_1 \text{ AND } \text{IoR}_2 \text{ AND } \text{IoR}_3))$$

### Bayesian Network





# PhD research work:

## Continuous cyber-risk assessment for ICS & IIoT

### *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue

# PhD research work: Continuous cyber-risk assessment for ICS & IIoT

## *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

### Block Command Message

#### Description

Adversaries may block a command message from reaching its intended target to prevent command execution. In OT networks, command messages are sent to provide instructions to control system devices. A blocked command message can inhibit response functions from correcting a disruption or unsafe condition.<sup>[1]</sup>

In the 2015 attack on the Ukrainian power grid, malicious firmware was used to render communication devices inoperable and effectively prevent them from receiving remote command messages.<sup>[2]</sup>





#### Procedure Examples

- In *Industroyer* the first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the IEC 101 payload component is able to take over and maintain control of the RTU device.<sup>[3]</sup>

#### Mitigation

- Implement Virtual Local Area Networks (VLANs) to divide physical networks into smaller, logical ones with isolated traffic from each other. This limits both broadcast traffic and unnecessary flooding.<sup>[4]</sup>
- Secure the environment to minimize wires susceptible to interference and limit access points to cables. Keep the ICS and IT networks separate.<sup>[4]</sup>
- Monitor the network for expected outcomes and to detect unexpected states.<sup>[4]</sup>
- Implement antivirus and malware detection tools to protect against threats, such as code enabling improper network access.<sup>[4]</sup>

#### References

1. <sup>^</sup> <sup>↑</sup> Bonnie Zhu, Anthony Joseph, Shankar Sastry. (2011). A Taxonomy of Cyber Attacks on SCADA Systems. Retrieved January 12, 2018. 
2. <sup>^</sup> <sup>↑</sup> Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. (2016, March 18). Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case. Retrieved March 27, 2018. 
3. <sup>^</sup> <sup>↑</sup> Anton Cherepanov; ESET. (2017, June 12). Win32/Industroyer: A new threat for industrial control systems. Retrieved September 15, 2017. 
4. <sup>a</sup> <sup>b</sup> <sup>c</sup> <sup>d</sup> <sup>↑</sup> Keith Stouffer. (2015, May). Guide to Industrial Control Systems (ICS) Security. Retrieved March 28, 2018. 

IoR403-Commands and responses do not match

IoR405-Unresponded commands

IoR107-Unknown programs

IoR109-Unknown files

#### Block Command Message

Technique	
ID	T803
Tactic	Inhibit Response Function
Data Sources	Alarm History, Network protocol analysis, Packet capture
Asset	Field Controller/RTU/PLC/IED

IoR002-Unnecessary open ports

IoR207-Malicious signature detected

# PhD research work:

## Continuous cyber-risk assessment for ICS & IIoT

### *Use of ICS ATT&CK to map Indicators of Risk (IoRs)*

### Future prospects

#### Challenges:

- Granularity of IoRs and trade-off between general (broad scope) and specific (easier to apply directly).
- Assignment of probabilities for each IoR-Technique pair
- Define logical relationships between IoRs for each technique

#### Highlight:

- ICS ATT&CK Impact techniques can be mapped with IoRs based on Physical based anomaly detection

# Use of ICS ATT&CK framework within the Bosch PSIRT

## *Use of ICS ATT&CK to learn from known TTPs*

Experience and expertise on ICS and IoT cybersecurity < Enterprise.

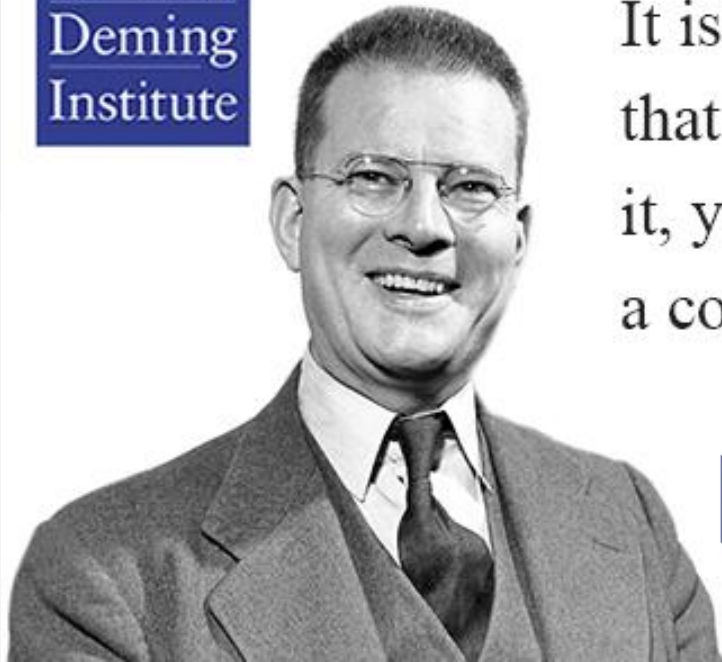
Hence reviewing attack cases and PoCs contributes enhancing our knowledge base.



- Review of ICS ATT&CK techniques and procedures to get more insight of attack mechanisms and regular discussion and sharing meetings.
- Group of colleagues is participating in a working group for Automotive TTPs based in the model of the ATT&CK framework.

# FINAL REMARKS

- ✓ MITRE ATT&CK is a useful source of knowledge for both Academic Research & Industries
- ✓ ATT&CK is allowing me to start identify IoCs/IoRs in a more systematic and structured way.
- ✓ Start **thinking about Cyber-Risks!** In ICS many targeted attacks have **low probability** but **critical impact** -> ICS ATT&CK provides useful insight for risk assessment.
- ✓ MITRE ATT&CK it already been used to identify IoCs, identifying IoRs can be a useful extension of these type of work/ models.



It is wrong to suppose  
that if you can't measure  
it, you can't manage it –  
a costly myth.

**W. Edwards Deming**

source: [quotes.deming.org/10147](https://quotes.deming.org/10147)

[www.psirt.bosch.com](http://www.psirt.bosch.com)

[carolina.adaros@bosch.com](mailto:carolina.adaros@bosch.com)

[carolina.adarosboye@mail.bcu.ac.uk](mailto:carolina.adarosboye@mail.bcu.ac.uk)

<https://www.linkedin.com/in/carolina-andrea-adaros-boye-b916185/>

