BUILDING AN INDICATORS OF RISK LIBRARY BASED ON ICS ATT&CK

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

BOSCH PSIRT
Product Security Incident Response Team

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

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/ IIoT)

Professional experience

Chile
- *Industrial Control & Automation*
- *Analytics /QA / Process improvement*
- *IT Consultancy*
- *Lecturer, CorporateTrainer*

UK
- *Cybersecurity Risk Mngmt. Lecturer*
- *Cybersecurity tutor*
- *PhD Researcher*

BIRMINGHAM CITY University

Germany
- *Bosch Product Security handler*

Publications

- An Indicators-of-Risk Library for Industrial Network Security (Accepted in SECRS, 2021)
- 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)

BOSCH

Building an Indicators of Risk Library based on ICS ATT&CK
About this Presentation

This presentation shows a part of the work done in my Thesis titled:

“A Continuous Risk Assessment Methodology for ICS”

recently submitted for Doctorate Degree in Birmingham City University.

Research outputs presented on this thesis were:

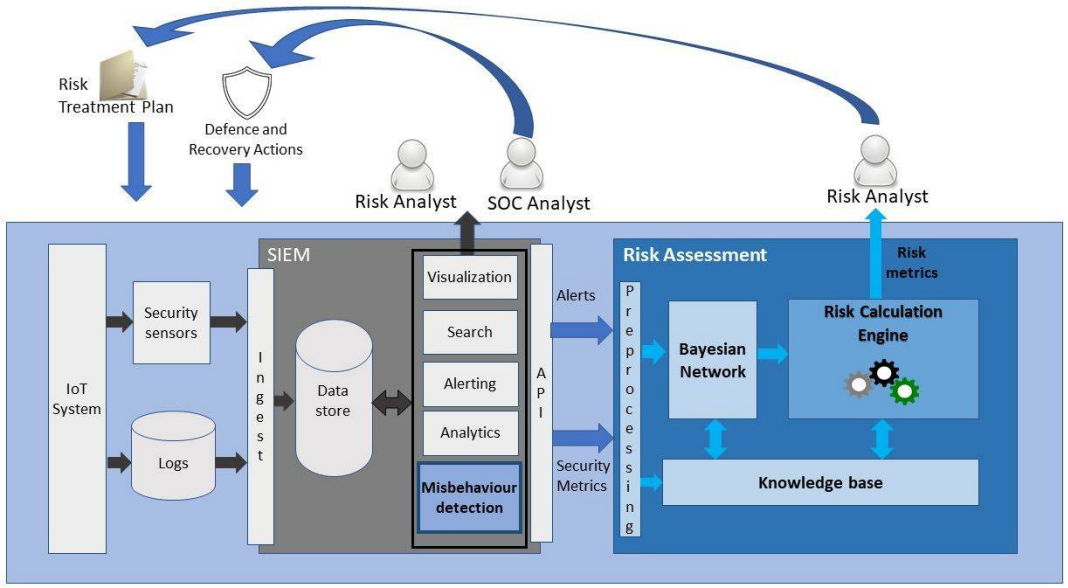
- Continuous Risk Assessment Methodology for ICS
- **The concept of “Indicator of Risk” (IoR) as part of this methodology**
- **The “IoR Library” based in ICS ATT&CK**
- **A Bayesian Network template based on the IoR Library**
- Some demonstrations of sensors base anomaly detection

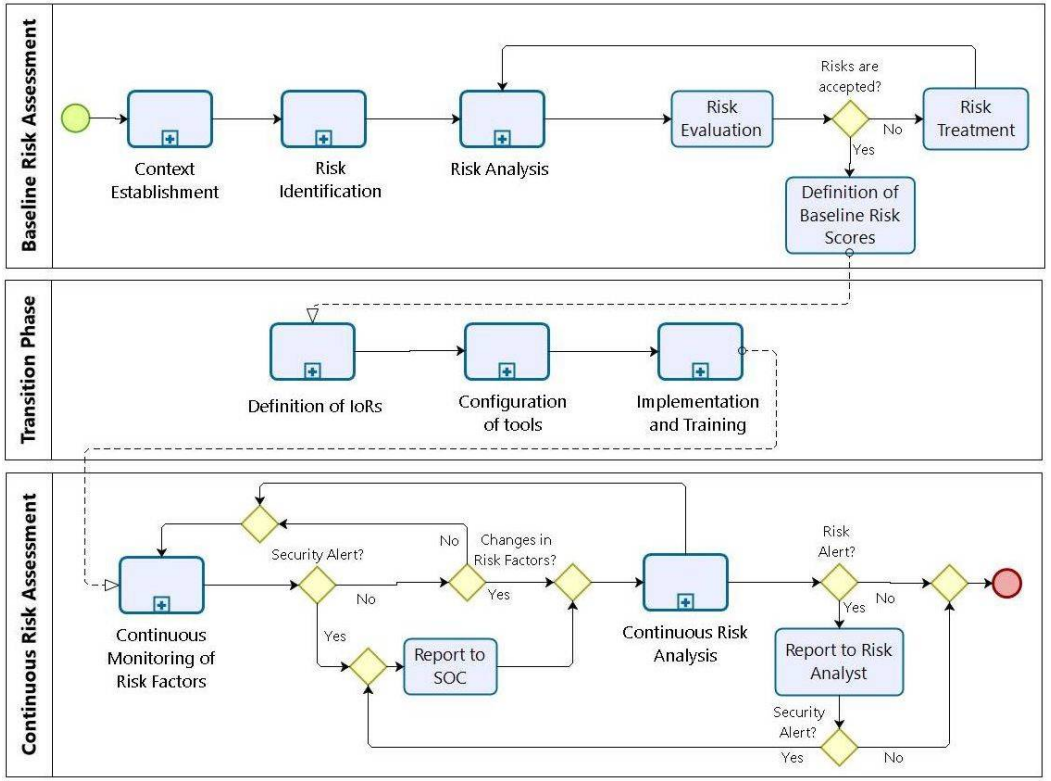
BIRMINGHAM CITY University

BOSCH

Building an Indicators of Risk Library based on ICS ATT&CK

Architecture and Methodology for the Continuous Risk Assessment





Papers:

- Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment (CRISiS, 2019)
- Continuous Risk Management for Industrial IoT: A Methodological View (ISC, 2018)

BIRMINGHAM CITY University

BOSCH

Building an Indicators of Risk Library based on ICS ATT&CK

About 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.

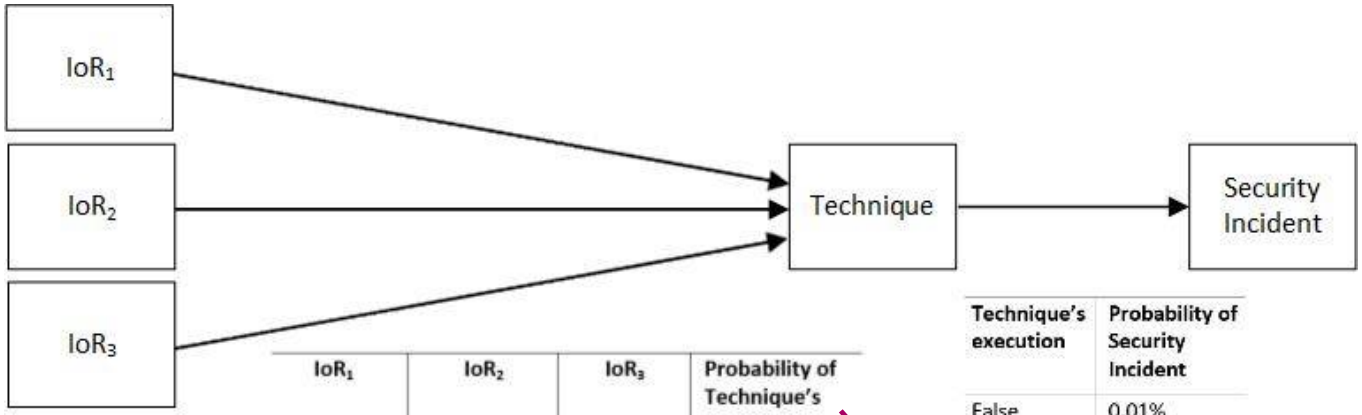
IoRs = Indication of RISK EXPOSURE ≠ Threat detection

Hence, there is a challenge on measuring effectiveness of IoRs

→ The concept of “false positive” is not always applicable

Building an Indicators of Risk Library based on ICS ATT&CK

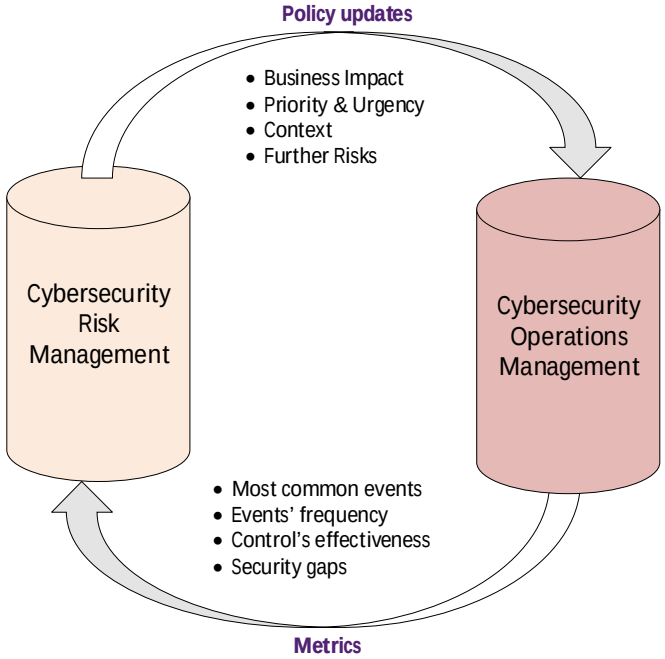
About IoRs



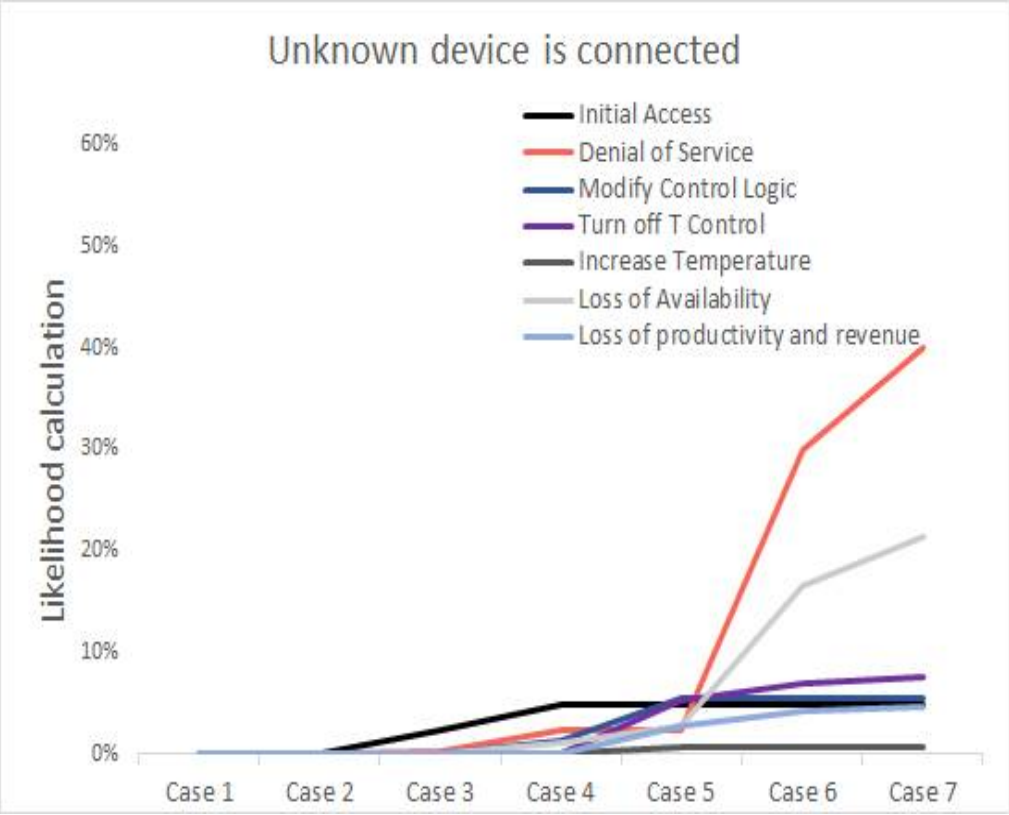
IoR_1	IoR_2	IoR_3	Probability of Technique's Execution
False	False	False	0.1%
False	False	True	5%
False	True	False	10%
False	True	True	20%
True	False	False	5%
True	False	True	15%
True	True	False	15%
True	True	True	50%

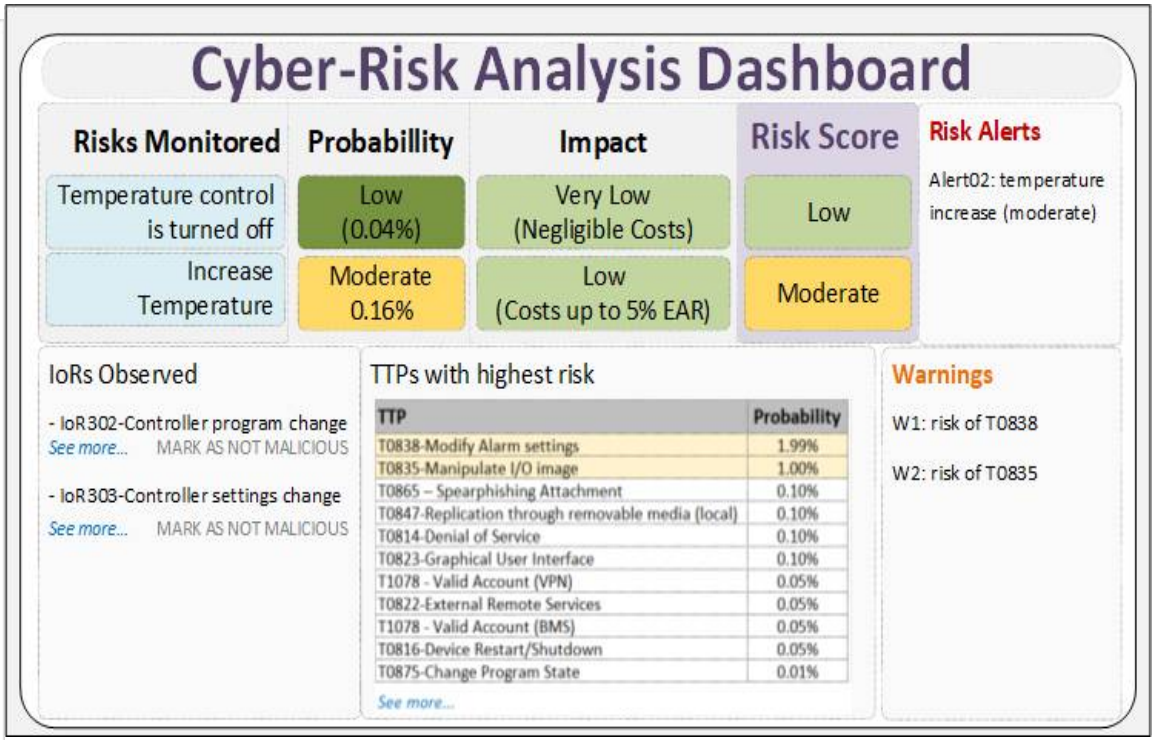
Technique's execution	Probability of Security Incident
False	0.01%
True	25%

The higher P% the closest to threat detection



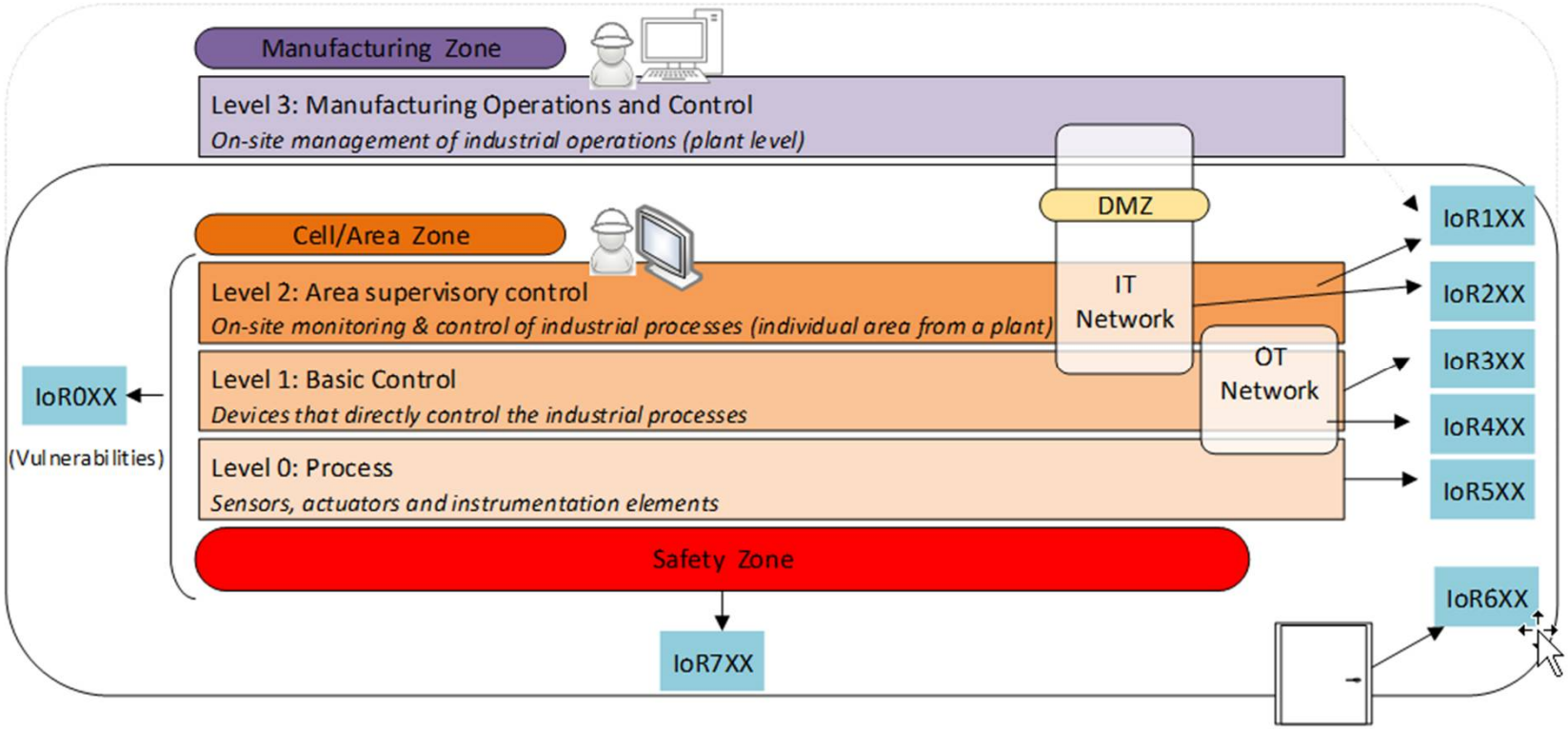
Building an Indicators of Risk Library based on ICS ATT&CK
IoRs and Continuous Risk Assessment





Building an Indicators of Risk Library based on ICS ATT&CK

The IoR Library – Scope & Naming Scheme



IoRs are used to observe conditions in all the levels of the system (based on Purdue Model)

BIRMINGHAM CITY University

BOSCH

Building an Indicators of Risk Library based on ICS ATT&CK

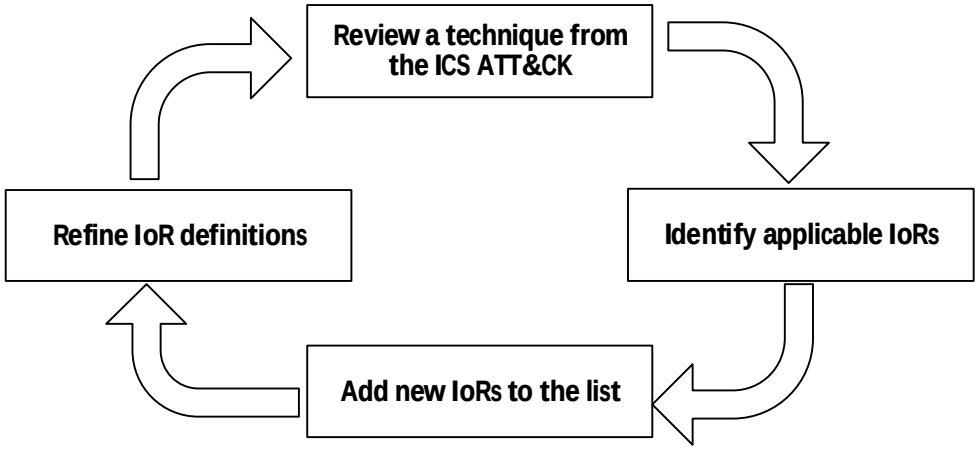
The IoR Library - Introduction

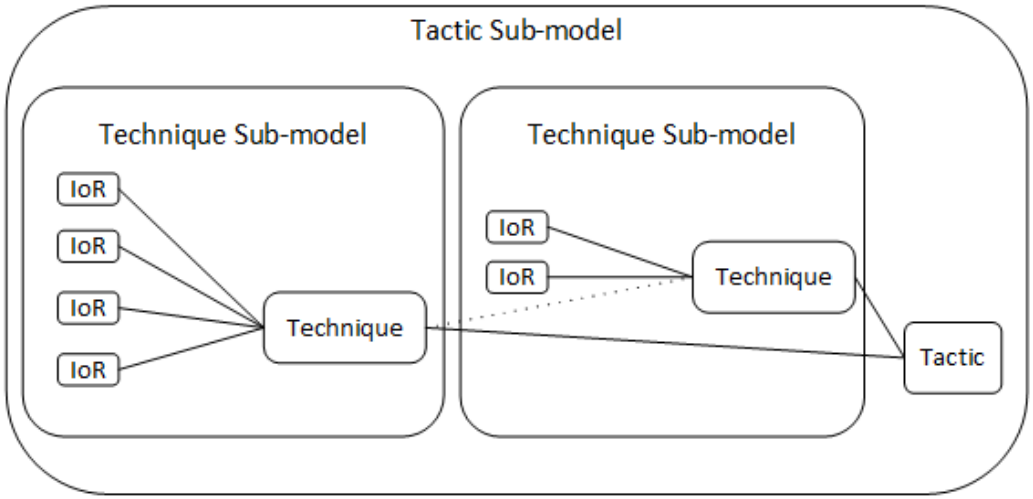
Problem 1: identify possible IoRs , **Problem 2:** relate IoRs with concrete risks

Solution (1 and 2): MITRE ICS ATT&CK + IoR Library

IoRs in the IoR Library are defined by:

- Rationale
- Observations
- Examples



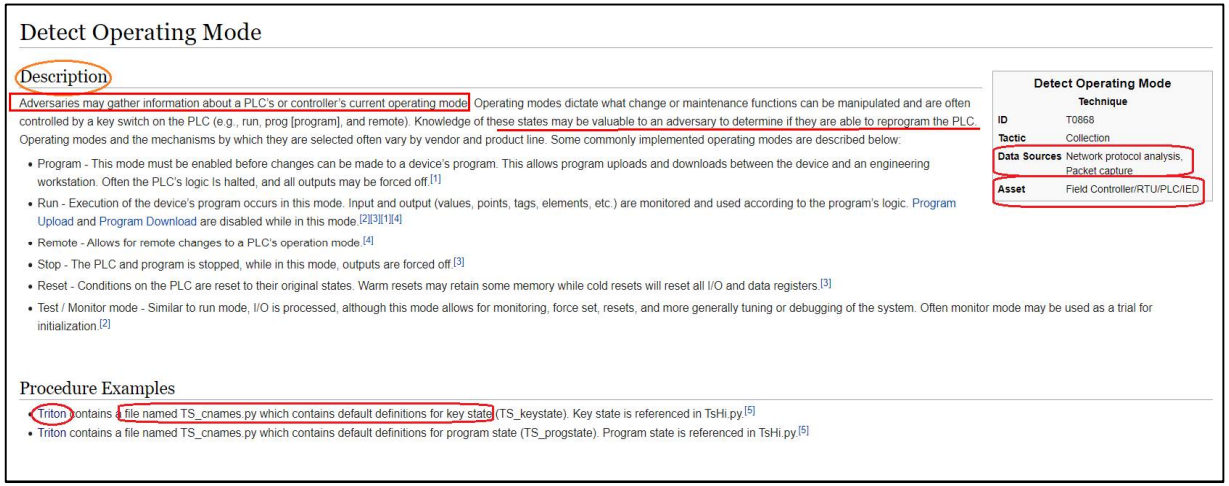


The latest version of the IoR Library has 95 IoRs related to 40 Techniques

Building an Indicators of Risk Library based on ICS ATT&CK

The IoR Library – Example of a Technique entry

T0868-Detect Operating Mode



Detect Operating Mode

Description

Adversaries may gather information about a PLC's or controller's current operating mode. Operating modes dictate what change or maintenance functions can be manipulated and are often controlled by a key switch on the PLC (e.g., run, prog [program], and remote). Knowledge of these states may be valuable to an adversary to determine if they are able to reprogram the PLC. Operating modes and the mechanisms by which they are selected often vary by vendor and product line. Some commonly implemented operating modes are described below:

- Program - This mode must be enabled before changes can be made to a device's program. This allows program uploads and downloads between the device and an engineering workstation. Often the PLC's logic is halted, and all outputs may be forced off.[1]
- Run - Execution of the device's program occurs in this mode. Input and output (values, points, tags, elements, etc.) are monitored and used according to the program's logic. Program Upload and Program Download are disabled while in this mode.[2][3][1][4]
- Remote - Allows for remote changes to a PLC's operation mode.[4]
- Stop - The PLC and program is stopped, while in this mode, outputs are forced off.[3]
- Reset - Conditions on the PLC are reset to their original states. Warm resets may retain some memory while cold resets will reset all I/O and data registers.[3]
- Test / Monitor mode - Similar to run mode, I/O is processed, although this mode allows for monitoring, force set, resets, and more generally tuning or debugging of the system. Often monitor mode may be used as a trial for initialization.[2]

Detect Operating Mode
Technique

ID	T0868
Tactic	Collection
Data Sources	Network protocol analysis, Packet capture
Asset	Field Controller/RTU/PLC/IED

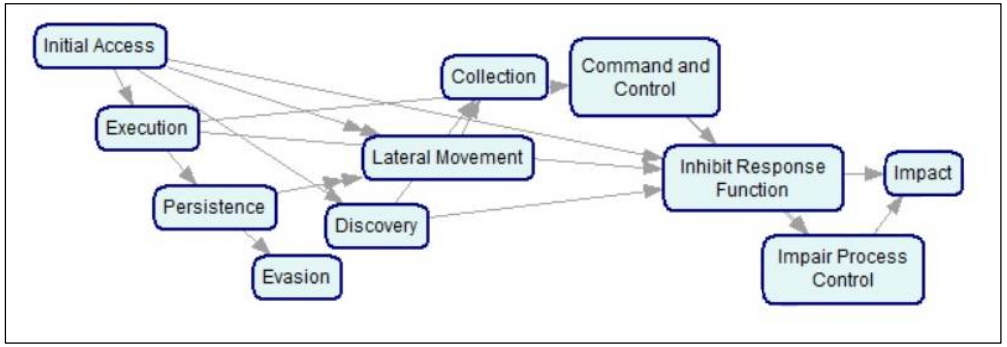
Procedure Examples

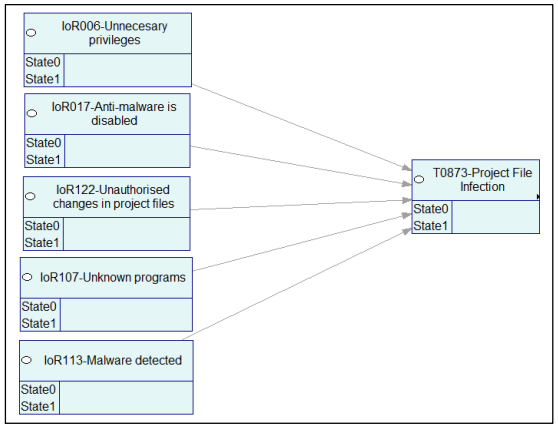
- Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.[5]
- Triton contains a file named TS_cnames.py which contains default definitions for program state (TS_progstate). Program state is referenced in TsHi.py.[5]

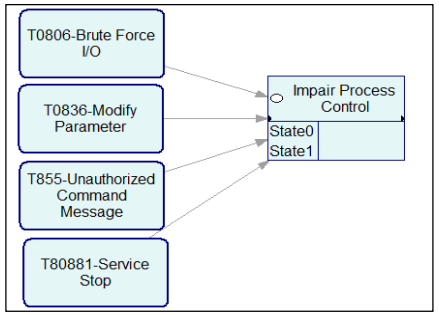
IoR	Explanation	Degree of Influence
IoR017-Anti-malware is disabled	Operating mode might be detected by known malware (e.g. Triton)	1
IoR018- Firewall is disabled	A firewall can allow filtering traffic stopping malicious traffic	1
IoR107-Unknown programs	Operating mode might be detected by an unauthorised software or unknown malware	1
IoR109-Unknown files	Files might contain tables with definitions for states and operating modes (e.g. Triton) or be used to collect the data	1
IoR113-Malware detected	Operating mode might be detected by known malware (e.g. Triton)	1
IoR117-Suspicious OPC commands	For example, commands to query on the operating mode	1
IoR206-Unusual or unexpected commands in network packets	Commands to query on operating mode	1
IoR311- Abnormal Process Variable Data Is Transmitted to the PLC	Commands to query on operating mode	1
IoR406-Unexpected command sequence over network	Commands to query on operating mode	1
IoR411-Use of unusual communication protocol	Commands to query on operating mode can be part of a malware procedure and use a communication protocol that is unusual in a particular environment	1
IoR412-Communication through unused ports	Commands to query on operating mode can be part of a malware procedure and use ports that are unused in a particular environment	1
IoR414-Abnormal OT communication	Commands to query on operating mode can result on observable abnormal OT communication patterns, such as increase on frequency of connections or malformed traffic, among others	1

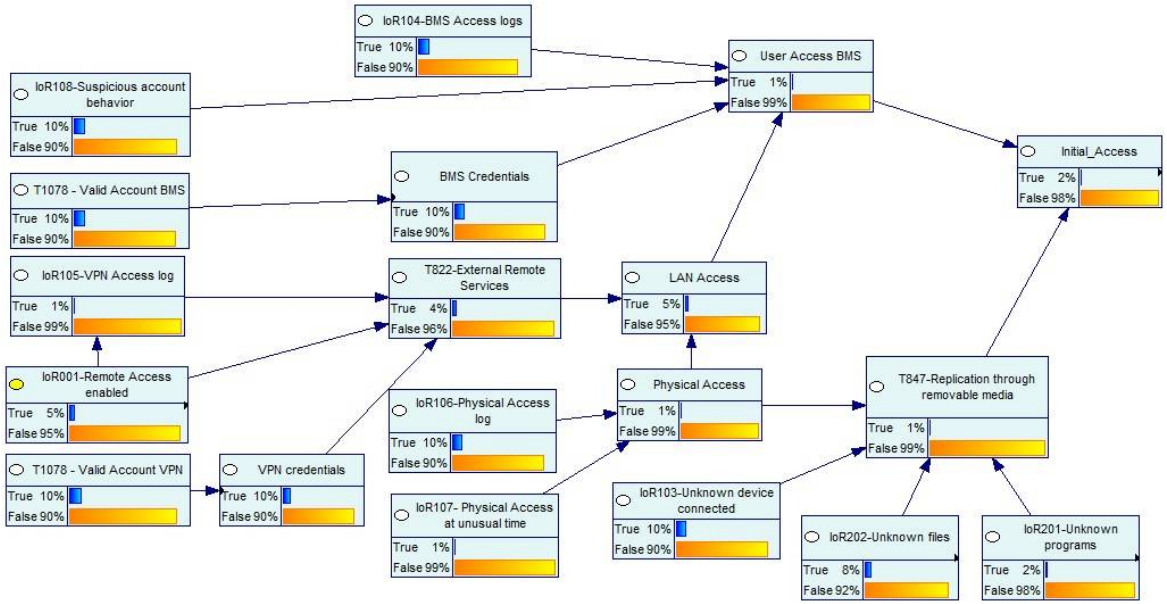
Building an Indicators of Risk Library based on ICS ATT&CK

Example of BN based on the IoR Library









BIRMINGHAM CITY University

BOSCH

Building an Indicators of Risk Library based on ICS ATT&CK
More datails?

More details about the IoR Library and its conceptual model:

- International Workshop on Secure and resilient smart manufacturing environments (SecRS) to be held in conjunction with the ARES (August 2021).
- Paper titled “An Indicators-of-Risk Library for Industrial Network Security” to be published in the procedures of ARES (August 2021).
- Send an e-mail: carolina.adarosboye@mail.bcu.ac.uk

Building an Indicators of Risk Library based on ICS ATT&CK
Conclusions

1. MITRE ATT&CK was essential for building the IoR Library so it was:
    - ✓ Built on a systematic and structured way
    - ✓ Relatable to a known framework

2. The concept of IoR brings together the worlds of Risk Management and Security Operations.

3. ICS targeted attacks can have low probability but critical impact (physical damage, HSE issues) for which a continuous risks monitoring approach is important.

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

W. Edwards Deming

"We use probability because we lack perfect information, not in spite of it"

Douglas W. Hubbard

"How to measure anything in Cybersecurity Risk"

carolina.adaros@bosch.com
carolina.adarosboye@mail.bcu.ac.uk
https://www.linkedin.com/in/carolina-andrea-adaros-boye-b916185/

BIRMINGHAM CITY University

BOSCH