

DESIGNING AND INTEGRATING IEC 62443 COMPLIANT THREAT ANALYSIS

@ 26th European System, Software & Service Process Improvement & Innovation Conference (EuroSPI 2019)

🐦 @mfockel

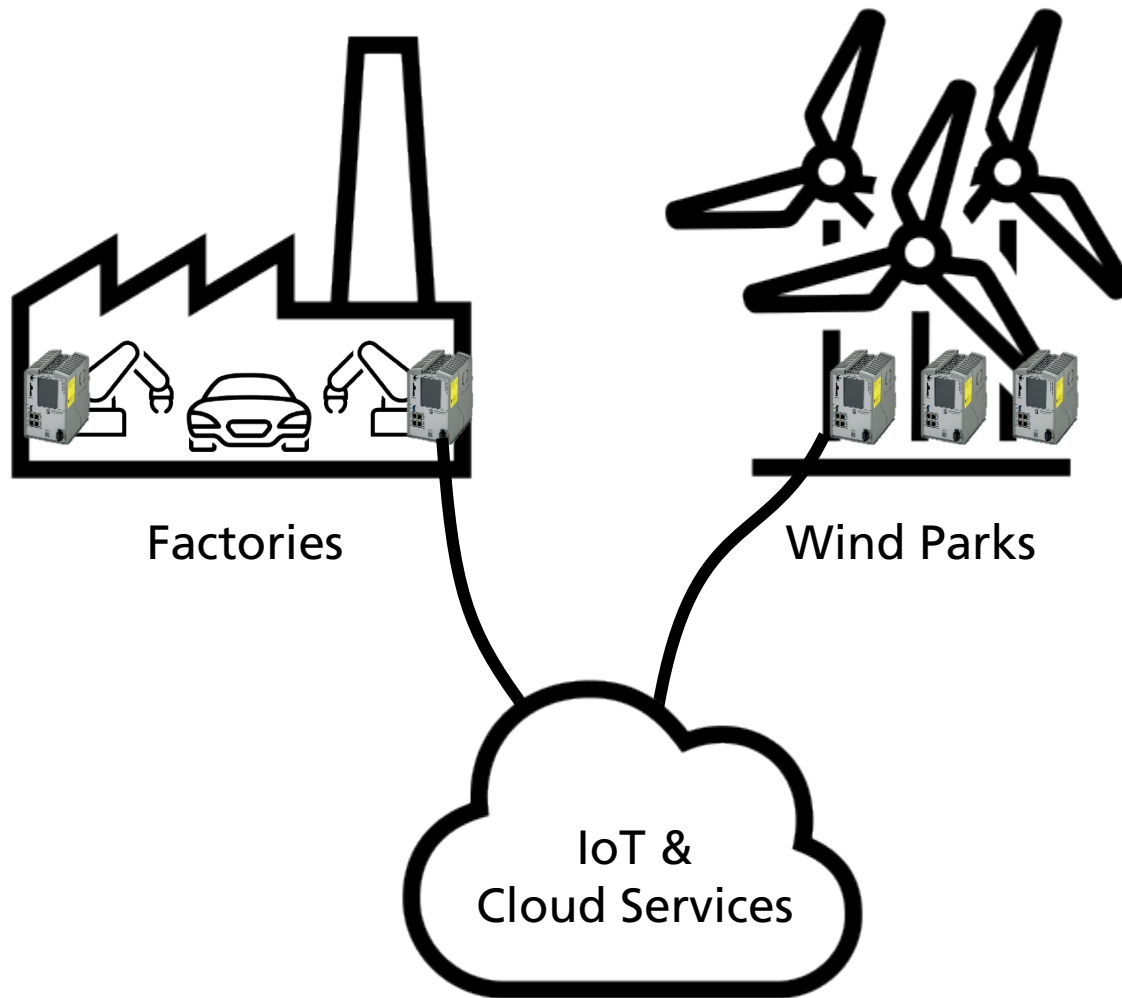
Markus Fockel, Sven Merschjohann, Masud Fazal-Baqaie,
Torsten Förder, Stefan Hausmann, Boris Waldeck

19. September 2019



Industrial Automation

Programmable Logic Controller (PLC)



- PLC:
- Industrial computer
 - Industry standard interfaces and software platform

Industrial Automation Security

MQTT Protocol: IoT communication of reactors and prisons publicly visible

17.02.2017 09:44 clock - Uli Ries

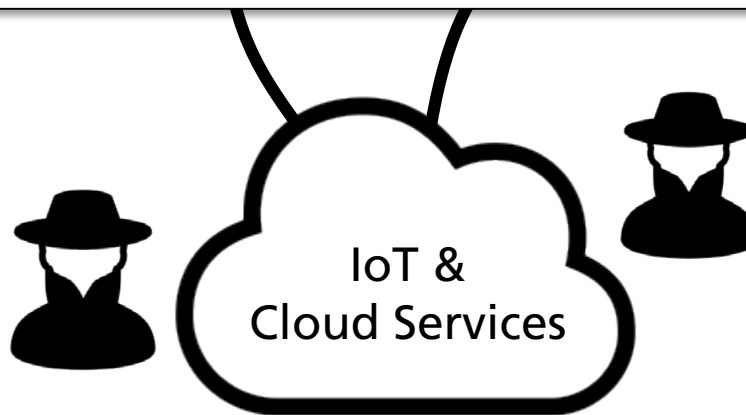


Hackers use Triton malware to shut down plant, industrial systems

The malware has been designed to target industrial systems and critical infrastructure.



By Charlie Osborne for Zero Day | December 15, 2017 -- 09:54 GMT (09:54 GMT) | Topic: Security



Industrial Automation Security

MQTT Protocol: IoT communication of reactors and prisons publicly visible

17.02.2017 09:44 clock - Uli Ries

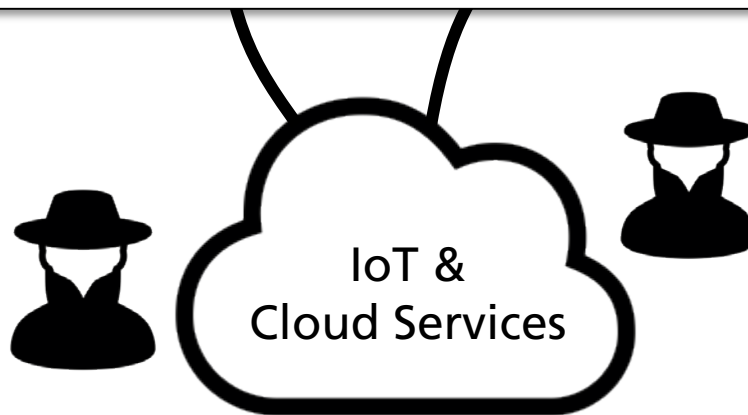


Hackers use Triton malware to shut down plant, industrial systems

The malware has been designed to target industrial systems and critical infrastructure.



By Charlie Osborne for Zero Day | December 15, 2017 -- 09:54 GMT (09:54 GMT) | Topic: Security



IEC 62443
Security for
Industrial Automation
and Control Systems

IEC 62443 –

Security for Industrial Automation and Control Systems

Set of standard documents that considers product and process security

General

Policies & Procedures

System

IEC 62443-3-x: System Security Requirements,
Risk Assessment, ...



Component

IEC 62443-4-x: Component Security Requirements,
Secure Development Lifecycle Requirements



IEC 62443-4-1

Requirements on Threat Analysis

- „is required to ensure that security threats for the product are identified, validated, documented, addressed and tested“
- “all products shall have a **threat model** with the following characteristics:
 - **Processes, data stores**, interacting **external entities**;
 - **Flow of** categorized **information** throughout the system;
 - **Trust boundaries**;
 - Internal and external **communication protocols** implemented in the product;
 - Potential attack vectors [...];
 - Potential **threats** and their **severity** [...];
 - **Mitigations** and/or dispositions for each threat;
 - [...]”

Motivation for Threat Analysis

“Is Your Product Secure?”



“Well, ...”



The real questions:

- Secure under what conditions (in what **context**)?
- Securing what (**assets**) against what (**threats**)?
- What are the product's **security objectives**?
- What security requirements does it fulfill? (taken **countermeasures**)
- What is the residual **risk**? (no 100% security)



Answer:
Systematic
Threat Analysis
Method

Motivation for Threat Analysis

“Is Your Product Secure?”



“Well, ...”



 **PHOENIX
CONTACT**



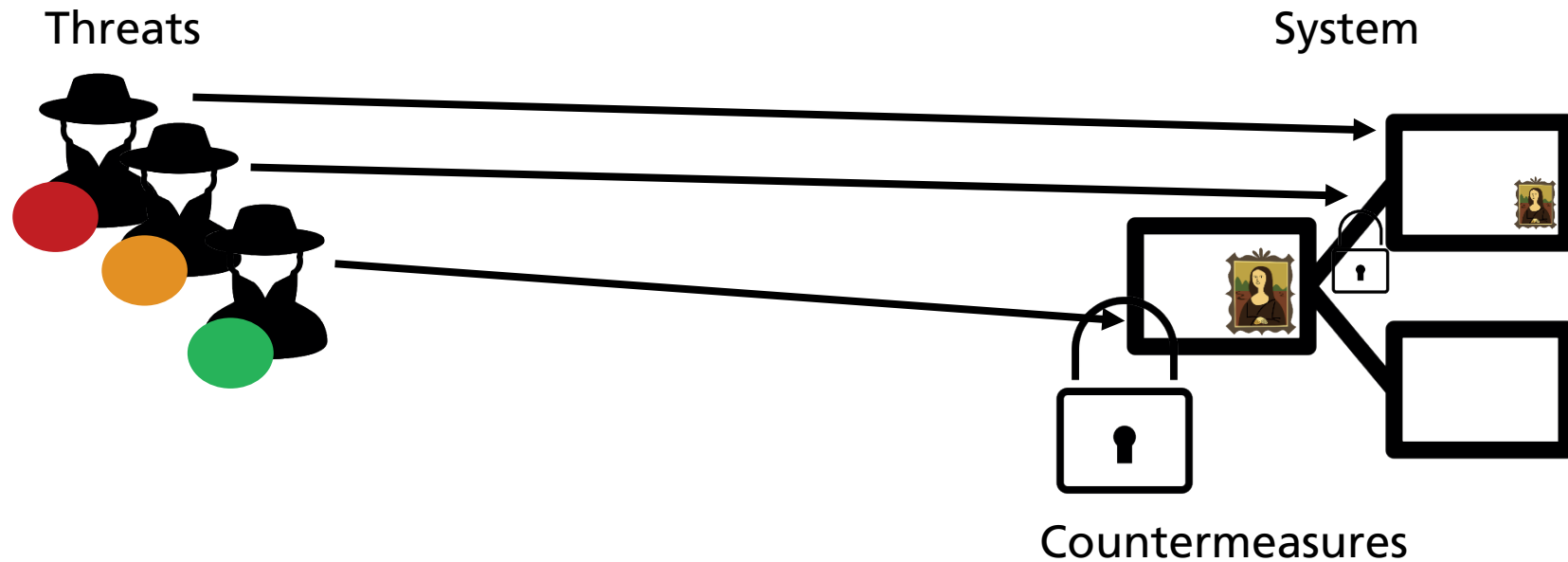
The real questions:






- Secure under what conditions (in what **context**)?
- Securing what (**assets**) against what (**threats**)?
- What are the product's **security objectives**?
- What security requirements does it fulfill?
(taken **countermeasures**)
- What is the residual **risk**? (no 100% security)

 **Fraunhofer**
IEM

Answer:
Systematic
Threat Analysis
Method

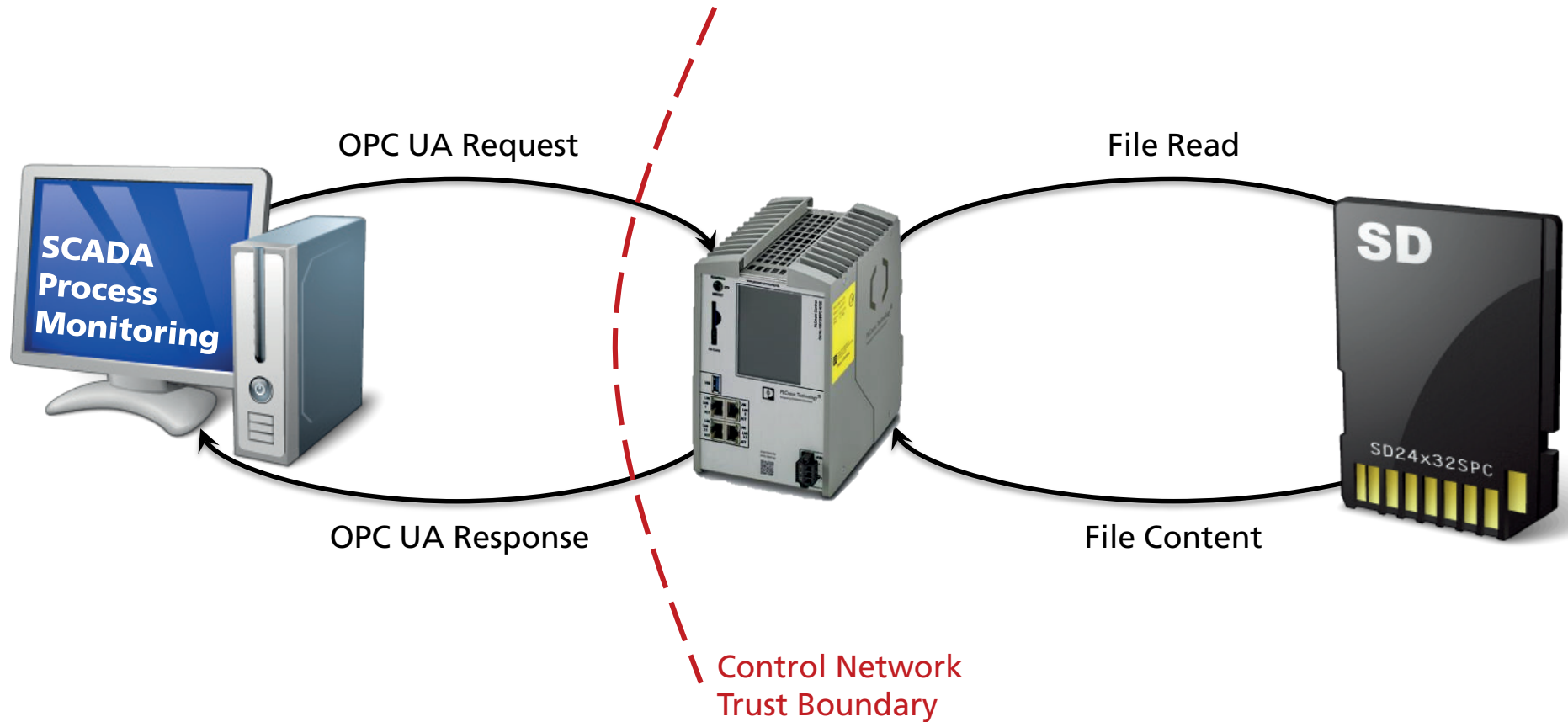
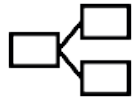
Threat Analysis Compliant with IEC 62443-4-1



1.  Specify System and its Security Context
2.  Determine Assets and Security Objectives
3.  Identify and Localize Threats
4.  Determine Countermeasures
5.  Assess Risk of Threats

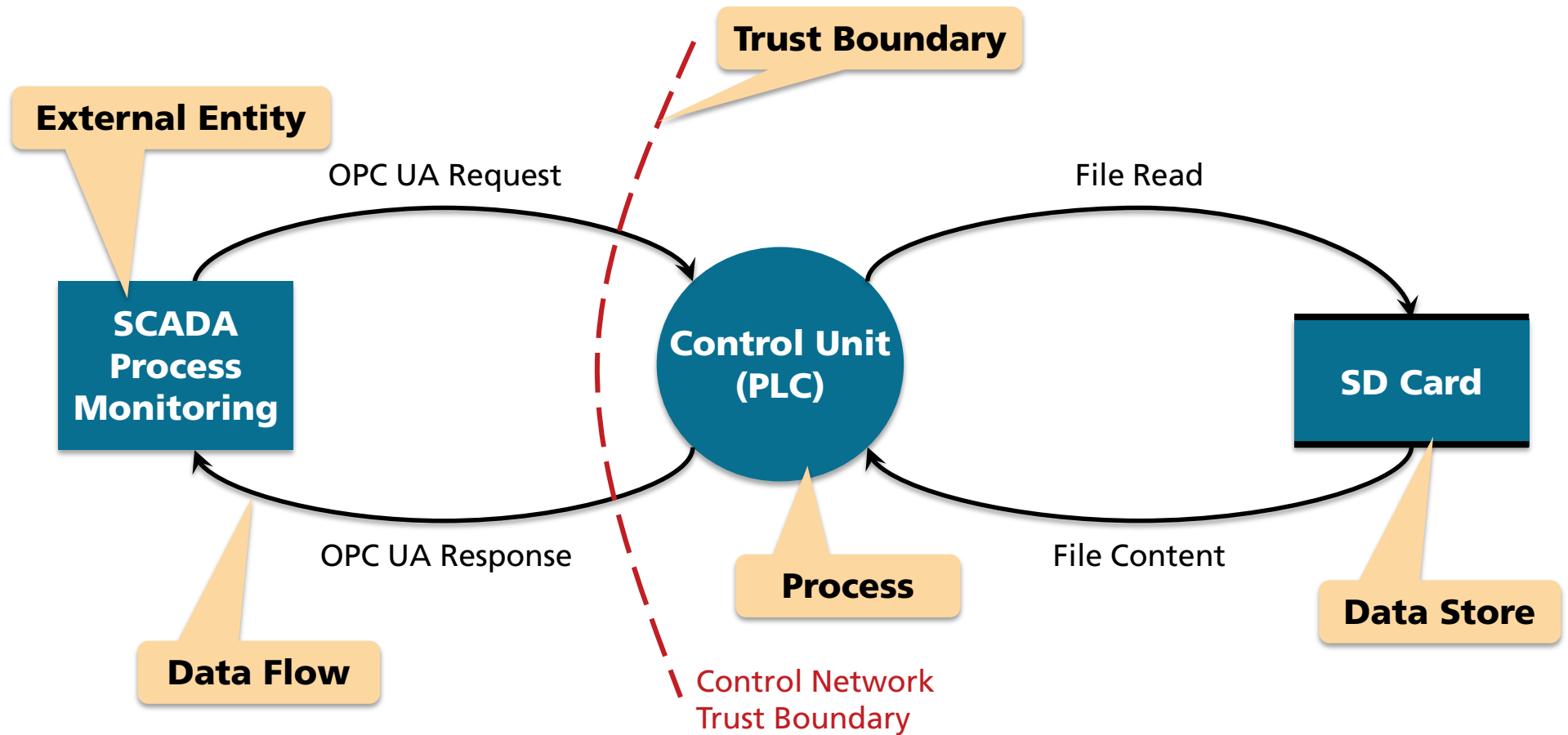
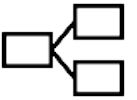
1. Specify System and its Security Context

Data Flow Diagram

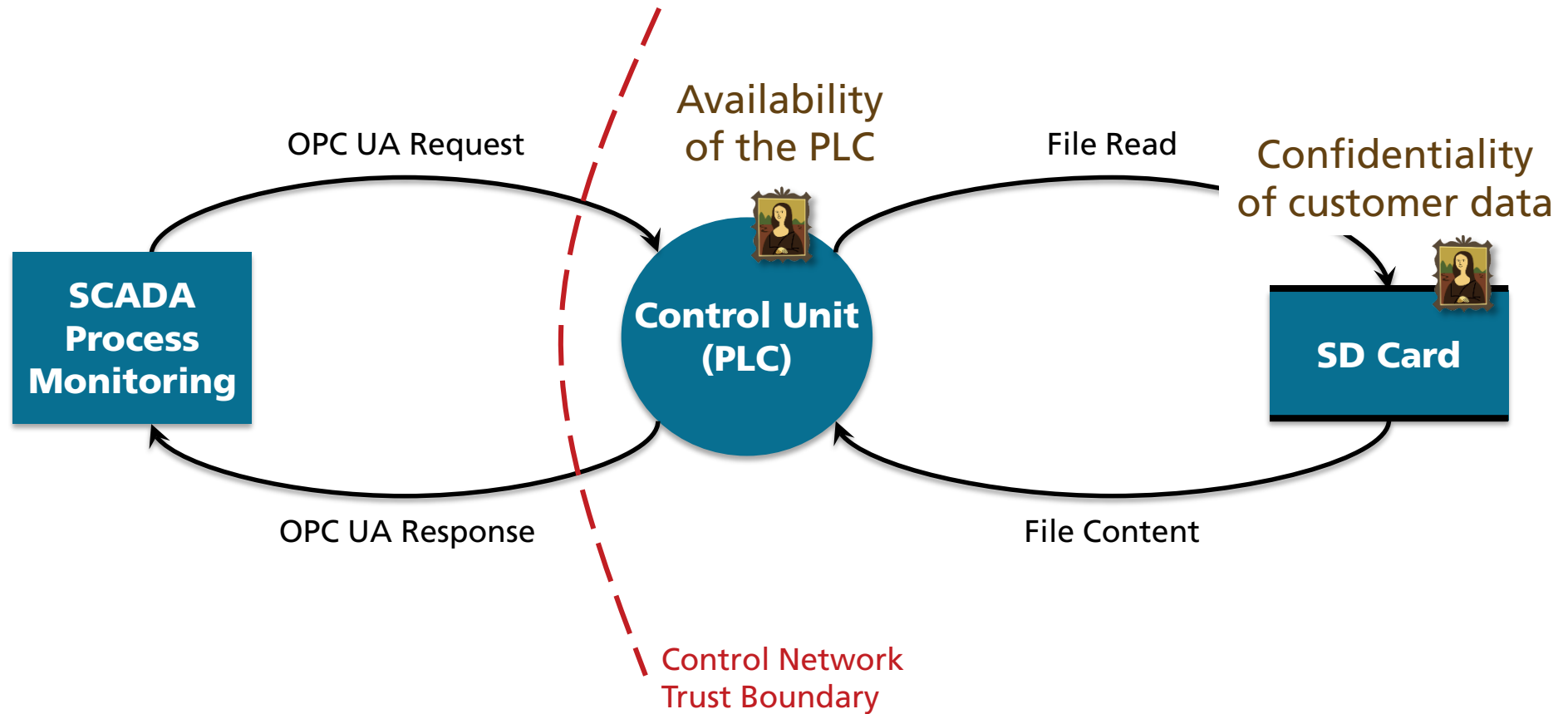


1. Specify System and its Security Context

Data Flow Diagram

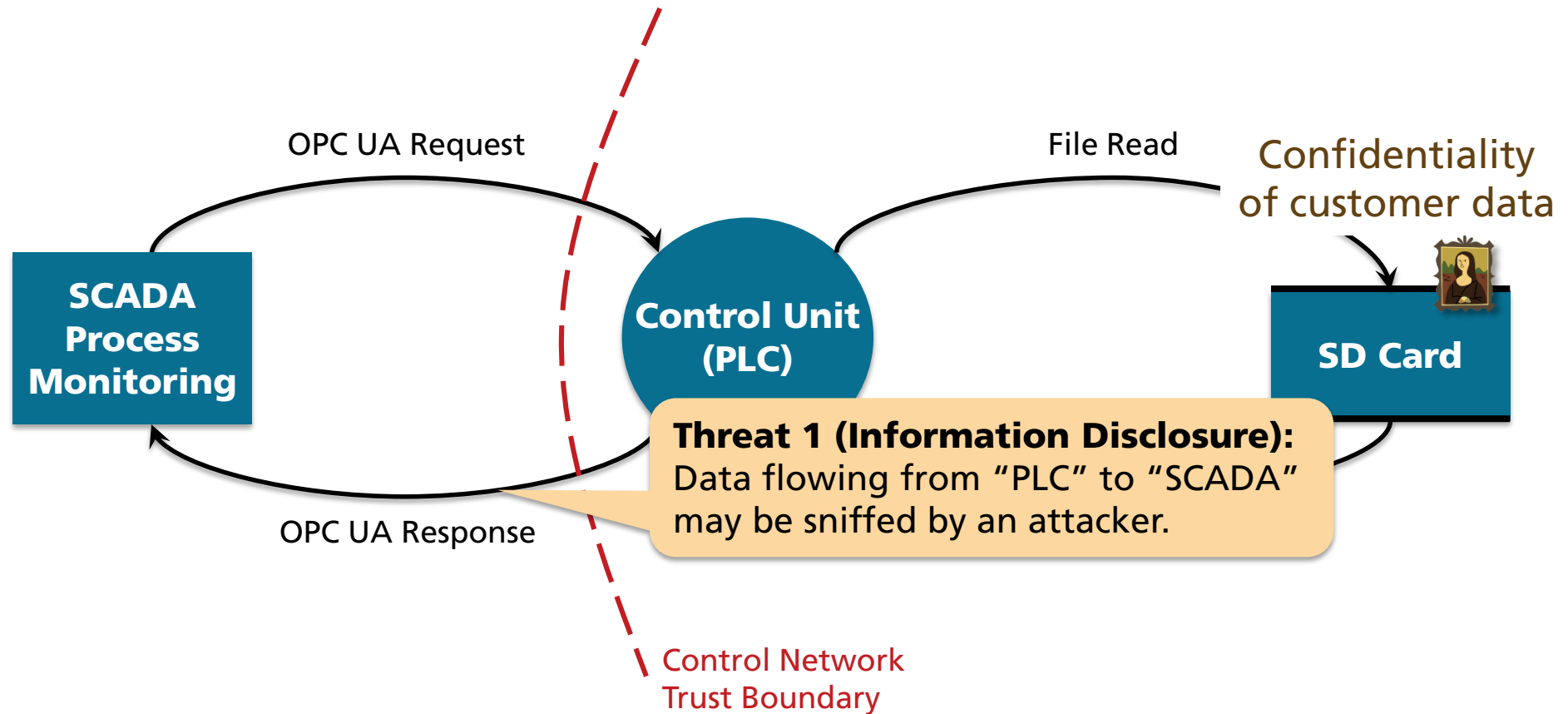


2. Determine Assets and Security Objectives



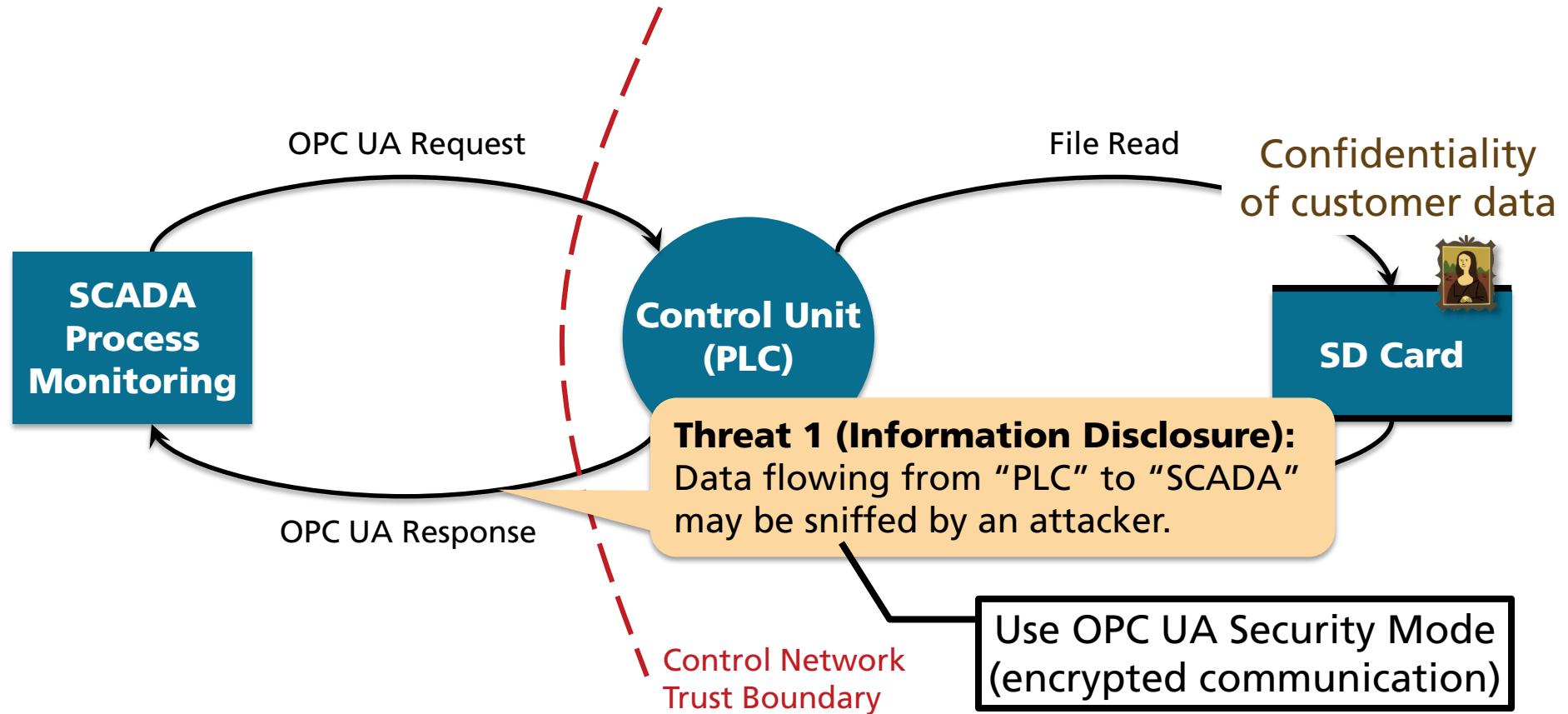
3. Identify and Localize Threats

STRIDE Approach - Example Threat for OPC UA Communication



4. Determine Countermeasures

Example Countermeasure for Information Disclosure Threat

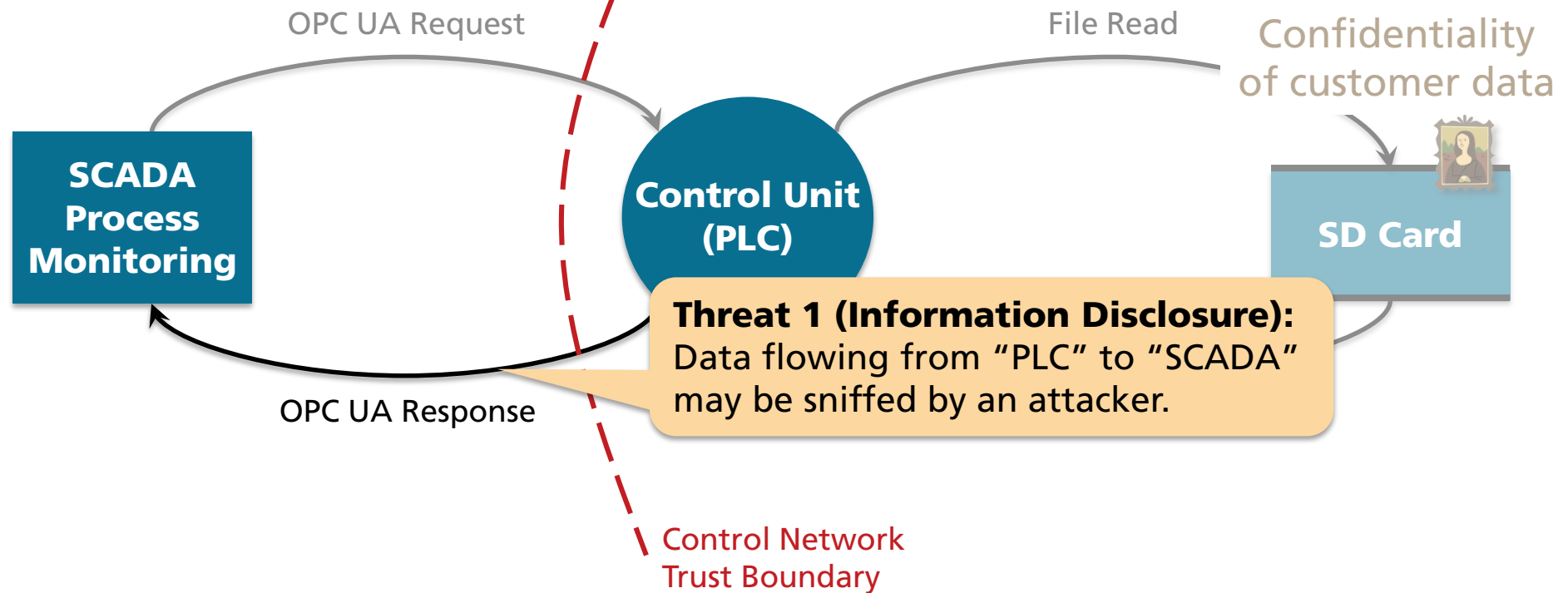


5. Assess Risk of Threats

Unmitigated Risk and Residual Risk



Risk Type	Attack Vector	Required Privileges	Required Skills	Required Resources
Unmitigated	Plant	None	No Secur.	Low



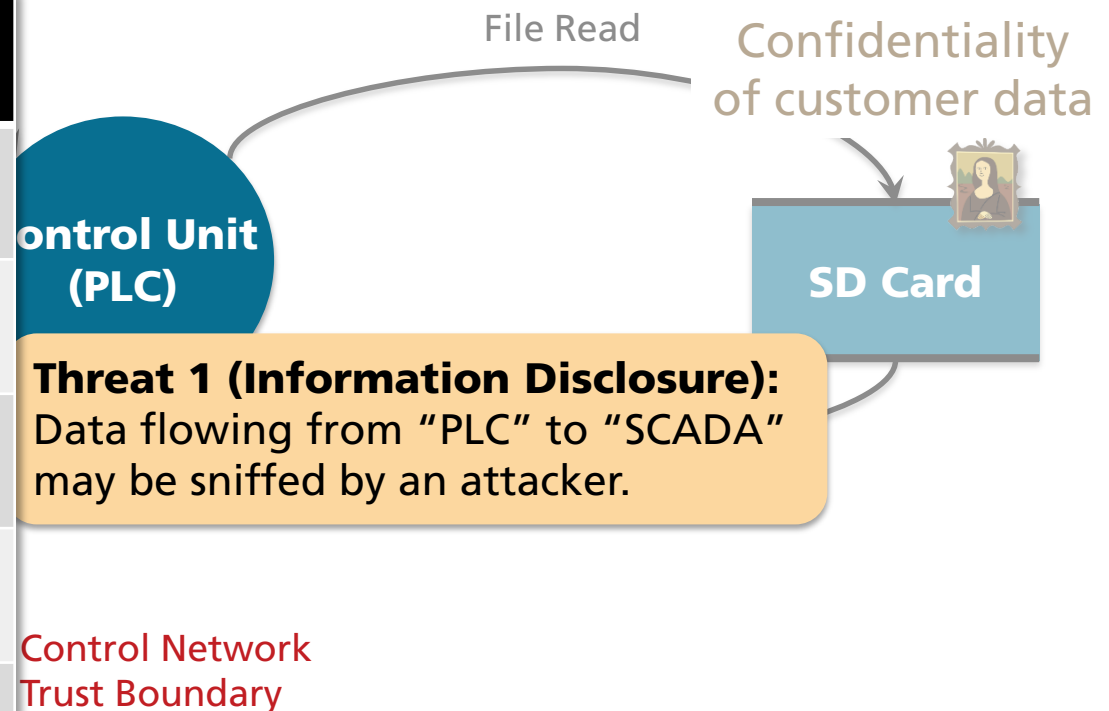
5. Assess Risk of Threats

Unmitigated Risk and Residual Risk



Risk Type	Attack Vector	Required Privileges	Required Skills	Required Resources	Severity
Unmitigated	Plant	None	No Secur.	Low	Major

Severity Bug Bar – Information Disclosure	
Catastrophic	Sensitive personal data disclosed
Major	Targeted sensitive data disclosed
Moderate	Random sensitive data disclosed
Minor	Random insensitive data disclosed
Negligible	Public data disclosed

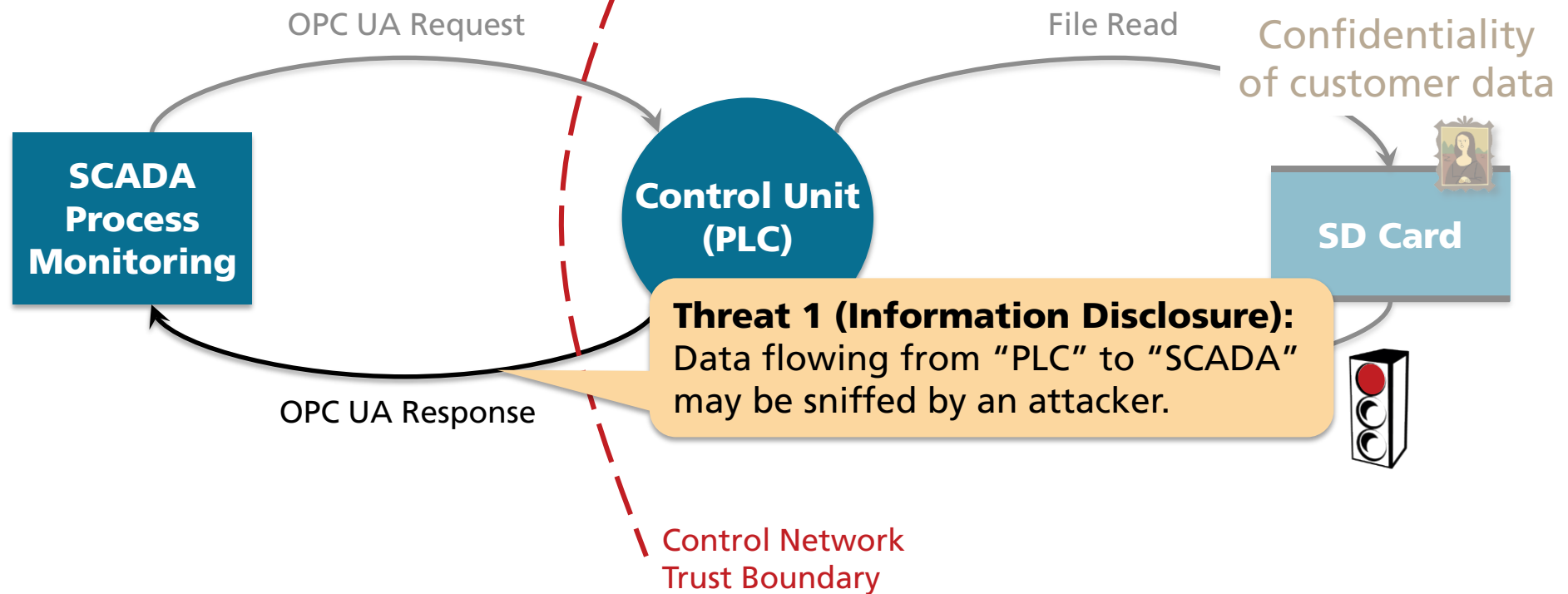


5. Assess Risk of Threats

Unmitigated Risk and Residual Risk



Risk Type	Attack Vector	Required Privileges	Required Skills	Required Resources	Severity	Risk
Unmitigated	Plant	None	No Secur.	Low	Major	Critical

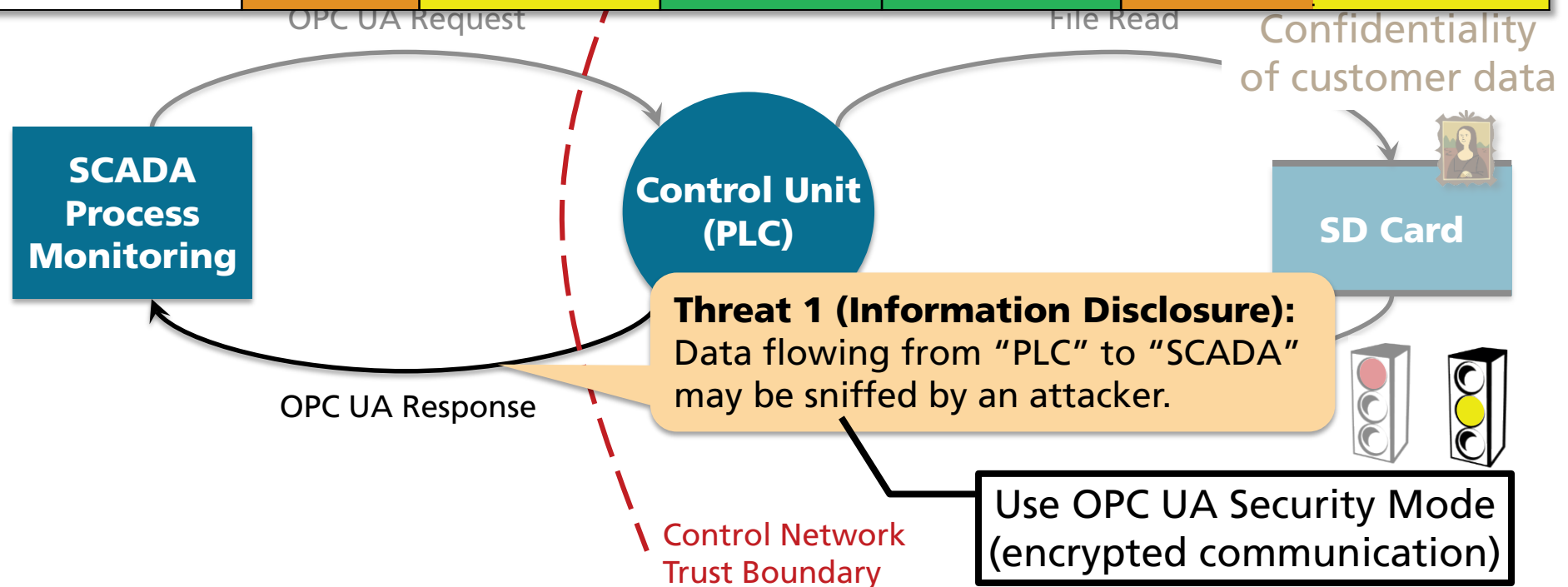


5. Assess Risk of Threats

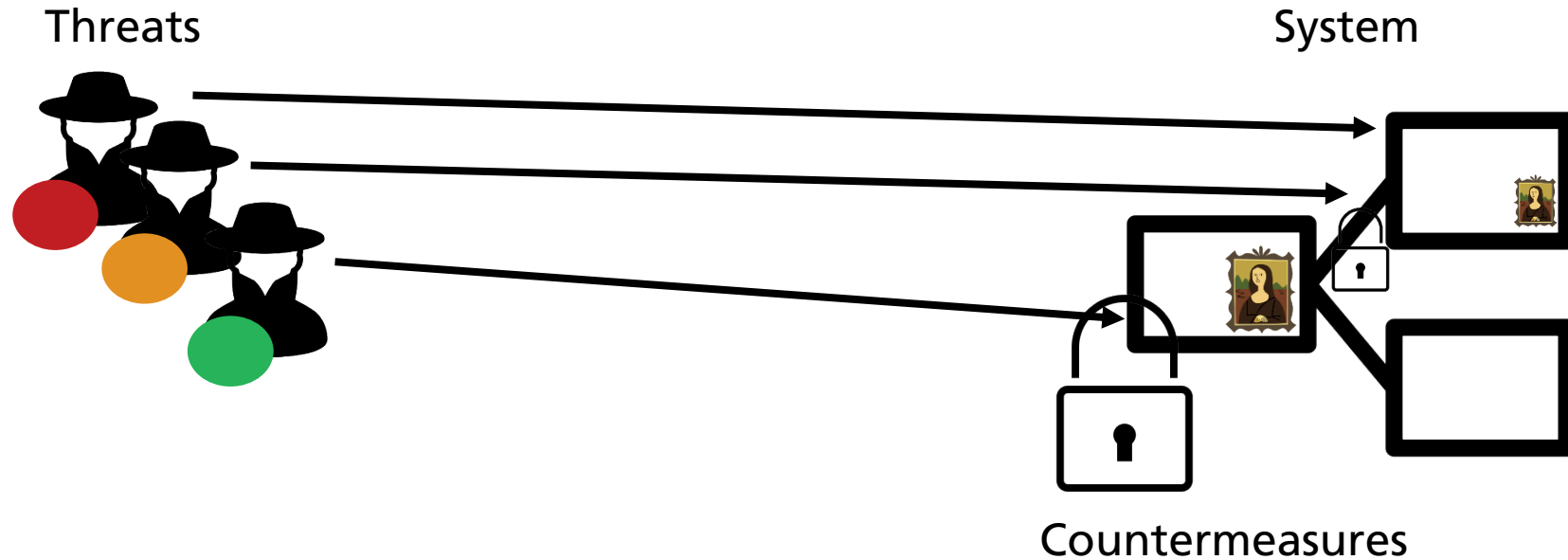
Unmitigated Risk and Residual Risk








Risk Type	Attack Vector	Required Privileges	Required Skills	Required Resources	Severity	Risk
Unmitigated	Plant	None	No Secur.	Low	Major	Critical
Residual	Plant	Authentic.	PLC & Sec.	High	Major	Moderate



Threat Analysis Compliant with IEC 62443-4-1



1.  Specify System and its Security Context
2.  Determine Assets and Security Objectives
3.  Identify and Localize Threats
4.  Determine Countermeasures
5.  Assess Risk of Threats

Threat Analysis Tool Support

Microsoft Threat Modeling Tool (TMT)

The screenshot displays the Microsoft Threat Modeling Tool (TMT) interface. The top section shows a diagram titled 'Diagram 1' with a grid background. The diagram includes several components: a 'Generic Data Store' on the left, an 'OS Process' in the center, a 'Web Service' on the right, and a 'Browser' on the far right. Arrows indicate data flow between these components. A 'SQL Query' box is connected to the 'OS Process' and the 'Generic Data Store'. A 'Service Data' box is connected to the 'OS Process' and the 'Web Service'. Two 'Data Request' boxes are connected to the 'Web Service' and the 'Browser'. A red dashed line separates the 'OS Process' from the 'Web Service'.

Below the diagram is the 'Threat List' section, which displays a table of generated threats. The table has columns for ID, Diagram, Changed By, Last Modified, State, Title, Category, Short Description, and Description. The table shows 17 threats, with the first five listed. The threat with ID 20 is highlighted.

ID	Diagram	Changed By	Last Modified	State	Title	Category	Short Description	Description
16	Diagram 1	Generated	Generated	Not Started	Spoofing the OS Process P...	Spoofing	Spoofing is whe...	OS Process ma...
17	Diagram 1	Generated	Generated	Not Started	Spoofing of Destination D...	Spoofing	Spoofing is whe...	Generic Data S...
18	Diagram 1	Generated	Generated	Not Started	The Generic Data Store Da...	Tampering	Tampering is th...	Data flowing a...
19	Diagram 1	Generated	Generated	Not Started	Data Store Denies Generic...	Repudiation	Repudiation thr...	Generic Data S...
20	Diagram 1	Generated	Generated	Not Started	Data Flow Sniffing	Information Disclosure	Information dis...	Data flowing a...

Below the table, it says '17 Threats Displayed, 17 Total'.

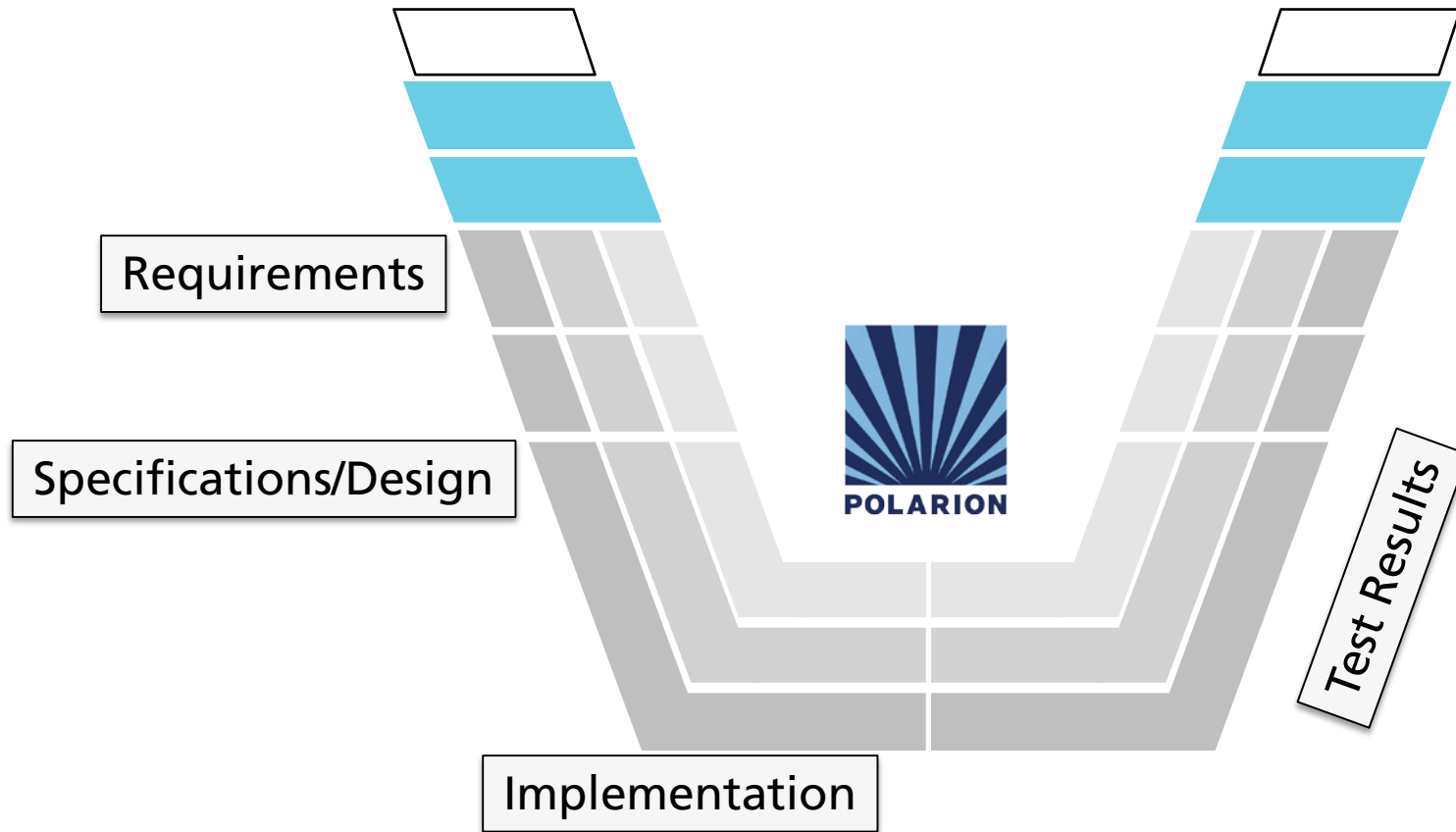
At the bottom is the 'Threat Properties' section, which shows the details for the selected threat (ID: 20). The properties include:

- ID: 20
- Diagram: Diagram 1
- Status: Not Started
- Last Modified: Generated
- Title: Data Flow Sniffing
- Category: Information Disclosure
- Description: Data flowing across SQL Query may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.
- Justification:
- Interaction: SQL Query
- Priority: High

At the bottom of the 'Threat Properties' section, it says 'Threat Properties Notes - no entries'.

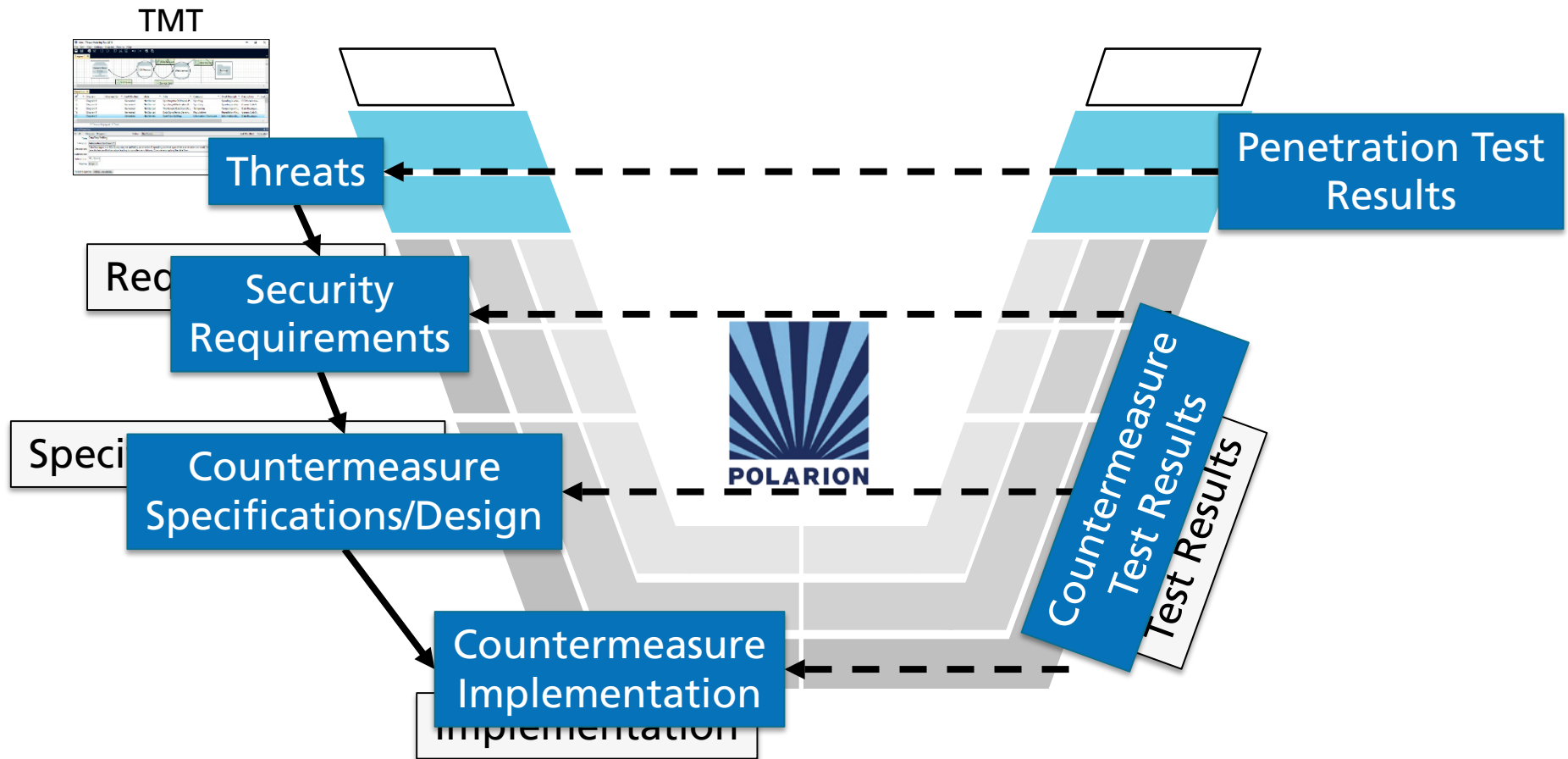
Threat Analysis in the Development Process

Work Products and Toolchain



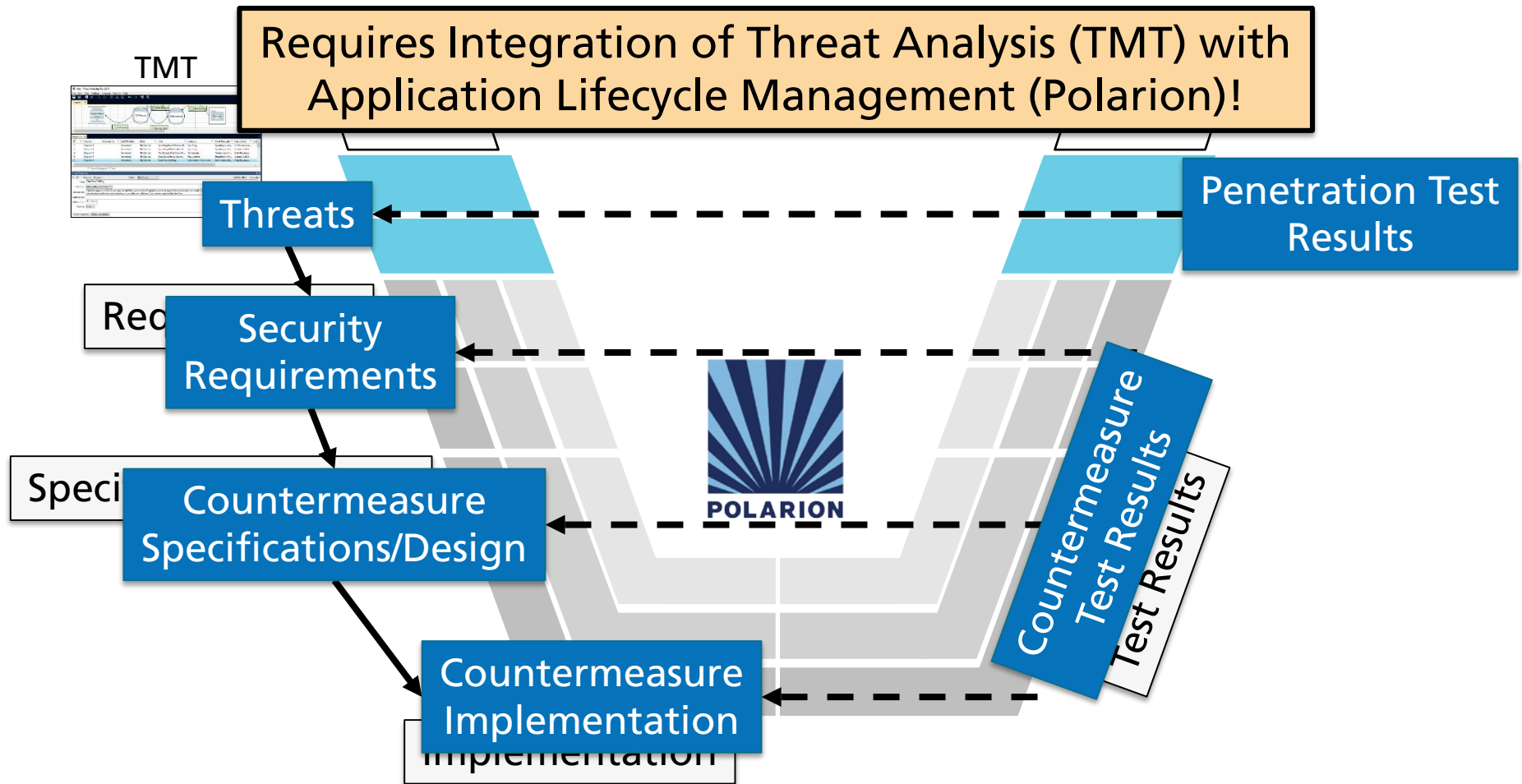
Threat Analysis in the Development Process

Work Products and Toolchain

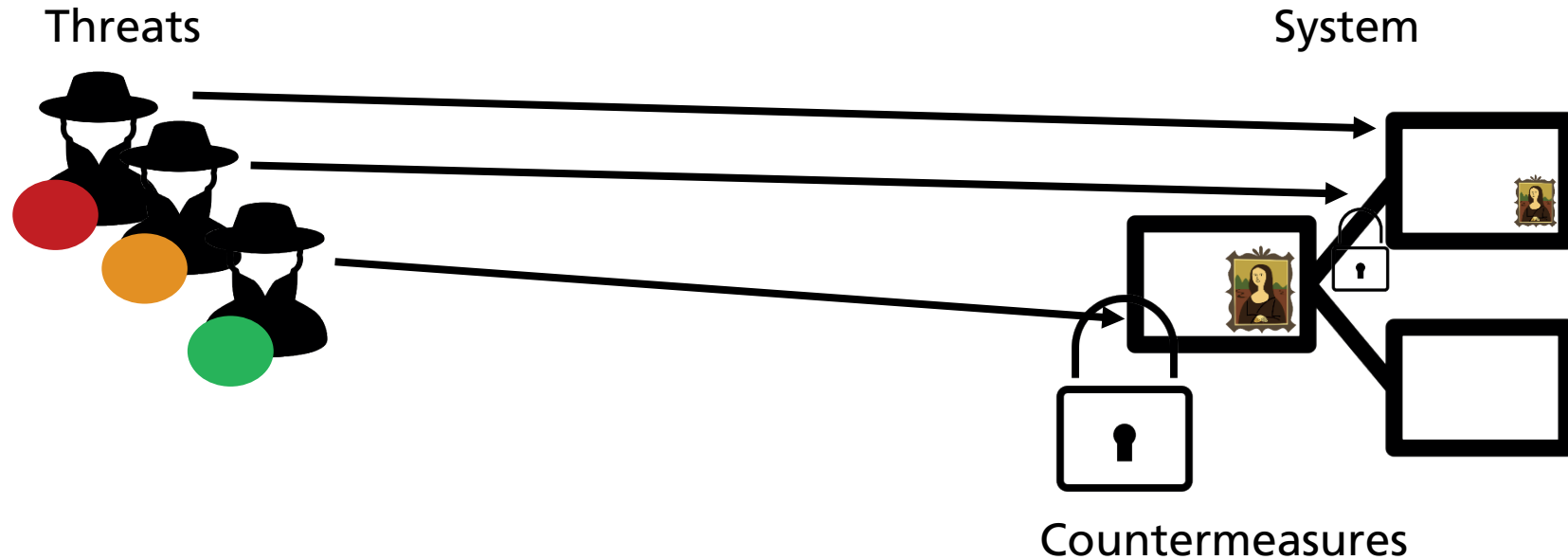







Threat Analysis in the Development Process

Work Products and Toolchain

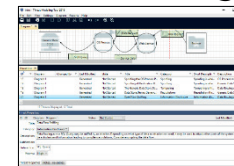


Threat Analysis Compliant with IEC 62443-4-1



1.  Specify System and its Security Context
2.  Determine Assets and Security Objectives
3.  Identify and Localize Threats
4.  Determine Countermeasures
5.  Assess Risk of Threats

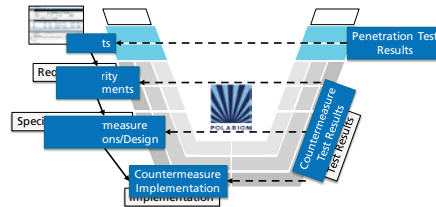
Threat Modeling Tool (TMT)



ReqIF
Requirements Interchange Format

Exchange format
for requirements

Lessons Learned

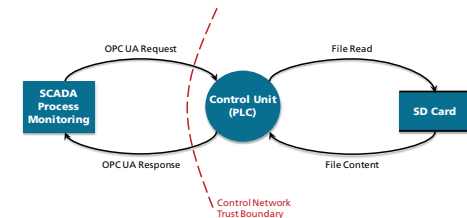


■ Findings concerning the process

- Integration with existing process and tools is crucial for low stakeholder effort and high stakeholder acceptance
- Automate as much as possible to support the developers ("make it easy to use for non-security-experts")

■ Findings concerning threat analysis

- The data flow diagram alone supports team communication and identifying threats
- The Threat Modeling Tool (template) has to be tailored to the domain (otherwise too many unreasonable, inapplicable, or too vague threats)
- Generated threats do not replace creative thinking!



Conclusion



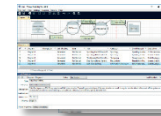
Certified
Threat
Analysis
Process

Results:

- Defined a threat analysis process compliant with IEC 62443-4-1 (for industrial automation components)
- Tailored the Microsoft Threat Modeling Tool to the domain
- Developed a tool-integration to export/update threats in ALM tool (Polarion)
- Defined risk assessment approach compliant with IEC 62443 (unmitigated and residual risk)



see details
in paper



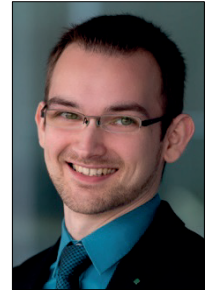
Risk Type	Attack Vector	Required Privileges	Required Skills	Required Resources	Severity	Risk
Unmitigated	Plant	None	No Secur.	Low	Major	Critical
Residual	Plant	Authentic.	PLC & Sec.	High	Major	Moderate

Contact



Dr. Markus Fockel

Senior Expert
Software Engineering & IT Security
Telephone: +49 5251 5465-120
markus.fockel@iem.fraunhofer.de



Sven Merschjohann

Research Associate
Software Engineering & IT Security
Telephone: +49 5251 5465-167
sven.merschjohann@iem.fraunhofer.de



Dr. Masud Fazal-Baqaie

Group Manager Software Lifecycle
Software Engineering & IT Security
Telephone: +49 5251 5465-153
masud.fazal-baqaie@iem.fraunhofer.de

