TARTU ÜLIKOOL
1632

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

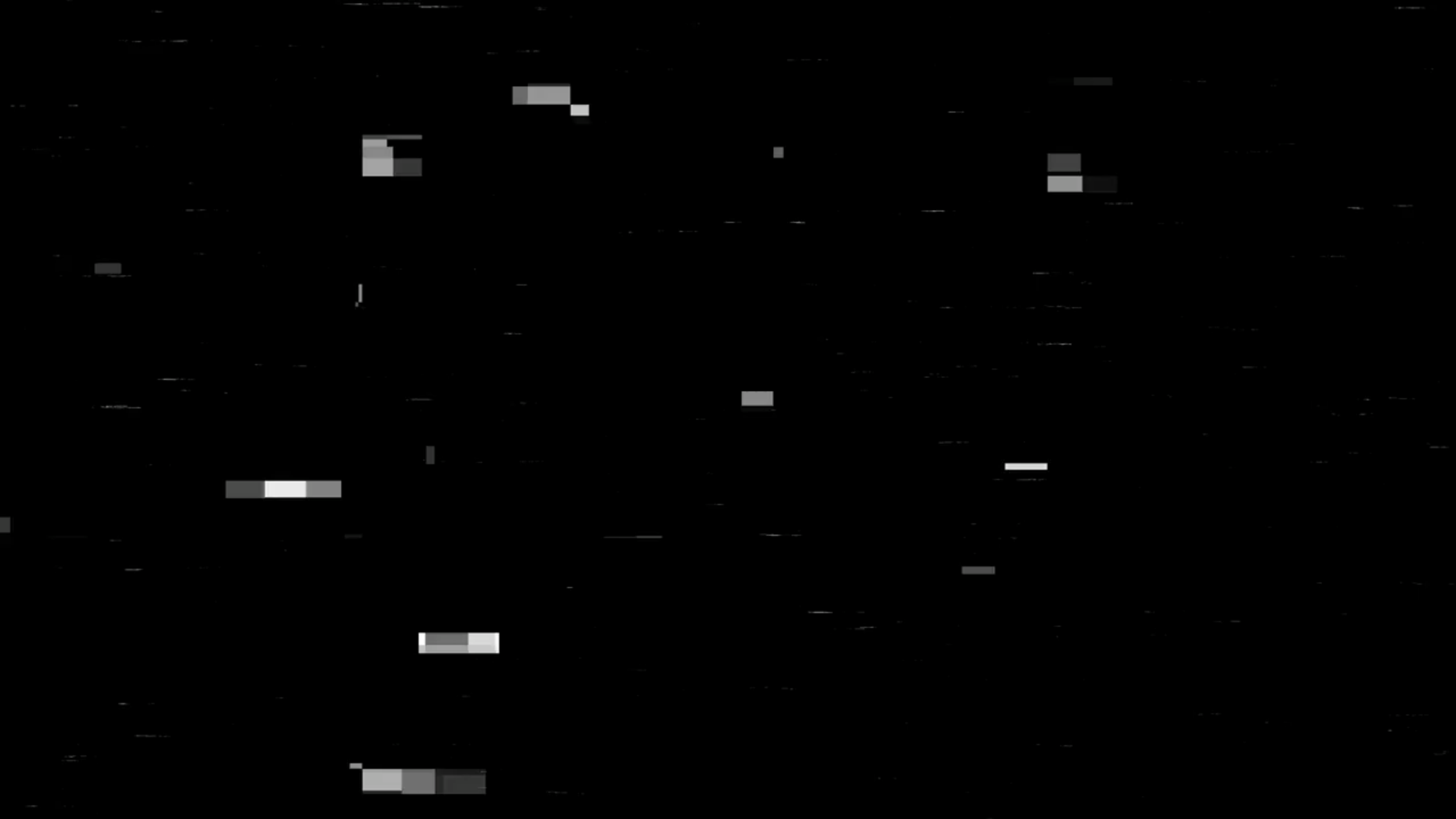
Function–Threat Alignment in CPS with FAST and MITRE ATT&CK

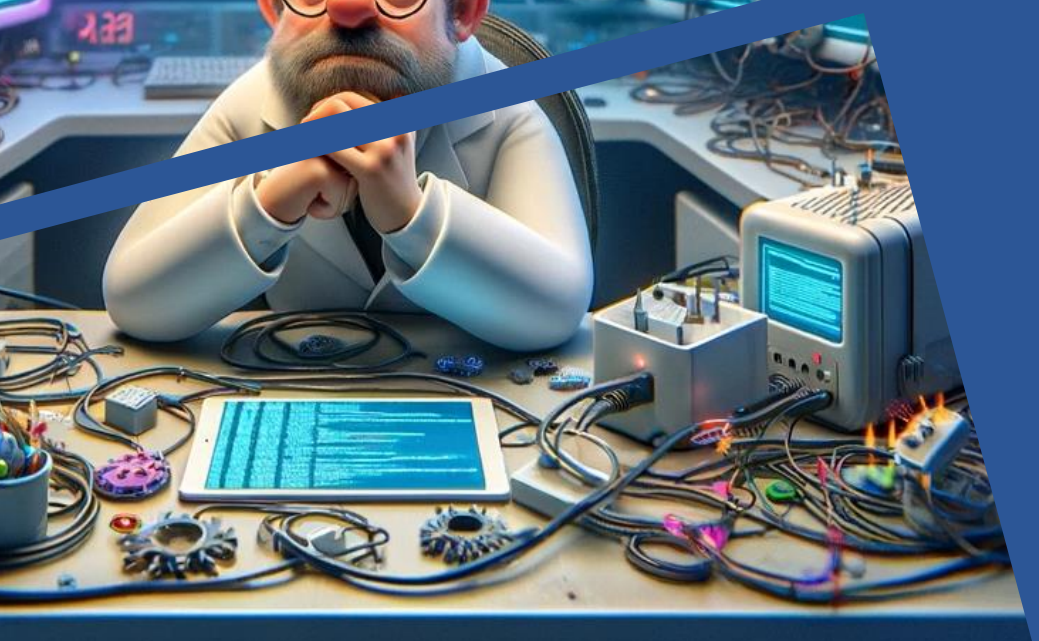
Vjatšeslav Antipenko

Raimundas Matulevičius

Institute of Computer Science
University of Tartu

BIR 2025, Riga, 18.09.2025





Searching for solutions

- ISO/IEC 27001
- NIST Cybersecurity Framework

Why not?

- Complex and Costly
- Resource-intensive upkeep

What else?

MITRE ATT&CK for ICS

- Empirical, threats aligned with ICS
- Detailed descriptions of adversarial strategies
- Actionable and reusable mitigation strategies

MITRE | ATT&CK®

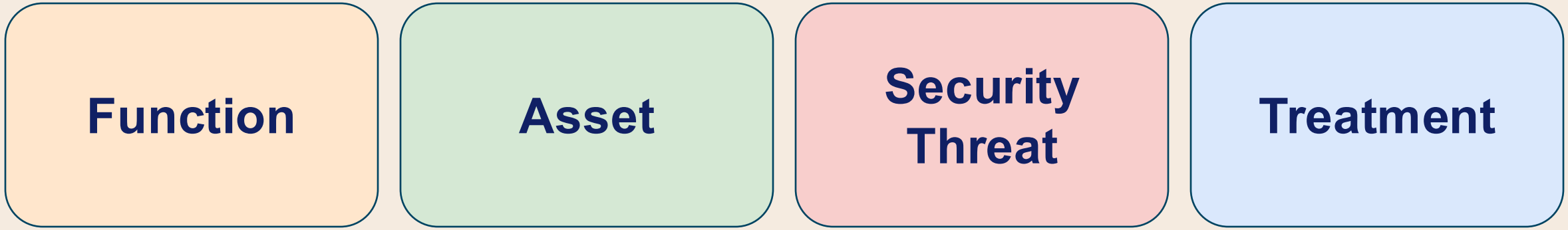
ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts
Rogue Master	Native API					
Spearphishing Attachment	Scripting					
Supply Chain Compromise	User Execution					
Transient Cyber Asset						
Wireless Compromise						

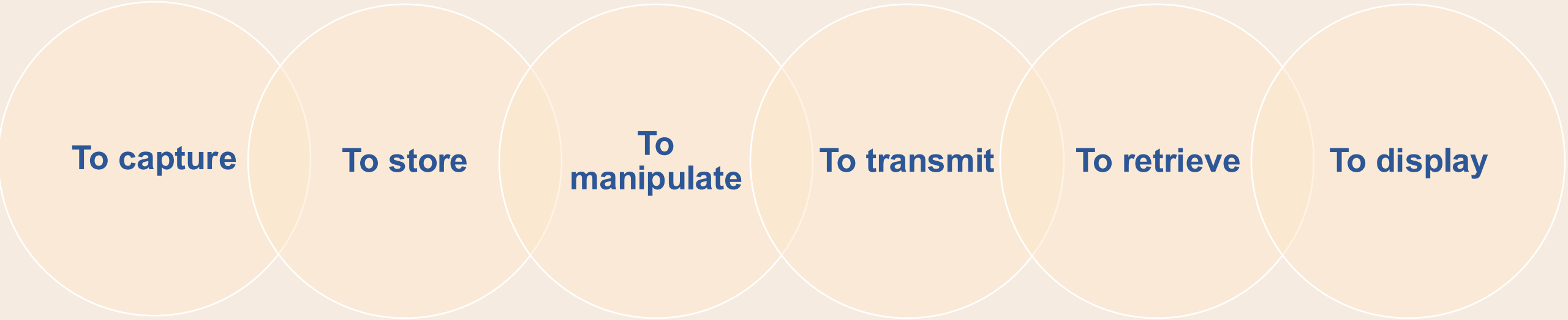
How can I understand the threats to my machines through their everyday operations?

The FAST Method



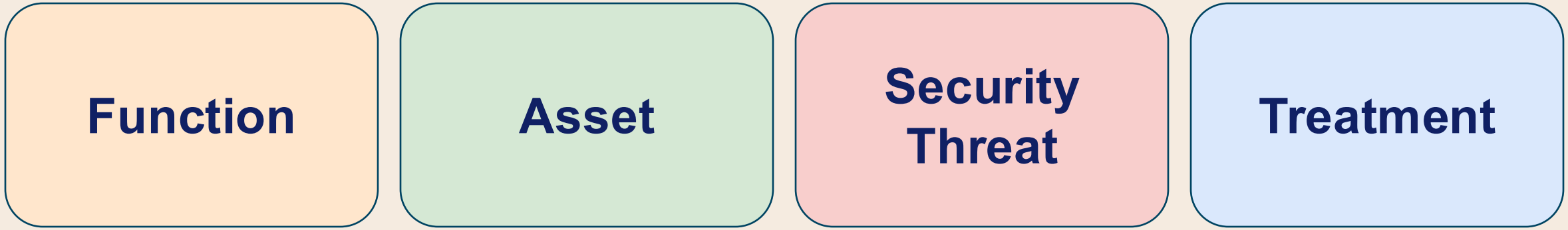
Antipenko, V., & Matulevičius, R. (2025). Functional Security in Automation: the FAST Approach. PoEM 2024

Information Processing Functions



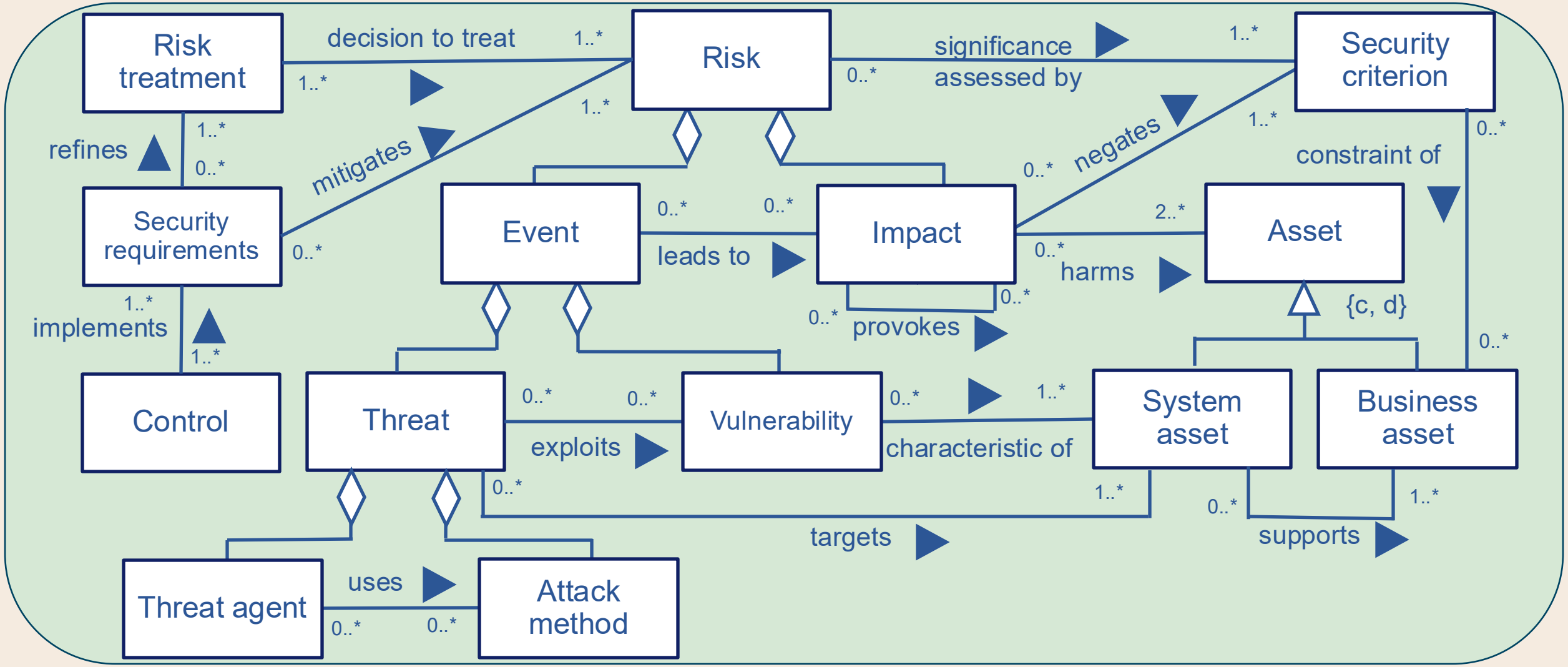
Alter, S. (2006). The work system method: Connecting people, processes, and IT for business results. Work System Method.

The FAST Method



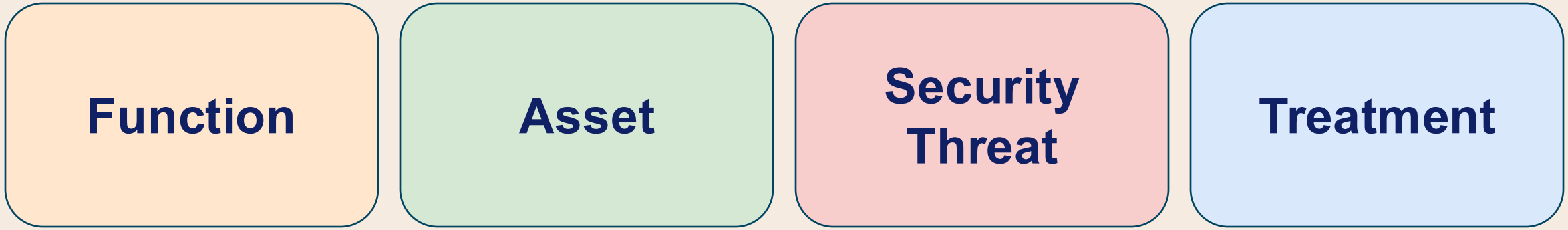
Antipenko, V., & Matulevičius, R. (2025). Functional Security in Automation: the FAST Approach. PoEM 2024

IS Security Risk Management



Matulevičius, R. (2017). Fundamentals of Secure System Modelling. Springer International Publishing.

The FAST Method



Antipenko, V., & Matulevičius, R. (2025). Functional Security in Automation: the FAST Approach. PoEM 2024

STRIDE

	Category	Description
	Spoofing	Impersonating another entity
	Tampering	Altering data or processes
	Repudiation	Denying an action with no evidence
	Information Disclosure	Exposing sensitive information
	Denial of Service	Disrupting availability of service
	Elevation of Privilege	Gaining unauthorized rights

Howard, M., & Lipner, S. (2006). The Security evelopment lifecycle (Vol. 8). Redmond: Microsoft Press.

The Drilling Cell as a Case Study

- *the ABB IRB 2400 robot*
- *the ATI torque sensor*
- *the IRC5 controller*


070R01
10R03

Function (FAST)	System Asset (FAST)	Business Asset (FAST)	MITRE Asset	MITRE Tactic	Threat (MITRE ICS)	Mitigation (MITRE ICS)
Capturing	ATI Delta 330–30	Force/Torque Data	Field I/O	Collection	Adversary-in-the-Middle	M0802 – Communication Authenticity
Manipulating	IRC5	Joint Position Data	PLC	Impair Process Control	Modify Parameter	M0818 – Validate Program Inputs
Storing	IRC5 / RobotStudio	Tool Path Configuration	PLC	Persistence	Module Firmware	M0945 – Code Signing
Displaying	FlexPendant	Robot Program Logic / Diagnostics	HMI	Evasion	Masquerading	M0945 – Code Signing

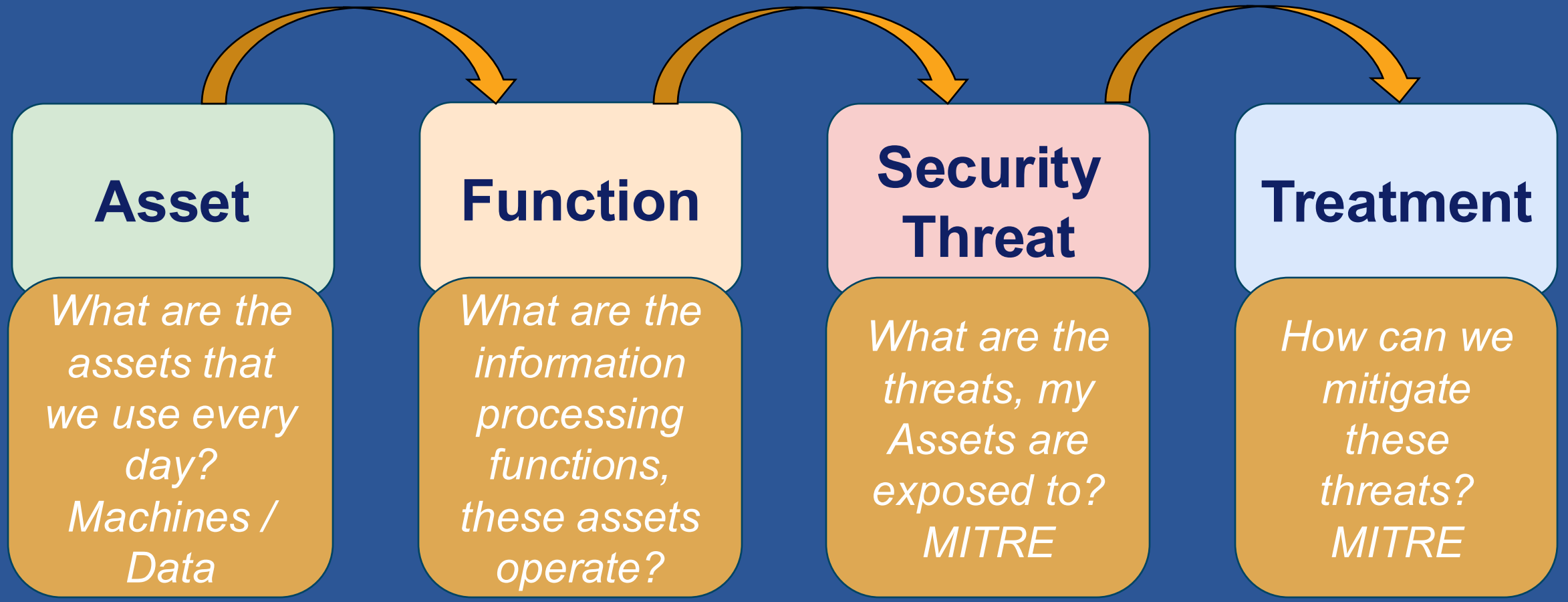
Function (FAST)	System Asset (FAST)	Business Asset (FAST)	MITRE Asset	MITRE Tactic	Threat (MITRE ICS)	Mitigation (MITRE ICS)
Capturing	ATI Delta 330–30	Force/Torque Data	Field I/O	Collection	Adversary-in-the-Middle	M0802 – Communication Authenticity
Manipulating	IRC5	Joint Position Data	PLC	Impair Process Control	Modify Parameter	M0818 – Validate Program Inputs
Storing	IRC5 / RobotStudio	Tool Path Configuration	PLC	Persistence	Module Firmware	M0945 – Code Signing
Displaying	FlexPendant	Robot Program Logic / Diagnostics	HMI	Evasion	Masquerading	M0945 – Code Signing

Function (FAST)	System Asset (FAST)	Business Asset (FAST)	MITRE Asset	MITRE Tactic	Threat (MITRE ICS)	Mitigation (MITRE ICS)
Capturing	ATI Delta 330–30	Force/Torque Data	Field I/O	Collection	Adversary-in-the-Middle	M0802 – Communication Authenticity
Manipulating	IRC5	Joint Position Data	PLC	Impair Process Control	Modify Parameter	M0818 – Validate Program Inputs
Storing	IRC5 / RobotStudio	Tool Path Configuration	PLC	Persistence	Module Firmware	M0945 – Code Signing
Displaying	FlexPendant	Robot Program Logic / Diagnostics	HMI	Evasion	Masquerading	M0945 – Code Signing

Function (FAST)	System Asset (FAST)	Business Asset (FAST)	MITRE Asset	MITRE Tactic	Threat (MITRE ICS)	Mitigation (MITRE ICS)
Capturing	ATI Delta 330–30	Force/Torque Data	Field I/O	Collection	Adversary-in-the-Middle	M0802 – Communication Authenticity
Manipulating	IRC5	Joint Position Data	PLC	Impair Process Control	Modify Parameter	M0818 – Validate Program Inputs
Storing	IRC5 / RobotStudio	Tool Path Configuration	PLC	Persistence	Module Firmware	M0945 – Code Signing
Displaying	FlexPendant	Robot Program Logic / Diagnostics	HMI	Evasion	Masquerading	M0945 – Code Signing

Function (FAST)	System Asset (FAST)	Business Asset (FAST)	MITRE Asset	MITRE Tactic	Threat (MITRE ICS)	Mitigation (MITRE ICS)
Capturing	ATI Delta 330–30	Force/Torque Data	Field I/O	Collection	Adversary-in-the-Middle	M0802 – Communication Authenticity
Manipulating	IRC5	Joint Position Data	PLC	Impair Process Control	Modify Parameter	M0818 – Validate Program Inputs
Storing	IRC5 / RobotStudio	Tool Path Configuration	PLC	Persistence	Module Firmware	M0945 – Code Signing
Displaying	FlexPendant	Robot Program Logic / Diagnostics	HMI	Evasion	Masquerading	M0945 – Code Signing

How can we apply?



Threat Scenario 1: Adversary-in-the-Middle

Aspect	Details
Business Asset	Force/Torque Measurement Data
System Asset	ATI Delta 330–30
MITRE Asset	Field I/O
Function (FAST)	Capturing
MITRE Tactic	Collection
Threat (MITRE ICS)	Adversary-in-the-Middle

Threat Scenario 1: Adversary-in-the-Middle

Aspect	Details
Business Asset	Force/Torque Measurement Data
System Asset	ATI Delta 330–30
MITRE Asset	Field I/O
Function (FAST)	Capturing
MITRE Tactic	Collection
Threat (MITRE ICS)	Adversary-in-the-Middle
Risk	Interception and manipulation of sensor data
Impact	Loss of data integrity, incorrect control decisions
Vulnerability	Unauthenticated communication protocols

Threat Scenario 1: Adversary-in-the-Middle

Aspect	Details
Business Asset	Force/Torque Measurement Data
System Asset	ATI Delta 330–30
MITRE Asset	Field I/O
Function (FAST)	Capturing
MITRE Tactic	Collection
Threat (MITRE ICS)	Adversary-in-the-Middle
Risk	Interception and manipulation of sensor data
Impact	Loss of data integrity, incorrect control decisions
Vulnerability	Unauthenticated communication protocols
Mitigation (MITRE ICS)	M0802 – Communication Authenticity
Controls	Sign messages, authenticate endpoints, validate sensor data at the controller

Threat Scenario 2: Modify Parameter

Aspect	Details
Business Asset	Robot Joint Position Data
System Asset	IRC5 Controller
MITRE Asset	PLC
Function (FAST)	Manipulating
MITRE Tactic	Impair Process Control
Threat (MITRE ICS)	Modify Parameter

Threat Scenario 2: Modify Parameter

Aspect	Details
Business Asset	Robot Joint Position Data
System Asset	IRC5 Controller
MITRE Asset	PLC
Function (FAST)	Manipulating
MITRE Tactic	Impair Process Control
Threat (MITRE ICS)	Modify Parameter
Risk	Subtle deviation of operational behaviour
Impact	Product degradation, mechanical wear, safety compromise
Vulnerability	Unchecked or unvalidated parameter updates

Threat Scenario 2: Modify Parameter

Aspect	Details
Business Asset	Robot Joint Position Data
System Asset	IRC5 Controller
MITRE Asset	PLC
Function (FAST)	Manipulating
MITRE Tactic	Impair Process Control
Threat (MITRE ICS)	Modify Parameter
Risk	Subtle deviation of operational behaviour
Impact	Product degradation, mechanical wear, safety compromise
Vulnerability	Unchecked or unvalidated parameter updates
Mitigation (MITRE ICS)	M0818 – Validate Program Inputs
Controls	Range checking, fallback defaults, validation logic at run-time

Lessons Learned & Outlook