

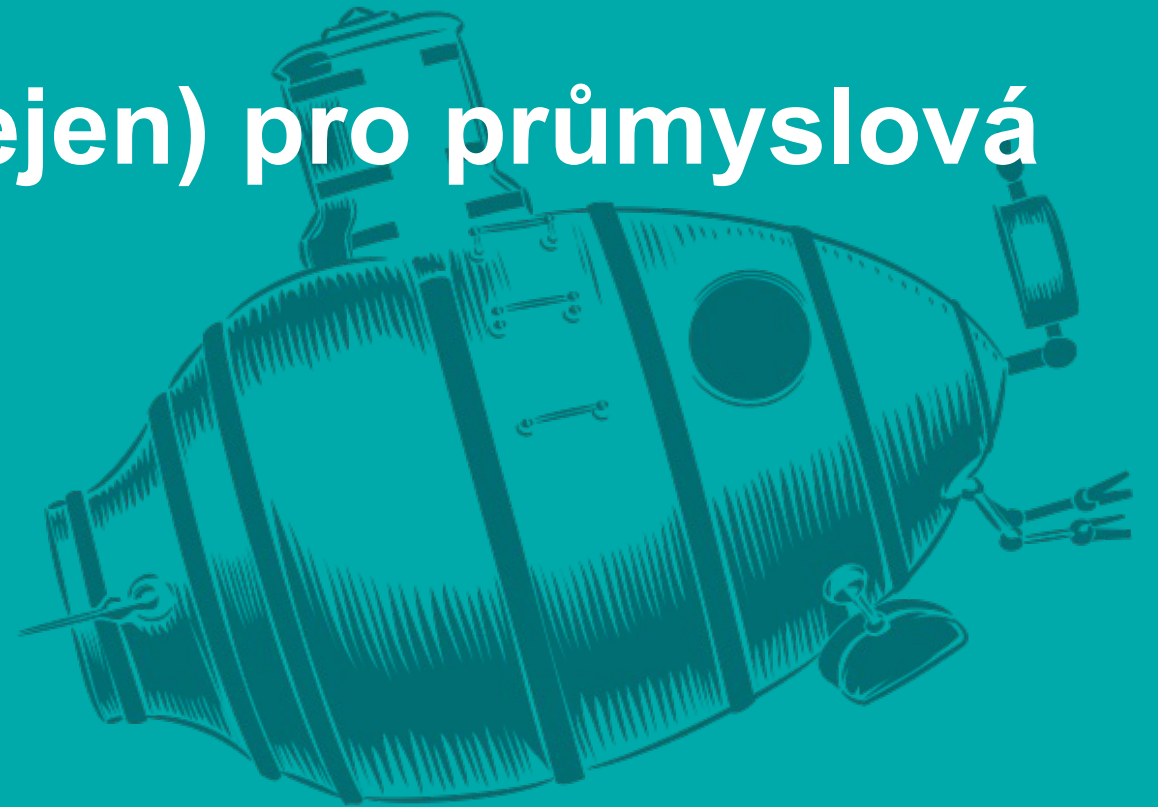


# Modelování hrozeb (nejen) pro průmyslová prostředí

**Jan Kopřiva**

[jan.kopriva@alef.com](mailto:jan.kopriva@alef.com)

 [@jk0pr](https://twitter.com/jk0pr)



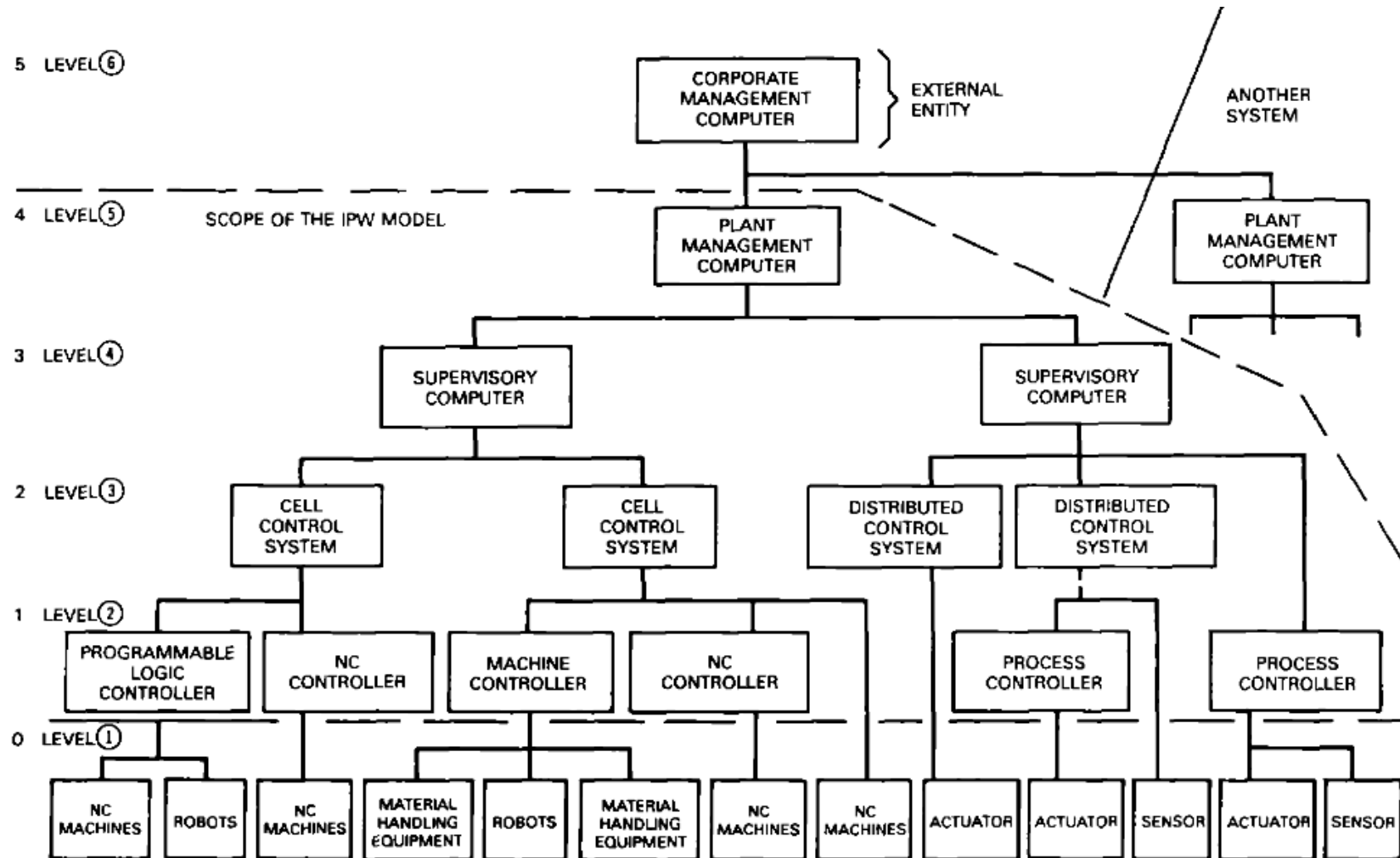
# Když se řekne průmyslový a specifický systém

- ICS, IACS, SCADA, IIoT, HIIoT, ...
- Historické sítě a systémy
  - Velmi dlouhý životní cyklus
  - Často proprietární, uzavřená řešení
- Moderní systémy blízké IT, historické spíše tradiční automatizační a zabezpečovací technice – specifické požadavky na bezpečnost
- Nezřídka neformalizovaný přístup k bezpečnosti

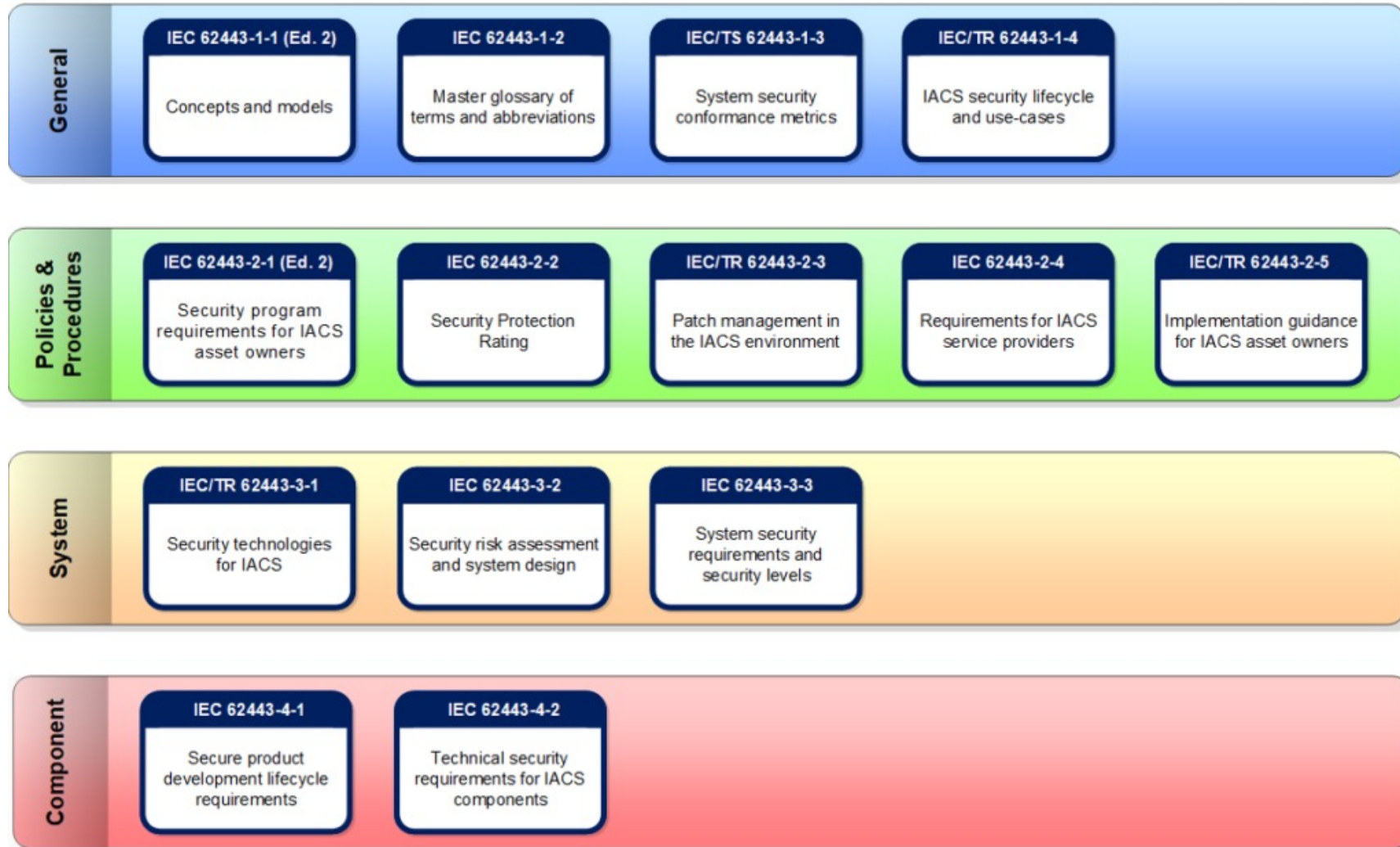
# Relevantní normativy a standardy

- Standardy se vztahem k vývoji, průmyslu a bezpečnostnímu inženýrství
  - ISO (21827:2008 – SSE-CMM)
  - NIST (SP 800-82, SP 800-160)
- (Nově vznikající) normativy a standardy pro specifické oblasti
  - Silniční doprava, kolejová doprava, IIoT,...
- I po letech stále relevantní
  - ISA/IEC 62443
  - PERA

# Purdue Enterprise Reference Architecture (PERA)



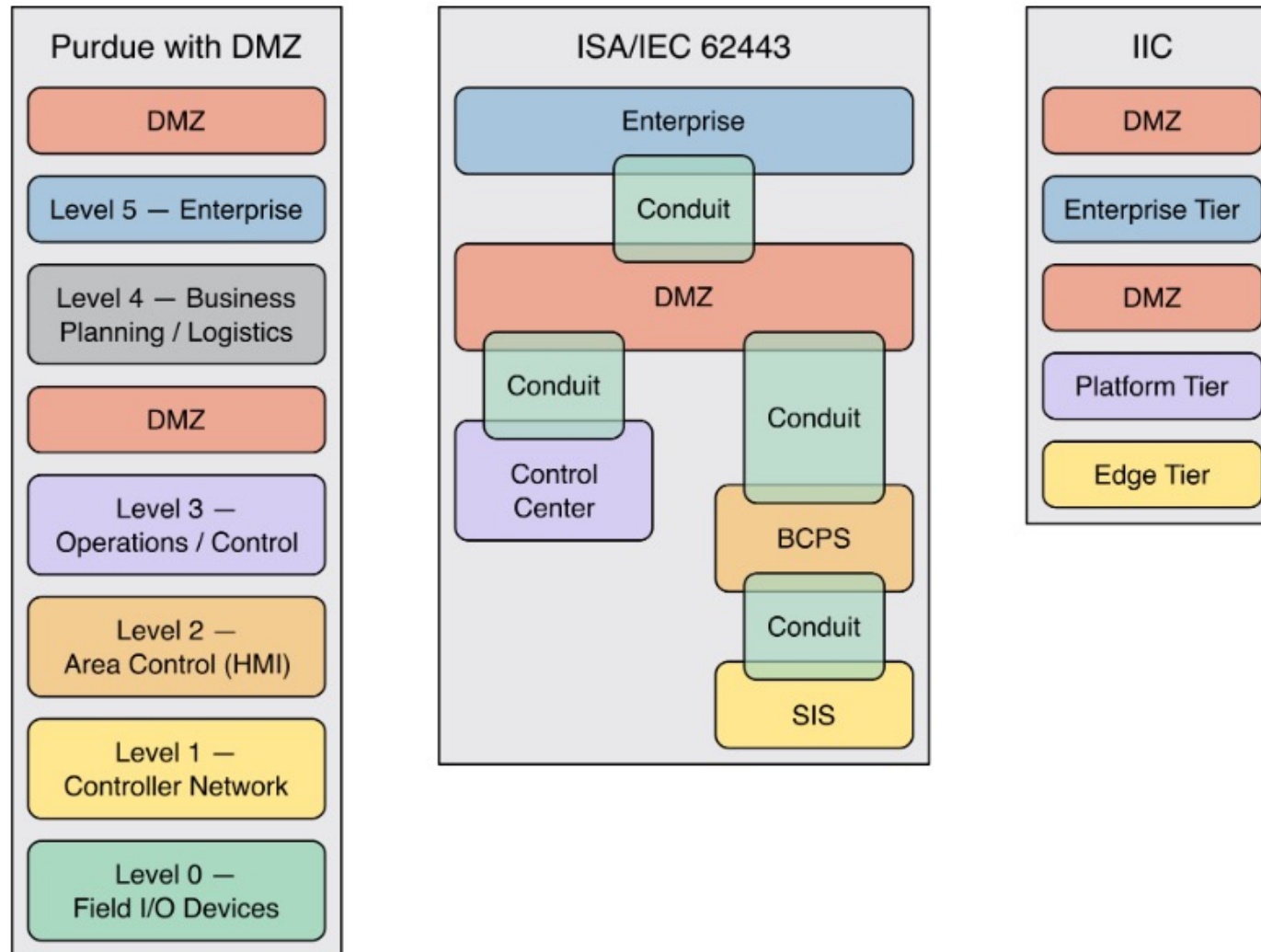
# IEC 62443



# Tradiční přístup

- PERA (levels) i IEC 62443 (zones & conduits) vychází z myšlenky logického či fyzického oddělení průmyslových systémů a sítí od zbytku světa a rigidního řízení přístupů k nim
- V současnosti zpravidla stále optimální, ne vždy však dosažitelné/možné (logování, IIoT, HIoT, vozidla,...)
- Obvyklým obecným řešením přístup přes vhodnou architekturu a řízení rizik

# Architektura na úrovni sítě



# Rizika v průmyslových a specifických systémech

- Standardní přístupy k určování rizik plně validní
  - Zejména u „safety“ (resp. RAMS) mnohdy více než u IT
- Naturogenní hrozby zpravidla jednoduché určit
- U antropogenních hrozeb je situace o něco složitější
  - Specifické typy technických aktiv i procesů spojeny se specifickými útočnými postupy a vektory
  - Interakční povrch (attack surface) systémů i prostředí (SoS) ne vždy zjevný



# Modelování hrozeb pro průmyslové systémy

- Řízení rizik
  - IEC 62443-3-2 – ZCR 5.1: Identify threats
- Bezpečnostní monitoring
  - IEC 62443 Foundational Requirement 6 - Timely response to events

# Modelování hrozeb pro průmyslové systémy

- Vývoj systémů
  - IEC 62443-4-1 – SR-2: Threat model
    - Data flows, trust boundaries, processes, data stores, interaction with external entities, communication protocols, externally-accessible physical ports, circuit board connections (e.g., JTAG), attacks on HW, external dependencies, ...
    - Explicitně zmíněna metodika STRIDE

# Modelování hrozeb pro průmyslové systémy

- Jak smysluplně postupovat
  - Tradiční metodiky pro modelování hrozeb
    - Úzce či naopak velmi široce zaměřené
    - Méně tradiční metodiky?

# STRIDE

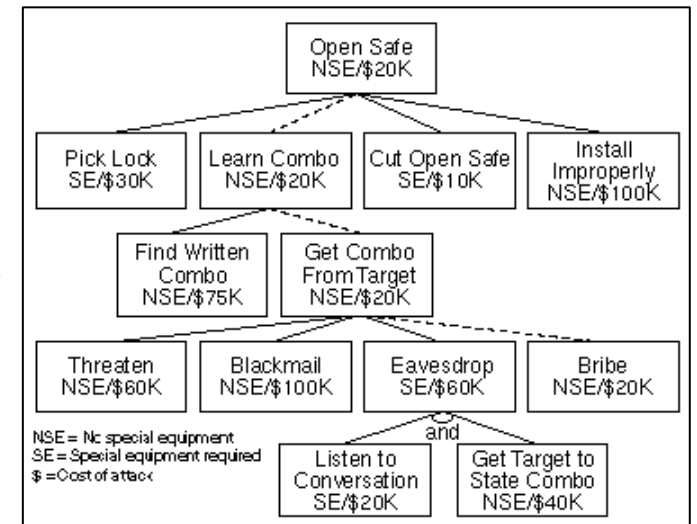
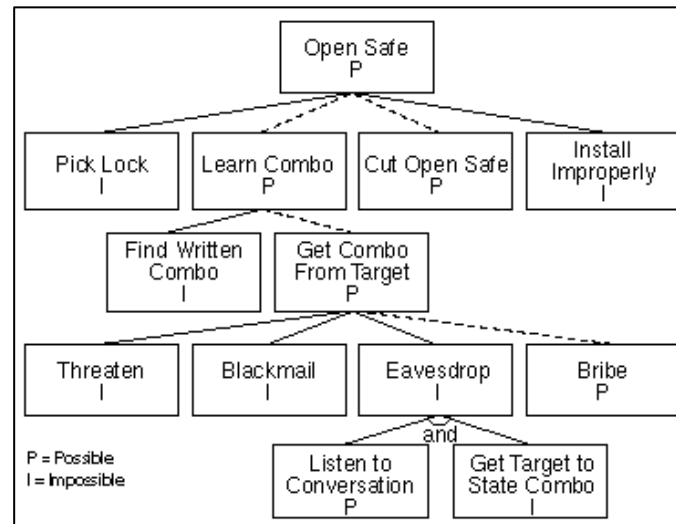
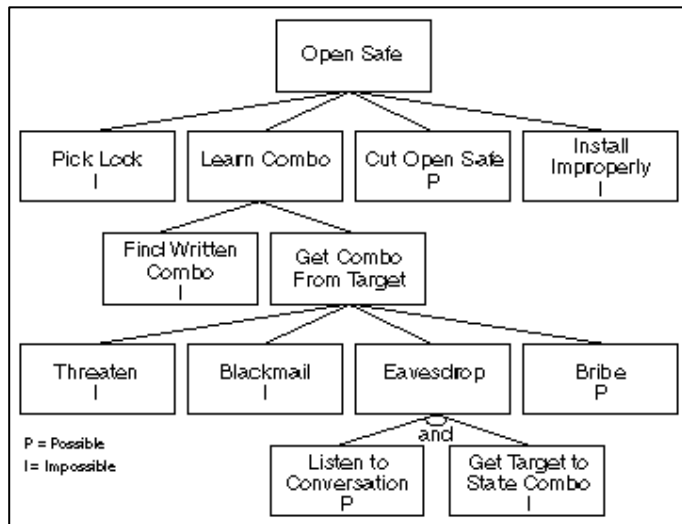
- Metodika pro modelování hrozeb primárně pro SW produkty
- Využitelná potenciálně i v jiných oblastech, kde ale není nezbytně vhodná
- Kategorie hrozeb
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of Service
  - Elevation of privilege

# Další relevantní metodiky pro modelování hrozeb

- Tradiční
  - Attack Trees
- Méně tradiční, avšak vysoce efektivní
  - OSSTMM
  - MITRE ATT&CK

# Stromy útoků (attack trees)

- Vysoce generická formální metodika pro modelování hrozeb pro libovolný (a tedy i průmyslový/specifický) systém
- Postupné vytváření stromu v němž cíl útoku je kořenem a listy jsou různými způsoby jeho dosažení



# OSSTMM

- Ve verzi 3 není OSSTMM (jen) metodikou pro bezpečnostní testování
- Velmi dobrá vazba na segmentaci do „zones and conduits“ a identifikaci „logical and physical access points“ dle IEC 62443, stejně tak na „levels“ v PERA
- Nepracuje s rizikem, ale s „porézností“ systému (velikostí interakčního povrchu)

# OSSTMM

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
	Alarm		
			Anomalies



# MITRE ATT&CK

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-in-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (2)	Access Token Manipulation (2)	Brute Force (2)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Infrastructure (2)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (1)	Boot or Logon Autostart Execution (1)	BITS Jobs	Credentials from Password Stores (2)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Gather Victim Network Information (2)	Develop Capabilities (2)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (2)	Boot or Logon Initialization Scripts (2)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Data Manipulation (2)
Gather Victim Org Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (2)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2)	Browser Session Hijacking	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Defacement (2)
Phishing for Information (2)	Obtain Capabilities (2)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (2)	Decompilate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create Account (2)	Escape to Host	Deploy Container	Input Capture (2)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (2)
Search Open Technical Databases (2)	Trusted Relationship	Valid Accounts (2)	Shared Modules	Create or Modify System Process (2)	Event Triggered Execution (1)	Direct Volume Access	Modify Authentication Process (2)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)	Windows Management Instrumentation		Software Deployment Tools	Event Triggered Execution (1)	Execution Guardrails (1)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (2)	Data from Information Repositories (2)	Multi-Stage Channels	Inhibit System Recovery	Resource Hijacking
Search Victim-Owned Websites			System Services (2)	External Remote Services	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Service Stop
			User Execution (2)	Hijack Execution Flow (1)	Hijack Execution Flow (1)	Event Triggered Execution (1)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	System Shutdown/Reboot
			Windows Management Instrumentation	Process Injection (1)	Process Injection (1)	Execution Guardrails (1)	OS Credential Dumping (2)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		
				Hijack Execution Flow (1)	Hijack Execution Flow (1)	File and Directory Permissions Modification (2)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (2)		
				Implant Internal Image	Implant Internal Image	Hide Artifacts (1)	Steal or Forge Kerberos Tickets (2)	Network Share Discovery		Email Collection (2)	Remote Access Software		
				Office Application Startup (2)	Office Application Startup (2)	Hijack Execution Flow (1)	Steal Web Session Cookie	Network Sniffing		Input Capture (2)	Traffic Signaling (1)		
				Pre-OS Boot (2)	Pre-OS Boot (2)	Impair Defenses (2)	Unsecured Credentials (1)	Network Service Discovery		Screen Capture	Web Service (2)		
				Scheduled Task/Job (2)	Scheduled Task/Job (2)	Indicator Removal on Host (2)		Network Share Discovery		Video Capture			
				Server Software Component (2)	Server Software Component (2)	Indirect Command Execution		Network Service Discovery					
				Traffic Signaling (1)	Traffic Signaling (1)	Masquerading (2)		Network Service Discovery					
				Valid Accounts (2)	Valid Accounts (2)	Modify Authentication Process (2)		Network Service Discovery					
						Modify Cloud Compute Infrastructure (2)		Network Service Discovery					
						Modify Registry		Network Service Discovery					
						Modify System Image (2)		Network Service Discovery					
						Network Boundary Bridging (1)		Network Service Discovery					
						Obfuscated Files or Information (2)		Network Service Discovery					
						Plist File Modification		Network Service Discovery					
						Pre-OS Boot (2)		Network Service Discovery					
						Process Injection (1)		Network Service Discovery					
						Reflective Code Loading		Network Service Discovery					
						Rogue Domain Controller		Network Service Discovery					
						Rootkit		Network Service Discovery					
						Subvert Trust Controls (2)		Network Service Discovery					
						System Binary Proxy Execution (1)		Network Service Discovery					
						System Script Proxy Execution (1)		Network Service Discovery					
						Template Injection		Network Service Discovery					
						Traffic Signaling (1)		Network Service Discovery					
						Trusted Developer Utilities Proxy Execution (1)		Network Service Discovery					
						Unused/Unsupported Cloud Regions		Network Service Discovery					
						Use Alternate Authentication Material (2)		Network Service Discovery					
						Valid Accounts (2)		Network Service Discovery					
						Virtualization/Sandbox Evasion (2)		Network Service Discovery					
						Weaken Encryption (2)		Network Service Discovery					
						XSL Script Processing		Network Service Discovery					

# MITRE ATT&CK ICS

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Last modified: 06 May 2022

# MITRE ATT&CK ICS

<b>Initial Access</b>	<b>Execution</b>	<b>Persistence</b>	<b>Privilege Escalation</b>
12 techniques	9 techniques	6 techniques	2 techniques
<b>Evasion</b>	<b>Discovery</b>	<b>Lateral Movement</b>	<b>Collection</b>
6 techniques	5 techniques	7 techniques	10 techniques
<b>Command and Control</b>	<b>Inhibit Response Function</b>	<b>Impair Process Control</b>	<b>Impact</b>
3 techniques	13 techniques	5 techniques	12 techniques

# MITRE ATT&CK ICS

Initial Access	Execution	Persistence
12 techniques	9 techniques	6 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials
Exploit Public-Facing Application	Command-Line Interface	Modify Program
Exploitation of Remote Services	Execution through API	Module Firmware
External Remote Services	Graphical User Interface	Project File Infection
Internet Accessible Device	Hooking	System Firmware
Remote Services	Modify Controller Tasking	Valid Accounts
Replication Through Removable Media	Native API	
Rogue Master	Scripting	
Spearphishing Attachment	User Execution	
Supply Chain Compromise		
Transient Cyber Asset		
Wireless Compromise		

## Procedure Examples

ID	Name	Description
S0603	Stuxnet	Stuxnet modifies the Import Address Tables DLLs to hook specific APIs that are used to open project files. <sup>[2]</sup>
S1009	Triton	Triton's injector, inject.bin, changes the function pointer of the 'get main processor diagnostic data' TriStation command to the address of imain.bin so that it is executed prior to the normal handler. <sup>[3]</sup>

## Mitigations

ID	Mitigation	Description
M0947	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses. Perform periodic integrity checks of the device to validate the correctness of the firmware, software, programs, and configurations. Integrity checks, which typically include cryptographic hashes or digital signatures, should be compared to those obtained at known valid states, especially after events like device reboots, program downloads, or program restarts.
M0944	Restrict Library Loading	Restrict the use of untrusted or unknown libraries, such as remote or unknown DLLs.

## Detection

ID	Data Source	Data Component	Detects
DS0009	Process	OS API Execution	Monitor for API calls that can be used to install a hook procedure, such as the SetWindowsHookEx and SetWinEventHook functions. <sup>[4][5]</sup> Also consider analyzing hook chains (which hold pointers to hook procedures for each type of hook) using tools <sup>[5][6][7]</sup> or by programmatically examining internal kernel structures. <sup>[8][9]</sup>
		Process Metadata	Verify integrity of live processes by comparing code in memory to that of corresponding static binaries, specifically checking for jumps and other instructions that redirect code flow.

# MITRE ATT&CK jako základ pro model hrozeb

- Možnost přímočarého mapování relevantních hrozeb:
  - Jaké skupiny škodlivých aktérů a jaké nástroje jsou pro nás relevantní?
  - S jakými (sub)technikami jsou spojené?
- Nezbytný alespoň elementární CTI program



# MITRE ATT&CK Navigator – modelování hrozeb

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Denial of Service		Device Restart/Shutdown		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Manipulate I/O Image		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Modify Alarm Settings		Loss of View
Supply Chain Compromise							Screen Capture		Rootkit		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Service Stop		Manipulation of View
Wireless Compromise									System Firmware		Theft of Operational Information

## MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#) [changelog](#) [theme ▾](#)

### Create New Layer

Create a new empty layer



Enterprise

Mobile

ICS

More Options



### Open Existing Layer

Load a layer from your computer or a URL



### Create Layer from other layers

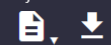
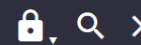
Choose layers to inherit properties from



### Create Customized Navigator

Create a hyperlink to a customized ATT&CK Navigator



**Initial Access**

12 techniques

**Execution**

9 techniques

**Persistence**

6 techniques

**Privilege Escalation**

2 techniques

**Evasion**

6 techniques

**Discovery**

5 techniques

**Lateral Movement**

7 techniques

**Collection**

11 techniques

**Command and Control**

3 techniques

**Inhibit Response Function**

14 techniques

**Impair Process Control**

5 techniques

**Impact**

12 techniques

Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware	Project File Infection	Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts	Rootkit	SpooF Reporting Message	Wireless Sniffing	Program Download	Detect Operating Mode	Block Serial COM	Loss of Control	Unauthorized Command Message	Loss of Productivity and Revenue
Remote Services	Modify Controller Tasking					Remote Services	I/O Image	Change Credential	Data Destruction		Loss of Protection
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State	Denial of Service	Denial of Service		Loss of Safety
Rogue Master	Scripting						Point & Tag Identification	Device Restart/Shutdown	Manipulate I/O Image		Loss of View
Spearphishing Attachment	User Execution						Program Upload	Modify Alarm Settings	Rootkit		Manipulation of Control
Supply Chain Compromise							Screen Capture	Service Stop	Service Stop		Manipulation of View
Transient Cyber Asset							Wireless Sniffing	System Firmware	System Firmware		Theft of Operational Information
Wireless Compromise											



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware	Indicator Removal on Host	Indicador Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection	Masquerading	Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware	Rootkit	Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Native API	Valid Accounts	Spoof Reporting Message	Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Scripting					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	User Execution						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment							Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Search

score 1

Search Settings

name  ATT&CK ID  description  data sources

Techniques (81)

select all      deselect all

Activate Firmware Update Mode	<a href="#">view</a>	select	deselect
Adversary-in-the-Middle	<a href="#">view</a>	select	deselect
Alarm Suppression	<a href="#">view</a>	select	deselect
Automated Collection	<a href="#">view</a>	select	deselect
Block Command Message	<a href="#">view</a>	select	deselect

Threat Groups (13)

select all      deselect all

Lazarus Group	<a href="#">view</a>	select	deselect
OilRig	<a href="#">view</a>	select	deselect
Sandworm Team	<a href="#">view</a>	select	deselect
TEMP.Veles	<a href="#">view</a>	select	deselect
Wizard Spider	<a href="#">view</a>	select	deselect

layer × layer1 × +

selection controls layer controls technique controls

Search Settings  name  ATT&CK ID  description score 1

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware	Indicator Removal on Host	Masquerading	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection				Remote System Information Discovery	Lateral Tool Transfer	Data from Local System	Block Reporting Message	SpooF Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware	SpooF Reporting Message	Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode	Change Credential	Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts				Remote Services	I/O Image	Data Destruction	Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State	Denial of Service	Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification	Device Restart/Shutdown	Data Destruction		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload	Manipulate I/O Image	Denial of Service		Loss of View
Supply Chain Compromise							Screen Capture	Modify Alarm Settings	Denial of Service		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing	Rootkit	Denial of Service		Manipulation of View
Wireless Compromise								Service Stop	Service Stop		Theft of Operational Information
								System Firmware	System Firmware		

### Techniques (81)

select all    deselect all

Activate Firmware Update Mode	<a href="#">view</a>	select	deselect
Adversary-in-the-Middle	<a href="#">view</a>	select	deselect
Alarm Suppression	<a href="#">view</a>	select	deselect
Automated Collection	<a href="#">view</a>	select	deselect
Block Command Message	<a href="#">view</a>	select	deselect

### Threat Groups (13)

### Software (21)

select all    deselect all

Industroyer	<a href="#">view</a>	select	deselect
Industroyer2	<a href="#">view</a>	select	deselect
KillDisk	<a href="#">view</a>	select	deselect
LockerGoga	<a href="#">view</a>	select	deselect
NotData	<a href="#">view</a>	select	deselect

### Mitigations (52)

### Campaigns (3)

MITRE ATT&CK® Navigator v4.8.1

legend

## MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

[help](#)[changelog](#)[theme](#) ▾

Create New Layer

Create a new empty layer



Open Existing Layer

Load a layer from your computer or a URL



Create Layer from other layers

Choose layers to inherit properties from



domain \*

ICS ATT&CK v13



Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.

score expression

a + b

Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found [here](#). Leave blank to initialize scores to 0. Here's a list of available layer variables:

- **a** (layer)
- **b** (layer1)

gradient



Choose which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring



Choose which layer to import manually assigned colors from. Leave blank to initialize with no colors.



layer by operation											
Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware	Indicator Removal on Host	Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System	Detect Operating Mode	Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware	Rootkit	Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts	Spoof Reporting Message	Rootkit	Wireless Sniffing	Remote Services	Monitor Process State	Change Credential	Data Destruction	Loss of Productivity and Revenue	
Replication Through Removable Media	Native API			Spoof Reporting Message		Valid Accounts	Point & Tag Identification	Data Destruction	Denial of Service	Loss of Protection	
Rogue Master	Scripting						Program Upload	Device Restart/Shutdown	Manipulate I/O Image	Loss of Safety	
Spearphishing Attachment	User Execution						Screen Capture	Modify Alarm Settings	Rootkit	Loss of View	
Supply Chain Compromise							Wireless Sniffing	Service Stop	System Firmware	Manipulation of Control	
Transient Cyber Asset								System Firmware		Manipulation of View	
Wireless Compromise										Theft of Operational Information	

# MITRE ATT&CK ICS – postup modelování hrozeb

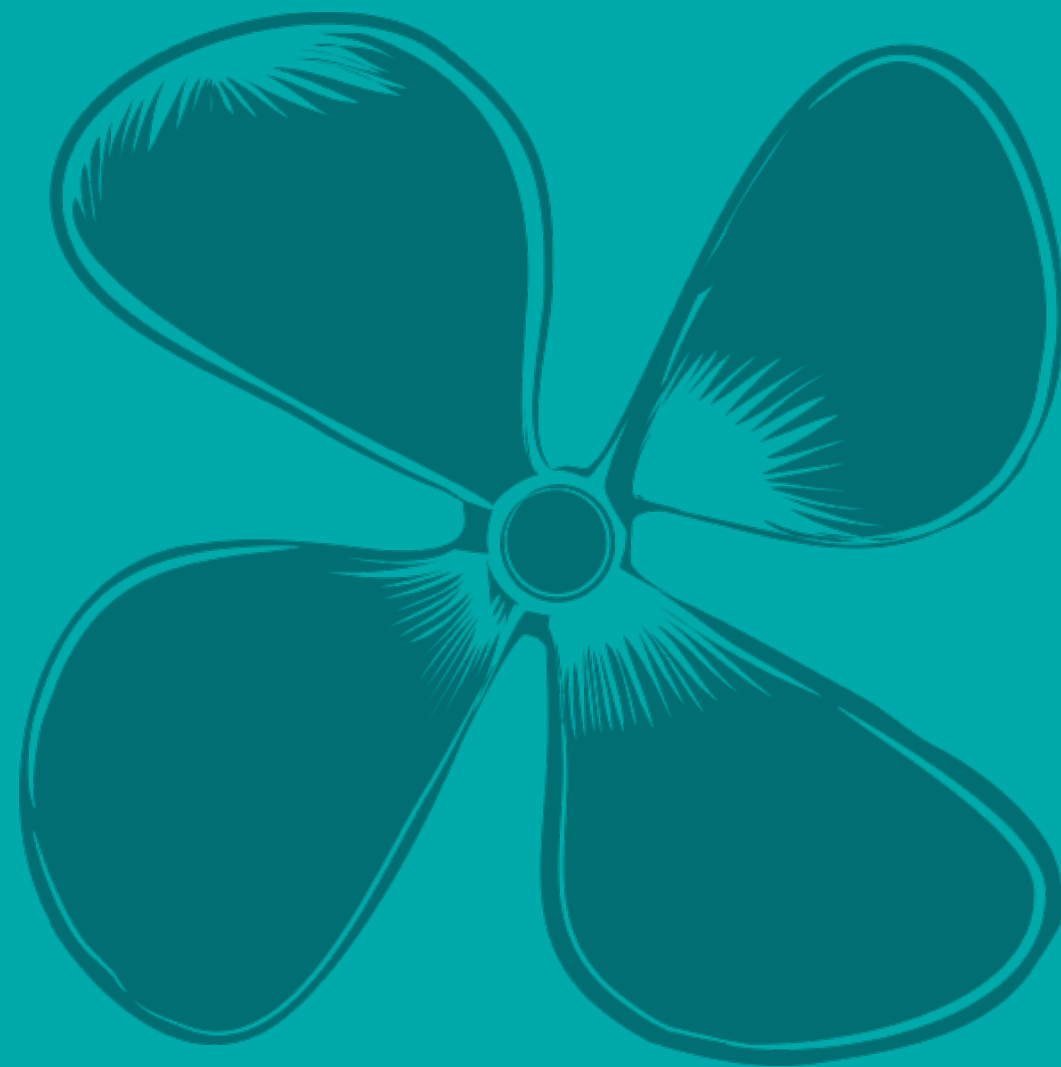
1. Stanovení rozsahu prostředí
2. Identifikace relevantních škodlivých aktérů a nástrojů
3. Identifikace relevantních technik
4. Mapování technik na MITRE ATT&CK v nástroji Navigator
5. Prioritizace relevantních technik
6. Zmapování pokrytí modelu existujícími opatřeními
7. Identifikace opatření pro pokrytí prozatím nepokrytých (sub)technik

# Co říci na závěr?

- Přínosy modelování hrozeb při vývoji i ochraně průmyslových a specifických systémů (případně SoS) jsou neoddiskutovatelné
- Vycházení z tradičních „katalogů hrozeb“ je přinejmenším nevhodné
- Využívání metodik a postupů určených původně pro IT, vývoj softwaru, či jiné průmyslové/specifické oblasti může být v případě konkrétních OT systémů pro zajištění bezpečnosti relativně zajímavé

**ALEF**

**Prostor pro Vaše  
dotazy**



**A ALEF**

**Děkuji Vám za  
pozornost**

