When 21434 and R155 ATT&CK™

Matt Mackay, GM

Agenda

ISO/SAE 21434 - **Road vehicles — Cyber Engineering**

UNECE WP.29/R155

- Compliance overview
- CSMS – Risk Focus
- 21434 dependence

21434 & Risk Assessment

Mitre ATT&CK™

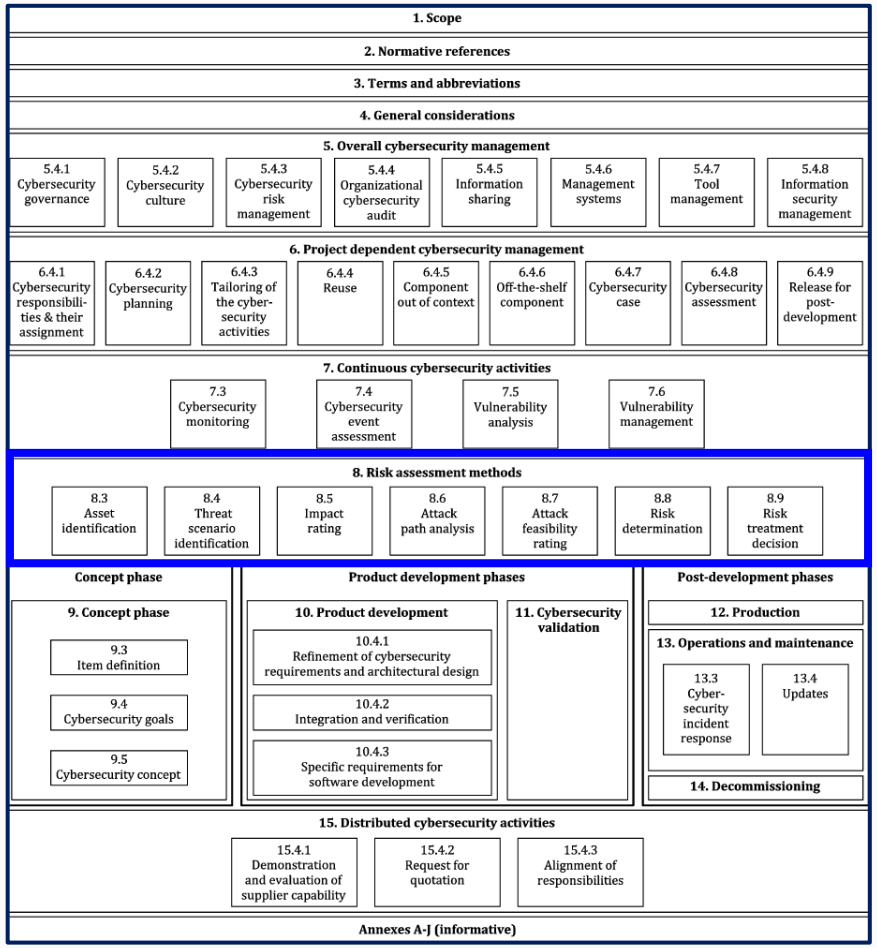
- Putting it all Together

ISO/SAE 21434

Road Vehicles – Cybersecurity Engineering

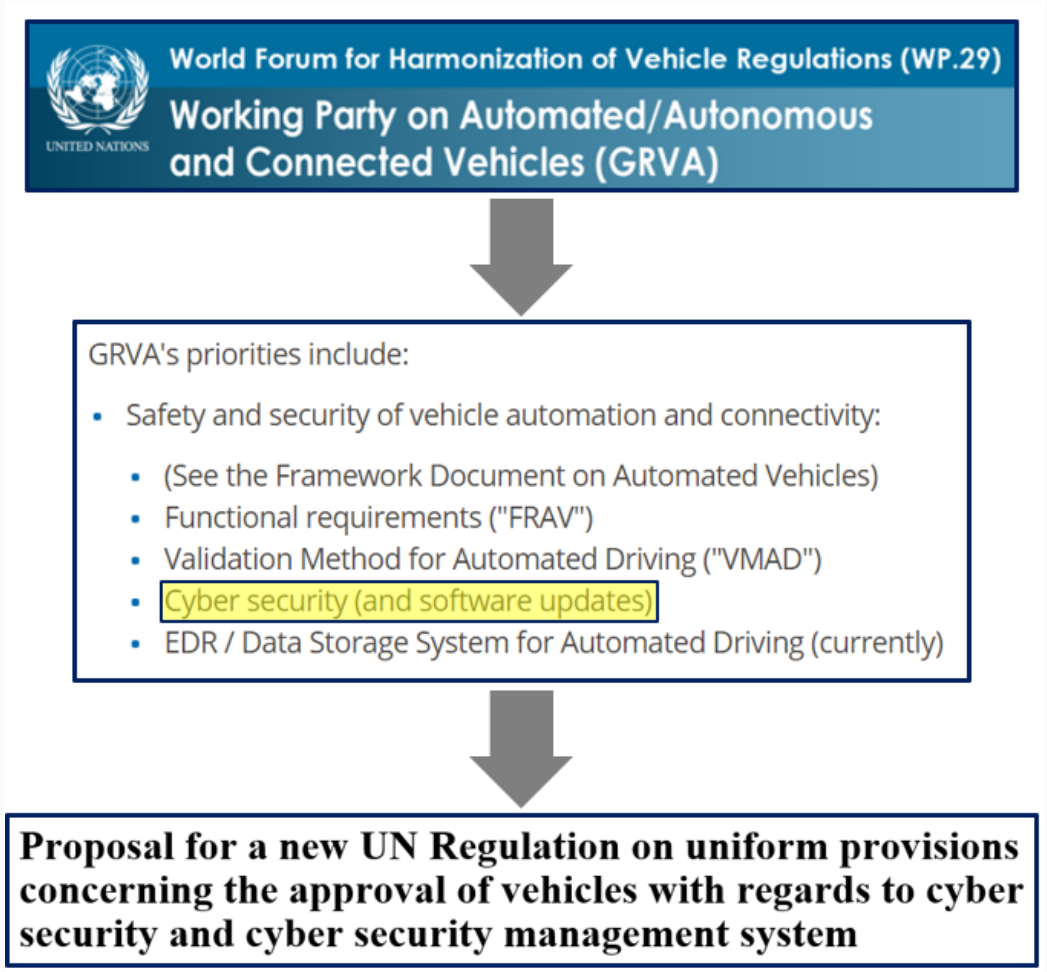
21434 purpose & scope

- Address the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles
  - Provide vocabulary, objectives, requirements and guidelines as a foundation for common understanding throughout the supply chain. This enables organizations to:
    - Define cybersecurity policies and processes;
    - Manage cybersecurity risk; and
    - Foster a cybersecurity culture.



UNECE WP.29/R155

“Wait…did someone say cybersecurity type approval?”



R155 Compliance Overview – CSMS Focus

1. Collect documentation that attest to section ***7.2 Requirements for the Cyber Security Management System***
2. Submit CSMS Certificate of Compliance application per ***6.2*** to include:
    a. The aforementioned documentation from 1. above
    b. Appendix I to Annex I Manufacturer's Declaration of Compliance for CSMS
3. Receive CSMS Certification of Compliance (formatted per ***Annex 4***)
4. Submit application for vehicle type approval per section ***3. Application for Approval***. Include:
    a. Completed ***Annex 1***
    b. Information that supports ***7.3 Requirements for Vehicle Types***
    c. The CSMS Certificate of Compliance from 3. above

CSMS – Risk Focus

7.2.2.2. The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:

(a) The processes used within the manufacturer's organization to manage cyber security;

(b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;

(c) The processes used for the assessment, categorization and treatment of the risks identified;

(d) The processes in place to verify that the risks identified are appropriately managed;

(e) The processes used for testing the cyber security of a vehicle type;

(f) The processes used for ensuring that the risk assessment is kept current;

(g) The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

(h) The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.

R155 & 21434 – Twinning!

- **R155**: "Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.

- **21434**: “The purpose of the cybersecurity case is to provide a clear, comprehensible and defensible rationale, supported by evidence and documentation, that an item or component achieves a sufficient degree of cybersecurity for a specific application in a specific environment.”

R155 ←→ 21434

- WP.29 Draft Interpretation Document
  - Lists attestation examples
  - Maps requirements to 21434
    - Annex is dedicated to 21434 mapping
- ISO/PAS 5112 *Road vehicles — Guidelines for Auditing Cybersecurity Engineering* development in progress
  - 21434 a safe attestation option

Link with ISO/SAE 21434 DIS (E)	
Sub-Category	**Clauses from ISO/SAE 21434 DIS**
7.2.1 For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.	
Verify that a Cybersecurity Management System is in place	*Not applicable*
7.2.2.1 The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases: - **Development phase;** - **Production phase;** - **Post-production phase.**	
Development phase	Clauses 9, 10,11
Production phase	Clause 12
Post-production phase	Clauses 7, 13, 14
7.2.2.2 (a) The processes used within the manufacturer's organization to manage cyber security	
Organization-wide cyber security policy	[RQ-05-01], [RQ-05-03]
Management of cyber security relevant processes	[RQ-05-02], [RQ-05-09]
(a3) Establishment and Maintenance of cyber security culture and awareness	[RQ-05-07]. [RQ-05-08]
7.2.2.2 (b) The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.	
(b1) Process for identifying cyber security risks to vehicle types established across development, production, and post-production	[RQ-08-01]. [RQ-08-02], [RQ-08-03], [RQ-08-08], [RQ-08-09], The threats in *Annex 5 of the UNECE document, part 5* are out of scope of ISO/SAE 21434
7.2.2.2 (c) The processes used for the assessment, categorization and treatment of the risks identified	
(c1) Is a process established to assess and categorize cyber security risks for vehicle types across development, production and post-production?	[RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10]

21434 & Risk Assessment

ISO/SAE 21434 – Risk Assessment

RISK ASSESSMENT CONCEPT

Risk Determination (see 8.8): The determination of the risk value of a threat scenario.

3.1.31 THREAT SCENARIO

Statement of potential negative actions that lead to a *damage scenario* (3.1.18).

3.1.18 DAMAGE SCENARIO

Adverse consequence or undesirable result due to the compromise of a *cybersecurity property* (3.1.16) (or properties) of an *asset* (3.1.1), or of a group of *assets*.

RISK ASSESSMENT EXECUTION

Attack Path Analysis (see 8.6): Identification and linking of potential attack paths to one or more threat scenarios.

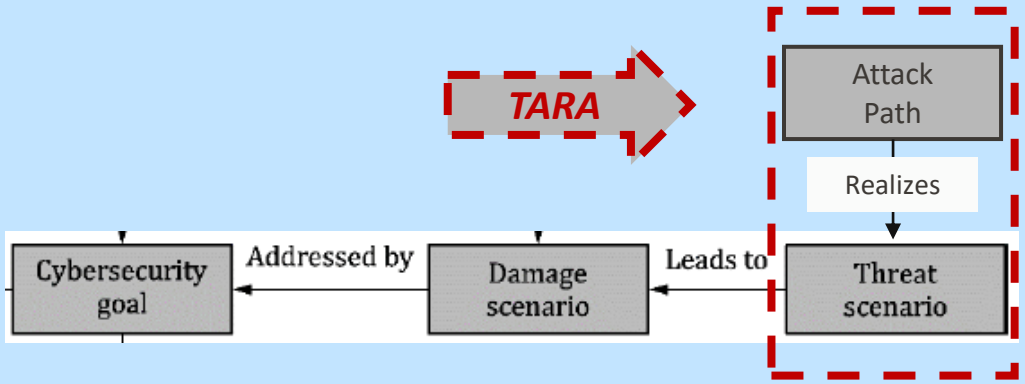
NOTE 4: Attack paths form the basis for the assessment of attack feasibility. They are also used for the refinement of cybersecurity goals to cybersecurity requirements and to support the selection of appropriate controls.

[RQ-08-08] The threat scenarios shall be analyzed to describe possible attack paths.

* NOTE 4: In the early stages of product development the attack paths are often incomplete or imprecise as specific implementation details are not yet known in sufficient detail to be able to identify specific vulnerabilities. During the lifecycle, the attack paths could be updated with additional detail as more information becomes available (e.g., after a vulnerability analysis).

*

RISK ASSESSMENT SUMMARY



***** Need automotive adversarial attack model***

MITRE ATT&CK™

Auto Threat Matrix (ATM)

- MITRE ATT&CK™ Framework
  - Global knowledge base
    - ***Known & vetted attacks***
    - Techniques
    - Mitigations
  - Existing Domains
    - Enterprise
    - Mobile
    - ICS
  - Future Domain
    - Automotive

Inspired by => MITRE | ATT&CK®

general motors

Enterprise Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

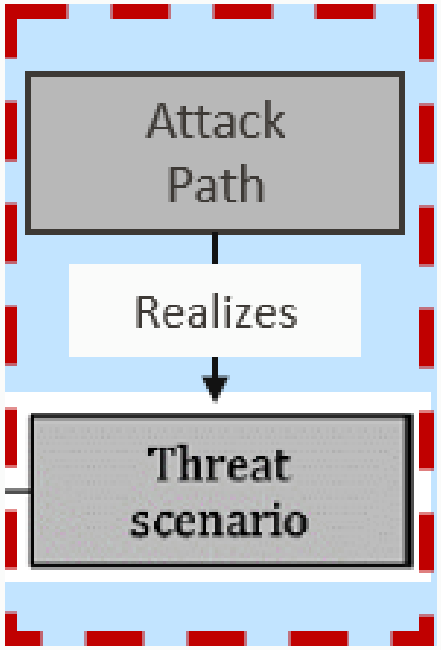
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Bash History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and Distributed COM	Data from Cloud Storage Object	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Bypass User Account Control	Credential Dumping	Cloud Service Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	Clear Command History	Credentials from Web Browsers	Domain Trust Discovery	Internal Spearphishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Code Signing	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compile After Delivery	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data Staged	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Email Collection	Fallback Channels	Transfer Data to Cloud Account	Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Input Capture	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Man in the Browser	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Connection Proxy	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Screen Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Video Capture	Multilayer Encryption		Stored Data Manipulation

Manipulate environment	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control	Exfiltration	Affect vehicle function	Impact
Downgrade to insecure protocols	Aftermarket, customer, or dealer equipment	Command and scripting interpreter	Abuse UDS for persistence	Abuse elevation control mechanism	Bypass code signing	Android intent hijacking	File and directory discovery	Abuse UDS for lateral movement	Abuse UDS for collection	Aftermarket, customer, or dealer equipment	Aftermarket, customer, or dealer equipment	Abuse UDS for affecting vehicle function	Damage to property
Jamming or denial of service	Browser compromise	Command-line interface	Disable software update	Exploit co-located computing device for privilege escalation	Disable firewall	Capture SMS message	Location tracking	Bridge vehicle networks	Access personal information	Bidirectional communication	Bidirectional communication	CAN bus denial of service	Denial of control
Manipulate communication	Exploit via radio interface	Native API	Modify OS kernel or boot partition	Exploit OS vulnerability	Bypass UDS security access	Exploit TEE vulnerability	Network service scanning	Exploit ECU for lateral movement	Access vehicle telemetry	Cellular communication	Cellular communication	Local function	Loss of availability
Measure and manipulation	Exploit via removable media		Modify system partition	Exploit TEE vulnerability	Bypass mandatory access control	Input capture	Process discovery	Remote services	Capture camera or audio	Covert command and control channels	Covert command and control channels	Modify bus message	Loss of control
Pre-transducer transduction attack	Malicious app		Modify TEE	Hardware fault injection		Input prompt	Software discovery	Reprogram ECU for lateral movement	Capture SMS message	Internet communication	Internet communication	Unintended vehicle network message	Loss of safety
Post-transducer EMI attack	Physical modification			Process injection		Network traffic capture or redirection	System information discovery		Data from local system	Receive-only communication channel	Removable media		Manipulation of control
Relay communications	Supply chain compromise			Reprogram co-located computing device for privilege escalation		OS credential dumping	System network configuration discovery		Input capture	Short range wireless communication	Short range wireless communication		Unauthorized access to personal information
Rogue cellular base station						Unsecured credentials	System network connections discovery		Location tracking	Standard cryptographic protocol	Standard cryptographic protocol		Vehicle or content theft
Rogue Wi-Fi access point									Network information discovery		Transmit-only communication channel		
									Network traffic capture or redirection				
									Screen capture				

Proposed Use

- Instrument ATM to derive inherent/residual risk
- Risk determination:

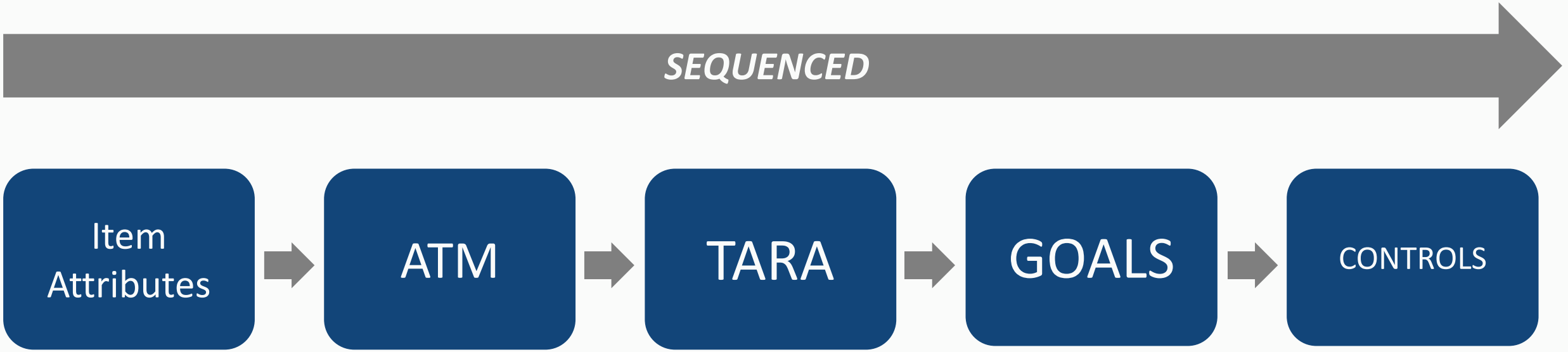
[RQ-08-08] The threat scenarios shall be analyzed to describe possible attack paths.



Realizes

Worst-Outcome Scenario	Cost	Skill	Locality	Scalability	Impact	Risk Index
Sequence{GM-ECU My1803 – Unauthenticated root SSH session, Develop exploit to Access Shared Memory, Send Arbitrary CAN Messages}	5	3	2	5	5	83
Sequence{GM-ECU My1804 – Multiple Command Injections in ksvc_swupdate service, Develop exploit to Access Shared Memory, Send Arbitrary CAN Messages}	5	2	3	5	5	83
Sequence{GM-ECU My1809 – Unauthenticated control over Audio}	5	5	2	5	2	66
Sequence{GM-ECU My1810 – Wireless Passwords Leaked in logs}	5	5	2	3	3	62
					Maximum Risk	83

Putting it all together



- *Collect component attributes*
- *Identify attack paths*
- *Perform initial risk assessment*
- *Assign appropriate goals*
- *Assign appropriate controls*


general motors