Corso Professionalizzante di Specializzazione (3 CFU)
Ingegneria delle Telecomunicazioni, Ingegneria Informatica,
Ingegneria dei Sistemi di Controllo e dell'Automazione,
Informatica

WSN and VANET Security

Part I: Security Analysis

Lecture I.1

Security Management

Ing. Marco Pugliese, Ph.D., SMIEEE
Senior Security Manager UNI 10459-2017 ICMQ cert. 25-00238
marco.pugliese@univaq.it
April 4th, 2025

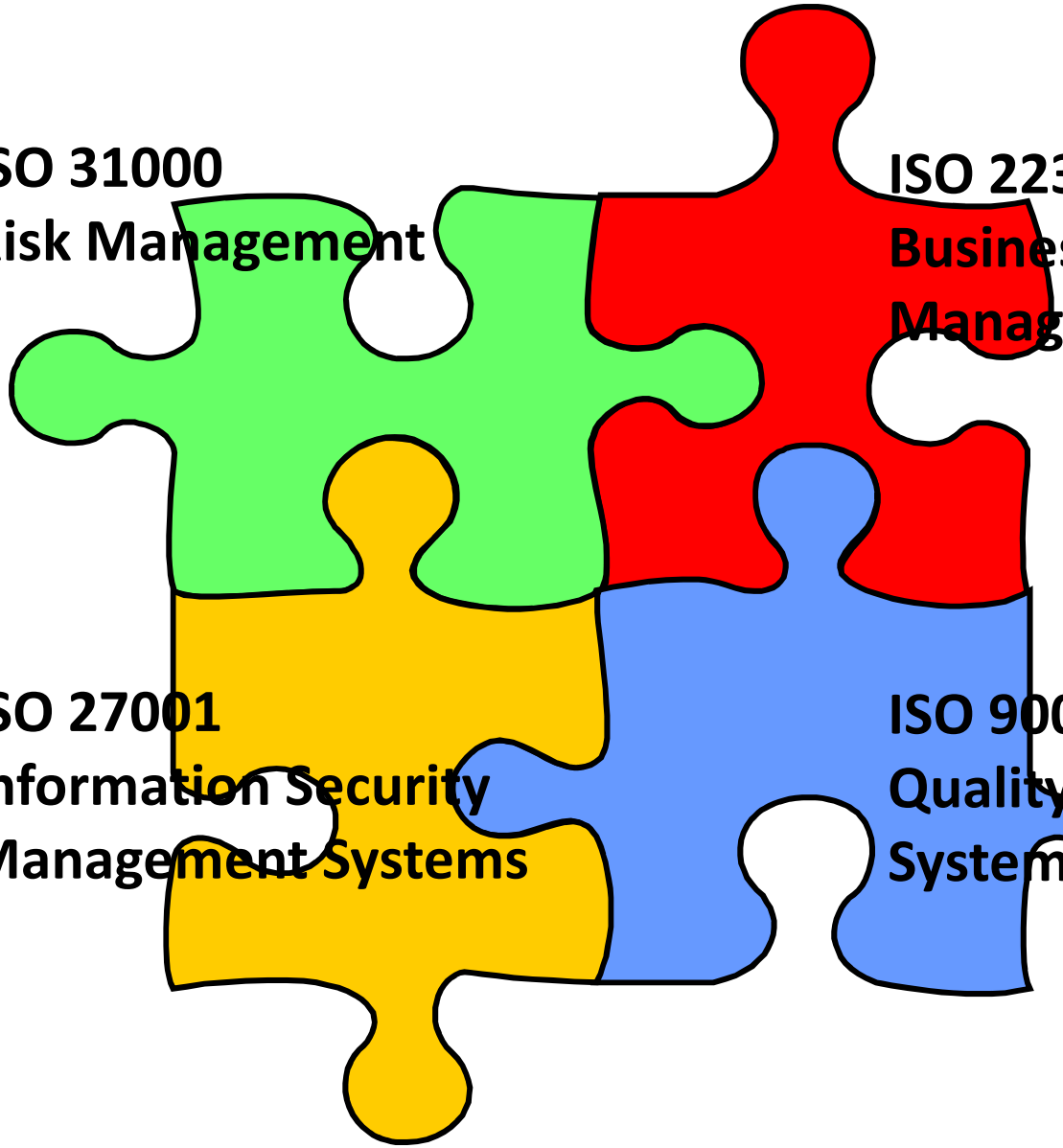
Outline

- The framework of Security Management
- From Risk to Security Management
  - Security Management Process
  - Approaches for Risk Evaluation
  - Techniques for Risk Evaluation
  - P-I Matrix and isorisk curves
  - FTA - CVSS
  - NIST SP 800-30 Guide for Conducting a Risk Assessment
- Security management in the automotive domain
  - ISO / SAE 21434
  - Threat Analysis and Risk Assessment (TARA)
  - Cybersecurity Risk Quantification technique: EVITA
  - Guide line for TARA execution using EVITA
- Reference Cyber Security functions
  - Security metrics
  - Timing constraints
  - Cyber Risk Mitigation

Outline

- The framework of Security Management
- From Risk to Security Management
  - Security Management Process
  - Approaches for Risk Evaluation
  - Techniques for Risk Evaluation
  - P-I Matrix and isorisk curves
  - FTA - CVSS
  - NIST SP 800-30 Guide for Conducting a Risk Assessment
- Security management in the automotive domain
  - ISO / SAE 21434
  - Threat Analysis and Risk Assessment (TARA)
  - Cybersecurity Risk Quantification technique: EVITA
  - Guide line for TARA execution using EVITA
- Reference Cyber Security functions
  - Security metrics
  - Timing constraints
  - Cyber Risk Mitigation

The framework of Security Management



ISO 31000
Risk Management

ISO 22301
Business Continuity
Management Systems

ISO 27001
Information Security
Management Systems

ISO 9001
Quality Management
Systems Requirements

From Risk to Security Management

- **Risk** is defined as the "***effect of uncertainty on objectives***" (ISO 31000:2018).
  - An **effect** is a deviation from the expected positive and / or negative.
  - **Objectives** can have different aspects (financial, health, safety, environmental) and can apply at different levels (strategic, organization-wide, project, product, process).
  - Risk is characterized by reference to potential events.
- **Risk Management** are the "*coordinated activities to direct and control an organization with regard to risk*" (ISO 31000:2018).
- **Risk Magnitude:** the estimated value of a risk.
- **Acceptable Risk:** risk correspondent to the acceptable damage ("TO BE" risk).
- **Inherent Risk:** risk magnitude before treatment ("AS IS" risk).

The generic Risk Management Process instance is the following:

- **Risk Assessment**
  - **Risk Identification**: process of finding, recognizing and describing risks
  - **Risk Analysis**: process of comprehending the nature of risk
  - **Risk Evaluation**: process of estimation of risk magnitude to determine whether the risk magnitude is acceptable.
- **Risk Treatment**: process to reduce risks if not acceptable.

From Risk to Security Management

W. E. Deming (1900-1993) cycle or PDCA (Plan-Do-Check-Act) cycle is an operational tool at the base of any finalized management system to the control and continuous improvement of production processes.

- **PLAN - context analysis; definition of security objectives; planning / scheduling of security activities; identification and assessment of the risks to which the resources are exposed; definition of the management of options applicable to residual risk after the application of the reduction measures.**
- **DO - implementation of what was established in the planning phase; implementation of physical, logical and organizational measures.**
- **CHECK - comparison between what emerged in the DO phase and what was established in the PLAN phase through periodic audits, monitoring the effectiveness of the measures, new context analysis to identify any changes.**
- **ACT - standardization of the process (maintenance and improvement) if no inefficiencies have been found; corrective actions focused on the elements of the process that gave rise to the differences between the expected results and those obtained, and therefore in case of inefficiencies.**

From Risk to Security Management

- A **threat** is the potential that an **attack** is engaged by an **attacker** or an accident / natural event occurs, which can insist on an …
- … **exposure** intended as a measurable quantity of tangible or intangible asset potentially subject to damage and exploits, or makes use of the weakness, of one or more **…**
- … **vulnerability** of the organization / system inducing the generation of a ...
- … **damage** / degrade or partially destroy of the organization / system.
- A risk is not a threat but a threat can turn into risk if no **mitigation measures** are taken
- A **mitigation measure** is a technical / organizative / procedural reaction applied to the organization / system to mitigate the risk by reducing the prability of its occurrence or by reducing the damage corresponding to its occurrence:
  - **Preventive measures**: to reduce the probability of risk occurrence.
    - **Passive Preventive:** when mitigation is reached by **delaying the effects** without feedbacks coming from the organization / system.
    - **Active Preventive:** when mitigation is reached by **intervening on the causes** exploiting feedbacks coming from the organization / system.
  - **Protective measures**: to reduce the damage in case of risk occurrence.

From Risk to Security Management

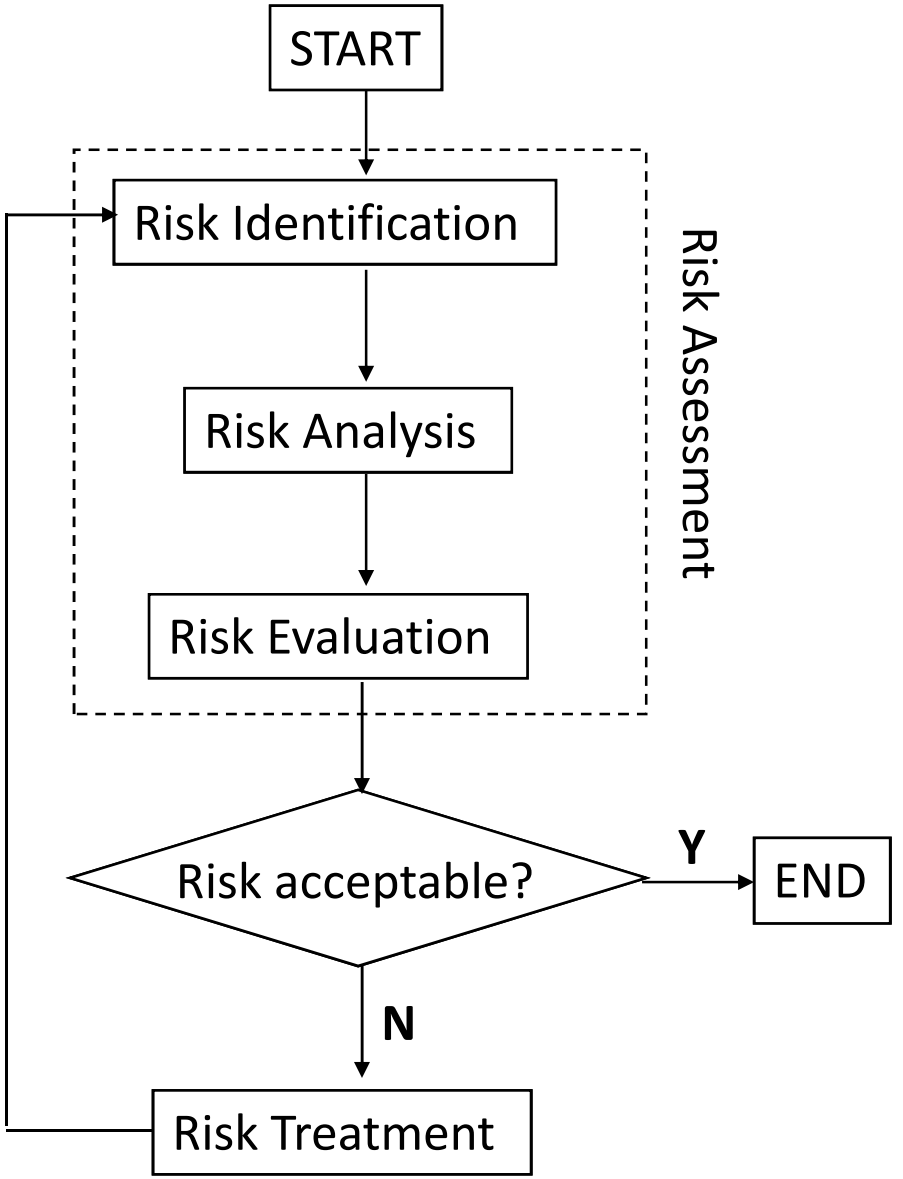
- **Risk Evaluation (by magnitude):**

$$R = P \times I$$

R = Risk
P = Probability
I = Impact (Damage)

- Therefore **risk is operatively defined as an economical damage (if negative) or an economical revenue (if positive) weighted by the probability of the occurrence of the damage / revenue**.

- **Always R > 0**: R=0 if P=0 (but P=0 means no cause or risk!) or if I=0 (but a risk produces effects by definition): therefore never R=0 and always P > 0 and I > 0 (q.e.d.)



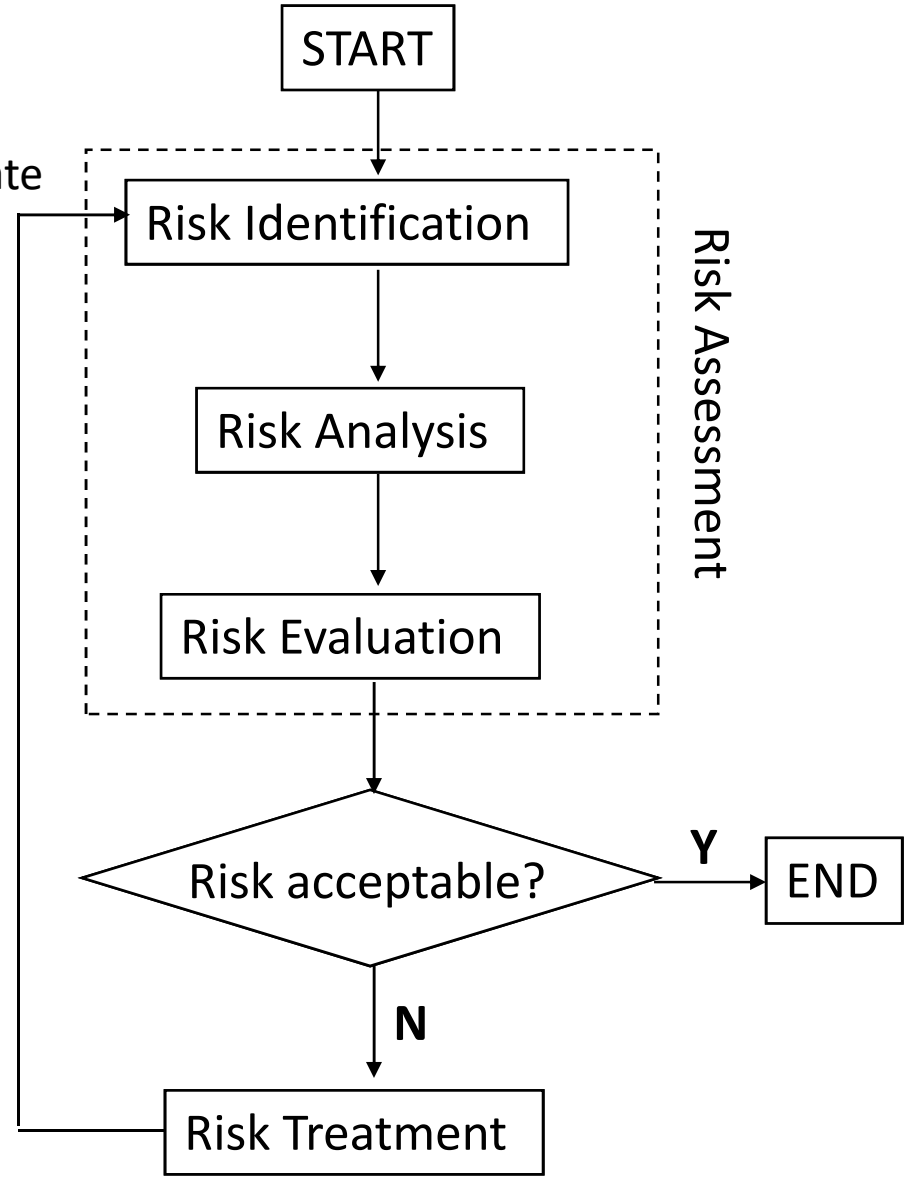
From Risk to Security Management

- **Risk Evaluation (by magnitude):**

$$P = f(V, F, E, \ldots)$$

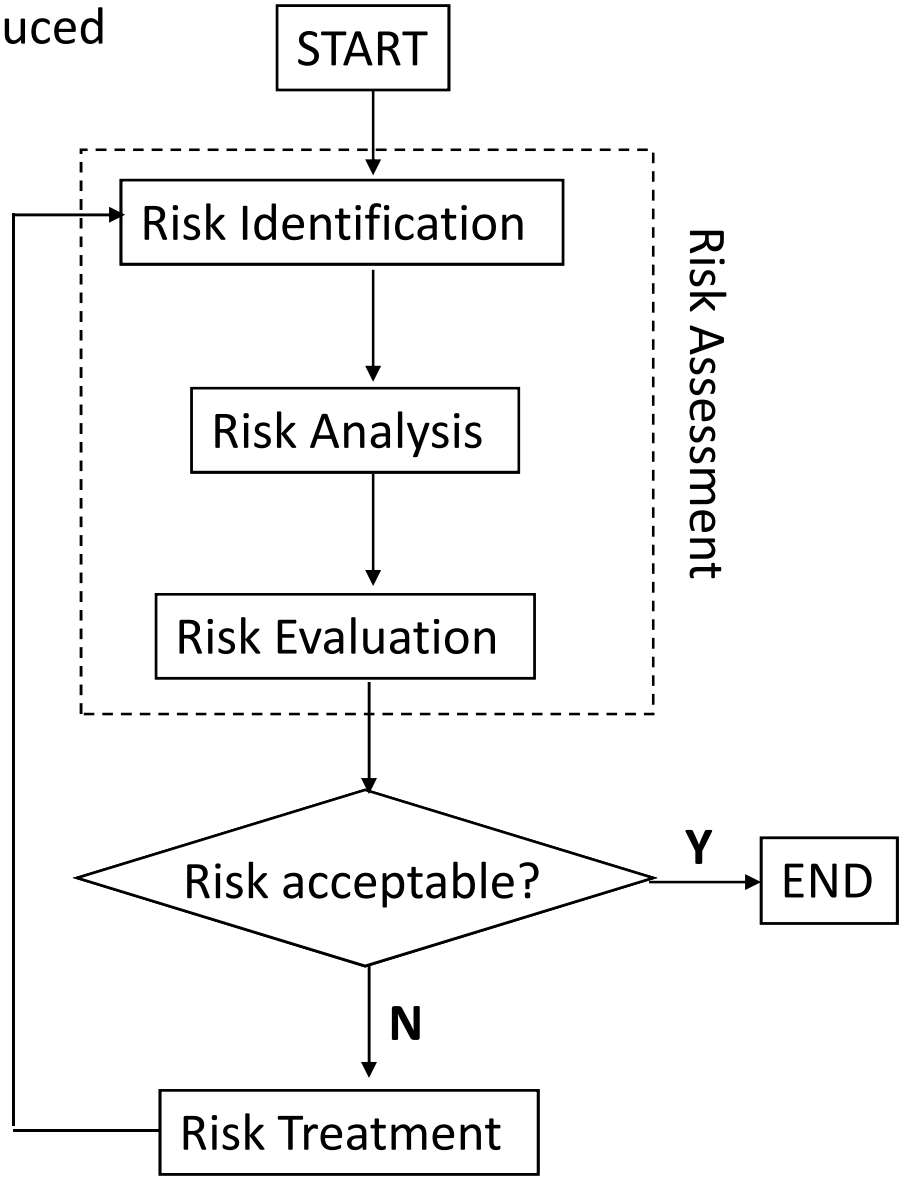
V = Vulnerability
F = past risk occurrence rate
E = Exposure

- Specific expressions for P depend on the class / typology of system (e.g. ICT system, OT system, production chain, …)
- The estimation of risk probability is an hard task: quantitative / semi-quantitative methods are mainly used.
- A central item for P estimation are the vulnerabilities that can be exploited by attackers (system exposure)
- Three classes of vulnerabilities
  - Procedural (V_P)
  - Technological (V_T)
  - Human factor (V_H)



From Risk to Security Management

- **Risk Treatment (or mitigation)**: risk is reduced according to specific measures.
- Here we focus only on mitigation measures to reduce V_T but V_P and V_H should be reduced too, otherwise the overall exposure to attack remains high.
- The majority of vulnerabilities can be reduced through the application of **security measures.**
- Two classes of security measures:
  - **Passive Preventive: "mitigation by delaying the effects (without feedbacks)"**
    - Physical: e.g. **Hardware tamper proof protection**
    - Logical: e.g. **Cryptography**
  - **Active Preventive: "mitigation by intervening on the causes (with feedbacks)"**
    - Physical : e.g. **E.M. Analysis, Static / Dynamic Power Analysis**
    - Logical: e.g. **Intrusion Detection**

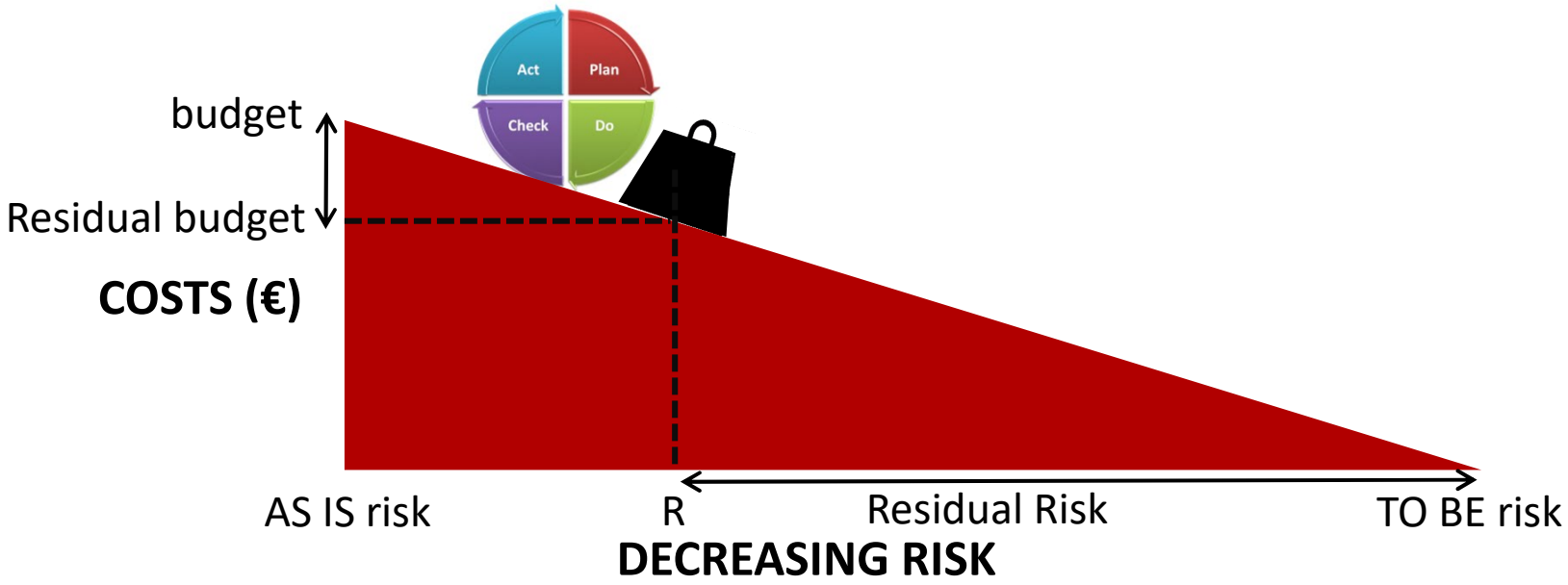


Security Management Process

- **Acceptable Risk:** risk correspondent to an acceptable damage ("TO BE" risk).
- **Inherent Risk:** risk magnitude before treatment ("AS IS" risk).

  At t=0 (PLAN-DO) usually is "AS IS" risk > "TO BE" risk, therefore mitigation starts (CHECK-ACT). If "AS IS" risk ≤ "TO BE" risk no mitigations are applied (CHECK).
- **Residual Risk** = R (risk value after applying mitigations) - "TO BE" risk.

  At t (PLAN-DO) if R > "TO BE" risk, further mitigations apply (CHECK-ACT). If R ≤ "TO BE" risk no further mitigations are applied (CHECK).
- Budget should be at least enough to make "AS IS" risk ≤ "TO BE" risk. Otherwise: 1) increase "TO-BE" risk or 2) increase budget or 3) transfer Residual Risk.



Security Management Process

1. **Risk Identification:** list of "AS IS" risks according to a WHAT-IF criterium considering the environmental context, the operating and application scenarios, reports from Intelligence services.

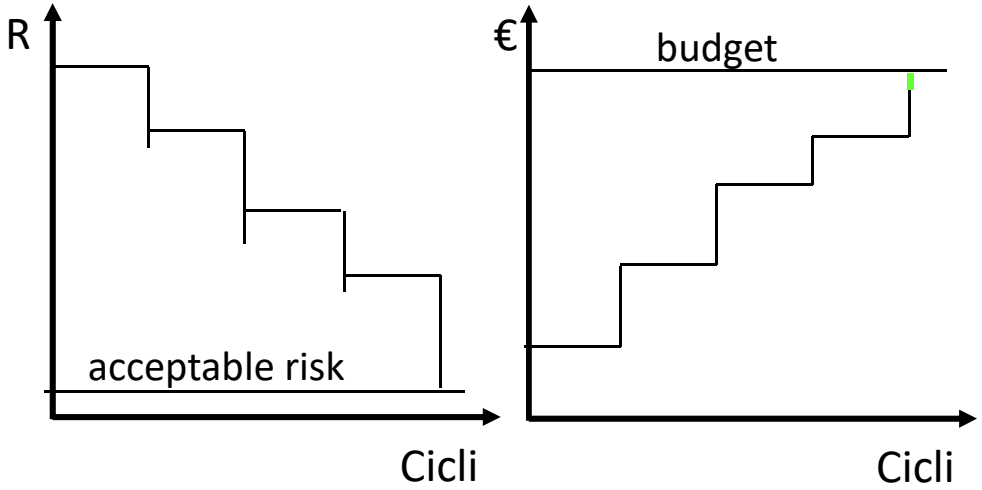
2. **Risk Analysis and Evaluation**: analysis of "AS IS" risks based on the damages suffered by both clients / users in case of risk occurrence evaluated in terms of costs of service outages as well as restoration costs weighted by the probability of risk occurrence.

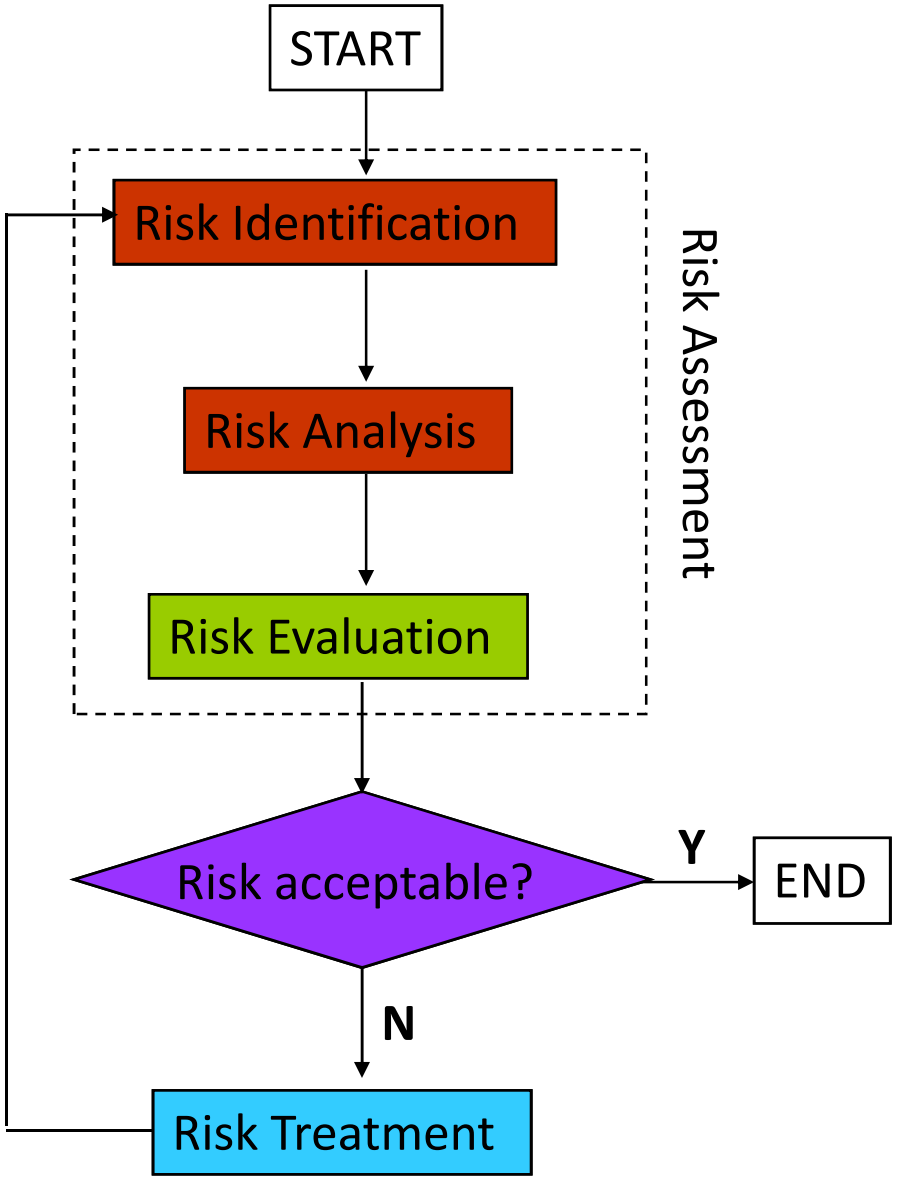
   Probability estimation is an hard task: quantitative / semi-quantitative methods are mainly used.

   - **class of potential attackers**
   - **class of potential attacks**
   - **identified vulnerabilities**

3. **Risk Treatment:** application of passive / active mitigation measures through the security functions (PSF / ASF) finalized at reducing "AS IS" risks at "TO BE" risks. The security level corresponding to the "TO BE" risks defines the **Required Security Level (RSL)** for the system and the **Minimum Security Requirements** for the corresponding mitigation measures PSF / ASF**.**

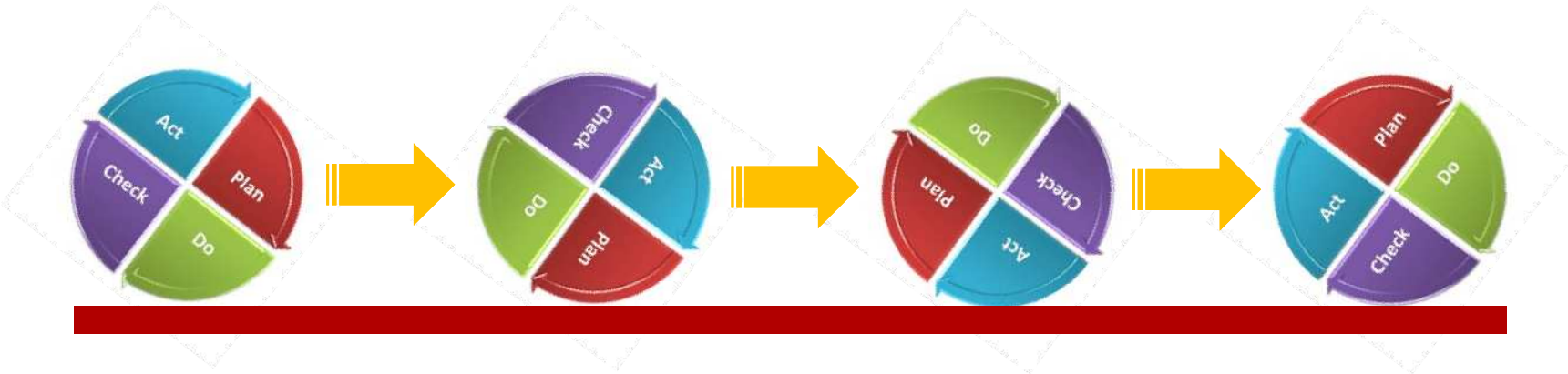
Security Management Process





Security Management Process

- The adoption of state-of-the-art protocols and algorithms compliant to the sector standards and the adoption of the related recommended protection mechanisms implies, by definition, that **"AS IS" risk = "TO BE" risk unless new vulnerabilities should emerge after the release of the standard.**
- Therefore, it is necessary to carry out a continuous cyclical activity of analysis, evaluation and mitigation of emerging risks associated with the provision of services, for example by monitoring the issue of any amendments to the standards applied and proceeding with the appropriate updates of the software and firmware components subsystems that implement countermeasures to new recognized vulnerabilities.



Cyber Risk Quantification Problem

- Cyber Risk Management frameworks exist (e.g. NIST SP 800-30 CSF, ISO/IEC 27005 ISMS, ISO / SAE 21434 TARA) which specify “WHAT we have to do “ but not specify “HOW we have to do”: this defines the Cyber Risk Quantification (CRQ) Problem. Any specific industral sector has agreed to suited and shared techniques to compute CRQ.
- WSN and VANET can be classified as information and communication technologies (ICT systems) enabling operational technologies (OT systems) and IoT (Internet of Things) services because they can be considered as “*the set of hardware and software that detects or causes changes by directly monitoring or controlling an enterprise's physical devices, processes, and events*”.
- IoT frameworks include ACS (Industrial Automation Control Systems) sub-systems as SCADA (Supervisory Control And Data Acquisition), PLC (Programmable Logic Controller)

  OT systems are typically Machine-to-Machine, natively CLOSED, not remotezable, with real time control requirement

  Conversely ICT systems are typically Human-to-Machine, natively OPEN, remotezable, with non real time control requirements

Cyber Risk Quantification Problem

- ICT system protection can coincide with the manteinance at a risk acceptance level of confidentiality, integrity and authentication of data and links (ref. ISO/IEC 27001).
- OT system protection can coincide with the manteinance at a risk acceptance level of safety, reliability, productivity of the production / control chain (ref. IEC 62443)

Cyber Risk Quantification Problem

- **Hence ICT and OT are basically disjoint classes of systems**.

- However the need for management (and therefore control) of "anything" that can be carried out "anywhere" (IIoT) and the optimization of industrial processes (Smart Factory) according to the Industry 4.0 paradigm enabled by 5G, is leading to a **slow, complex (and controversial) convergence process.**

- **Hence, from a cybersecurity point of view, ICT and OT are overlapped**.

- Therefore it appears mandatory the definition of CRQ techniques for integrated ICT-OT systems.

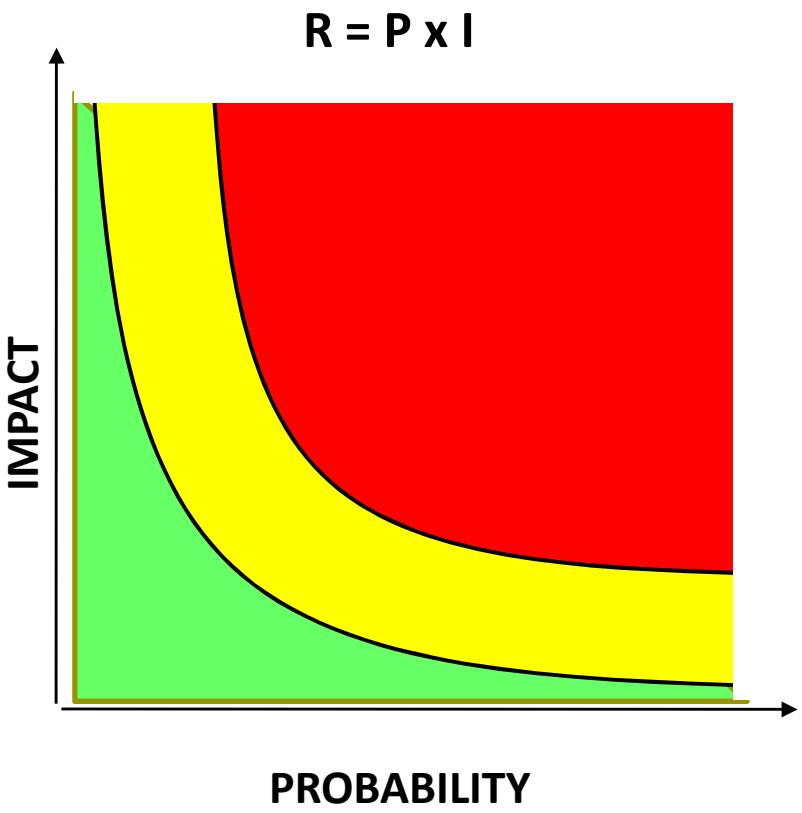
- Three CRQ methods (**pure qualitative, pure quantitative, mixed qualitative-quantitative or semi-quantitative**) can be defined and specific CRQ techniques can be defined and classified according to these methods.

Methods for Cyber Risk Quantification

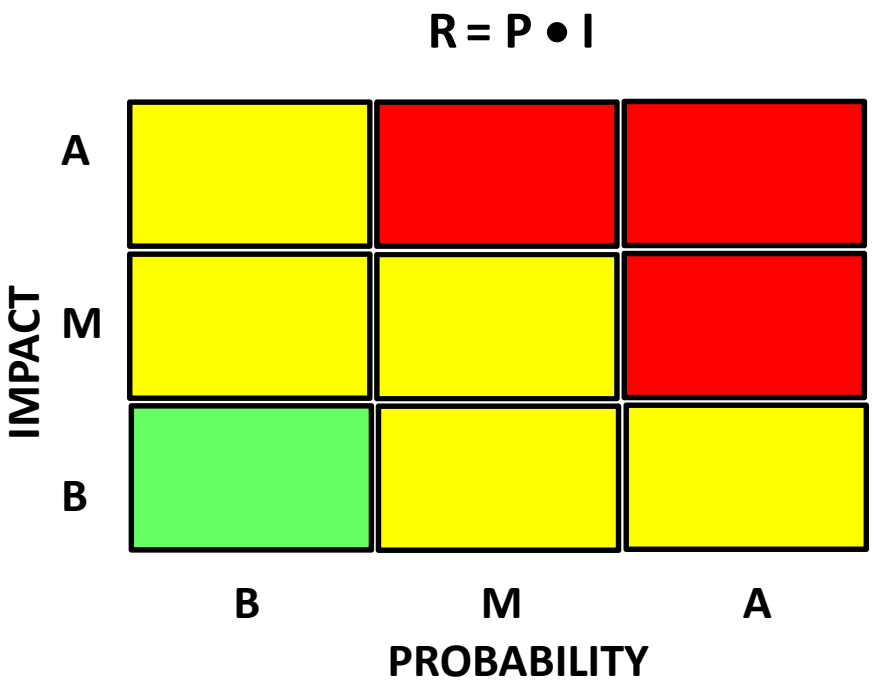
- **Qualitative methods**: based on subjective estimations of the probability of an event where "*la probabilità di un evento è la misura del grado di fiducia che un individuo coerente attribuisce, secondo le sue informazioni e opinioni, all'avverarsi".* (B. De Finetti, Sul significato soggettivo della probabilità, in *Fundamenta Mathematicae*, Warszawa, T. XVII, pp. 298–329, 1931)
- **Quantitative methods**: for any identified risk is possible to write the analytical expression for P=f(…) and the corresponding impact I, hence risk R can be **analytically computed** as R = P x I (a hyperbole on P-I plane).
- **Semi-quantitative methods**: only qualitatitely expression (ranking / score evaluations) for P and I can be written. Ranking for the risk R is computed replacing the formula R = P x I with a risk matrix R = P ● I, where ● is a defined operator between ranks or scores. Two basic approaches:
  - **RANK-BASED**: ranks (usually Low, Medium, High) can be assigned to any parameter concurring in the expression for P and I. Rank for R results from a specific risk matrix (*e.g. NIST SP 800-30 – Information Security – Guide for Conducting Risk Assessments*)
  - **SCORE-BASED**: scores (usually an integer) can be assigned to any parameter concurring in the expression for P and I. Score for R is arithmetically computed by specific algorithms (*e.g. ISO / SAE 21434 Threat Analysis and Risk Assessment*).
- Scores and ranks can be mapped each into the other.

P-I Matrix and Iso-Risk Curves

Quantitative methods



Semi-quantitative methods

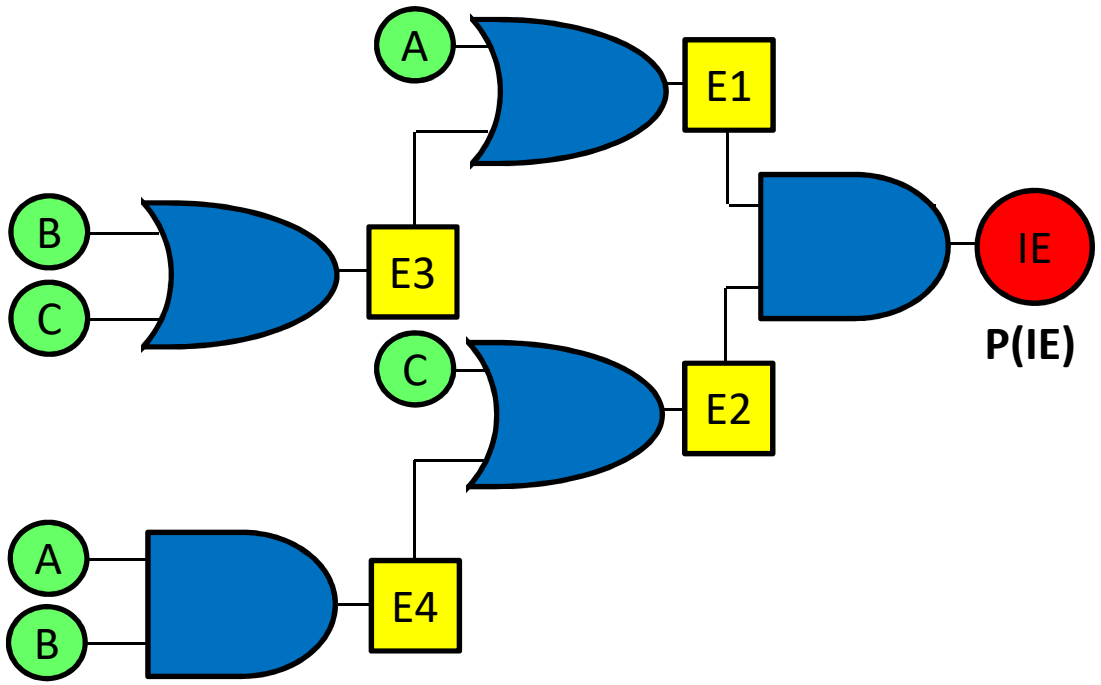


Techniques for Risk Likehood Estimation

- **Fault Tree Analysis (FTA**): represents the **cause-effect tree** from **prime events** (the "primes causes") that can lead to the occurrence of an adverse event (the effect) here denoted as the "**Initial Event" (IE**).
- FT is a reverse tree where leaves are the "prime causes", IE is the root and at any intermediate level there are "intermediate events".
- Starting from root we first investigate the event that have generated IE then backwards in the "cause-effect" chain up to the leaves, the "prime causes".
- Events at the same level should be statistically independent.
- The logical cause-effect relationships are AND / OR type.
- P(IE) will be computed using the probability theory. If P(A) is the probability of event A and P(B) is the probability of event B:
  - In quantitative methods is P(A AND B) = P(A)P(B), P(A OR B) = P(A)+P(B).
  - In semi-quantitative methods we can set **P(A AND B) = Min[P(A),P(B)]** and **P(A OR B) = Max[P(A),P(B)]**.

- The **Attack Tree (AT)** is a kind of FTA where leaves are the asset attacks and the root is an attack method.

FTA



P(IE) = AND(E1, E2) = Min[P(E1),P(E2)]

P(E1) = OR(A, E3) = Max[P(A),P(E3)]

P(E3) = OR(B, C) = Max[P(B),P(C)]

P(E2) = OR(C, E4) = Max[P(C),P(E4)]

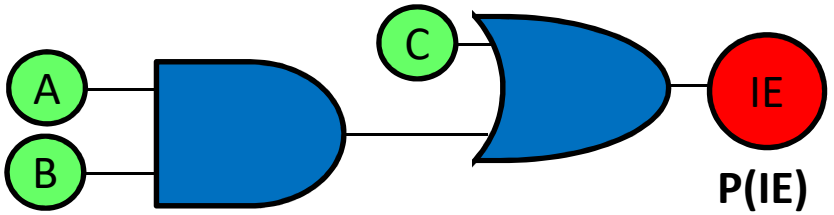
P(E4) = AND(A, B) = Min[P(A),P(B)]

P(IE) = OR(C, AND(A,B)) = Max[P(C),Min[P(A),P(B)]]

FTA

The FT corresponding to P(IE) = OR(C, AND(A,B)) follows

- A cut set in a FT is a set of basic events whose (simultaneous) occurrence ensures that IE occurs.



- A cut set is said to be a Minimal Cut Set (MCS) if, when any basic event is removed from the set, the remaining events collectively are no longer a cut set.
- The result of MCS analysis is a new FT, logically equivalent to the original, consisting of an OR gate beneath the top event, whose inputs are the MCSs. Each MCS is an AND gate containing a set of basic inputs necessary and sufficient to cause the IE.
- In this example $\mathbf{MCS_1 = \{C\}}$ and $\mathbf{MCS_2 = \{A,B\}}$
- Mitigation measures will be applied ONLY on the causes included in MCS

NIST CVSS

- **NIST Common Vulnerability Scoring System (CVSS)** is a semi-quantitative **score–based** "free" and "open" tool availabe from NIST which returns an estimation of the **severity of cyber vulnerabilities**.
- CVSS is based on CVE® Program (US), which mission is identity and classify ALL worldwide vulnerabilities in the ICT sector (i.e. SW platforms, systems, telecommunication protocols, …) and publish the solving patches. Currently CVSS rel. 3.1 (https://cve.mitre.org/).
- Scores range from **0 to 10** [**Low 0.1-3.9, Medium 4.0-6.9, High 7.0-8.9, Critical 9.0-10.0**]. Metrics are subdivided in three domains:
  - **Base Metrics**: measure static (permanent) vulnerabilities: mandatory
  - **Temporal Metrics**: measure dynamic (time evolving) vulnerabilities: optional (mandatory from rel. 4.0)
  - **Environmental Metrics**: measure the context-dependent vulnerabilities: optional (mandatory from rel. 4.0)
- On-line score computer: https://www.first.org/cvss/calculator/3.1
- On-line score computer: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- Examples on https://www.first.org/cvss/v3.1/examples
- https://www.first.org/cvss/calculator/4.0 in PUBLIC REVIEW

NIST CVSS – Base Metrics

Exploitability Metrics

Exploitability metrics in CVSS Base Scores **evaluate how easily a vulnerability can be exploited**. These metrics include:

- **Attack Vector (AV):** Assesses the level of access required for exploitation, from remote Network (N) access to Physical (P) access. The Attack Vector metric is scored in one of four levels:
  - **Network (N):** Vulnerabilities with this rating are remotely exploitable, from one or more hops away, up to and including remote exploitation over the Internet.
  - **Adjacent (A):** A vulnerability with this rating requires network adjacency for exploitation. The attack must be launched from the same physical or logical network.
  - **Local (L):** Vulnerabilities with this rating are not exploitable over a network. The attacker must access the system locally or remotely (via a protocol like SSH or RDP) or use social engineering or other techniques to trick an unsuspecting user into helping initiate the exploit.
  - **Physical (P):** In this type of attack, the adversary must physically interact with the target system.
- **Attack Complexity (AC)** measures the difficulty of exploitation, with Low (L) requiring no special conditions and High (H) needing specific preconditions. This metric indicates conditions beyond the attacker's control that must exist in order to exploit the vulnerability. Most commonly, this refers to either required user interaction or specific configurations of the target system. The Attack Complexity metric is scored as either Low or High:
  - **Low (L):** There are no specific pre-conditions required for exploitation.
  - **High (H):** Conditions beyond the attacker's control must exist for a successful attack. For this type of attack, the attacker must complete a number of preparatory steps to get access. This might include gathering reconnaissance data, overcoming mitigations, or becoming a man-in-the-middle.
- **Privileges Required (PR):** Indicates the level of privileges needed by the attacker, ranging from None (N) to High (H).
  - **None (N):** No privilege or special access is required to conduct the attack.
  - **Low (L):** The attacker requires basic "user" level privileges to leverage the exploit.
  - **High (H):** Administrative or similar access privileges are required for a successful attack.
- **User Interaction (UI):** Determines whether user involvement is necessary. User Interaction is a yes/no metric:
  - **None (N):** No user interaction is required.
  - **Required (R):** A user must complete some steps for the exploit to succeed. For example, a user might be required to install some software.

NIST CVSS – Base Metrics

Impact Metrics

Impact Metrics in CVSS Base Scores are critical for **assessing the potential consequences of a successful exploitation of a vulnerability** in the security of a system. These metrics focus on the well-known CIA Triad—Confidentiality, Integrity, and Availability—which are fundamental principles in information security:

- **Confidentiality (C):**

  This metric measures the extent to which unauthorized access to data could occur due to a vulnerability. If confidentiality is compromised, sensitive information may be exposed to unauthorized parties. Confidentiality has three metric values:

  - **High (H):** The attacker has full access to all resources in the impacted system, including highly sensitive information such as encryption keys.
  - **Low (L):** The attacker has partial access to information and no control over what they can access.
  - **None (N):** No data is accessible to unauthorized users due to the exploit.

- **Integrity (I):**

  Integrity refers to the trustworthiness and accuracy of data. This metric evaluates the possibility of data being tampered with or altered by an attacker. A loss of integrity could mean that critical data is changed, inserted, or deleted, leading to incorrect information being stored or displayed. Integrity has three metric values:

  - **None (N):** There is no loss of the integrity of any information.
  - **Low (L):** A limited amount of information might be tampered with or modified, but the protected system has no serious impact.
  - **High (H):** The attacker can modify any or all information on the target system, resulting in a complete loss of integrity.

- **Availability (A):**

  Availability measures the impact of a vulnerability on the accessibility of the system or its data, such as when a system crashes or goes through a DDOS attack. A compromise in availability means that users may be unable to access the system or its services as needed. Availability has one of three metric values:

  - **None (N):** There is no loss of availability.
  - **Low (L):** Availability might be intermittently limited, or a successful attack might negatively impact performance.
  - **High (H):** There is a complete loss of availability of the impacted system or information.

- **Scope (S) Metrics:** Scope metrics in CVSS Base Scores evaluate whether a vulnerability's exploitation can affect systems beyond its immediate environment.

NIST SP 800-30

- **NIST Special Publications:** Guidelines, technical specifications, recommendations and reference materials, comprising multiple sub-series:
- SP 800 **Computer security**
- SP 1800 **Cybersecurity practice guides**
- SP 500 **Information technology** (only pubs on cybersecurity and privacy)

- **NIST Special Publication 800-30 rev. 1 "Guide for Conducting Risk Assessments"** (https://csrc.nist.gov/pubs/sp/800/30/r1/final)

- The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

NIST SP 800-30

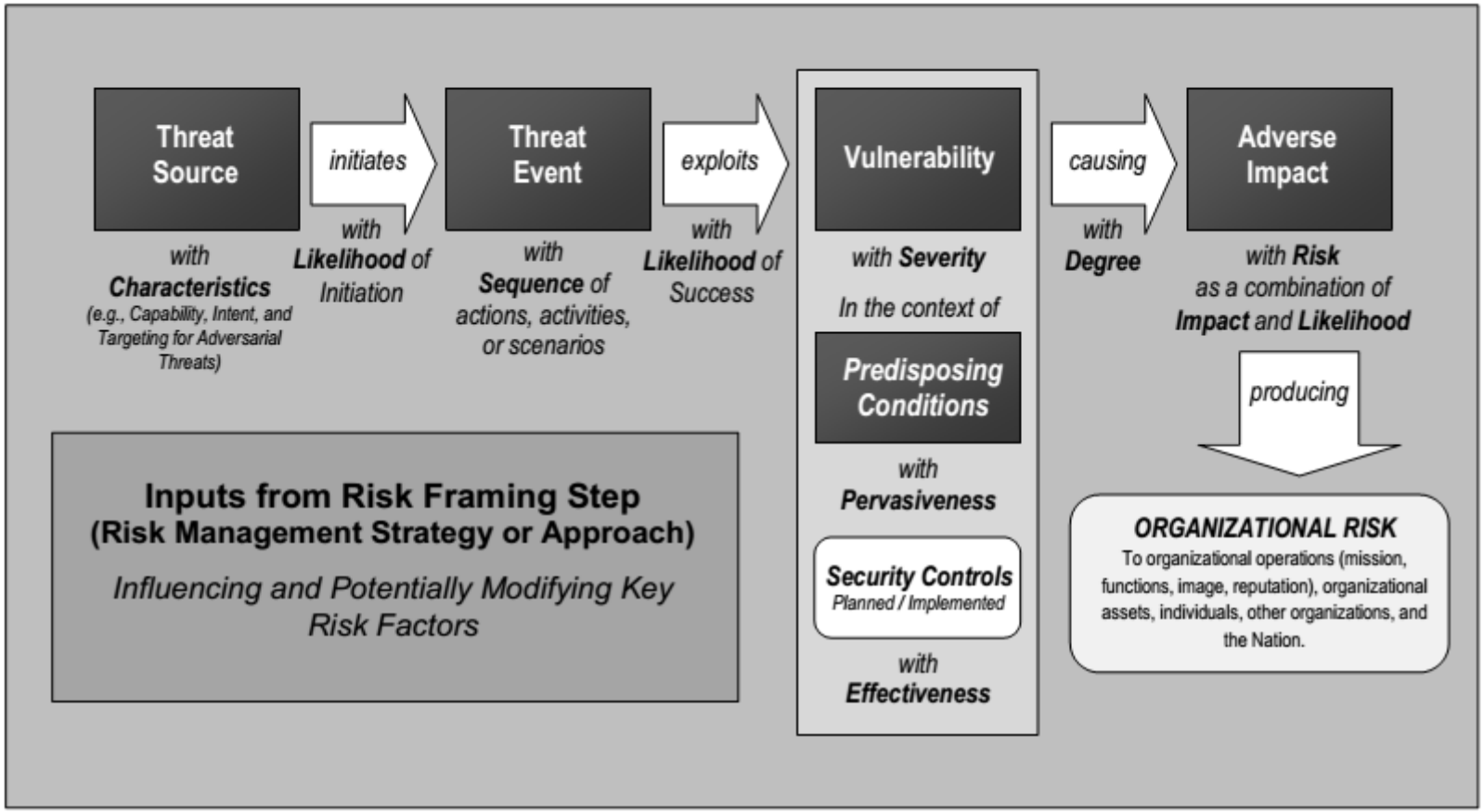


FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

NIST SP 800-30

- NIST SP 800-30 introduces a semi-quantitative technique for conducting a risk assessment.
- Mainly 11 tables into 5 groups
  - *D-1, D-2 THREAT SOURCE IDENTIFICATION and Taxonomy (here not reported)*
  - *D-3 Adversarial Capability*
  - *D-4 Adversarial Intent*
  - *D-5 Adversarial Targeting*
  - E-1, E-2, E-4: THREAT EVENT IDENTIFICATION and Relevance (here not reported)
  - *F-2 Assessment Scale - Vulnerability Severity*
  - *F-5 Assessment Scale – Pervasiveness of Predisponing Conditions*
  - G-2 Likehood of Threat Event Initiation
  - G-4 Likehood of Threat Event Resulting in Adverse Impact
  - G-5 Overall Likehood
  - *H-3 Impact of Threat Events*
  - I-2 Level of Risk (combination of Likehood and Impact)
  - I-3 Level of Risk
- I-4 Column description for Adversarial Risk table
- I-8 Adversarial Risk Table

NIST SP 800-30

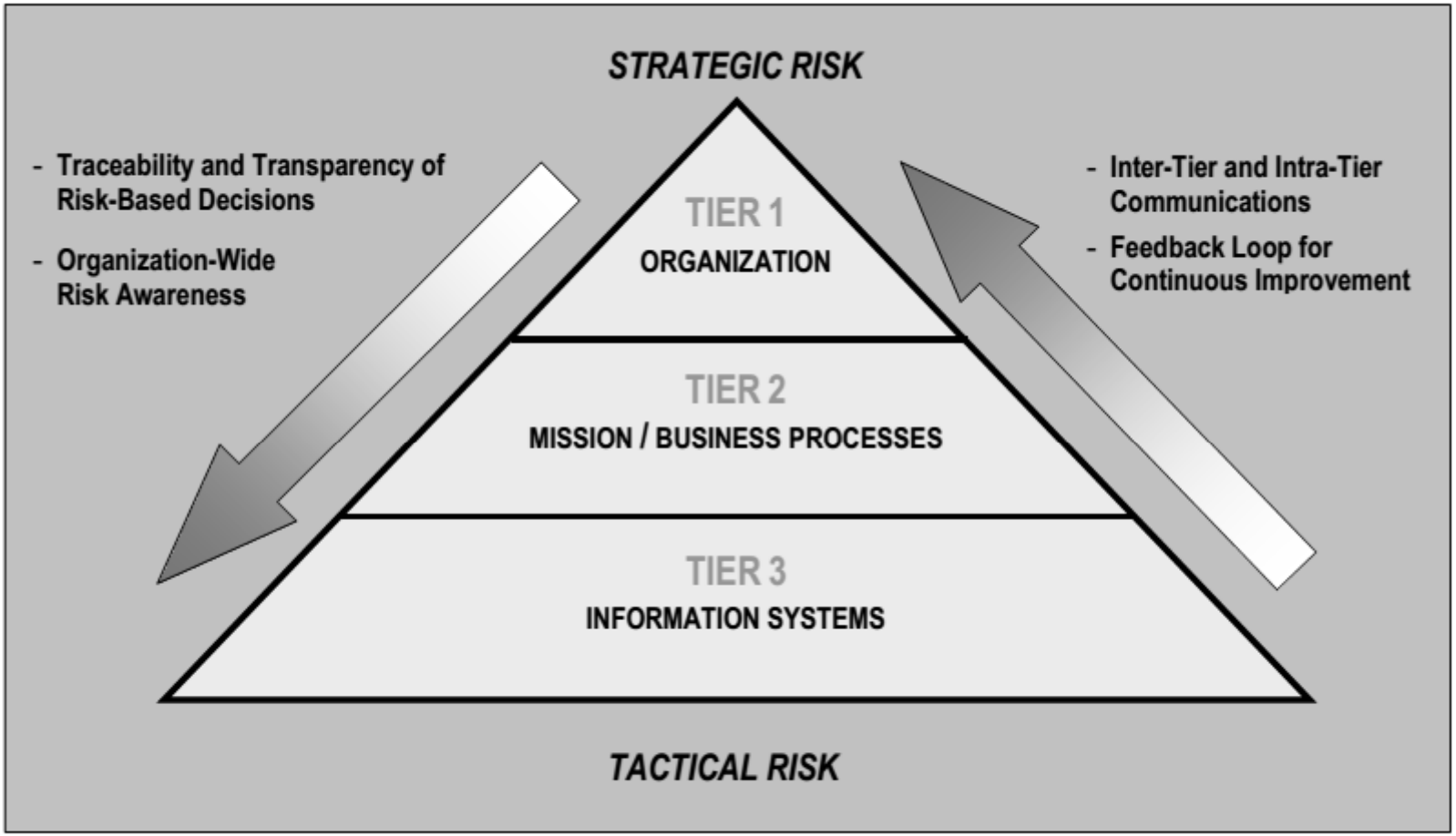


FIGURE 4: RISK MANAGEMENT HIERARCHY

NIST SP 800-30

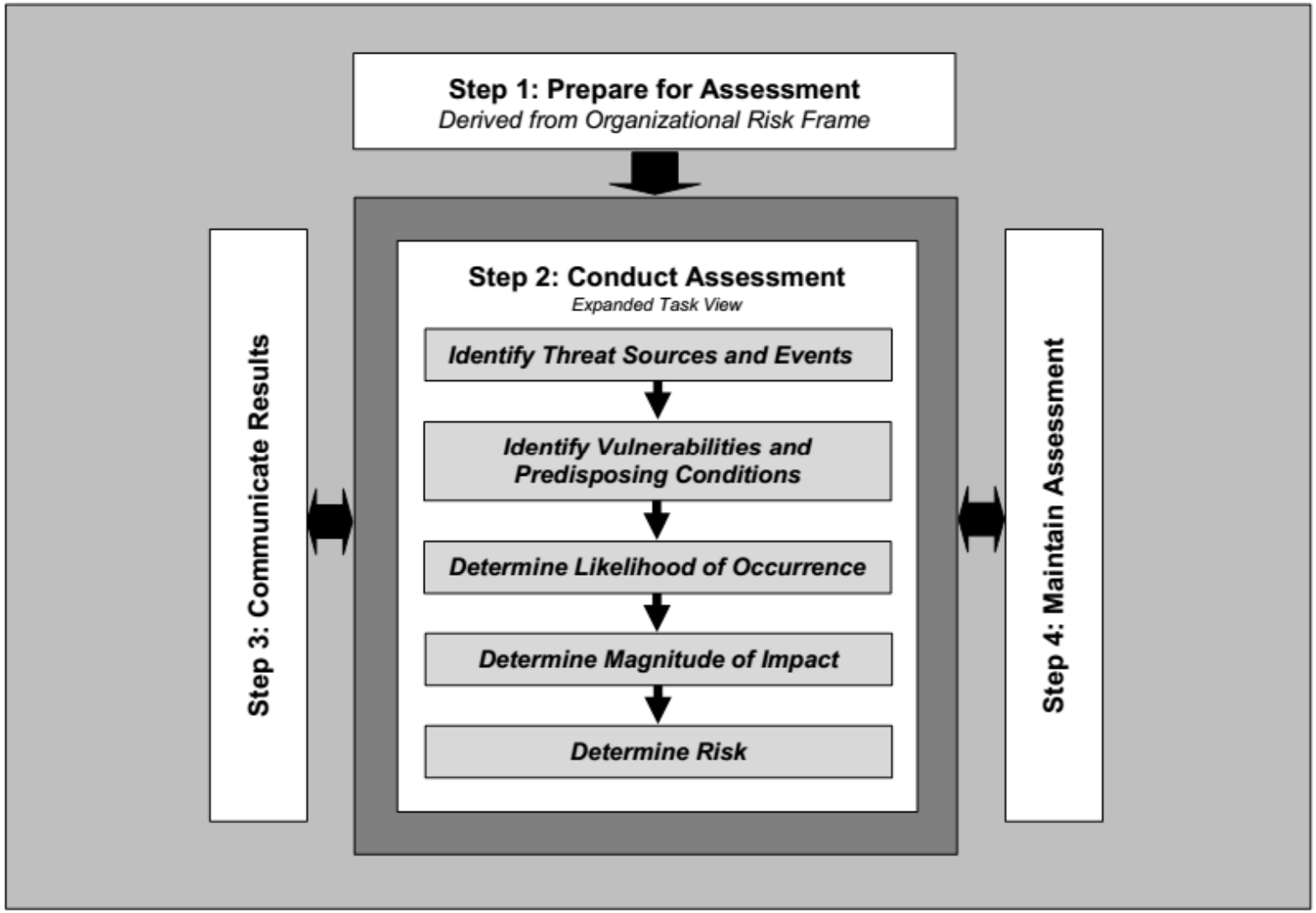


FIGURE 5: RISK ASSESSMENT PROCESS

NIST SP 800-30

TABLE D-3: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY CAPABILITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.
High	80-95	8	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-79	5	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.
Low	5-20	2	The adversary has limited resources, expertise, and opportunities to support a successful attack.
Very Low	0-4	0	The adversary has very limited resources, expertise, and opportunities to support a successful attack.

NIST SP 800-30

TABLE D-4: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY INTENT

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary seeks to undermine, severely impede, or destroy a core mission or business function, program, or enterprise by exploiting a presence in the organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.
High	80-95	8	The adversary seeks to undermine/impede critical aspects of a core mission or business function, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.
Moderate	21-79	5	The adversary seeks to obtain or modify specific critical or sensitive information or usurp/disrupt the organization's cyber resources by establishing a foothold in the organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the organization's missions/business functions to achieve these ends.
Low	5-20	2	The adversary actively seeks to obtain critical or sensitive information or to usurp/disrupt the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.
Very Low	0-4	0	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

NIST SP 800-30

TABLE D-5: ASSESSMENT SCALE – CHARACTERISTICS OF ADVERSARY TARGETING

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.
High	80-95	8	The adversary analyzes information obtained via reconnaissance to target persistently a specific organization, enterprise, program, mission or business function, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.
Moderate	21-79	5	The adversary analyzes publicly available information to target persistently specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.
Low	5-20	2	The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.
Very Low	0-4	0	The adversary may or may not target any specific organizations or classes of organizations.

NIST SP 800-30

TABLE F-2: ASSESSMENT SCALE – VULNERABILITY SEVERITY

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The vulnerability is exposed and exploitable, and its exploitation could result in severe impacts. Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.
High	80-95	8	The vulnerability is of high concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is planned but not implemented; compensating controls are in place and at least minimally effective.
Moderate	21-79	5	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
Low	5-20	2	The vulnerability is of minor concern, but effectiveness of remediation could be improved. Relevant security control or other remediation is fully implemented and somewhat effective.
Very Low	0-4	0	The vulnerability is not of concern. Relevant security control or other remediation is fully implemented, assessed, and effective.

NIST SP 800-30

TABLE F-5: ASSESSMENT SCALE – PERVASIVENESS OF PREDISPOSING CONDITIONS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Applies to **all** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
High	80-95	8	Applies to **most** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Moderate	21-79	5	Applies to **many** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Low	5-20	2	Applies to **some** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).
Very Low	0-4	0	Applies to **few** organizational missions/business functions (Tier 1), mission/business processes (Tier 2), or information systems (Tier 3).

NIST SP 800-30

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

NIST SP 800-30

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

NIST SP 800-30

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

NIST SP 800-30

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

NIST SP 800-30

TABLE I-3: ASSESSMENT SCALE – LEVEL OF RISK

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

NIST SP 800-30

TABLE I-4: COLUMN DESCRIPTIONS FOR ADVERSARIAL RISK TABLE

Column	Heading	Content
1	Threat Event	Identify threat event. (**Task 2-2**; **Table E-1**; **Table E-2**; **Table E-5**; **Table I-5**.)
2	Threat Sources	Identify threat sources that could initiate the threat event. (**Task 2-1**; **Table D-1**; **Table D-2**; **Table D-7**; **Table I-5**.)
3	Capability	Assess threat source capability. (**Task 2-1**; **Table D-3**; **Table D-7**; **Table I-5**.)
4	Intent	Assess threat source intent. (**Task 2-1**; **Table D-4**; **Table D-7**; **Table I-5**.)
5	Targeting	Assess threat source targeting. (**Task 2-1**; **Table D-5**; **Table D-7**; **Table I-5**.)
6	Relevance	Determine relevance of threat event. (**Task 2-2**; **Table E-1**; **Table E-4**; **Table E-5**; **Table I-5**.) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting. (**Task 2-4**; **Table G-1**; **Table G-2**; **Table I-5**.)
8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts. (**Task 2-5**; **Table F-1**; **Table F-3**; **Table F-4**; **Table F-6**; **Table I-5**.)
9	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (**Task 2-5**; **Table F-1**; **Table F-2**; **Table F-5**; **Table F-6**; **Table I-5**.)
10	Likelihood Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration threat source capability, vulnerabilities, and predisposing conditions. (**Task 2-4**; **Table G-1**; **Table G-4**; **Table I-5**.)
11	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in adverse impact (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds). (**Task 2-4**; **Table G-1**; **Table G-5**; **Table I-5**.)
12	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (**Task 2-5**; **Table H-1**, **Table H-2**; **Table H-3**; **Table H-4**; **Table I-5**.)
13	Risk	Determine the level of risk as a combination of likelihood and impact. (**Task 2-6**; **Table I-1**; **Table I-2**; **Table I-3**; **Table I-5**.)

NIST SP 800-30

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

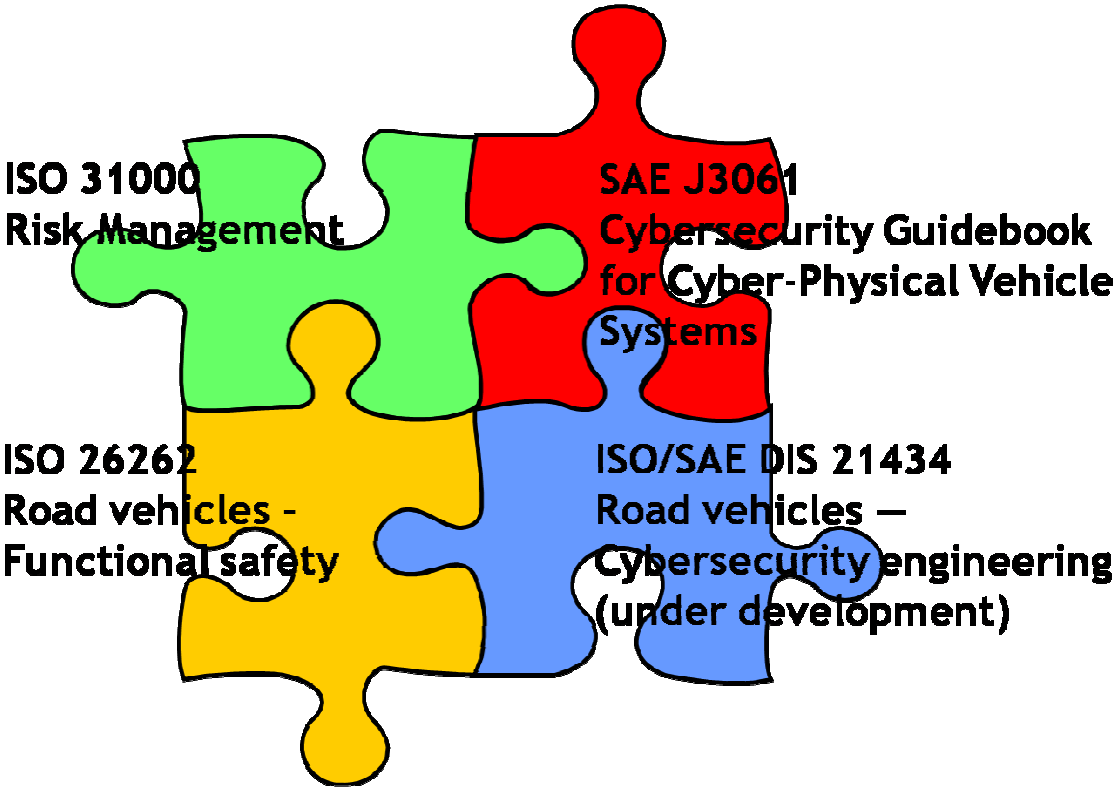
1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Outline

- The framework of Security Management
- From Risk to Security Management
  - Security Management Process
  - Approaches for Risk Evaluation
  - Techniques for Risk Evaluation
  - P-I Matrix and isorisk curves
  - FTA - CVSS
  - NIST SP 800-30 Guide for Conducting a Risk Assessment
- Security management automotive domain
  - ISO / SAE 21434
  - Threat Analysis and Risk Assessment (TARA)
  - Cybersecurity Risk Quantification technique: EVITA
  - Guide line for TARA execution using EVITA
- Reference Cyber Security functions
  - Security metrics
  - Timing constraints
  - Cyber Risk Mitigation

Security management automotive domain

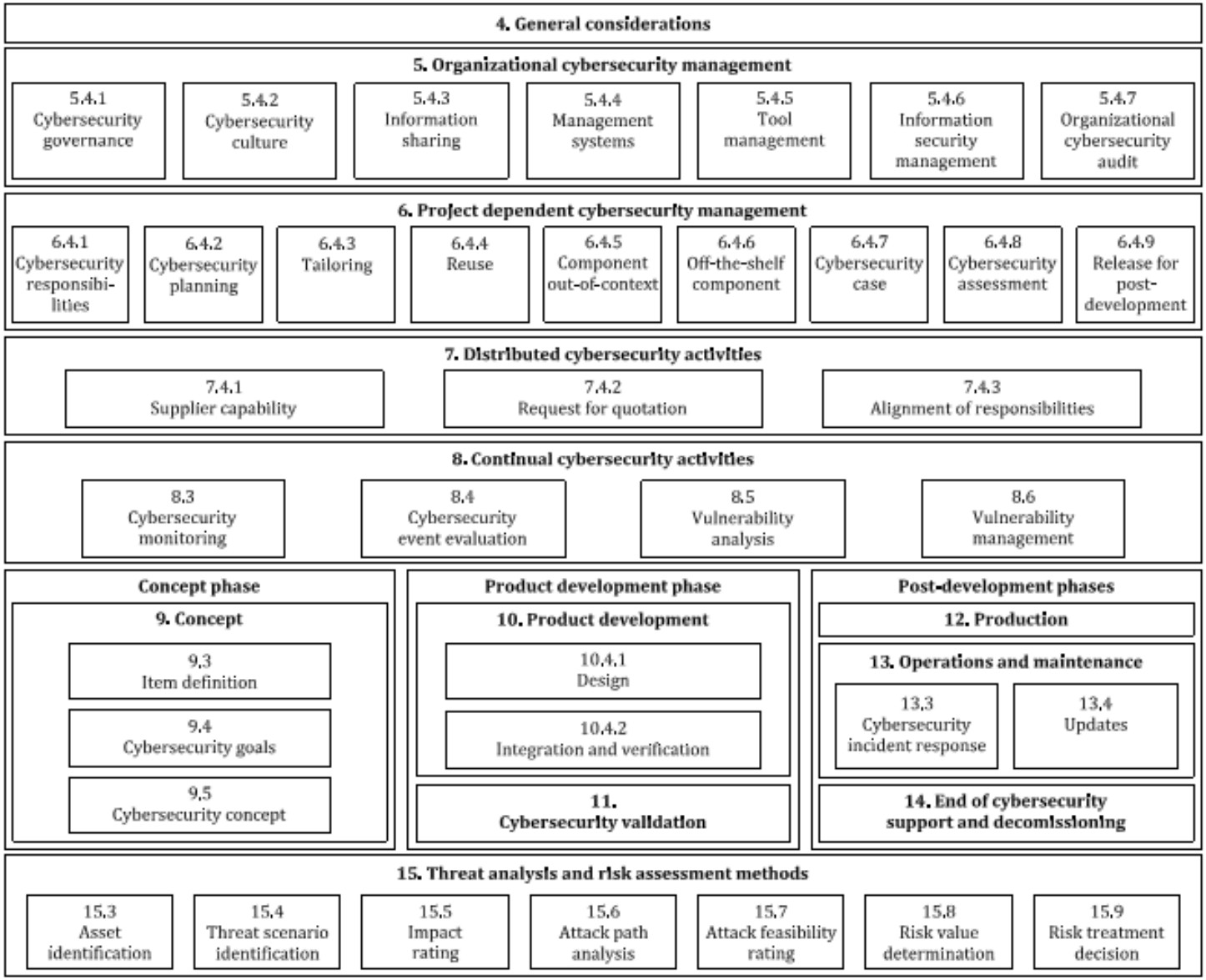
- ISO 26262 Road vehicles – Functional safety
- ISO 11898 Road vehicles - Controller Area Network (CAN)
- SAE J3061 Cybersecurity Guidebook for Cyber-physical vehicle systems
- ISO/SAE 21434 **Road vehicles – Cybersecurity Engineering**, SAE (Society of Automotive Engineers, 1905), https://www.sae.org/standards/



ISO / SAE 21434:2021

- ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering) defines a framework to ensure a consistent, well defined and robust approach to foster a cybersecurity culture, to manage cybersecurity risks across the complete vehicle lifecycle, to allow adaptation to a continually changing threat landscape and to institute a cybersecurity management system.
- ISO / SAE 21434 addresses the cybersecurity perspective in engineering of Electrical and Electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods.
- It provides vocabulary, objectives, requirements and guidelines related to cybersecurity engineering as a foundation for common understanding throughout the supply chain. This enables organizations to:
  - define cybersecurity policies and processes;
  - manage cybersecurity risk;
  - foster a cybersecurity culture.

ISO / SAE 21434:2021



ISO / SAE 21434:2021

- Clause 4 (General considerations) is informational and includes the context and perspective of the approach to road vehicle cybersecurity engineering taken in this document.
- Clause 5 (Organizational cybersecurity management) includes the cybersecurity management and specification of the organizational cybersecurity policies, rules and processes.
- Clause 6 (Project dependent cybersecurity management) includes the cybersecurity management and cybersecurity activities at the project level.
- Clause 7 (Distributed cybersecurity activities) includes requirements for assigning responsibilities for cybersecurity activities between customer and supplier.
- Clause 8 (Continual cybersecurity activities) includes activities that provide information for ongoing risk assessments and defines vulnerability management of E/E systems until end of cybersecurity support.

ISO / SAE 21434:2021

- Clause 9 (Concept) includes activities that determine cybersecurity risks, cybersecurity goals and cybersecurity requirements for an item.
- Clause 10 (Product development) includes activities that define the cybersecurity specifications, and implement and verify cybersecurity requirements.
- Clause 11 (Cybersecurity validation) includes the cybersecurity validation of an item at the vehicle level.
- Clause 12 (Production) includes the cybersecurity-related aspects of manufacturing and assembly of an item or component.
- Clause 13 (Operations and maintenance) includes activities related to cybersecurity incident response and updates to an item or component.
- Clause 14 (End of cybersecurity support and decommissioning) includes cybersecurity considerations for end of support and decommissioning of an item or component.
- Clause 15 (**Threat analysis and risk assessment (TARA) methods**) includes modular methods for analysis and assessment to determine the extent of cybersecurity risk so that treatment can be pursued.

ISO / SAE 21434:2021 – Clause 15

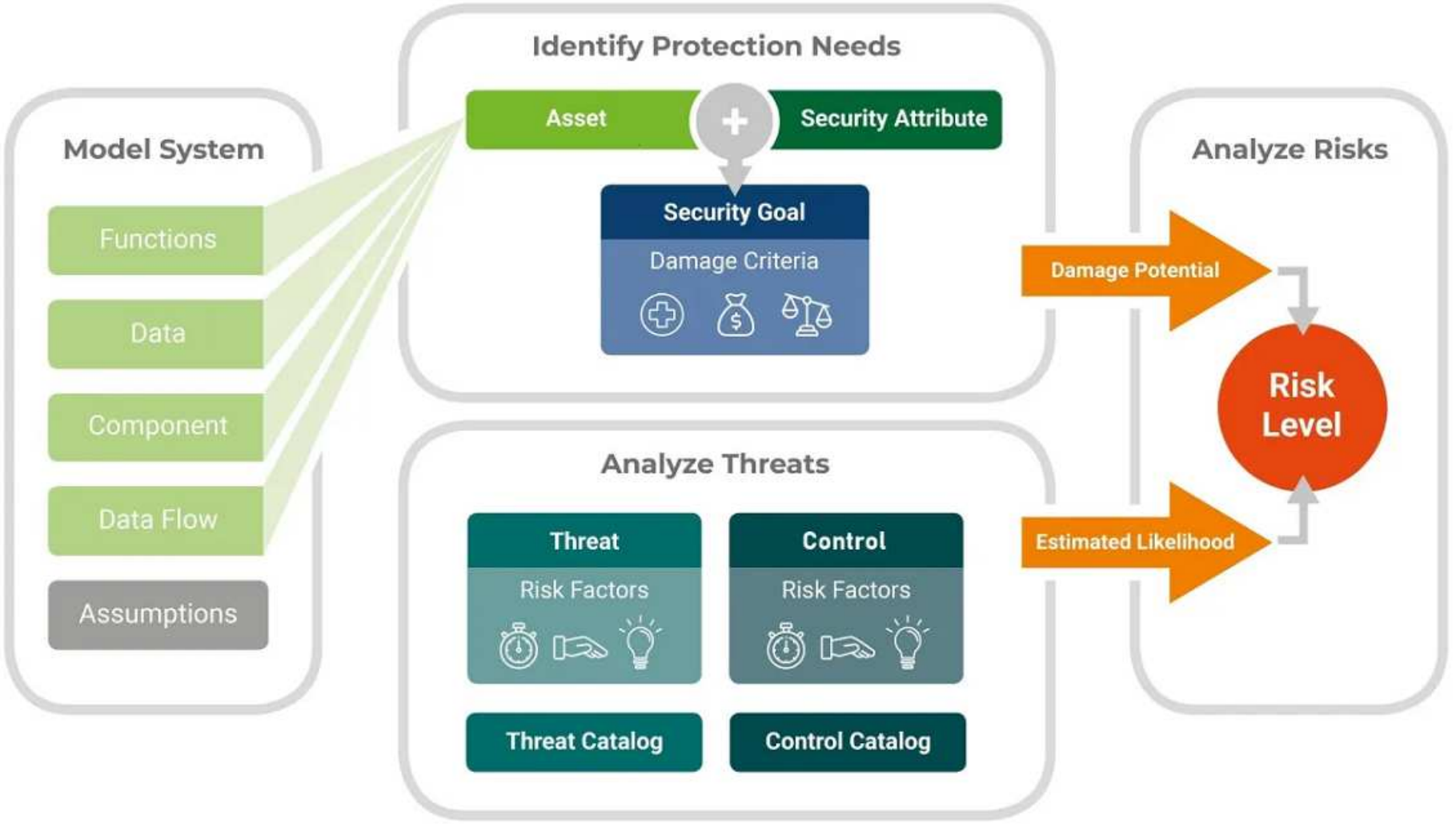
- This clause describes methods to determine the extent to which a road user can be impacted by a threat scenario.

- These methods and their work products are collectively known as a **Threat Analysis and Risk Assessment (TARA)** and are performed from the viewpoint of affected road users.

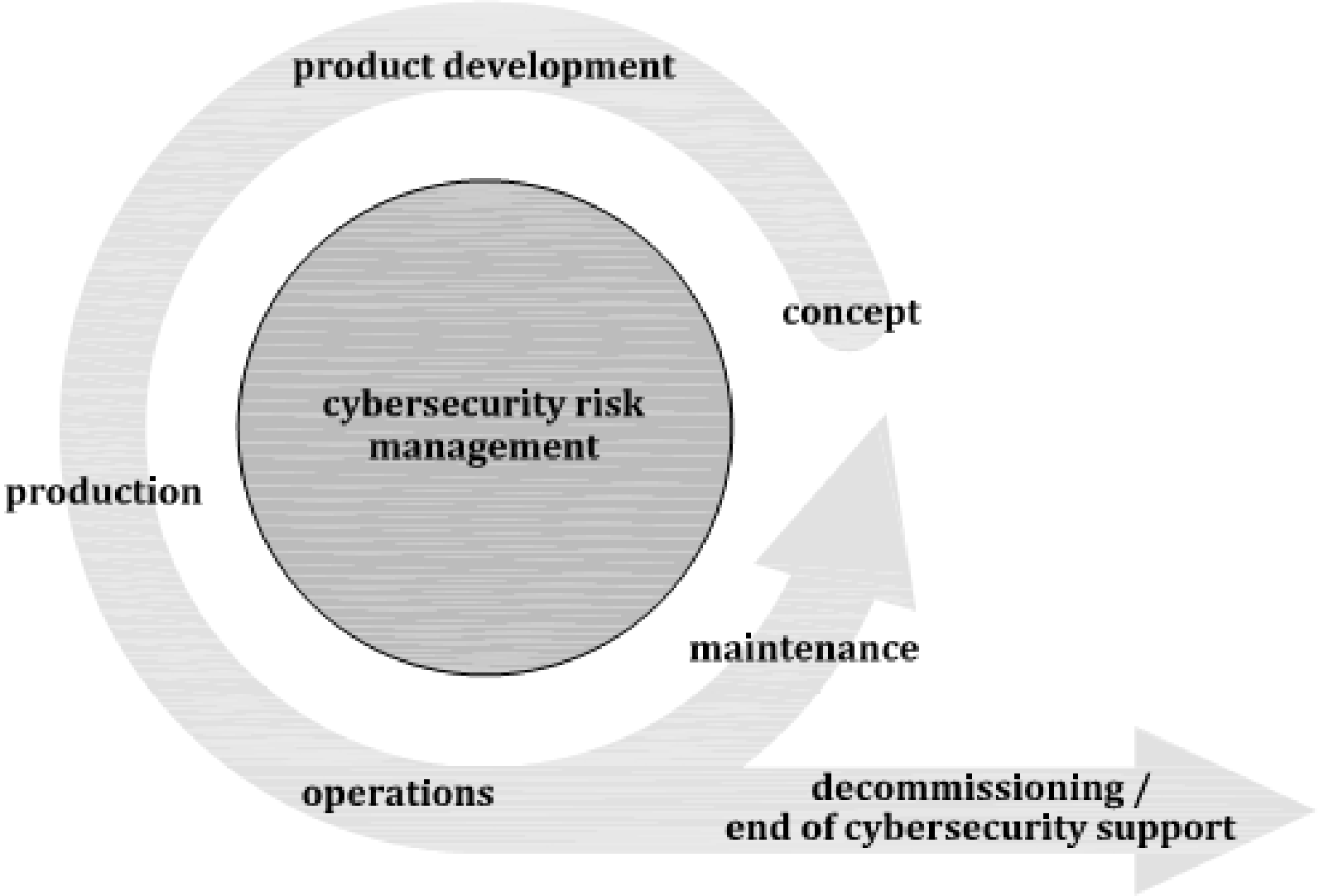
- The methods defined in this clause are generic modules that can be invoked systematically, and from any point in the lifecycle of an item or component:

  - asset identification (see 15.3);
  - threat scenario identification (see 15.4);
  - impact rating (see 15.5);
  - attack path analysis (see 15.6);
  - attack feasibility rating (see 15.7);
  - risk value determination (see 15.8);
  - risk treatment decision or risk determination (see 15.9)

ISO / SAE 21434:2021 – Clause 15



ISO / SAE 21434:2021 - General consideration



ISO / SAE 21434:2021 - General considerations

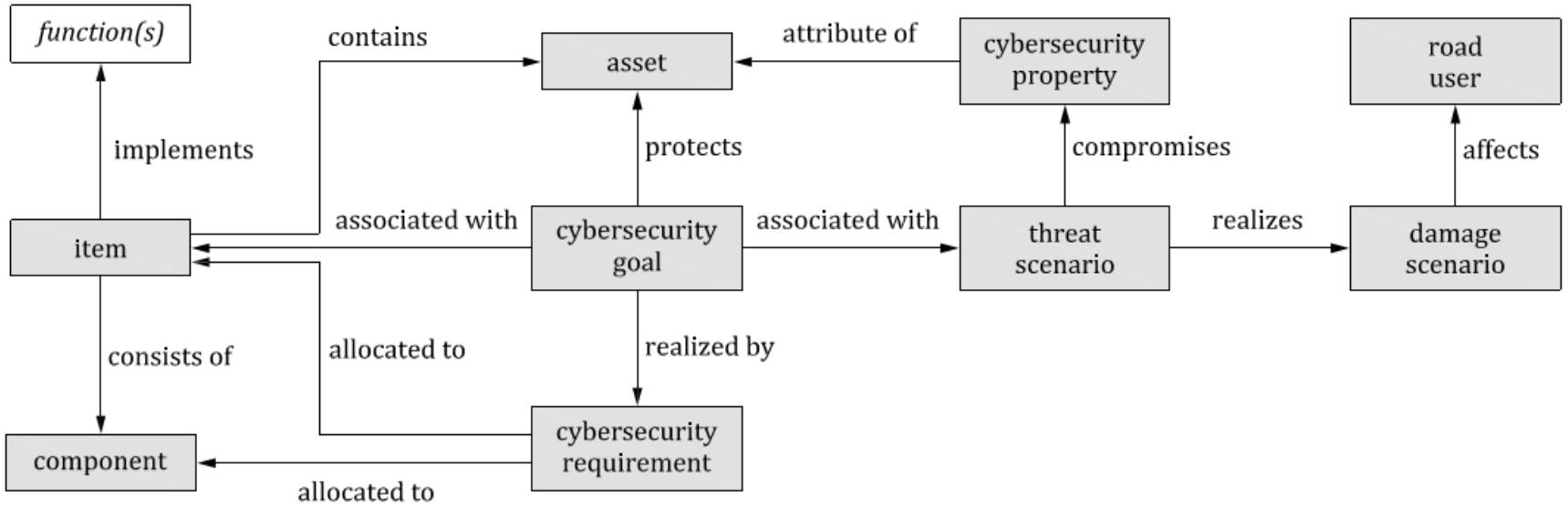
- An item comprises all E/E equipment and software (i.e. its components) in a vehicle involved in the realization of a specific functionality at vehicle level, e.g. braking.
- An item or a component interacts with its operational environment.
- ISO / SAE 21434 applies to cybersecurity-relevant items and components of a series production road vehicle (i.e. not a prototype) including aftermarket and service parts.
- Systems external to the vehicle (e.g. back-end servers) can be considered for cybersecurity purposes but are not in the scope ISO / SAE 21434.

- ISO / SAE 21434 describes cybersecurity engineering from the perspective of a single item. For the vehicle as a whole, the vehicle E/E architecture or the set of the cybersecurity cases of its cybersecurity-relevant items and components can be considered.

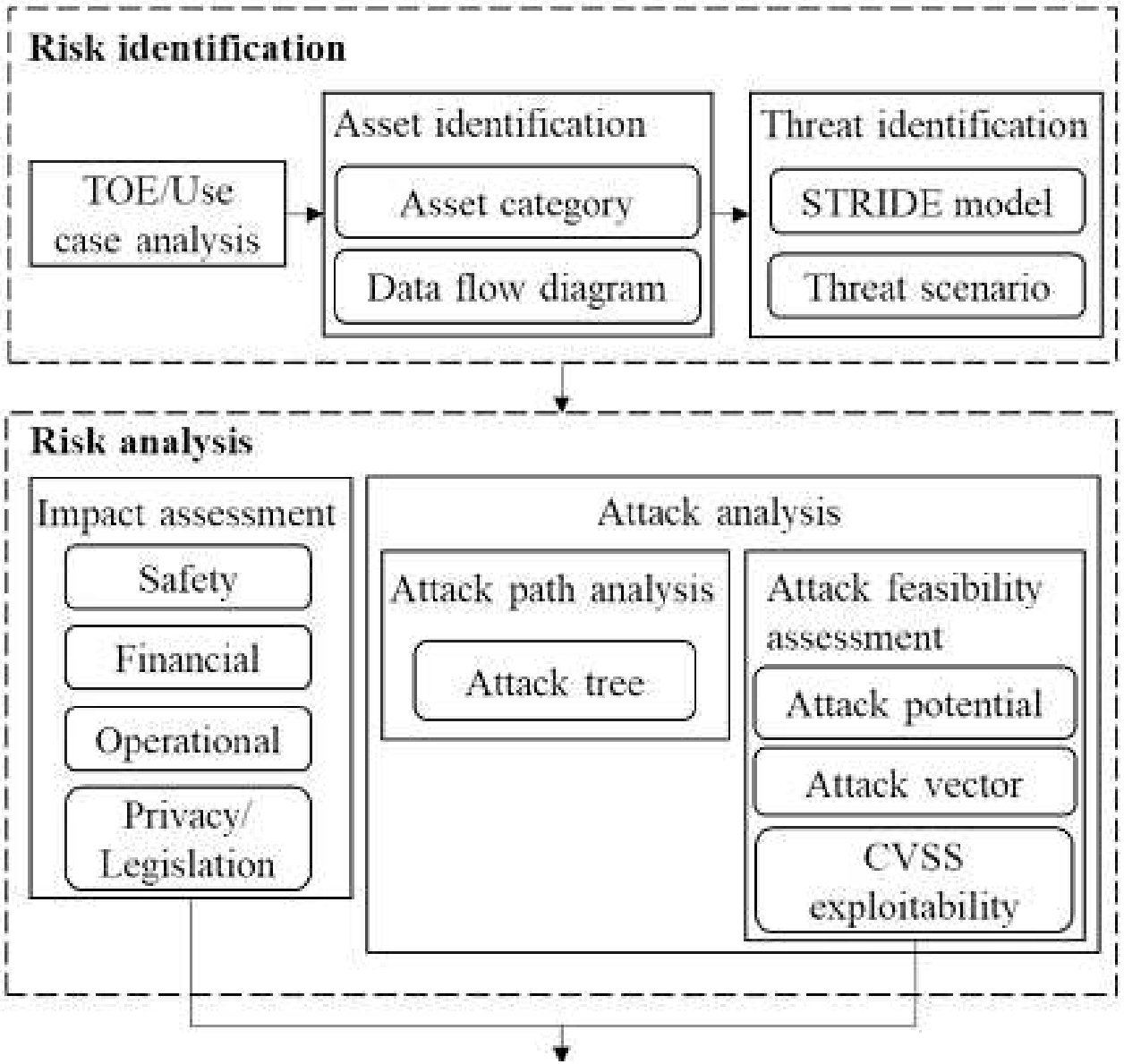
- The overall cybersecurity risk management of an organization in this document applies throughout all lifecycle phases as illustrated below

ISO / SAE 21434:2021 - General considerations

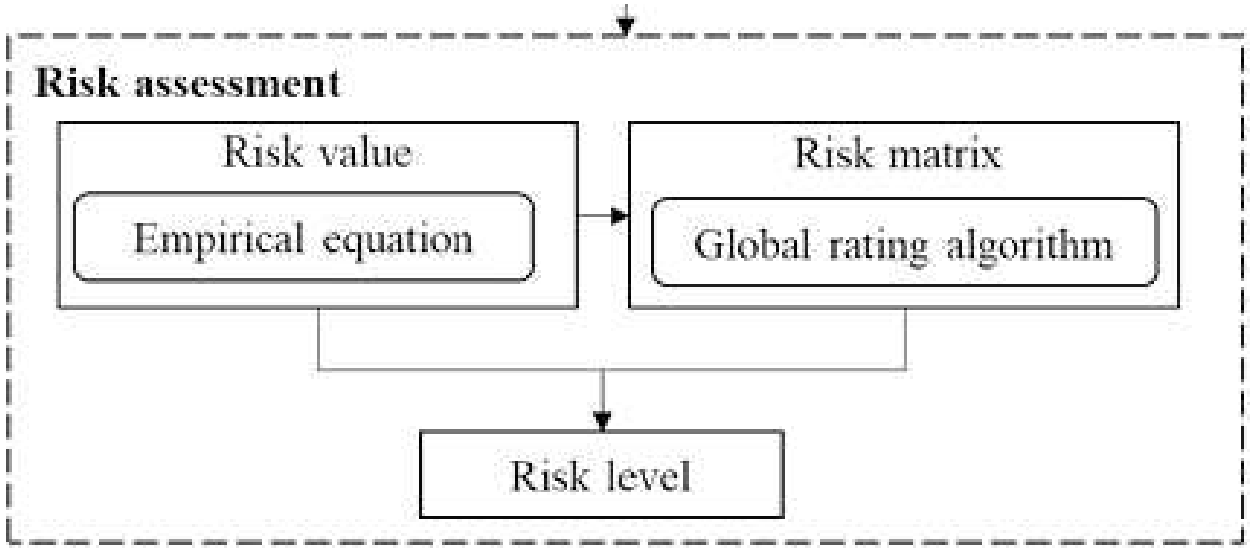
- Cybersecurity risk management is applied throughout the supply chain.



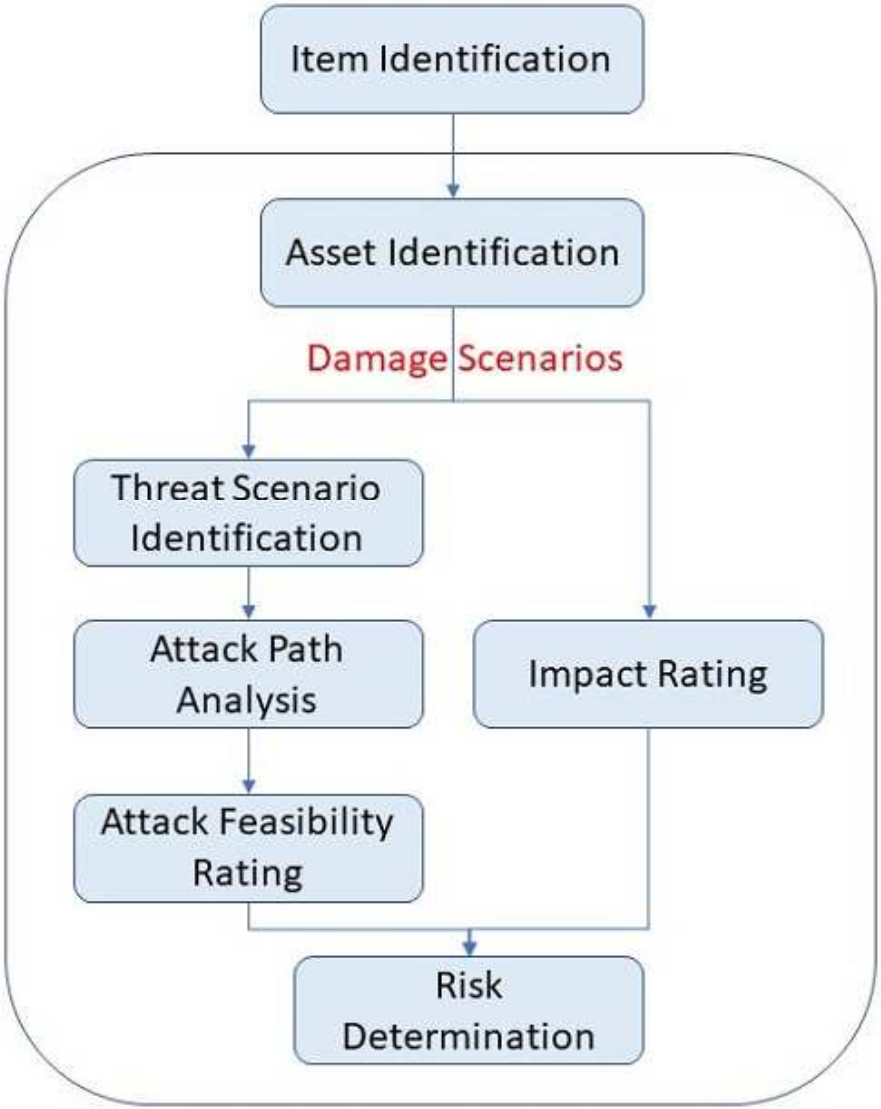
ISO / SAE 21434:2021 – TARA



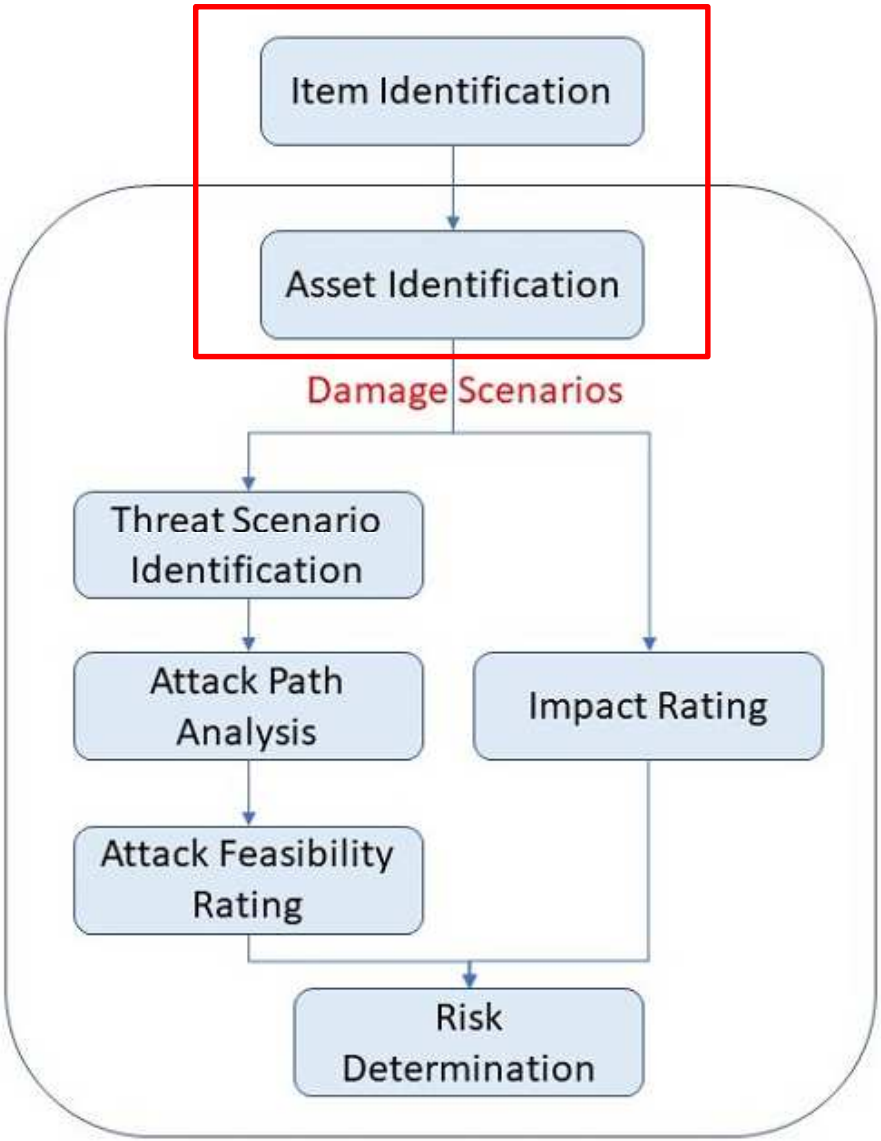
ISO / SAE 21434:2021 – TARA



ISO / SAE 21434:2021 – TARA



TARA – Item Definition Asset Identification

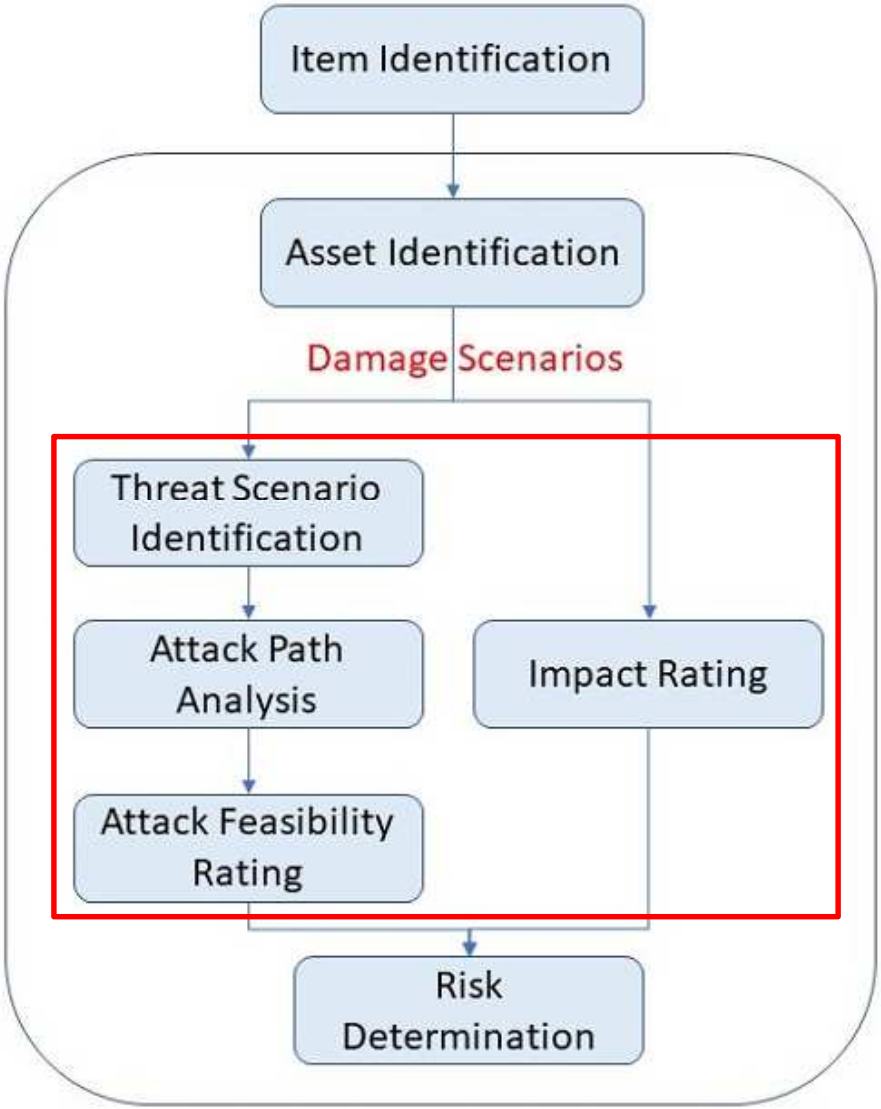


TARA – Item Definition Asset Identification

- We carry out TARA steps after defining the Target of Evaluation (TOE) or **item definition**. This step includes:
  - **Item boundary**: it distinguishes the item from other internal or external items to the vehicle and defines the interfaces between the item and the other items
  - **Item functions**: this describes the item's behavior during different phases (concept, development, production, maintenance)
  - **Preliminary architecture**: this describes the various components of the item, their connections, and external interfaces of the item
  - **Assumptions**: relevant information regarding the security assumptions, e.g., using encrypted messages

- **Asset identification**: an asset is any resource that has value. In a vehicle, assets can be in-vehicle devices such as ECUs, sensors and actuators, applications running on in-vehicle devices, and communication data.
- We can identify assets using the preliminary architecture and the assumptions obtained from the item definition activity.

TARA – Damage Scenarios



TARA – Damage Scenarios

- We can infer the damage scenarios from asset identification by associating the asset with specific cybersecurity properties.
- The ISO/SAE 21434 deals with the following C.I.A. properties:
  - **Confidentiality**: data must not be revealed to unauthorized parties
  - **Integrity**: data is complete and intact, so it should not be modified unauthorizedly or accidentally
  - **Availability**: data or system must be accessible when needed
- Further cybersecurity properties from S.T.R.I.D.E. threat model:

Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Someone obtaining information they are not authorized to access
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

TARA – Damage Scenarios

- **Threat scenario** is the potential cause of compromise of assets' cybersecurity properties, which leads to the damage scenarios. For example, spoofing of CAN messages for brakes ECU leads to loss of integrity of those messages and thereby the loss of integrity of the braking functionality.
- **Impact rating**: we assess damage scenarios against potential consequences for road users in four different categories: **safety (S), financial (F), operational (O), and privacy (P).** Impact rating for each category has to be one of four values: ”severe,” major,” moderate,” or ”negligible.” (from ISO 26262-3:2018).
- **Attack path analysis**: threat scenarios analysis to identify the attack paths by either top-down approaches - such as attack trees- which analyze each threat scenario to deduce attack paths that realize it or bottom-up approaches using vulnerability or weakness analysis.
- **Attack feasibility (AF) rating**: we should assess each attack path according to four categories: High, if the attack path utilizes a low effort; Medium, if the attack path utilizes a medium effort; Low, if the attack path utilizes a high effort; Very low, if the attack path utilizes a very high effort.
- This rating should be determined using one of the following approaches:
  - Attack potential-based approach
  - Attack vector-based approach
  - Common Vulnerability Scoring System (CVSS)

TARA – Impact assessment

S		*F*		*O*		*P*	
Level	Value	Level	Value	Level	Value	Level	Value
No impact	0	No impact	0	No impact	0	No impact	0
Low	10	Low	10	Low	1	Low	1
Medium	100	Medium	100	Medium	10	Medium	10
High	1000	High	1000	High	100	High	100

- **I = S + F + O + P**

Summation of parameter value	Level	Level value
1–19	Low	1
20–99	Medium	2
100–999	High	3
≥ 1000	Critical	4

[ISO / SAE 21434:2021]

TARA – Attack Feasibility rating

- **Attack potential-based approach**: defined in ISO/IEC 18045, it measures the effort needed for successfully performing the attack and relies on the potential of the attacker and used resources. Five core factors:
  - **Elapsed time (ET)**: the time required to identify the vulnerability and perform a successful attack
  - **Knowledge of the item or the component (KN)**: acquired by the attacker
  - **Attacker expertise (EX)**: related to the skill and the experience of the attacker
  - **Window of the opportunity (WI)**: related to the access conditions as access type, whether it is physical or logical, and the access time for the attacker to perform a successful attack
  - **Equipment (EQ)**: available to the attacker to discover the vulnerability and perform the attack

  AF Rating = sum of scores from each factor.

- **Attack vector-based approach**: according to the logical and physical distance between the attacker and the item or the component: **the more remote, the higher AF Rating**.

TARA – Attack Feasibility rating

Parameter				Value
EX	*KN*	*WI*	*EQ*	
Layman	Public	Critical	Standard	0
Proficient	Restricted	High	Specialized	1
Expert	Sensitive	Medium	Bespoke	2
Multiple experts	Critical	Low	Multiple bespokes	3

- **AF = EX + KN + WI + EQ**

Summation of parameter values	Level	Level value
7–9	Low	1
4–6	Medium	2
2–3	High	3
0–1	Critical	4

[ISO / SAE 21434:2021]

TARA – Attack Feasibility rating

- **Attack vector method**: in the early phase of product development, the attack feasibility can be qualitatively estimated based on the attack vector, when the available information is insufficient to determine a specific attack path.
- Attack vectors can be divided into 4 categories, namely network, adjacent, local, and physical, as shown below.
- The attack feasibility level increases with the increasing of the remoteness of the attack path.

Parameter	Level	Level value
Physical	Low	1
Local	Medium	2
Adjacent	High	3
Network	Critical	4

[ISO / SAE 21434:2021]

TARA – Attack Feasibility rating

- **CVSS exploitability based method** can be determined by the exploitability metrics group in the CVSS base metrics. Exploitability metrics group (E) are **attack vector (V), attack complexity (C), privileges required (P), and user interaction (U)** as shown below:

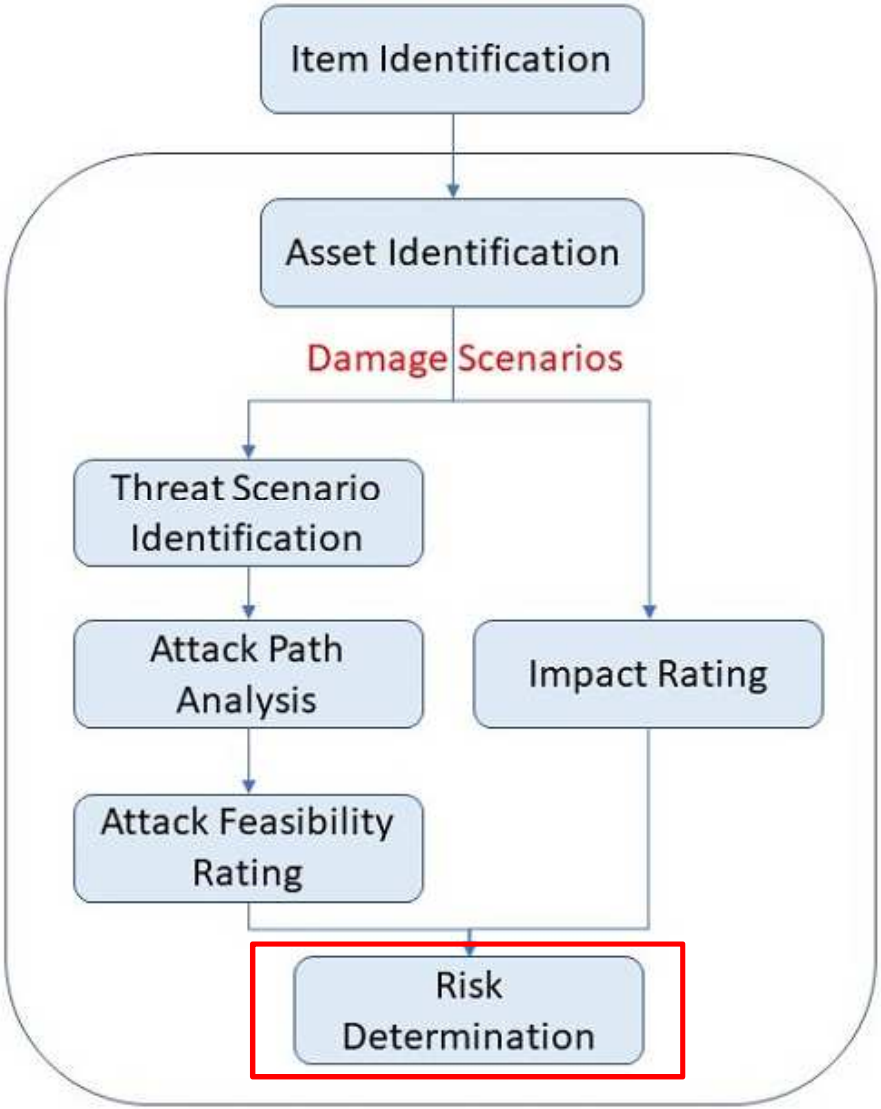
Parameter	Value
V	0.2–0.85
C	0.44–0.77
P	0.27–0.85
U	0.62–0.85

- **E = 8.22 x V x C x P x U** computed using CVSS v3.1 Calculator [https://www.first.org/cvss/calculator/3.1]

Exploitability value	Level	Level value
0.12–1.05	Very low	1
1.06–1.99	Low	2
2.00–2.95	Medium	3
2.96–3.89	High	4

[ISO / SAE 21434:2021]

TARA – Risk Determination



TARA – Risk Determination

- **Risk determination**: The risk of a threat scenario can be determined using the parameters **AF Rating and the Impact Rating of the associated damage scenario**
- Risk values can be calculated forming a risk matrix.
- The construction of the risk matrix mainly depends on the evaluation experience. The global rating algorithm used to construct the risk matrix of automotive cybersecurity, is

$$R = \sqrt{m(I)^2 + n(AF)^2}$$

where R is the risk value, m and n are the weight parameters of I and AF, respectively. Impact and Attack Feasibility factors are hypothesized to have the same contribution to risk: hence m and n are both set to 0.5

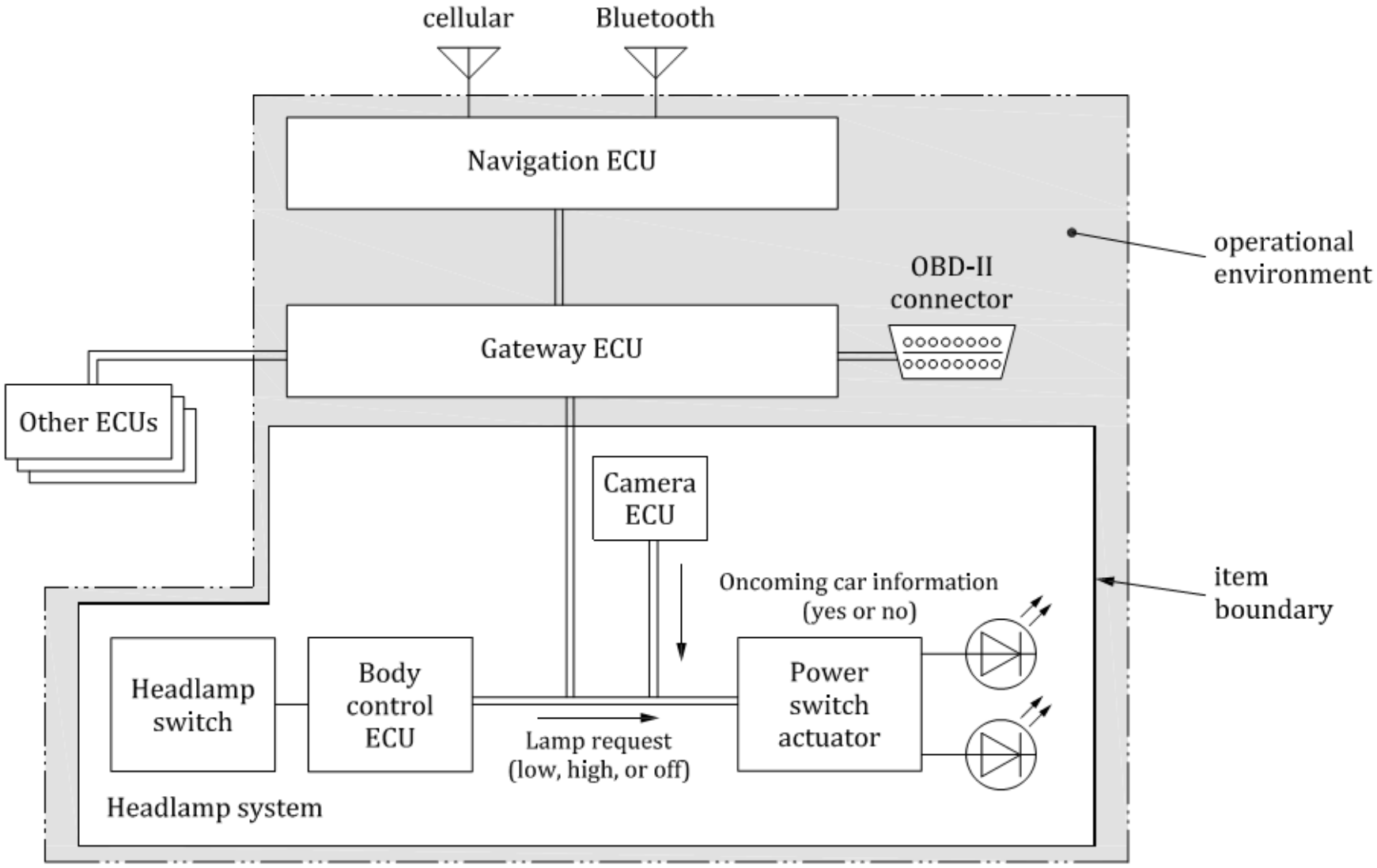
Risk level		Impact level			
		1	2	3	4
Attack feasibility level	1	1	2	2	3
	2	2	2	2	3
	3	2	2	3	3
	4	3	3	3	4

[ISO / SAE 21434:2021]

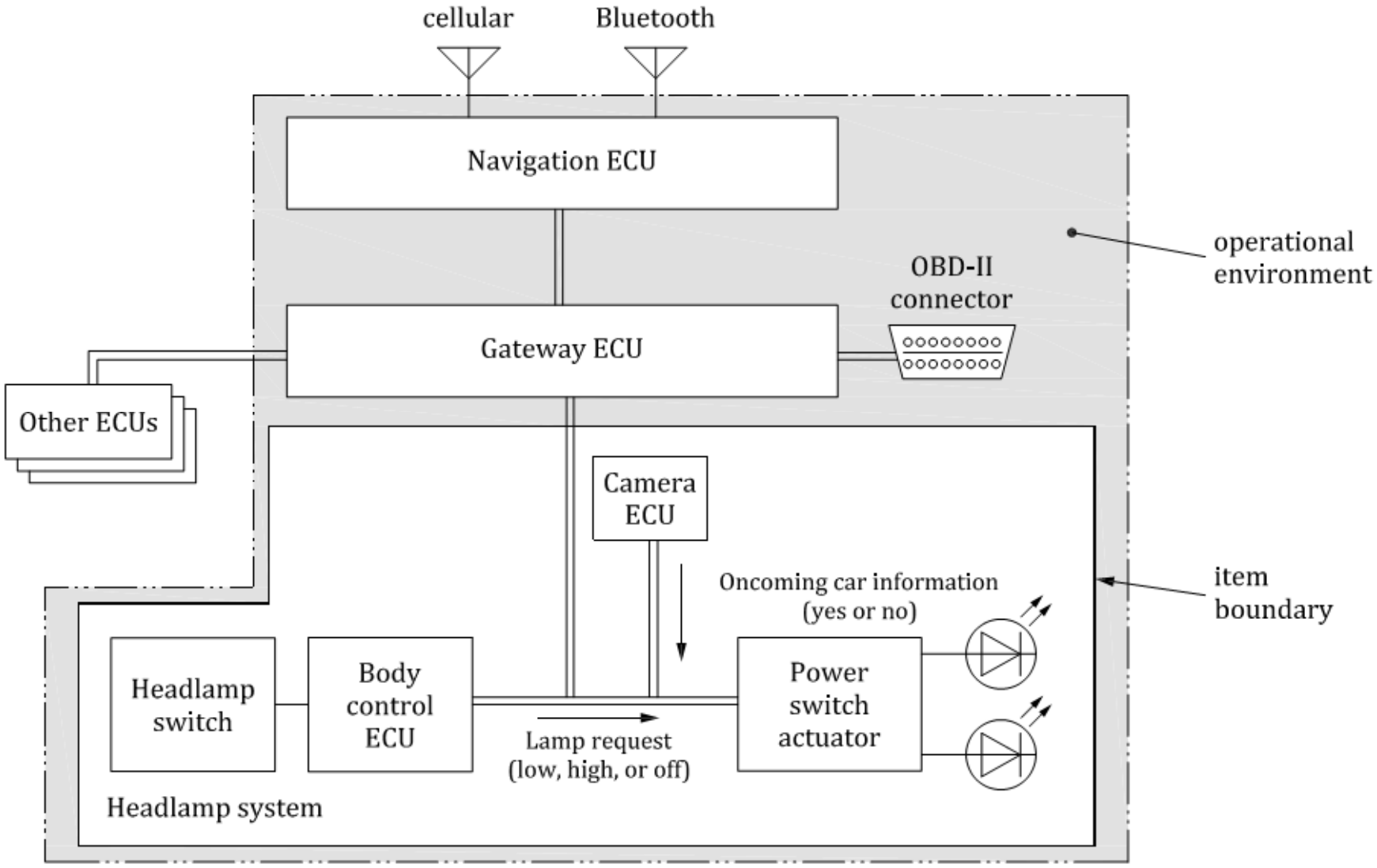
Example – Headlamp system (Annex H)

- i. asset identification;
- ii. impact rating;
- iii. threat scenario identification;
- iv. attack path analysis;
- v. attack feasibility rating;
- vi. risk value determination;
- vii. risk treatment decision.

Example – Headlamp system (Annex H)



Example – Headlamp system (Annex H)



Example – Headlamp system (Annex H)

Table H.1 — Example description of the operational environment

The item (headlamp system) is connected with the gateway ECU, and the gateway ECU is connected with the navigation ECU by data communication.
Navigation ECU has external communication interfaces: — Bluetooth; — cellular. Assumption: — navigation ECU has a firewall to prevent invalid data communication from external interfaces.
Gateway ECU has external communication interfaces: — OBD-II. Assumption: — gateway ECU has strong security controls including a firewall function (developed as CAL4).

Example – Headlamp system (Annex H)

Table H.2 — Example list of assets and damage scenarios

Asset	Cybersecurity property			Damage scenario
	C	I	A	
Data communication (lamp request)	—	X	X	Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.
	—	X	—	Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.
Data communication (oncoming car information)	—	X	—	Drivers of oncoming vehicles are blinded, it is caused by not being able to change to low beam during night driving.
	—	—	X	Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.
Firmware of body control ECU	X	X	—	...

Example – Headlamp system (Annex H)

Table H.3 — Example of impact ratings for damage scenarios

Damage scenario	Impact category	Impact rating
Vehicle cannot be driven at night, because (the driver perceives) the headlamp function was inhibited while parked.	O	Major
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed.	S	Severe (S3)
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving.	O	Moderate

Example – Headlamp system (Annex H)

Table H.4 — Example threat scenarios

Damage scenario	Threat scenario
Front collision with a narrow stationary object (e.g. a tree) caused by unintended turning-off of headlamp during night driving at medium speed	Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
	Tampering with a signal sent by body control ECU leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally.
Malfunctioning automatic high beam caused by headlamp always remaining at low beam during night driving	Asset: oncoming car information Cybersecurity property: availability Associated cause: denial of service of oncoming car information

Example – Headlamp system (Annex H)

Table H.5 — Example attack paths for threat scenarios

Threat scenario	Attack path
Spoofing of a signal leads to loss of integrity of the data communication of the "Lamp Request" signal to the power switch actuator ECU, potentially causing the headlamp to turn off unintentionally	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker compromises navigation ECU from Bluetooth interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
	i. Attacker gets local (see Table G.9) access to OBD connector. ii. Attacker sends malicious control signals from OBD connector. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (OFF).
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.

Example – Headlamp system (Annex H)

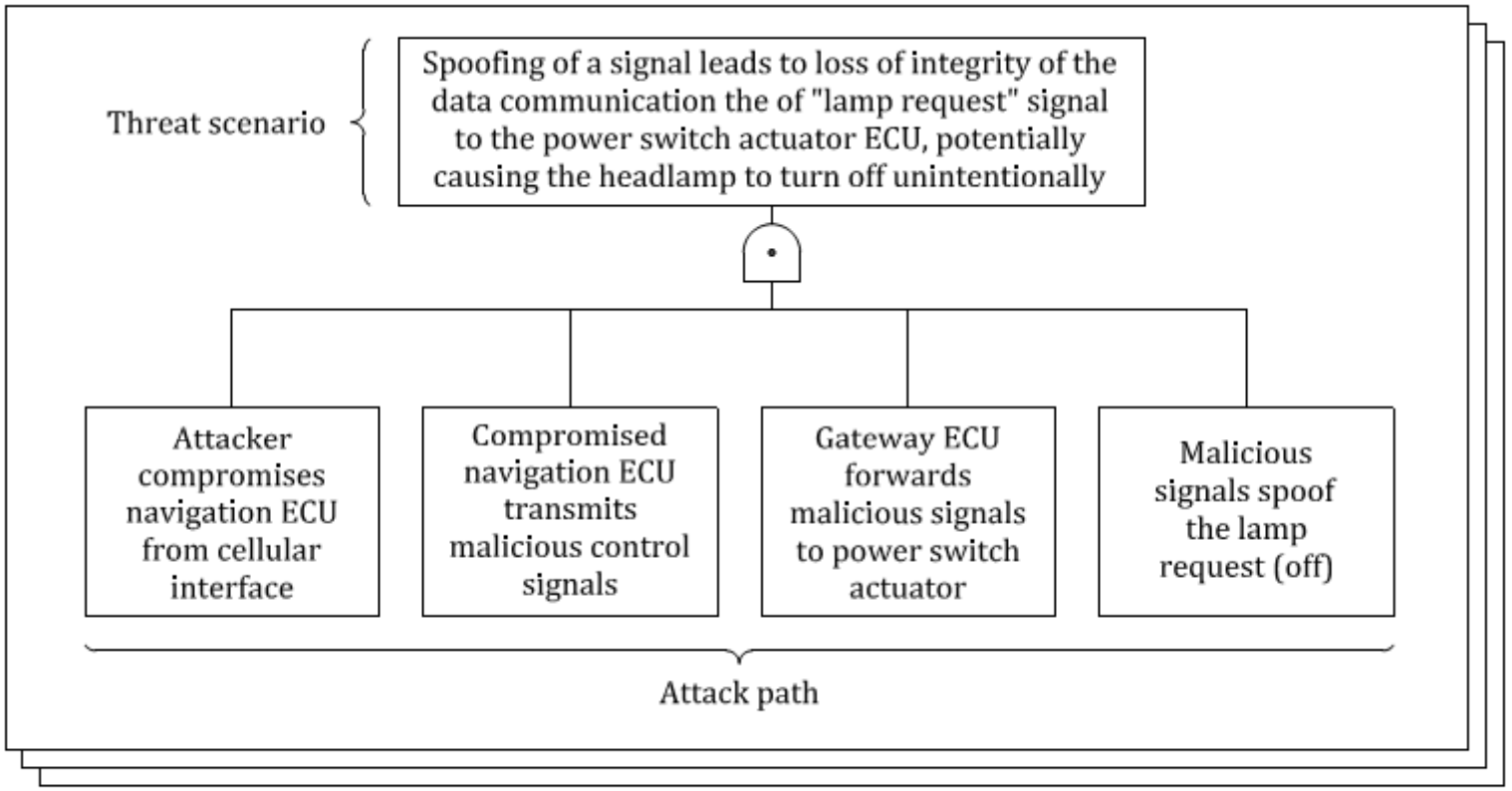


Figure H.3 — Example of an attack path derived by attack tree analysis

Example – Headlamp system (Annex H)

Table H.6 — Examples of attack feasibility rating with the attack vector-based approach

Attack path	Attack feasibility rating
i. Attacker compromises navigation ECU **from cellular interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	High
i. Attacker compromises navigation ECU **from Bluetooth interface**. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Malicious signals spoof the lamp request (ON).	Medium
i. Attacker sends malicious control signals **from OBD2 connector**. ii. Gateway ECU forwards the malicious signals to power switch actuator. iii. Malicious signals spoof the lamp request (ON).	Low

Example – Headlamp system (Annex H)

Table H.7 — Examples of attack feasibility rating with the attack potential-based approach

Threat scenario	Attack path	Attack feasibility assessment						
		ET	SE	KoIC	WoO	Eq	Value	Attack feasibility rating
Denial of service of oncoming car information	i. Attacker compromises navigation ECU from cellular interface. ii. Compromised navigation ECU transmits malicious control signals. iii. Gateway ECU forwards malicious signals to power switch actuator. iv. Attacker floods the communication bus with a large number of messages.	1	8	7	0	4	20	Low
	i. Attacker attaches a Bluetooth-enabled OBD dongle to OBD connector when vehicle is parking unlocked. ii. Attacker compromises driver's smartphone with Bluetooth interface. iii. Attacker sends message via smartphone and Bluetooth dongle to Gateway ECU. iv. Gateway ECU forwards malicious signals to power switch actuator. v. Attacker floods the communication bus with a large number of messages.	1	8	7	4	4	24	Low

Key

ET elapsed time

SE specialist expertise

KoIC knowledge of the item or component

WoO window of opportunity

Eq equipment

Example – Headlamp system (Annex H)

Table H.8 — Risk matrix example

		Attack feasibility rating			
		Very Low	Low	Medium	High
Impact rating	Severe	**2**	**3**	**4**	**5**
	Major	**1**	**2**	**3**	**4**
	Moderate	**1**	**2**	**2**	**3**
	Negligible	**1**	**1**	**1**	**1**

Table H.9 — Examples of determined risk values

Threat scenario	Aggregated attack feasibility rating	Impact rating	Risk value
Spoofing of a signal leads to loss of integrity of the data communication of "Lamp Request" signal for power switch actuator ECU	**High**	**Severe**	**S: 5**
Denial of service of oncoming car information	Low	Moderate	O: 2

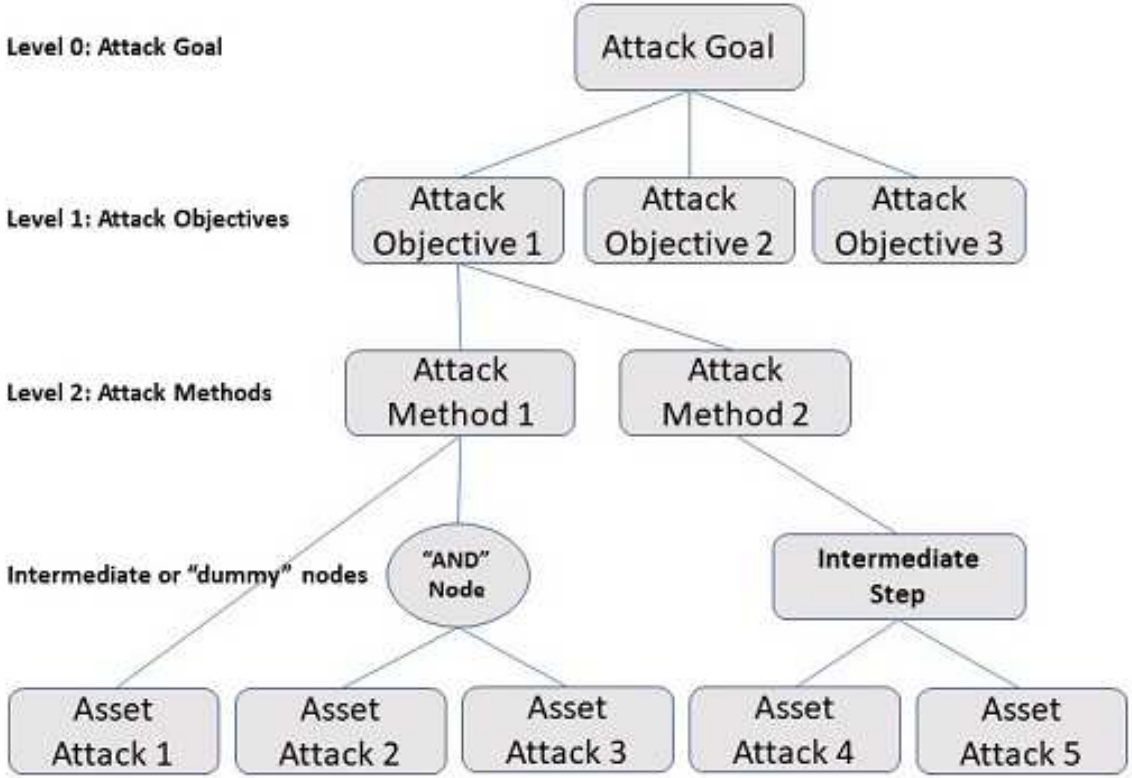
EVITA Technique

- **E-safety Vehicle Intrusion protecTed Applications (EVITA)** is a wide used cybersecurity risk quantification technique compliant to ISO / SAE 21434 for automotive on-board systems networks.
- It represents a well defined answer to HOW.

1) **Asset identification**: wired / wireless infrastructure, RSU, ECU, OBU, …
2) **Threat scenarios and attack paths**: attacker-centric approach, it derives possible starting ASSET ATTACKs to reach the ATTACKER GOAL. Categories for possible attack motivations can be:
   - **Reputational gain as a hacker**: the attacker's primary goal is not to harm the system or the users but rather to publish the results of a successful attack to gain a reputation
   - **Financial gain**: for example, the attacker may tamper with the vehicle for insurance fraud; he attacks the steering or brakes of another vehicle to provoke an accident
   - **Personal gain (non-financial)**: for example, going faster in the traffic, e.g., switching all traffic lights to green or directing other vehicles to alternative routes to make the way clear in front of the attacker
   - **Gain industrial information** about the manufacturer or destroy the reputation of a particular manufacturer
   - **Mass terrorism**
   - **Harm to the economy**: attacking the infrastructure, which may lead to accidents, generate traffic jams, or disrupt the normal state of roads

EVITA: Threat scenarios & Attack paths

- EVITA models attack paths through the ATTACK TREE
- Level 0 (root) represents an abstract **ATTACK GOAL**.
- Level 1 nodes describe the **ATTACK OBJECTIVES** satisfying the **ATTACK GOAL**: the attack risk is computed at this level.
- Level ≥2 nodes introduce the different **ATTACK METHODS** to achieve each **ATTACK OBJECTIVE**. Each **ATTACK METHOD** is composed of (AND/OR) logical combinations of attacks against assets known as **ASSET ATTACKS** representing the tree's leaves.



EVITA: IMPACT Rating

3) Impact rating:

- EVITA separates and categorizes different aspects of the consequences (or **impact**) of possible security breaches.
- The starting point for impact rating in EVITA is the **safety severity** classification of ISO/DIS 26262.

- However for the purposes of EVITA, this has been adapted and augmented to consider both the greater numbers of vehicles that may be involved and implications for aspects other than safety, including:

  - **Privacy**: identification and tracking of vehicles or individuals;
  - **Financial**: financial losses that may be experienced by individuals or ITS operators;
  - **Operational**: interference with vehicle systems and functions that do not impact on functional safety

EVITA: IMPACT Rating (Table 1)

Security threat severity class	Aspects of security threats			
	Safety (S_S)	**Privacy (S_P)**	**Financial (S_F)**	**Operational (S_O)**
0	No injuries.	No unauthorized access to data.	No financial loss.	No impact on operational performance.
1	Light or moderate injuries.	Anonymous data only (no specific driver of vehicle data).	Low-level loss (~€10).	Impact not discernible to driver.
2	Severe injuries (survival probable). Light/moderate injuries for multiple vehicles.	Identification of vehicle or driver. Anonymous data for multiple vehicles.	Moderate loss (~€100). Low losses for multiple vehicles.	Driver aware of performance degradation. Indiscernible impacts for multiple vehicles.
3	Life threatening (survival uncertain) or fatal injuries. Severe injuries for multiple vehicles.	Driver or vehicle tracking. Identification of driver or vehicle, for multiple vehicles.	Heavy loss (~1000). Moderate losses for multiple vehicles.	Significant impact on performance. Noticeable impact for multiple vehicles.
4	Life threatening or fatal injuries for multiple vehicles.	Driver or vehicle tracking for multiple vehicles.	Heavy losses for multiple vehicles.	Significant impact for multiple vehicles.

EVITA: ATTACK potential

- The probability that an attack, once launched, will be successful depends on
  - the “attack potential” of the attacker and
  - the “attack potential” that the system under investigation is able to withstand (which the attack potential of the attacker needs to exceed).

- If the attack potential of the attacker exceeds the attack potential that the system is able to withstand, then the system will definitely not withstand the attack and the attack will be successful.
- The ATTACK potential is a measure of the minimum effort to be expended in an attack to be successful.
- The ATTACK potential for an attack corresponds to the effort required creating and carrying out the attack.

- The ATTACK potential is computed **by summing up the values of 5 potential categories:**

EVITA: ATTACK potential (Table 2)

1) **Elapsed time**: ”**0**” for (≤1 day), ”**1**” for (≤1 week), ”**4**” for (≤1 month), ”**10**” for (≤6 months), ”**19**” for (>6 months)
2) **Expertise**: ”**0**” for layman level: the attacker is unknowledgeable compared to professionals or experts, ”**3**” for proficient level: the attacker is familiar with the security behavior of the system, ”**6**” for expert-level: familiar with security algorithms, hardware, different attack technique, necessary tools, cryptography, ”**8**” if multiple experts in different fields are required
3) **Knowledge of the system**: ”**0**” if the information is publicly available, ”**3**” if the information is restricted (e.g., between organizations), ”**7**” if the information is sensitive (e.g., internal to the organization, ”**11**” if the information is critical (e.g., restricted to a limited number of individuals).
4) **Window of opportunity**: ”**0**” if the access is highly available with no time limitation, ”**1**” if the required access time (≤1 day) and the number of targets needed to be accessed to perform the attack (≤10), ”**4**” if the required access time (≤1 month) and the number of targets needed to be accessed to perform the attack (≤100), ”**10**” if the required access time (>1 month) and the number of targets needed to be accessed to perform the attack (>100)
5) **Equipment**: ”**0**” if it is already available to the attacker (standard), ”**4**” if it is not available but can be obtained without noticeable effort (specialized), ”**7**” if it is specially produced (bespoke), ”**9**” if different bespoke equipment is needed (multiple bespoke).

EVITA: ATTACK feasibility rating (Table 3)

- The **ATTACK potential** is computed **by summing up the values of the attack potential categories** (the values in table below)

4) Attack feasibility analysis: according to ISO/IEC 18045 the attack potential-based approach determines the feasibility rating (or **probability**, or **likelihood**) of performing a successful attack.
It describes the effort needed to mount a successful attack; the lower values for the attack potential, the higher likelihood of a successful attack.

The table below depicts the **ATTACK feasibility rating** derived from the values obtained for the ATTACK potential.

Values	Attack potential required to identify and exploit attack scenario	Attack probability *P* (reflecting relative likelihood of attack)
0-9	Basic	5
10-13	Enhanced-Basic	4
14-19	Moderate	3
20-24	High	2
≥ 25	Beyond High	1

EVITA: ATTACK feasibility rating

- Key elements of the attack trees can be augmented with the severity (S, a vector) for the ATTACK OBJECTIVE and the estimated ATTACK POTENTIAL for the contributing asset attacks, using the numerical scale proposed in the ATTACK feasibility table to reflect the relative probability of a successful attack (P, a scalar). The relationships between the latter are then used to derive a **combined attack feasibility rating** for the particular ATTACK METHOD (A, a scalar).

- If an attack method can be implemented **using any one** of a number of asset attacks (i.e. OR relationship) the combined attack potential is taken to be the **highest** of the attack probabilities (Pi) for the available asset attack options:

  A = max{Pi}

- If an attack method can be implemented **only in conjuction** of a number of asset attacks (i.e. AND relationship) the combined attack potential is taken to be the **lowest** of the attack probabilities (Pi) for the available asset attack options:

  A = min{Pi}

EVITA: ATTACK feasibility rating

Attack Objective	Attack Method	Asset attack
A	A1	a & b
	A2	d
		e
		f
B	B1	a & b & c
		c & h
	B2	g

Attack Objective	Severity (S)	Attack Method	Risk level (R)	Combined attack potential (*A*)	Asset (attack)	Attack Probability (*P*)
A	S_A	A1	$R_{A1}(S_A, A_{A1})$	$A_{A1}=\min\{Pa,Pb\}$	a & b	*Pa* *Pb*
		A2	$R_{A2}(S_A, A_{A2})$	$A_{A2}=\max\{Pd,Pe,Pf\}$	d	*Pd*
					e	*Pe*
					f	*Pf*
B	S_B	B1	$R_{B1}(S_B, A_{B1})$	$A_{B1}=\max[\min\{Pa,Pb,Pc\}, \min\{Pc,Ph\}]$	a & b & c	*Pa* *Pb* *Pc*
					c & h	*Pc* *Ph*
		B2	$R_{B2}(S_B, A_{B2})$	$A_{B2}=Pg$	g	*Pg*

EVITA: Risk determination (Table 4)

5) **Risk determination**: risk values range into 7 classes (from R0 "minimum" to R7+ "critical"). The risk of an attack is seen as a function of the possible **severity** (i.e. the cost and loss) of the attack for the stakeholders and the **estimated probability** of occurrence of a successful attack.

- The risk level (R, a vector) is determined from the severity (S) associated with the attack objective and the combined attack probability (A) associated with a particular attack method.
- This is achieved by mapping the severity and attack probability to the risk using a "risk graph" approach.
- For severity aspects that are not safety related the risk graph maps two parameters (attack probability and severity) to a qualitative risk level. Combinations of severity and combined attack probability are mapped to a range of "security risk levels" (denoted Ri, where "i" is an integer).

Security Risk Level (R)		**Combined attack probability (A)**				
		A=1	A=2	A=3	A=4	A=5
Non-safety severity (S_i)	S_i=1	R0	R0	R1	R2	R3
	S_i=2	R0	R1	R2	R3	R4
	S_i=3	R1	R2	R3	R4	R5
	S_i=4	R2	R3	R4	R5	R6

EVITA: Risk determination (Table 5)

- Where the severity vector includes **a non-zero safety component**, the risk assessment may include an additional probability parameter that represents the **potential for the driver to influence the severity of the outcome**.

- In the MISRA Safety Analysis Guidelines and ISO/DIS 26262 this possibility is reflected in a qualitative measure referred to as "**controllability**":

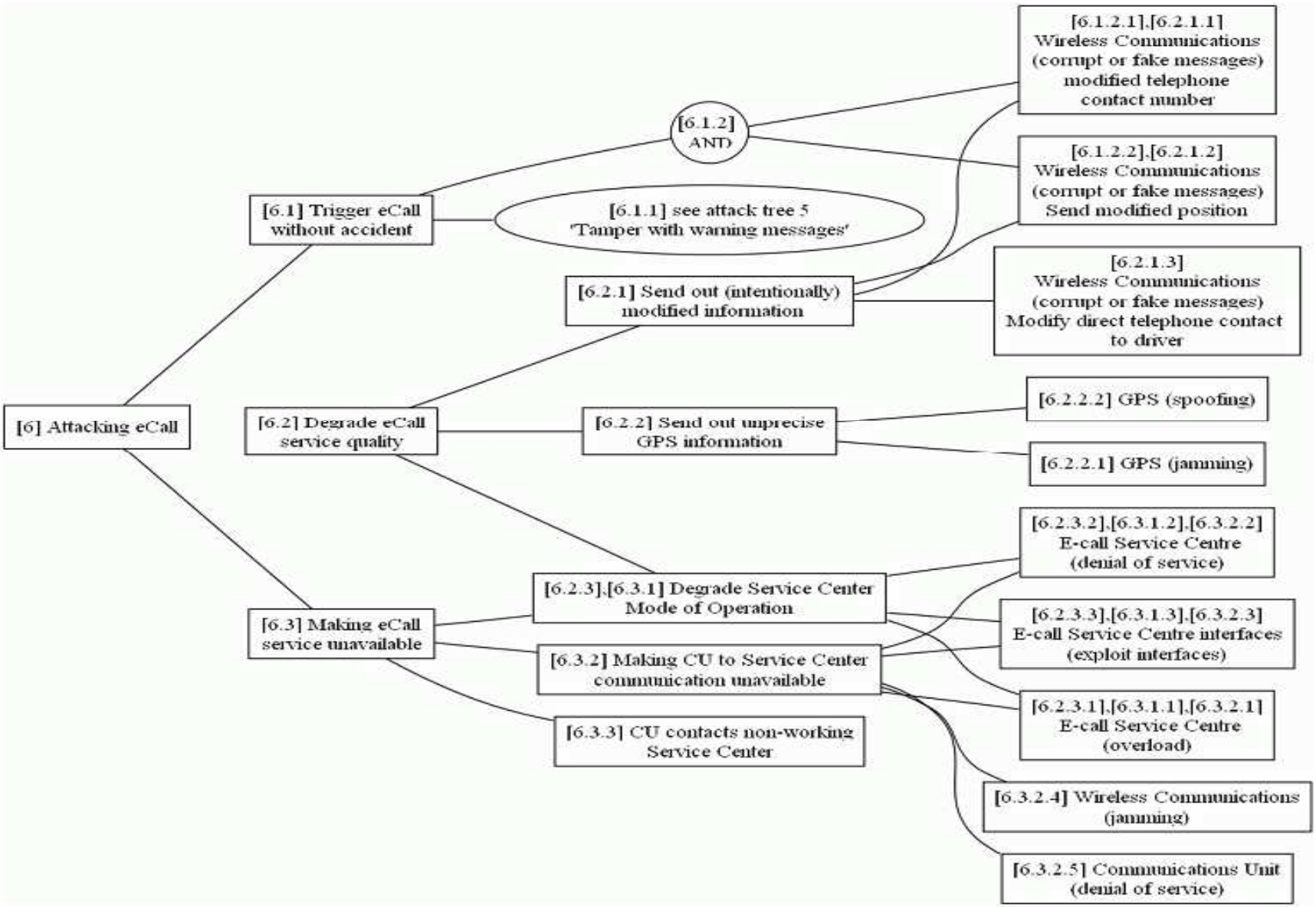
Class	Meaning
C1	Despite operational limitations, avoidance of an accident is normally possible with a normal human response.
C2	Avoidance of an accident is difficult, but usually possible with a sensible human response.
C3	Avoidance of an accident is very difficult, but under favourable circumstances some control can be maintained with an experienced human response.
C4	Situation cannot be influenced by a human response.

EVITA: Risk determination (Table 6)

- In order to include the additional parameter (controllability) in the assessment of safety related security risks it is necessary to use of a different risk graph as proposed in the table below which maps three parameters (severity, attack probability, and controllability) to qualitative risk levels.
- Class "R7+" denotes levels of risk that are unlikely to be considered acceptable, such as safety hazards with the highest severity classes and threat levels, coupled with very low levels of controllability.

Controllability (C)	Safety-related Severity (S_S)	Combined Attack Probability (A)				
		A=1	A=2	A=3	A=4	A=5
C=1	S_S=1	R0	R0	R1	R2	R3
	S_S=2	R0	R1	R2	R3	R4
	S_S=3	R1	R2	R3	R4	R5
	S_S=4	R2	R3	R4	R5	R6
C=2	S_S=1	R0	R1	R2	R3	R4
	S_S=2	R1	R2	R3	R4	R5
	S_S=3	R2	R3	R4	R5	R6
	S_S=4	R3	R4	R5	R6	R7
C=3	S_S=1	R1	R2	R3	R4	R5
	S_S=2	R2	R3	R4	R5	R6
	S_S=3	R3	R4	R5	R6	R7
	S_S=4	R4	R5	R6	R7	R7+
C=4	S_S=1	R2	R3	R4	R5	R6
	S_S=2	R3	R4	R5	R6	R7
	S_S=3	R4	R5	R6	R7	R7+
	S_S=4	R5	R6	R7	R7+	R7+

Attack Path – ex. “Attacking eCall”

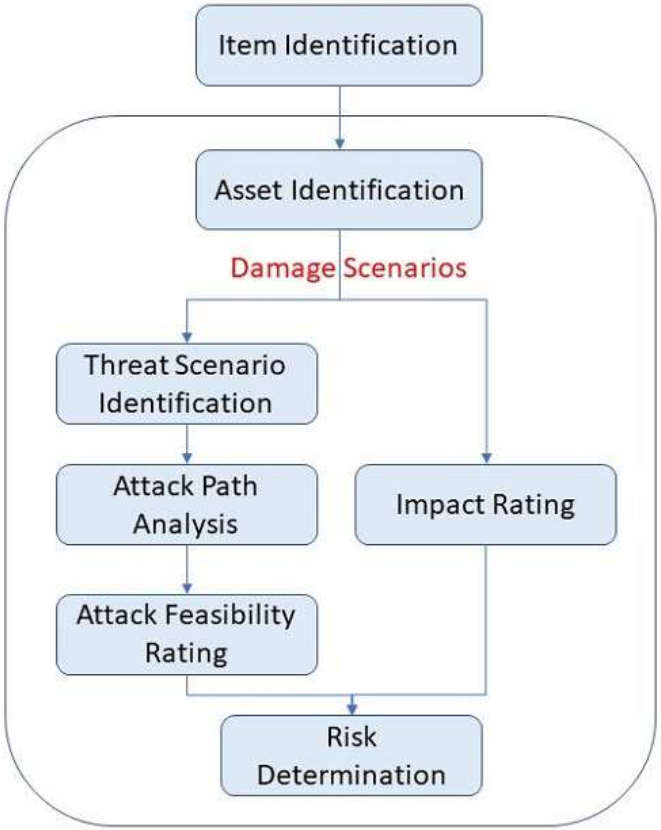


Risk Determ. – ex. “Attacking eCall”

Attack Objective	Severity (S)	Attack Method	Risk level (R)	Combined attack probability (*A*)	Asset (attack)	Attack probability (*P*)
6.1 Trigger spurious E-Call	S_S=0 S_P=0 S_F=0 S_O=3	Generate false emergency brake message	R_O=R4	4	5.3.1.1 Backbone bus Communications (listen, intercept, alter, inject, replay)	2
					5.3.3.2 GPS (spoofing) & 5.3.3.1 Wireless Communications (corrupt or fake warning messages)	**4** *5*
		Generate false e-Call message	R_O=R2	2	6.1.2.1/2 Wireless Communications (listen, intercept, alter, inject, replay)	**2**
6.2 Degrade E-Call service quality	S_S=0 S_P=0 S_F=0 S_O=3	Attack service centre	R_O=R3	3	6.2.3.1 Service Centre (overload)	2
					6.2.3.3 Service Centre interfaces (denial of service)	1
					6.2.3.3 Service Centre Interfaces (exploit interfaces)	**3**
		Corrupt transmitted information	R_O=R2	2	6.2.1.1-3Wireless Communications (listen, intercept, alter, inject, replay)	2
		Corrupt GPS information	R_O=R5	5	6.2.2.1 GPS (jamming)	**5**
					6.2.2.2 GPS (spoofing)	4
6.3 Denial of service For E-Call	S_S=0 S_P=0 S_F=0 S_O=3	Attack service centre	R_O=R3	3	6.3.3.1 Service Centre (overload)	2
					6.3.3.2 Service Centre interfaces (denial of service)	1
					6.3.3.3 Service Centre Interfaces (exploit interfaces)	**3**
		Attack communications with service centre	R_O=R5	5	6.3.2.5 Communications Unit (denial of service)	4
					6.3.2.4 Wireless Communications (jamming)	**5**
					6.3.2.1 Service Centre (overload)	2
					6.3.2.2 Service Centre interfaces (denial of service)	1
					6.3.2.2 Service Centre Interfaces (exploit interfaces)	3
		Make Communications Unit contact non-working service centre	R_O=R2	2	6.3.3.1 Communications Unit (corrupt data)	2

Guide Line for TARA execution using EVITA

1. **Item Identification and Asset Identification**: build the ASSET lists.
2. **Impact Rating** by using TABLE 1 (impact severity).
3. **Threat Scenario Identification**: identify the ATTACK GOAL, the ATTACK OBJECTIVEs, the ATTACK METHODS and the ASSET ATTACKS.
4. **Attack Path Analysis** by drawing the ATTACK TREE (AT): ATTACK GOAL (AT root), the ATTACK OBJECTIVEs, ATTACK METHODS (AT intermediates) and ASSET ATTACKS (AT leaves). Each ATTACK METHOD is composed of (AND/OR) logical combinations of ASSET ATTACKS. Compute the attack potential by using TABLE 2 (attack potential).
5. **Attack Feasibility Rating** by using TABLE 3 (attack feasibility rating from attack potential results).
6. **Risk Determination** by using TABLE 4 (risk matrix with S_S=0), TABLE 5 (human controllability) and TABLE 6 (risk matrix with S_S>0).



Outline

- The framework of Security Management
- From Risk to Security Management
  - Security Management Process
  - Approaches for Risk Evaluation
  - Techniques for Risk Evaluation
  - P-I Matrix and isorisk curves
  - FTA - CVSS
  - NIST SP 800-30 Guide for Conducting a Risk Assessment
- Security management automotive domain
  - ISO / SAE 21434
  - Threat Analysis and Risk Assessment (TARA)
  - Cybersecurity Risk Quantification technique: EVITA
  - Guide line for TARA execution using EVITA
- Reference Cyber Security functions
  - Security metrics
  - Timing constraints
  - Cyber Risk Mitigation

Reference Cyber Security Functions

- **Passive (preventive) Security Measure (PSM) or functions (PSF): no feedback information on the state of the system is returned**, i.e. pure deterrence, **risk probability is reduced by delaying risk occurrence or by discouraging attacks**:
  - Typically spread spectrum modulations, ciphering and authentication techniques, hashing, nouncing, ….
  - Main performance indicator can be considered the **deterrence delay** formally defined as the **time needed for an attacker to finalize its attack**.
- **Active (preventive) Security Measure (ASM) or functions (ASF): feedback information on the state of the system is returned in time for intervention, risk probability is reduced by applying contrast countermeasures**
  - Typically intrusion detection systems (IDS) i.e. system behavior estimators through techniques as AI, ML , …
  - Main performance indicators can be considered the **FPR (False Positive Rate)** defined as FP/(FP+TN) and **FNR (False Negative Rate)** defined as FN/(FN+TP) with FP, FN, TP, TN are respectively the probabilities to estimate a normal event as abnormal (false positive), an abnormal event as normal (false negative), as truly abnormal (true positive) and truly normal (true negative); hance FP + TN = probability to estimate an event as normal and FN + TP = probability to estimate an event as abnormal.

Security Metrics

- **PERFECT Security** (or UNCONDITIONED Security)
  - For PSF when **deterrence delay = infinite**
  - For ASF when **FPR = 0 and FNR = 0**
- **REALISTIC Security** (or CONDITIONED Security)
  - For PSF when **deterrence delay < infinite**
  - For ASF when **FPR > 0 and FNR > 0**
- Deterrence delay value is directly proportional to the entropy associated to ciphered data flows: infact if entropy per binit = 1 then ciphered data flows can be regarded as pure random bit sequences. Deterrence delay would be infinite because the inverse problem (which is a deterministic algorithm) underlying the cryptographic scheme would result in infinite complexity as pure random generators using deterministic algorithms do not exist. Realistically entropy per binit < 1, inverse problems complexity is finite and deterrence delay is finite.
- FPR and FNR values are inversely proportional to the Representation Capacity (RC) of a behaviour estimator. Given a representation model, the higher is RC, the more are the behaviours that can be detected. A specific behaviour is associated to a specific state sequence, therefore a behaviour estimator can be modelled as a state machine: the more the states, the more are the different possible state sequences. Any "unexpected" / "expected" behaviour that happens to be not represented by a specific state sequence, leads to a "false negative" / "false positive". FPR=0 e FNR=0 only if state sequences are infinite, hence states are infinite. Realistically state machine are finite states, hence FPR > 0 e FNR > 0.

Timing Constraints

- **Computation Capacity**: performance indicator for a processor is the FLoating point Operations Per Second (FLOPS).

- **T_P: deterrence delay** of a PSM. Given a problem of lower bound complexity O(f(x)), with f() the average number of bit operations vs. x predominant factor in the algorithm, then **$T_P \geq f(x) / CC$**.

An example:
A powerful server has CC ≈ 300 GFLOPS ≈ $3 \cdot 10^{11}$ operations /sec.
For RSA scheme $f(n) \sim \exp((\ln n)^{1/3} \cdot (\ln \ln n)^{2/3})$
Setting k=3072 bit, hence $n=2^{3072}$, $f(n) \approx 10^{21}$ operations.

$T_p \geq 0{,}3 \cdot 10^{10}$ seconds ≈ **100 years**

Therefore key life-time must be << 100 years !!
The same security level with k = 256 bit for ECC cryptoschemes !!

A typical communication session life-time in WSN / VANETS is about **seconds**!!

Timing Constraints

- T_P: **deterrence delay** of a PSF.
- T_A: **reaction time** of an ASF (latency from detection to alarm issue).
- T_O: latency for attack resolution (**intervention time** is the feedback latency of an organization from alarm reception to attack resolution). Attack resolution includes actuations as disconnections, quarantines, ad hoc monitoring (T_O includes latencies for actuation execution).
- T_{ATT}: attack duration against the function / system.
- T_{OP}: operation time of the function / system.

Time equations for PSM and ASM:

$$\begin{cases} T_P > T_{OP} \\ T_{ATT} < T_P \\ T_A + T_O < T_{ATT} \end{cases}$$

deterrence delay > operation time

attack duration < **deterrence delay**

reaction time + **intervention time** < attack duration

Required vs. Offered Security Level

- The **Required Security Level (RSL)** or **(Technical) Security Requirements** define the requested minimum technical security measures associated to risk acceptance. Example of RSL are:
  - Minimum Deterrence Time (mDT)

    mDT = MAX(operation time, attack duration)
  - Maximum Reaction Time (MRT), Maximum Intervention Time (MIT)

    MRT + MIT = attack duration
  - Maximum FPR (MFPR), Maximum FNR (MFNR)

- The **Offered Security Level (OSL)** of a security function defines the offered security magnitudes according to the security metrics that should comply to the required security levels. Example of compliant OSL are:
  - $(\text{Deterrence Time})_{PSF} \geq \text{mDT}$
  - $(\text{Reaction Time})_{ASF} \leq \text{MRT}$
  - $(\text{Intervention Time})_{SOC} \leq \text{MIT}$ (depends on SOC organization)
  - $FPR_{ASF} \leq \text{MFPR}$
  - $FNR_{ASF} \leq \text{MFNR}$

Cyber Risk Mitigation

- **KEEP IN MIND** Kerckhoffs' principle: "**A cryptosystem should be secure even if everything about the system, except the key, is public knowledge, and it should not be a problem if it falls into enemy hands**"
- **DERIVE** the **(Technical) Security Requirements** from **Cyber Risk Assessment**
- **DEPLOY** the suited **PSF / ASF** fitting **(Technical) Security Requirements**
- **BE COMPLIANT TO** the Timing Constraints
- **DERIVE** the PSF / ASF performance indicators for Conditioned Security
- **KEEP IN MIND** Shannon's security theorems for PSF performance indicators:
  - Perfect Secrecy → **secret keys should be kept at random and each message should ciphered using a different secret key**
  - Key Equivocation → **an observer should not gain information about the secret key by recording a ciphered message**
  - Unicity Distance → **an observer should record infinite ciphered messages (i.e. should wait for ever) to reduce key equivocation to zero (i.e. get the secret key)**