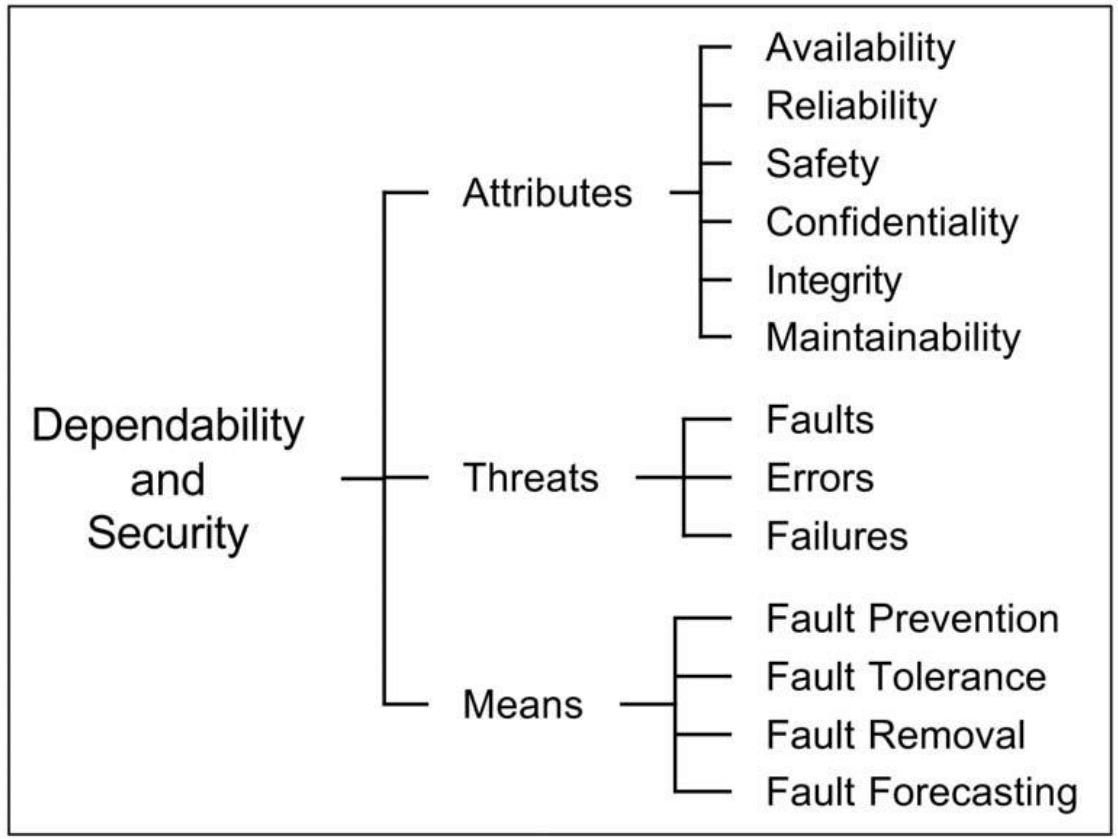
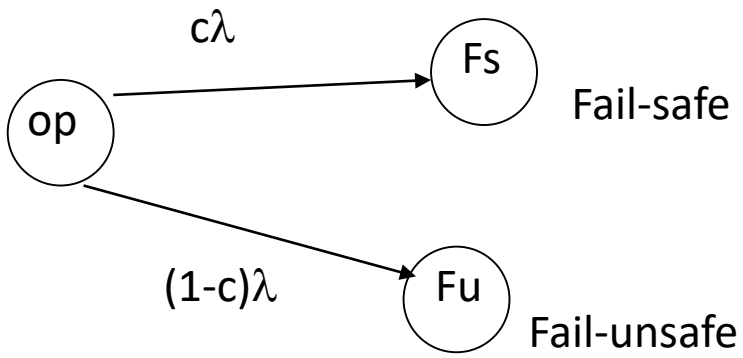

Dependability and Security
Attributes
Availability
Reliability
Safety
Confidentiality
Integrity
Maintainability
Threats
Faults
Errors
Failures
Means
Fault Prevention
Fault Tolerance
Fault Removal
Fault Forecasting

Safety

Safety - avoidance of catastrophic consequences -
As a function of time, S(t), is the probability that the system either behaves correctly or will discontinue its functions in a manner that causes no harm (operational or Fail-safe)

Coverage – The coverage is the measure **c** of the system ability to reach a fail-safe state after a fault.

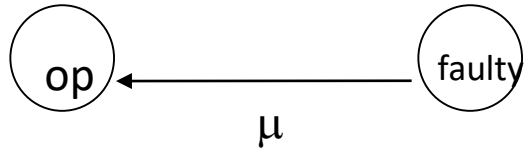


Modeling coverage in a Markov chain means that every unfailed state has two transitions to two different states, one of which is fail-safe, the other is fail-unsafe.

Maintenability

MTTR - The Mean Time To Repair is the average time required to repair the system. MTTR is expressed in terms of a repair rate m which is the average number of repairs that occur per time period, generally number of repairs per hours

$$\mu = 1/MTTR$$



Maintenability - M(t) is the conditional probability that the system is repaired *throughout the interval* of time [0, t], given that the system was faulty at time 0

$$M(t) = 1 - e^{-\mu t}$$

with μ constant repair rate.

Security

Security is defined as resilience to malicious attacks

This can be viewed as

computer systems failures due to intentional attacks

Causes of security violations are different from the causes of failures in hw or sw

Failures are caused by human intent
Failures are correlated
Failures depend on subtle way on the system structure

Attackers learn over time

Security

Survivability:

Capability of a system to fulfill its mission in a timely manner, in presence of attacks, failures or accidents

Survivability is related to the ability of the system to perform an intended function (modelling approaches related to reliability and availability can be applied)

Security

Reliability in the face of system's vulnerability and malicious attacks

Development of stochastic descriptions of events that may occur during a cyber attack

Probabilities in modelling cyber attacks

Stochastic models for computing measures

Security

Availability in the face of system's vulnerability and malicious attacks

Depends on
- attack's own impact on the system
- effort to diagnose the attack
- restore system service following the attack

how long a system remains following a successful attack

Security

- Safety under malicious attacks

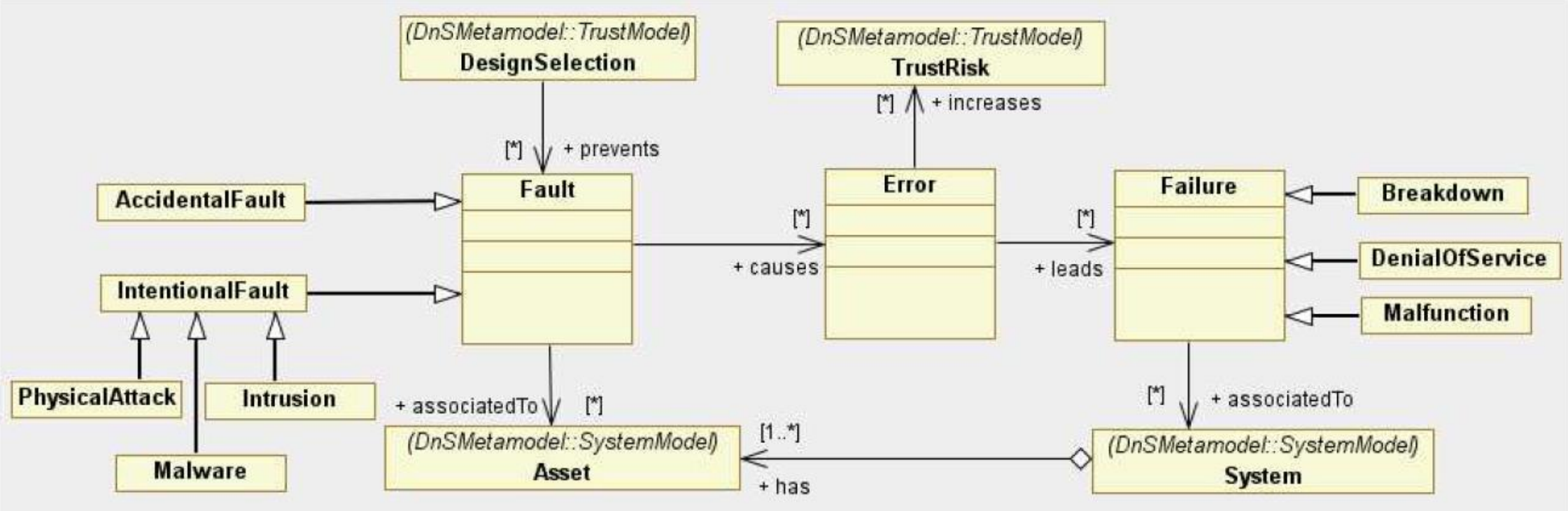
  - safety depends on the effects of a system failure other than on the causes of failures

  - quantification of safety in the context of cyber attacks

Example: Denial of service cyber attack

- Impact of that type of attack on system safety

EVITA project: classification of fault



[EVITA-D2.3] E-safety vehicle intrusion protected applications (EVITA) project. Project reference: 224275 Programme: EU Seventh Reserch Framework Programme (2007–2013) Deliverable D2.3. *Security requirements for automotive on-board networks based on dark-side scenarios*.

Security

Additional attribute of security not included in reliability and availability

- **Data confidentiality**
  protected data not read by unauthorized users
- **Data integrity**
  protected data not modified by unauthorized users

both attributes are not related to the functionality of the system

- **Nonrepudiation**
  Prevents future false denial of involvement by either party in a transaction
- **Authentication**
  The claimed identity of a party to a transaction can be independently verified

Security

Models for security analysis must describe

1. How and when security attacks occur
2. Impact of an attack on the system when it is executed successfully
3. Mechanisms, effects and costs of system recovery, system maintenance and defenses

There are differences with classical dependability

- In the nature and details of security models

Asset: information or resources that could be subject to attack

Security

Example: Denial of service cyber attack

- Impact of that type of attack on system safety
- The system's attempts to cope with it

  -> we can evaluate the time spent in states that reflect the attack

Examples of Security failure

Misconfiguration (at any level of the application stack: network service, web server, databases, virtual machine, …) is a source of security vulnerability

Failure due to misconfiguration can occur in many context

but

some external agent must deliberately exercise the vulnerability in order for the failure to occur

Examples of Security failure

Latent software faults (e.g., buffer overflow problems)
Are another cause of security failure

Any given fault has a specific behavior and requirements for accessing and exploiting it.

Security penetration
made possible by latent sw fault
does not occur accidentally but is induced by an attacker

A security penetration may require an attacker to exercise several vulnerabilities before compromising an asset

Microsoft Security Development Lifecycle (SDL) Threat Modeling tool

The STRIDE threat model provides a way to methodically review system designs and highlight security threats.

STRIDE uses six security threat categories to review system design (developed at Microsoft):

Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

"what can go wrong in this system we're working on?"

SDL report

Element Name	Threat Type
ECU:OBD:Response	Tampering
ECU:OBD:Response	InformationDisclosure
ECU:OBD:Response	DenialOfService
ECU:RequestMemLocation:Request	Tampering
ECU:RequestMemLocation:Request	InformationDisclosure
ECU:RequestMemLocation:Request	DenialOfService
MemLocation:RequestMemLocation:Response	Tampering
MemLocation:RequestMemLocation:Response	InformationDisclosure
MemLocation:RequestMemLocation:Response	DenialOfService
OBD:ECU:Request	Tampering

Shostack (2014). Threat Modeling: Designing for Security. Wiley.

.....

Other Threat classifications

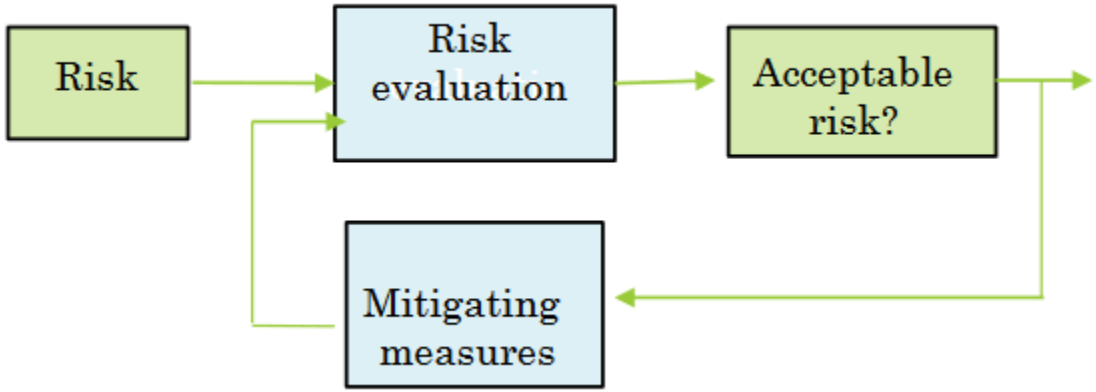
Other approaches classify vulnerabilities ad threats that may appear in general in a computer system

PLOVER : Preliminary List Of Vulnerability Examples for Researchers identifies 28 specific Weaknesses, Idiosyncrasies, Faults and Flaws (WIFFs)

Authentication error
Buffer overflows
Permissions, Priviledges, Access Control List
…….

Risk analysis

Also approaches for the risk analysis are applied to security threats



Risk analysis has been extensively applied in safety critical systems, using established techniques for quantitative evaluation of dependability, like Fault Trees and Failure Mode and Effects Analysis, Stochastic models.

Hazards identification

Quantitative evaluation of the risk

Risk analysis

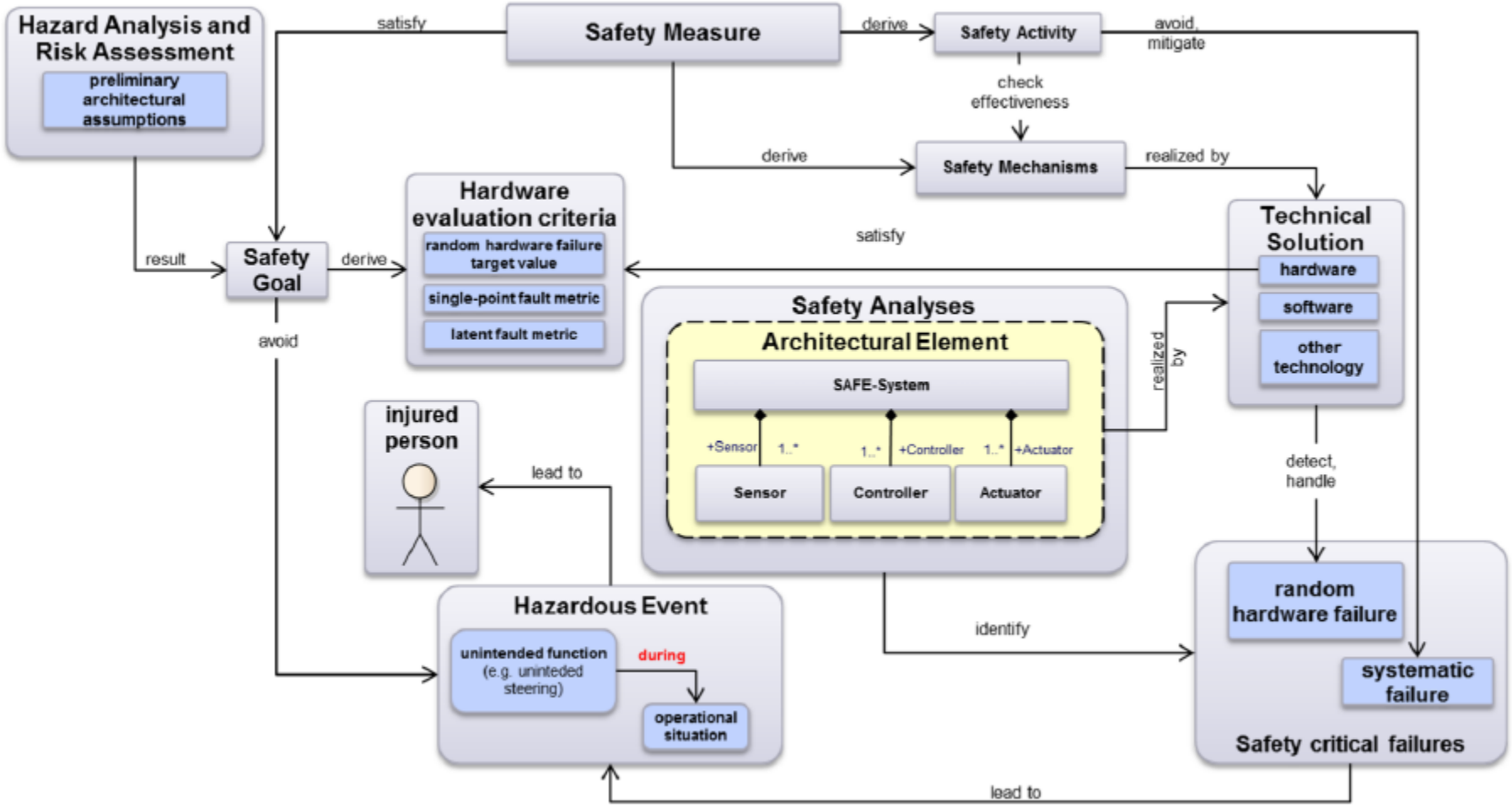
Functional safety:
the ability of the system to deliver the expected functionality during its operational life

The objective of functional safety is to reduce the probability of failures at a given acceptable rate in presence of malfunctioning behaviors

In the hazard and risk analysis, hazardous events are identified and the necessary risk reduction for these events determined.

Tolerable risk: risk which is accepted in context based on the current values of society

SAFURE project: System development and Safety analyses



SAFURE - Safety And Security By Design For Interconnected Mixed-Critical Cyber-Physical Systems, H2020 project EU project (https://safure.eu/)

Safety critical systems regulations

IEC 61508:
Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems
an international standard of rules for programmable systems applied in industry

ISO 26262: Road vehicles – Functional safety

adaptation of IEC 61508 specific to the application sector of electrical and electronic systems in automotive industry

ISO 26262 is the established safety standard in automotive

IEC - International Electrotechnical Commission

ISO - International Organization for Standardization

Risk analysis

Problems caused by malicious attacks are not addressed by the hazard analysis and risk assessment within the ISO 26262 standard

Cyber-security as a risk factor to be considered in the hazard and risk analysis

ISO/SAE CD 21434 -Road Vehicles –Cybersecurity engineering
https://www.iso.org/standard/70918.html (under development)

Schmittner et al., Towards a Framework for Alignment between Automotive Safety and Security Standards Conference Paper · September 2015

Risk assessment tools

risk assessment tools implement several risk assessment methodologies

- DREAD risk assessment method
- Common Vulnerability Scoring System (CVSS)
- OWASP Risk Rating Methodology
- SAHARA

DREAD risk assessment method

Categories of risk analysis

– **D**amage potential
Ranks the extent of damage that occurs if a vulnerability is exploited

– **R**eproducibility
Ranks how often an attempt at exploiting a vulnerability really works

– **E**xploitability
Effort required to exploit the vulnerability (a number) e.g. authentication is considered

– **A**ffected users
number of instances of the system that would be affected if an exploit became widely available

– **D**iscoverability Measures
the likelihood that a vulnerability will be found by hackers

DREAD risk assessment method

$$\text{Risk} = \frac{\text{Damage} + \text{Reproducibility} + \text{Exploitability} + \text{Affected Users} + \text{Discoverability}}{5}$$

Rating scale for each category: 0-10

1 being the least probability of the occurrence
and the least damage potential

Common Vulnerability Scoring System (CVSS) - open framework

CVSS is comprised of three different metric groups: Base, Temporal, and Environmental.
Each one consists of their own set of metrics.

Base:
- Access Vector
- Access Complexity
- Authentication
- Confidentiality Impact
- Integrity Impact
- Availability Impact

Temporal
- Exploitability
- Remediation Level
- Report Confidence

Environmental
- Collateral damage potential
- Target distribution
- Confidentiality requirement
- Integrity requirement
- Availability requirement

Common Vulnerability Scoring System (CVSS) - open framework

Risk =

Base Metrics
f(x1, x2, …., xn)

Exploitability sub-score equation
Impact sub-score equation

refined by

Temporal Metrics
f(y1, y2, …, yn)

Environmental Metrics
f(z1, z2, …, zn)

severity posed by a vulnerability to a user's environment at a specific point in time in a computing environment .

https://www.first.org/cvss/calculator/3.0

CVSS : example

Category	Subcategory	Value
Access Vector (AV)	- L (Local) accessible only on device	0.395
	- A (Adjacent network) accessible via directly attached bus	0.646
	- N (Network) accessible via any number of networks	1
Authentication (Au)	- M(Multiple) multiple auth. steps	0.45
	- S (Single) one auth. step	0.56
	- N (None) No authentication is required	0.704

Score: 0 – 10

OWASP risk assessment rating methodologies

https://owasp.org/

Open Web Application Security Project (**OWASP**) web application security
Estimates both technical and business impact factors

Starts from the standard risk model:

Risk = Likelihood * Impact

The following methodology is defined, where factors for the likelihood and impact of each risk are considered

OWASP risk assessment rating methodologies

Step 1: Identify Risk

Step 2: Factors for estimating likelihood

- Threat Agent Factors
- Vulnerability Factors

Step 3: Factors for estimating impact

- Technical Impact Factors
- Business Impact Factors

Step 4: Determining severity of risk

- Informal Method
- Repeatable Method
- Determining Severity

Step 5: Deciding what to fix

Step 6: Customizing your risk rating model

OWASP top 10 vulnerabilities in web applications
https://www.ibm.com/developerworks/library/se-owasptop10/

Security-Aware Hazard Analysis and Risk Assessment SAHARA

SAHARA method allows the evaluation of the impact of security issues on safety at the system level.

Threats are **quantified** according to

- **Required Resources**
- **Know-How** that are required to define threats
- Threats **Criticality**

The impact of the threat on the system determines whether the threat is safety-related or not. If the threat is safety-related, it will be analysed and the resulting hazards will be evaluated.

Georg Macher, et al.. SAHARA: A Security-Aware Hazard and Risk Analysis Method. DATE 2015
https://past.date-conference.com/proceedings-archive/2015/pdf/0622.pdf.

Security-Aware Hazard Analysis and Risk Assessment SAHARA

Level	Threat Criticality	Example
0	no security impact	No security impact
1	Moderate security relevance	Reduced availability
2	High security relevance	non availability, privacy intrusion
3	High security and possibly safety relevance	Life threatening abuse possible

Level	Required Know-How	Example
0	no prior knowledge (black-box approach)	Unknown internals
1	Technical knowledge (gray-box approach)	Electrician, mechanic basic understanding of internals
2	Domain knowledge (white-box approach)	person with technical training, internal disclosed

Security-Aware Hazard Analysis and Risk Assessment SAHARA

Level	Required resourse	Example
0	no additional tool or everyday commodity	randomly using of user intìerface screwdriver, coin
1	standard tool	
2	simple tool	CAN sniffer, oscilloscope
3	advanced tool	debugger, bus communication simulator …

		Threat Level 'T'			
Required Resources 'R'	**Required Know-How 'K'**	0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

Security Level Determination matrix

Classification of hazards according to the matrix
4 is the highest security class

Evaluation of Security

Combinatorial models

All basic events must be statistically independent

Do not model state - they model operational dependency of the system on the components

Reliability block diagrams: not used in security

Fault trees -> Attack trees

Attack trees:

used to explore a system to find possible vulnerabilities

Attack Trees

The tree describes sets of events that can lead to the goal in a combinatorial way

Security of the system:

set of attack trees, where the root of each tree is the goal of a attacker that can damage the system operation

1. Root = goal of an attacker
2. Leaf nodes = different basic ways to achieve that goal (atomic attacks)
3. OR nodes = a node of which only one of its child nodes needs to be successful
4. AND nodes = a node of which all of its child nodes need to be successful

Attack tree published in [Buldas 20]
Ahto Buldas et al. Attribute evaluation on attack trees with incomplete information, Computers & Security 88 (2020)

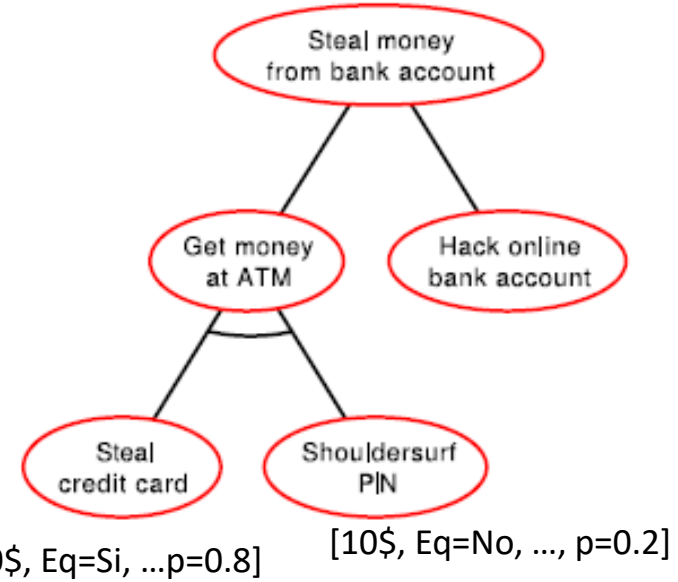
Attack Trees

Evaluation of different aspects of the system security, depending on the kind of values assigned to the leaf nodes

Since an atomic attack can have multiple values, the attack tree can be used to combine these values and help users to learn more about a system's vulnerability

Example

Possible/impossible, cost -> lowest possible cost attack



Example

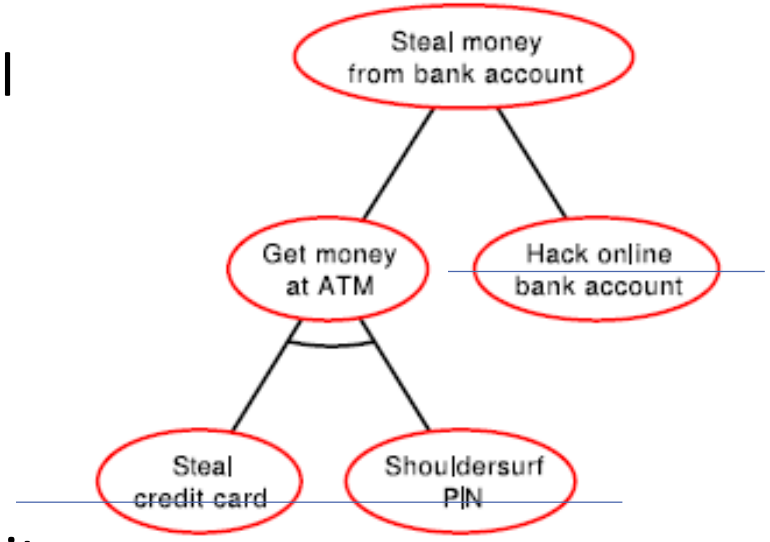
probability, special equipment value -> most probable attack with no special equipment required

assign values to leaf nodes and propagate the node value up to the root

Evaluation of Security

Minimum cut-set -> set of atomic attacks that achieve a goal

S = {{Steal credit card, Shouldersurf PIN}
{Hack online Bank acount}}

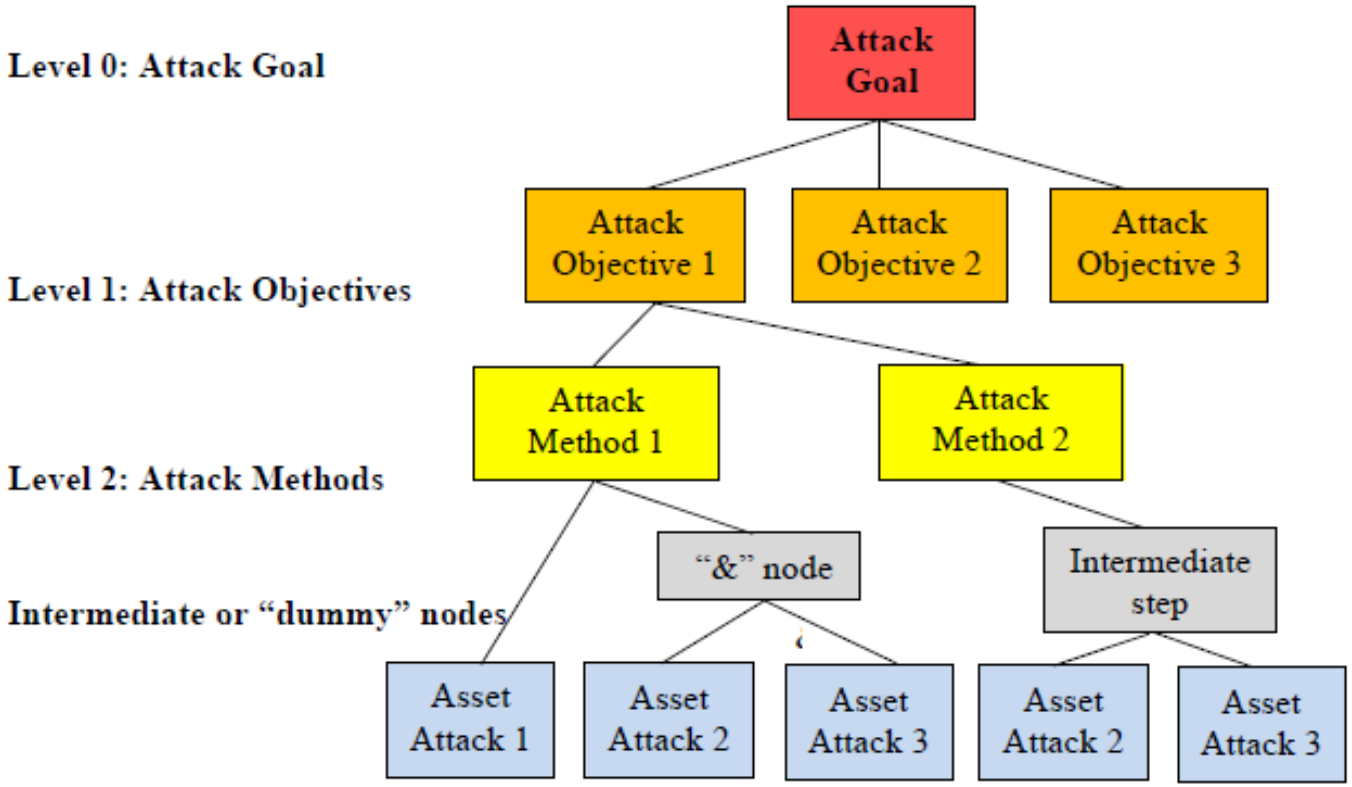


Impact of certain atomic attacks on the overall system security

Attack Trees: systematic ways to describe system vulnerability , making possible to assess risks and making security decisions

Attack trees: reusable as part of a larger attack tree for a system

EVITA: Attack tree structure

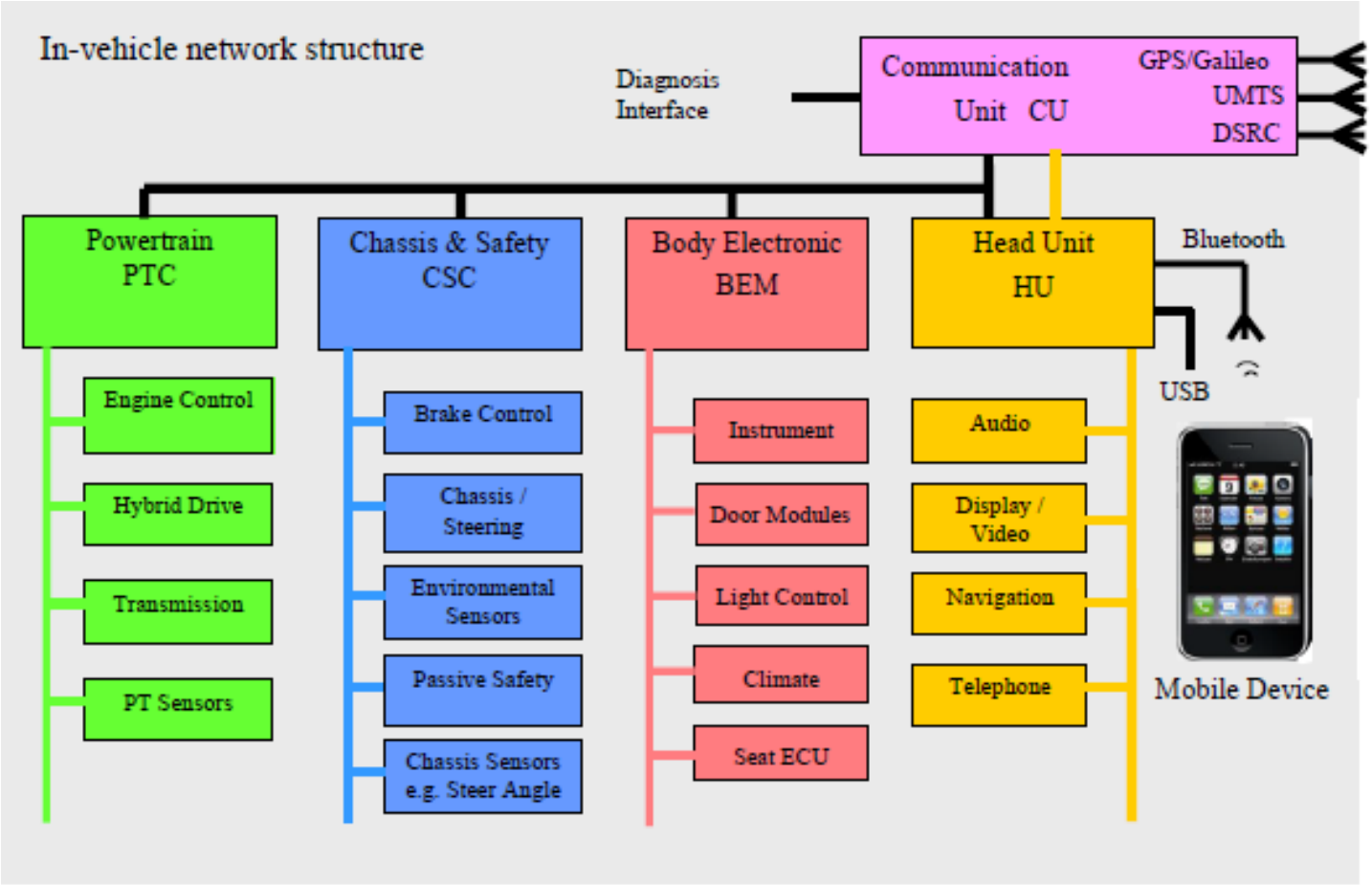


Each attack method will be based on a logical combination (AND/OR) of attacks against one or more "assets" populating the lowest levels of the attack tree.

Probability of success can be estimated for asset attacks

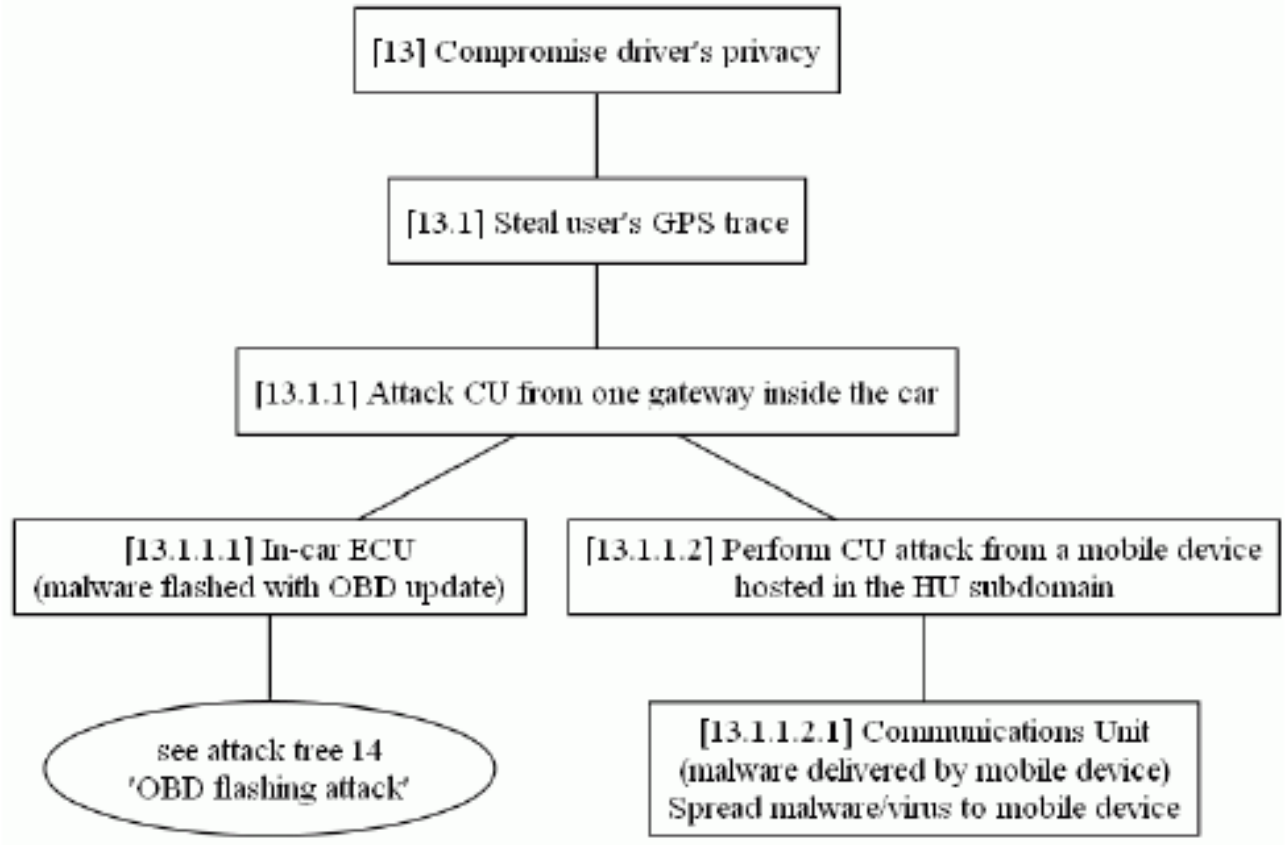
[EVITA-D2.3] E-safety vehicle intrusion protected applications (EVITA) project. Project reference: 224275 Programme: EU Seventh Reserch Framework Programme (2007–2013) Deliverable D2.3. *Security requirements for automotive on-board networks based on dark-side scenarios*.

Reference architecture



Taken from [EVITA-D2.3]

Attack tree : Compromise driver privacy



Misuse the OBD updates or manipulate the CU to gain access to personal data.