Security risk analysis approach for on-board vehicle networks

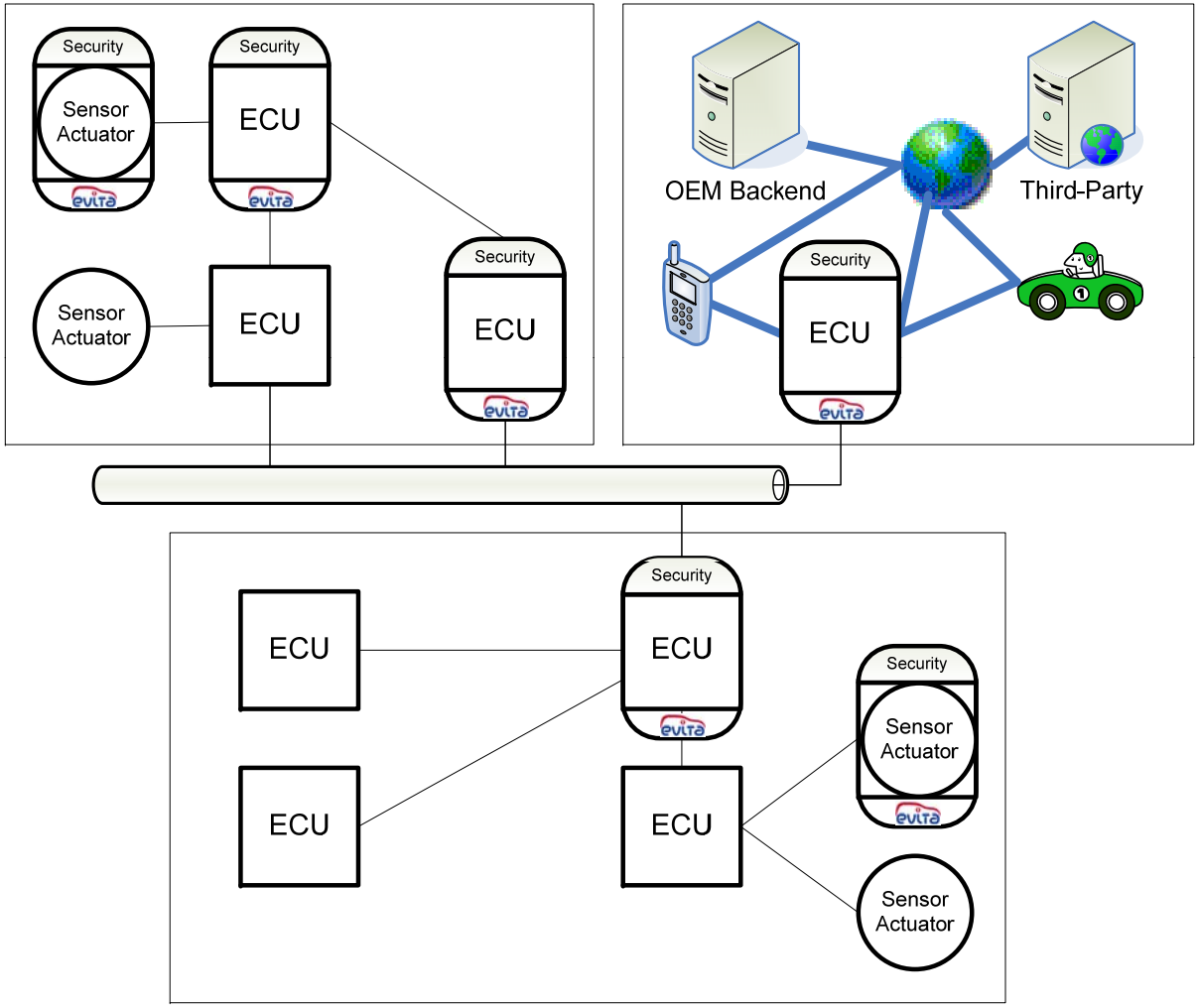
Alastair Ruddle
Consultant, MIRA Limited

ISO IEC ITU International Telecommunication Union

Motivation

- Future vehicles will become mobile nodes in a dynamic transport network
  - vehicle systems will be under threat from malicious individuals and groups seeking to gain personal or organizational advantage
  - ensuring security will be critical for the successful deployment of V2X technology
- EU project **EVITA** aims to prototype a toolkit of techniques and components to ensure the security of in-vehicle systems
  - hardware, software, analysis methods

EVITA scope and assets



EVITA only aims to investigate network security solutions at vehicle level

Different levels of security protection are envisaged, depending on need

Some assets may not require security measures (low risk)

Risk analysis aims to prioritize security requirements

ISO IEC ITU International Telecommunication Union

EVITA project security risk analysis rationale

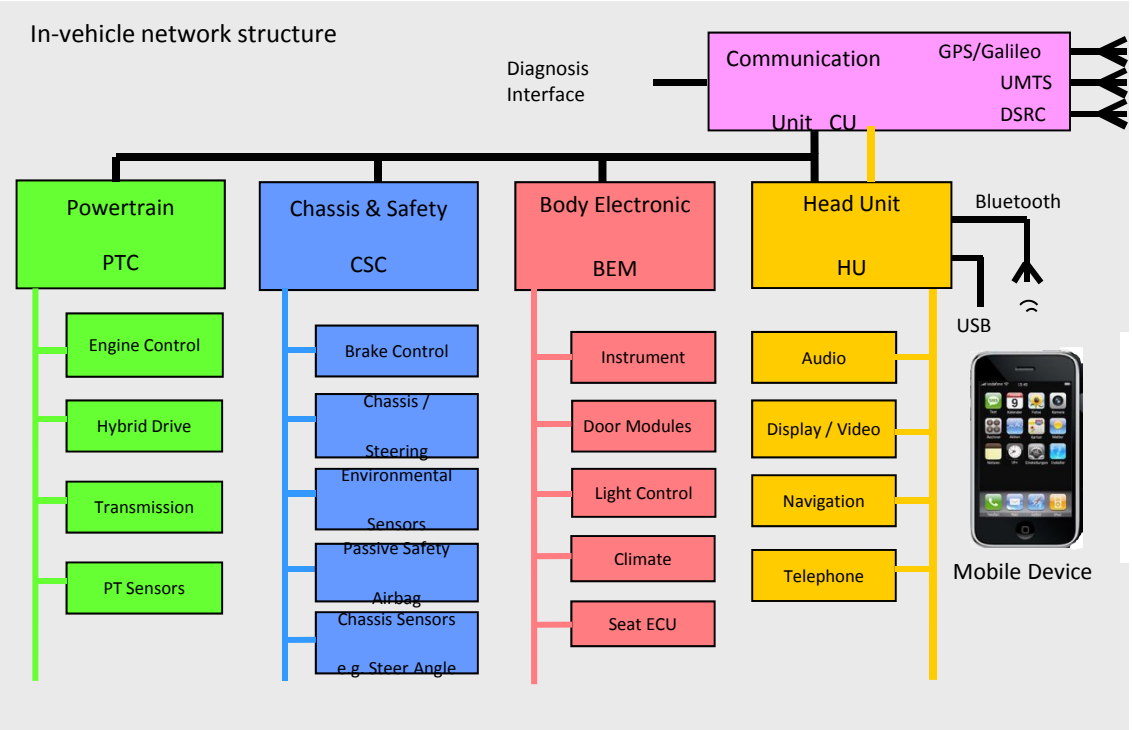
- Too costly to protect against every threat, so need to rank risks in order to prioritize countermeasures
- **Risk** associated with a security attack depends on:
  - **severity** of impact (ie. harm to stakeholders)
    - drivers, other road users, civil authorities, ITS operators, vehicle manufacturers and system suppliers
  - **probability** of successful attack
    - depends on attacker resources, nature of attack
- Physical safety is a key aspect of security
  - physical harm may be an objective of an attack
  - harm may also be an unintended consequence

Safety and security

- Physical safety is a key aspect of security
  - physical harm may be an objective of an attack
  - harm may also be an unintended consequence
- Automotive functional safety standards are based on qualitative measures of relative risk, severity and probability
  - natural basis for automotive security risk analysis
- For safety-related security risks, probability needs to include “controllability” of hazardous situations
  - opportunity for drivers to influence outcome for safety-related security hazards

Starting point – EVITA Use Cases

A suite of 18 potential use cases was defined, based on EASIS project network architecture



Assumed reference architecture

Scenario classes:

- car-car
- car-infrastructure
- mobile devices
- aftermarket
- maintenance

ISO IEC ITU International Telecommunication Union

Security threat agents and their motivations

- **Dishonest drivers**
  - avoid financial obligations, gain traffic advantages;
- **Hackers**
  - gain/enhance reputation as a hacker;
- **Criminals and terrorists**
  - financial gain, harm or injury to individuals or groups;
- **Dishonest organisations**
  - driver profiling, industrial espionage, sabotage of competitor products;
- **Rogue states**
  - achieve economic harm to other societies

Generic security threats and objectives

Generic security threats				Security objectives
Aims	**Target**	**Approach**	**Motivation**	
Harming individuals	Driver or passenger	Interference with safety functions of a specific vehicle	Criminal or terrorist activity	Safety Privacy
Harming groups	City or state economy, through vehicles and/or transport system	Interfere with safety functions of many vehicles or traffic management functions	Criminal or terrorist activity	Safety Operational
Gaining personal advantage	Driver or passenger	Theft of vehicle information or driver identity, vehicle theft, fraudulent commercial transactions	Criminal or terrorist activity	Privacy Financial
	Vehicle	Interference with operation of vehicle functions	Build hacker reputation	Operational Privacy
	Transport system, vehicle networks, tolling systems	Interference with operation of traffic management functions or tolling systems	Enhanced traffic privileges, toll avoidance	Operational Privacy Financial
Gaining organizational advantage	Driver or passenger	Avoiding liability for accidents, vehicle or driver tracking	Fraud, criminal or terrorist activity, state surveillance	Privacy Financial
	Vehicle	Interference with operation of vehicle functions, acquiring vehicle design information	Industrial espionage or sabotage	Privacy Operational Safety

ISO IEC ITU International Telecommunication Union

Security hazard classification

- Different security aspects are not independent
  - "safety" is definitely a sub-set of "operational"
  - "financial" is perhaps a subset of "privacy"
- Why separate the proposed security aspects?
  - certain aspects relate to particular attacker types
    - privacy – industrial espionage, surveillance
    - operational – industrial sabotage, nuisance hacker
    - safety – opportunistic harm (terrorism)
    - privacy and safety – targeted harm (crime)
    - privacy and financial – crime (opportunistic, organized)
  - safety has special features
    - potential for driver to intervene to mitigate some hazards

Threat analysis – Attack Trees

Common model to map attack trees to risk analysis

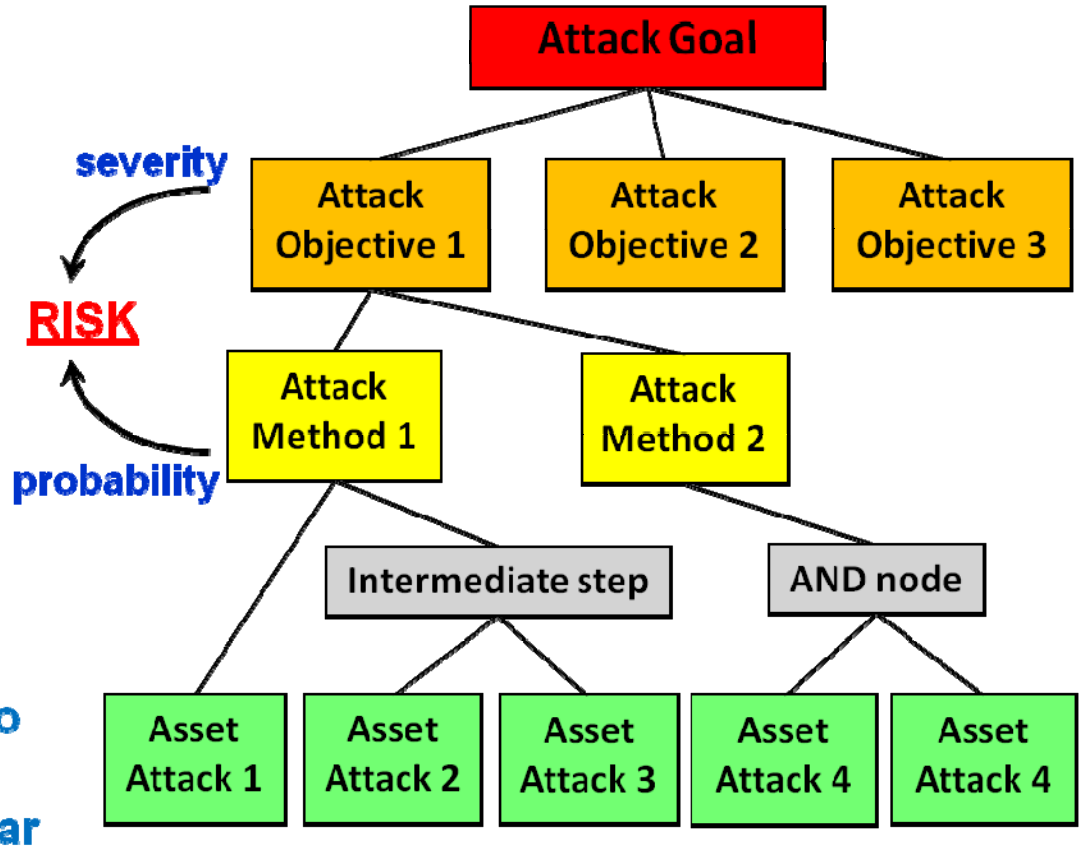
Level 0: Attack Goal
(Illegal benefit to attacker)

Level 1: Attack Objectives
(Harm for stakeholders – severity)

Level 2: Attack Methods
(Combined probability of successful attack)

Intermediate/dummy nodes

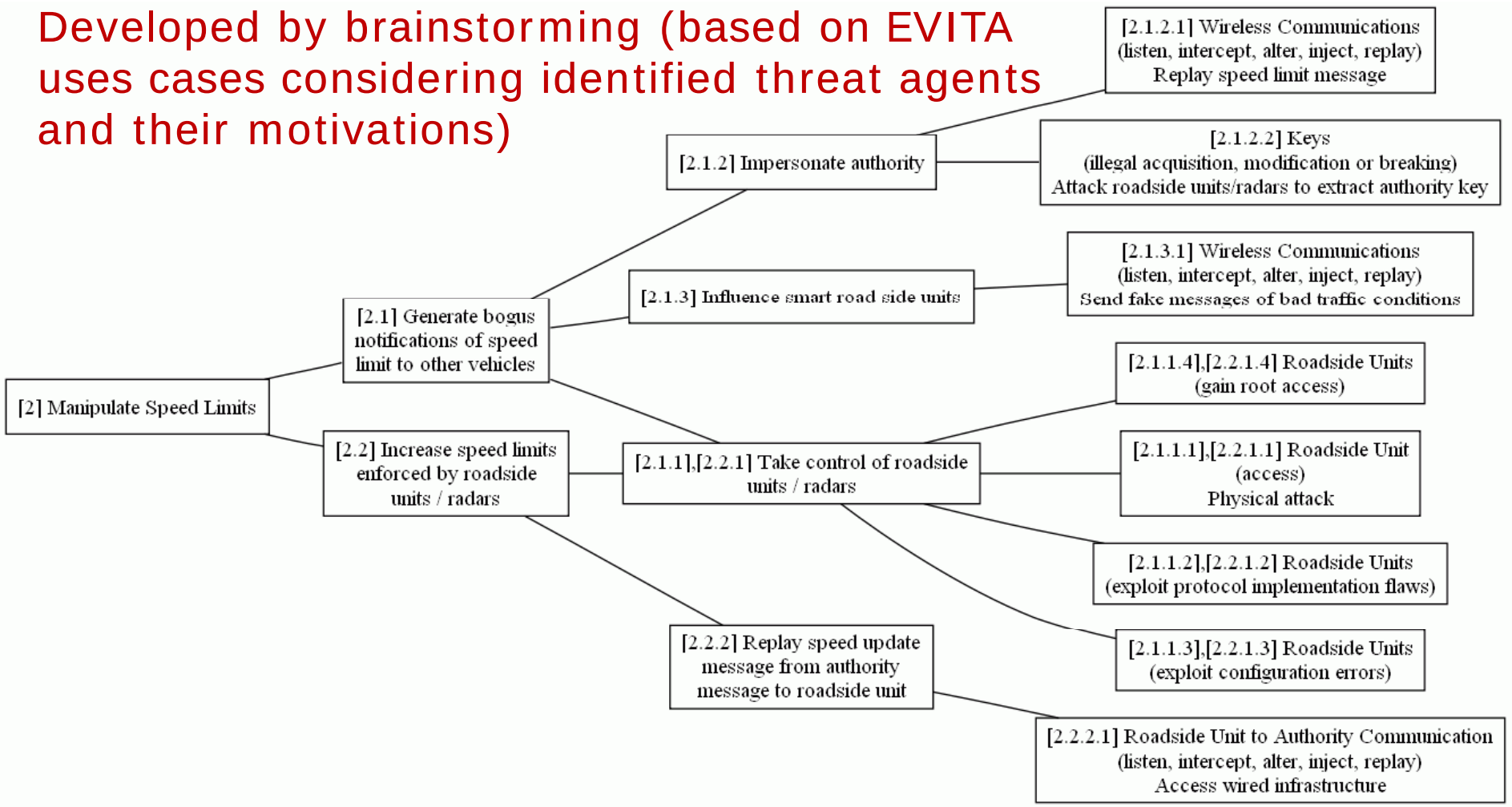
Level 3: Asset Attacks
(Attack potential – related to probability of success for specific attacks on particular assets)



ISO IEC ITU International Telecommunication Union

Sample attack tree

Developed by brainstorming (based on EVITA uses cases considering identified threat agents and their motivations)



ISO IEC ITU International Telecommunication Union

Severity classification in vehicle safety engineering

Class	Safety outcome
S0	No injuries.
S1	Light/moderate injuries.
S2	Severe injuries (survival probable).
S3	Life threatening or fatal injuries.

Safety is an important aspect that could potentially be compromised as a result of security breaches

Starting point is safety severity scale used in automotive safety standard ISO/CD 26262 and similar guidelines (eg. MISRA for safety-related software and systems)

Qualitative classification scheme based on Abbreviated Injury Scale

Extending from safety to security

Class	Safety	Privacy	Financial	Operational
S0	No injuries.			
S1	Light/moderate injuries.			
S2	Severe injuries (survival probable). Moderate injuries for multiple units.			
S3	Life threatening or fatal injuries. Severe injuries for multiple units.			
S4	Fatal for multiple vehicles.			

Additional aspects that may be compromised by security breaches

Security issues may have more widespread implications than just a few vehicles

ISO IEC ITU International Telecommunication Union

Severity classification of privacy infringements

Class	Safety	Privacy
S0	No injuries.	No data access.
S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).
S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.
S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.
S4	Fatal for multiple vehicles.	Driver identity access for multiple units.

Similar approach to that adopted for safety:

S1 – minor driver privacy infringement.

S2 – major driver privacy infringement, or widespread minor privacy infringements.

S3 – severe driver privacy infringement, or possible industrial espionage activity.

S4 – widespread severe driver privacy infringement.

ISO IEC ITU International Telecommunication Union

Financial severity classification

Class	Safety	Privacy	Financial
S0	No injuries.	No data access.	No financial loss.
S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).	Low level loss (~€10).
S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.	Moderate loss (~€100). Low losses for multiple units.
S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.	Heavy loss (~€1000). Multiple moderate loss.
S4	Fatal for multiple vehicles.	Driver identity access for multiple units.	Multiple heavy losses.

Calibration for this scale may depend on exactly who bears these losses.

Individual?
Credit card company?
Tolling body?

Security severity classification – a 4-component vector

Class	Safety	Privacy	Financial	Operational
S0	No injuries.	No data access.	No financial loss.	No impact on operation.
S1	Light/moderate injuries.	Anonymous data only (no specific user or vehicle data).	Low level loss (~€10).	Impact not discernible to driver.
S2	Severe injuries (survival probable). Moderate injuries for multiple units.	Vehicle specific data (vehicle or model). Anonymous data for multiple units.	Moderate loss (~€100). Low losses for multiple units.	Driver aware. Not discernible in multiple units.
S3	Life threatening or fatal injuries. Severe injuries for multiple units.	Driver identity compromised. Vehicle data for multiple units.	Heavy loss (~€1000). Multiple moderate loss.	Significant impact. Multiple units with driver aware.
S4	Fatal for multiple vehicles.	Driver identity access for multiple units.	Multiple heavy losses.	Significant impact for multiple units.

Attack potential and probability

- **Attack potential** evaluation
  - using established, structured approach from “Common Criteria”
  - applied in EVITA at “asset attack” level of attack trees
- Indicative of **attack probability** (inverse relationship)
  - numerical scale used to represent relative ranking of attack probability

Attack potential		Attack probability	
Rating	**Description**	**Likelihood**	**Ranking**
0–9	Basic	Highly likely	5
10–13	Enhanced basic	Likely	4
14–19	Moderate	Possible	3
20–24	High	Unlikely	2
≥25	Beyond high	Remote	1

Evaluation of attack potential

- Factors considered (ISO/IEC 18045)
  - elapsed time
  - attacker expertise
  - system knowledge required
  - window of opportunity
  - equipment required
- Each factor has a number of classes each assigned with a numerical value
  - e.g. attacker expertise
    - layman (0), proficient (3), expert (6), multiple experts (8)
- Attack potential classes based on ranges of total numerical value

Controllability – safety hazards

Possibility for the driver (and/or other traffic participants) to mitigate possible safety hazards

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

Risk graph (fragment only)

Non-safety aspects addressed with table for controllability C=1 (C>1 only for safety issues)

Controllability	Severity (S_i)	Combined Attack Method Probability (A)				
		1	2	3	4	5
C=1	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
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

Attack tree tables for risk analysis

A compressed tabular attack tree representation provides a convenient framework for documenting the risk analysis

Attack Objective	Severity (S)	Attack Method	Risk level (R)	Combined attack method probability (A)	Asset (attack)	Attack Probability (P)
B	$\mathbf{S_B}$	B1	$\mathbf{R_{B1}}(\mathbf{S_B}, A_{B1})$	$A_{B1}=\min\{Pa,Pb\}$	a & b	Pa Pb
		B2	$\mathbf{R_{B2}}(\mathbf{S_B}, A_{B2})$	$A_{B2}=\max\{Pd,Pe,Pf\}$	d	Pd
					e	Pe
					f	Pf

OR: as easy as the easiest option

AND: as hard as the hardest component

Overview of EVITA attack trees

- The 18 EVITA use cases suggested 10 attack trees:
  - attack E-call, attack E-toll
  - tamper with warnings, attack active break
  - manipulate speed limits, force green light
  - manipulate traffic flow, simulate traffic jam
  - unauthorized braking, engine denial-of-service
- These are representative, but not exhaustive
- Rationalization of the attack trees revealed:
  - 44 different asset attacks, involving 16 different assets
- Risk analysis provides the means to assess the relative importance of protecting these assets

Risk-based prioritisation of counter-measures

Identified threats		Risk analysis results		Security requirements
Asset	*Attack*	*Risk level*	*Instances*	
Chassis Safety Controller	Denial of service	1	3	Authenticity_6, Availability_102, Availability_106 — Low priority
		2	1	
	Exploit implementation flaws	4	1	Authenticity_1, Authenticity_2, Authenticity_3 …
		5	1	
Wireless Comms	Corrupt or fake messages	2	5	… Confidentiality_1, Confidentiality_2, Authenticity_101 … — Important to protect against this asset attack
		3	5	
		4	4	
		5	1	
		6	4	
		7	3	
	Jamming	4	3	… Availability_107, Availability_108, Integrity_102
		5	2	

Conclusions

- A security risk analysis approach has been developed from automotive safety and IT security practices
  - **attack trees** to identify asset attacks from use cases, attacker type and motivations
  - **4-component security risk vector**, potentially including security-related safety issues
  - **attack potential** and **controllability** to assess probability of successful attack
- Level and frequency of risks associated with asset attacks identified in attack trees indicate priorities for counter-measures

Acknowledgements

Fraunhofer SIT

BMW Group Research and Technology

BOSCH

Continental

escrypt Embedded Security

EURECOM

Fraunhofer ISI

FUJITSU

infineon

TELECOM ParisTech

KATHOLIEKE UNIVERSITEIT LEUVEN

MIRA

TRIALOG

For further information see: **www.evita-project.org**

evita

ISO IEC ITU International Telecommunication Union