Riskpool – A Security Risk Management Methodology

Martin Ring, Robert Bosch GmbH, martin.ring@bosch.com;

Paul Duplys, Robert Bosch GmbH;

Sven Köhler, ITK Engineering GmbH

#whoami

Name	Martin Ring
Education	Apprenticeship Kfz-Mechatroniker, Bachelor of Engineering, Master of Science, Doctor of Engineering (Dr.-Ing.)
Employers	VW/Audi Garage, Dekra, Mercedes-Benz Special Trucks, Volkswagen Motorsport, IEEM, Bosch Engineering (Security Manager, Product Secuirty Officer), Robert Bosch GmbH

Riskpool – A Security Risk Management Methodology

Overview

- What is Risk & Risk Management
- Security Risk Management – Database
- Riskpool – Concept & Examples

Introduction
Risk

- ***Risk*** – *noun* - The possibility of something bad happening at some time in the future; a situation that could be dangerous or have a bad result [Oxford Dictionary]

Introduction

Risk Management

- Managing First Oder Risk

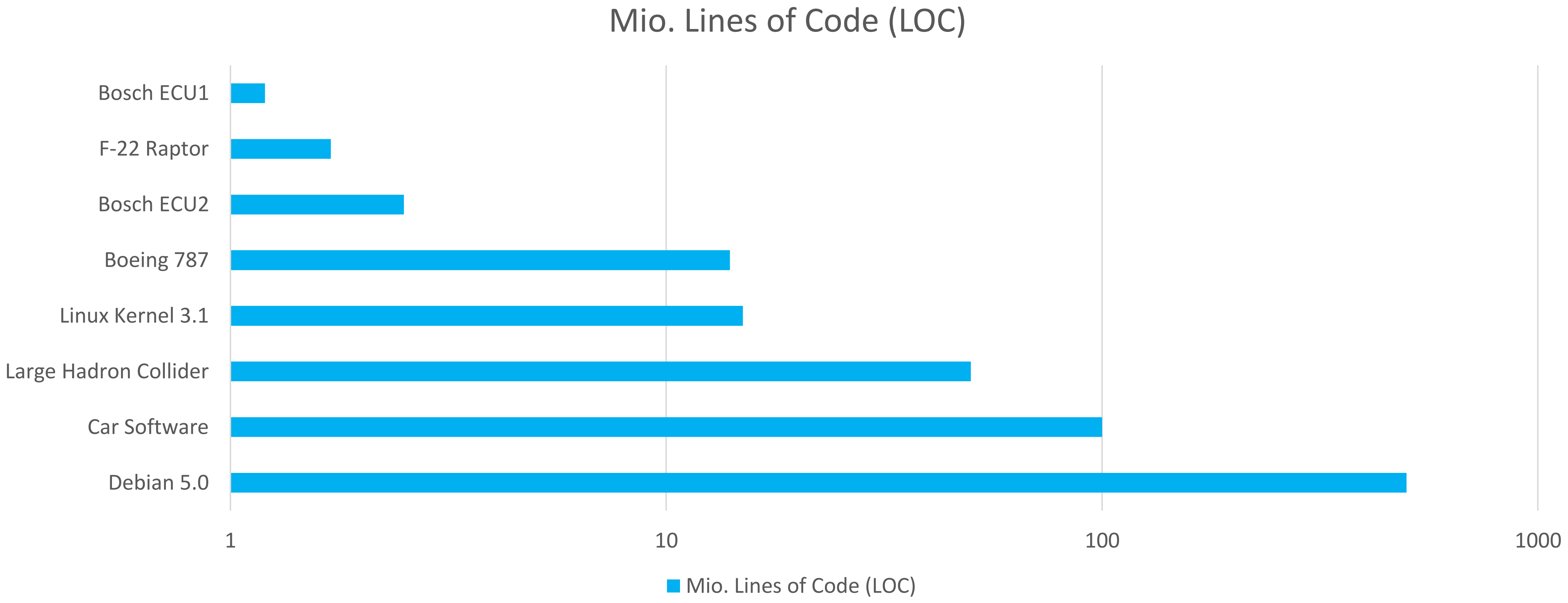
[https://www.flickr.com/photos/val_s/8603033695]

- Managing Second Order Risk

[https://margomyers.com/crisis-communications-pr-guidelines/]

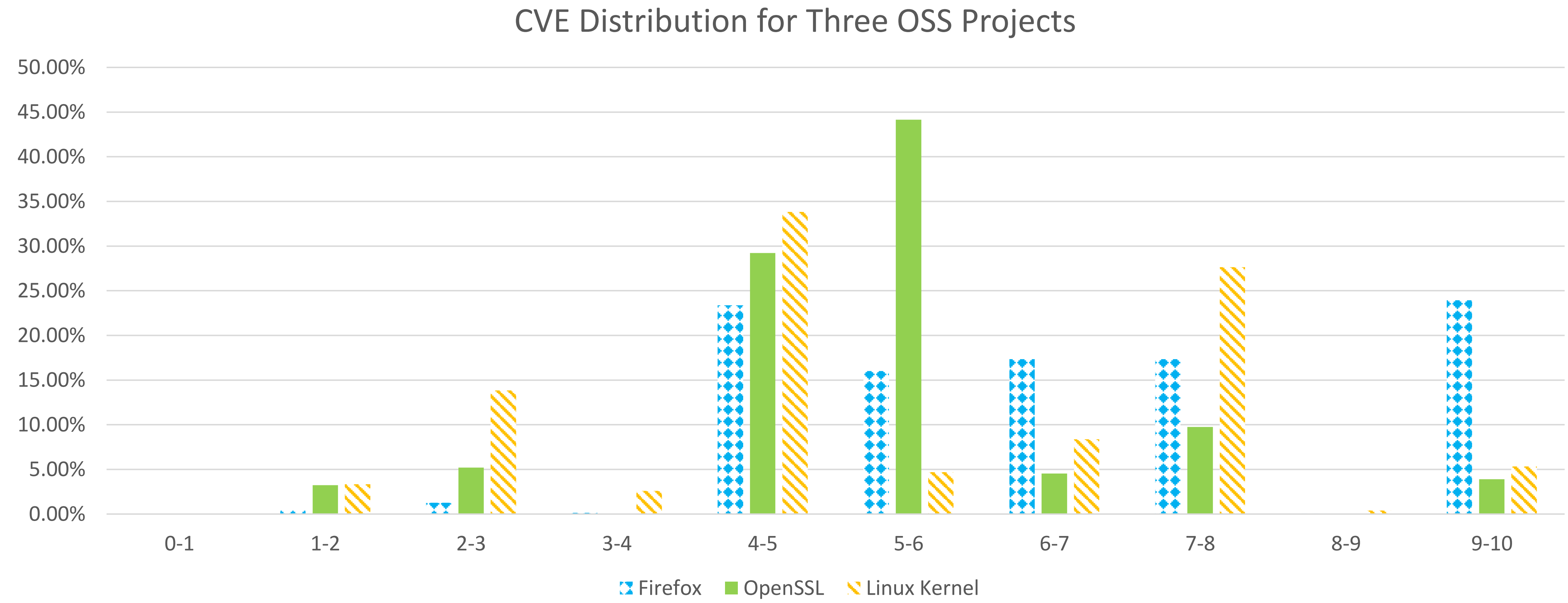
Security Risk Management

Database – Software Size



Security Risk Management

Database - Vulnerabilities



Security Risk Management
Database

Software	Vulnerabilities per 1,000 LoC	LoC (2023)	∑ CVEs 2012-2022
Google Chrome	0.08	25,600,000	2,154
Firefox	0.06	25,300,000	1,459
Linux Kernel	0.07	33,600,000	2,230
OpenSSL	0.11	1,540,000	163
Python	0.06	1,320,000	77
PHP	0.23	1,510,000	349

min. 2,000 exploitable vulnerabilities waiting to be discovered in a top of the line car over the next five years.

Riskpool
Concept

- Risks associated with all products that are not at the end of their lifetime on one side and a risk pool, representing the available capacity to fix defects in a product over its lifetime on the other side:

$$\sum_i Project_i \cdot TARA\ Residual\ Risks_i \cdot Weight_i \leq \sum Developers \cdot Fixing\ Capability \cdot Capacity$$

  - i: products in expected lifetime (lifetime, legal definition open – e.g., Porsche mean age of fleet = 25 years, Automotive OEM1 requests 6 years after SOP)
  - $TARA\ Residual\ Risks$: Residual risk values depend on the used TARA methodology
  - $Weight$: Residual risks will have an associated weight, 2-10% of the expected risks (TARA) manifest (scaling with code age, innovation level, delivery with known vulnerabilities, LoC & FotA capability)
  - $Fixing\ Capability$: capability of developers to fix vulnerabilities, value depends on TARA methodology
  - $Capacity$: how much capacity of the available developers is assigned for maintenance and fixing vulnerabilities

Riskpool

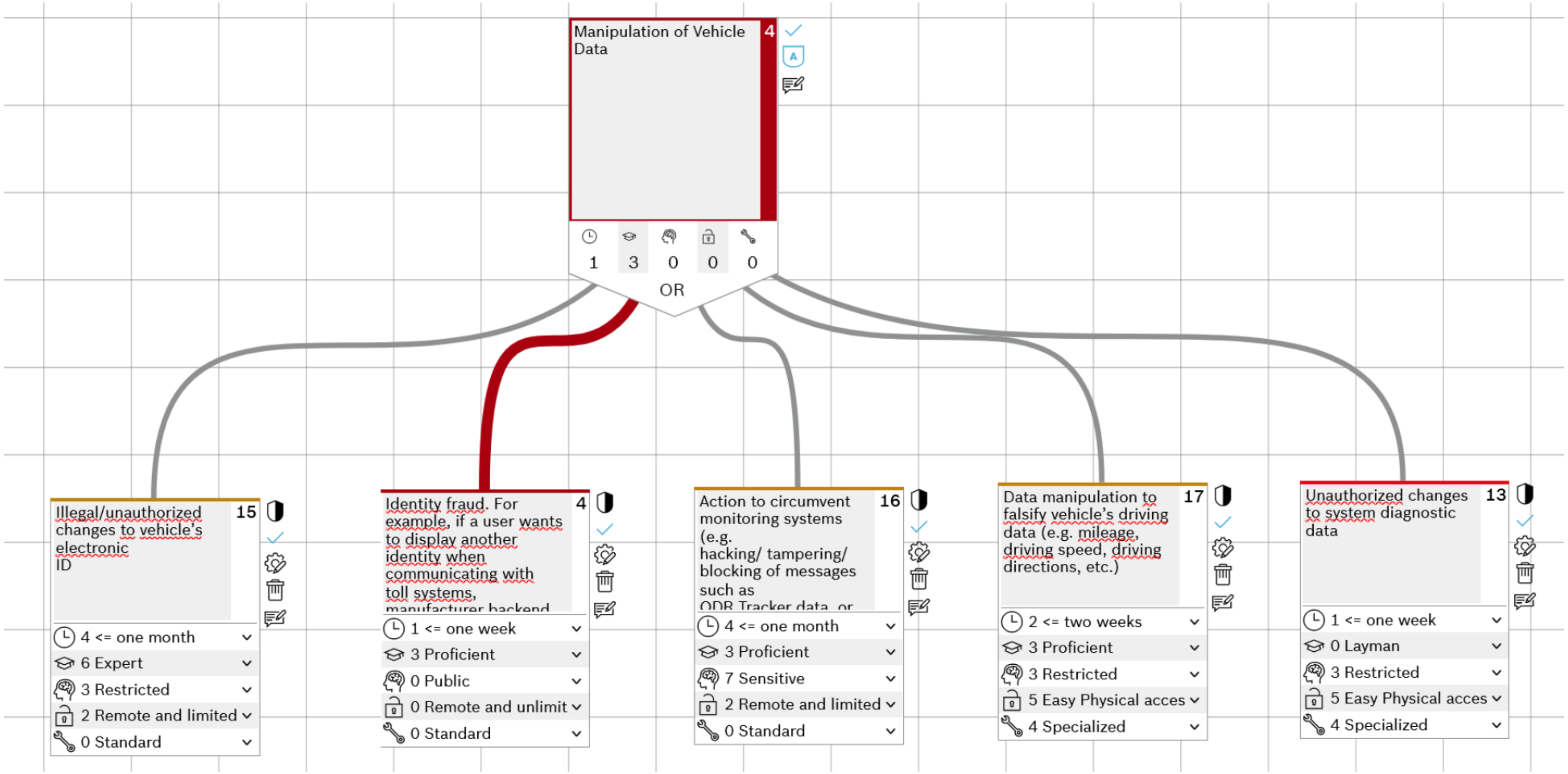
Example UNECE

		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

Values	Attack Feasibility
>25	Very Low
20-24	Low
14-19	Medium
0-13	High

Impact Rating	Criteria *(based on ISO 26262)*
Sever	S3: Life Threatening
Major	S2: Severe Injuries
Moderate	S1: Light Injuries
Negligible	S0: No Injuries

Riskpool
Example UNECE



Manipulation of Vehicle Data 4

1 3 0 0 0

OR

Illegal/unauthorized changes to vehicle's electronic ID 15
- 4 <= one month
- 6 Expert
- 3 Restricted
- 2 Remote and limited
- 0 Standard

Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend 4
- 1 <= one week
- 3 Proficient
- 0 Public
- 0 Remote and unlimit
- 0 Standard

Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or 16
- 4 <= one month
- 3 Proficient
- 7 Sensitive
- 2 Remote and limited
- 0 Standard

Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.) 17
- 2 <= two weeks
- 3 Proficient
- 3 Restricted
- 5 Easy Physical acces
- 4 Specialized

Unauthorized changes to system diagnostic data 13
- 1 <= one week
- 0 Layman
- 3 Restricted
- 5 Easy Physical acces
- 4 Specialized

Riskpool

Example UNECE

		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

Values	Attack Feasibility
>25	Very Low
20-24	Low
14-19	Medium
0-13	High

Impact Rating	Criteria *(based on ISO 26262)*
Sever	S3: Life Threatening
Major	S2: Severe Injuries
Moderate	S1: Light Injuries
Negligible	S0: No Injuries

Riskpool
Example

- Company ExCom, 2 products: ECU_A & ECU_B, TARA according to ISO21434
- ECU_A:
  - Automotive Safety Integrity Level (ASIL) D ECU
  - low innovation level
  - deviations proven in field
  - low range wireless communication capabilities.
  - Residual Risk: 29 points, Weight: 0.02, 250 projects with this product each year, one year support
- ECU_B:
  - ASIL B ECU
  - new product
  - No wireless interfaces
  - Residual Risk: 116 points, Weight: 0.05, 250 projects with this product each year, one year support

Riskpool
Example

- Company ExCom employs 1,000 developers, has 2 products ECU1 (RR: 29, Weight 0.02, 250 projects p.a.) & ECU2 (RR: 116, Weight 0.05, 250 projects p.a.)

$$\sum_i Project_i \cdot TARA\ Residual\ Risks_i \cdot Weight_i \leq \sum Developers \cdot Fixing\ Capability \cdot Capacity$$

- $\sum_{250} 29 \cdot 0.02 + \sum_{250} 116 \cdot 0.05 \overset{?}{\leq} \sum 1{,}000 \cdot 30 \cdot 0.05$
- $1{,}595 \ > 1{,}500$
- The company in this example is exceeding its risk pool
    - Possible solutions might be increasing aloted developer capacity (increase to 6% would result in an available pool of 1,800 points)

Riskpool
Conclusion

- The proposed method enables centralized management and monitoring of the company's risk appetite.
- The inequation can be affected by:
  - The projects, by mitigating the residual risks
  - Management, by increasing the number of developers or the assigned percentage to vulnerability management
- Risk pool shall be recalculated with every project going into production
- The weight might be adjusted by the individual company and the approach fine tuned over multiple years, so a realistic view on individual vulnerabilities and fixing capabilities becomes available.