HoliSec

Holistic Approach to Improve Data Security

Topic: Security requirements and classification of security mechanisms

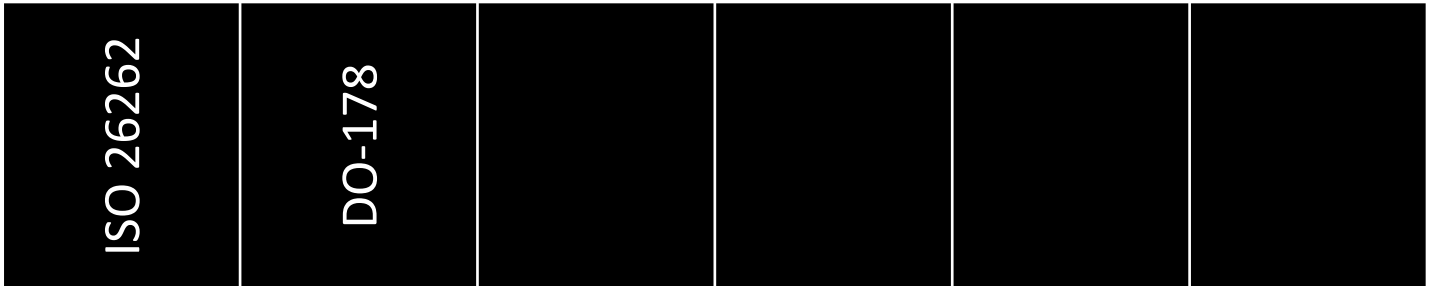
Presenter: Thomas Rosenstatter, Chalmers

September 7, 2017. Time 10:50 – 11:10

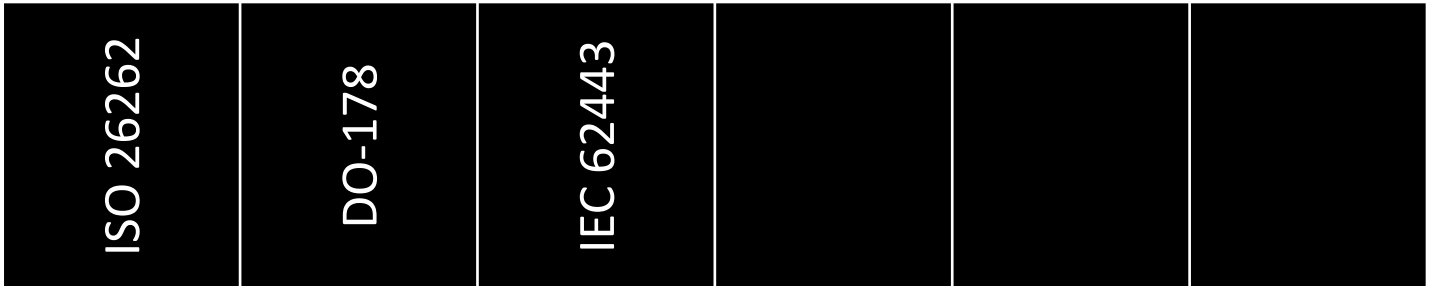
How to classify security in the automotive domain?

- Classification of security and safety
- Levels within a certain range
- What do levels mean?
- Guiding the developer

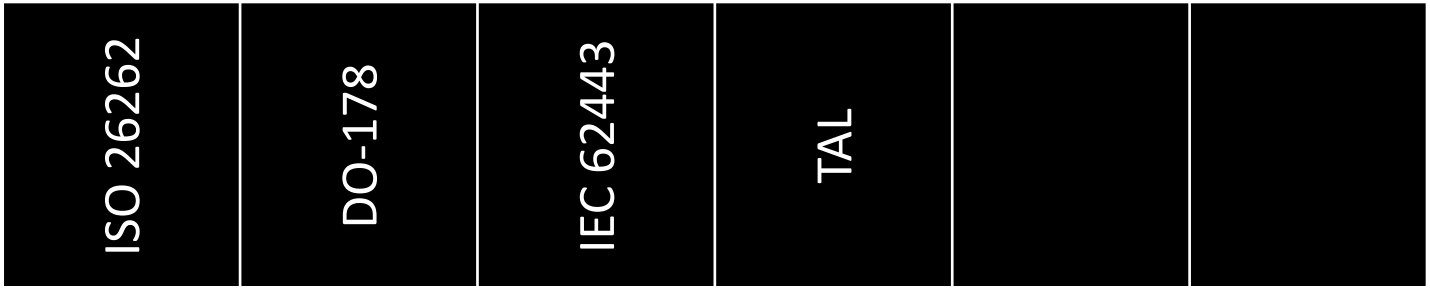
Reviewed Standards and Models



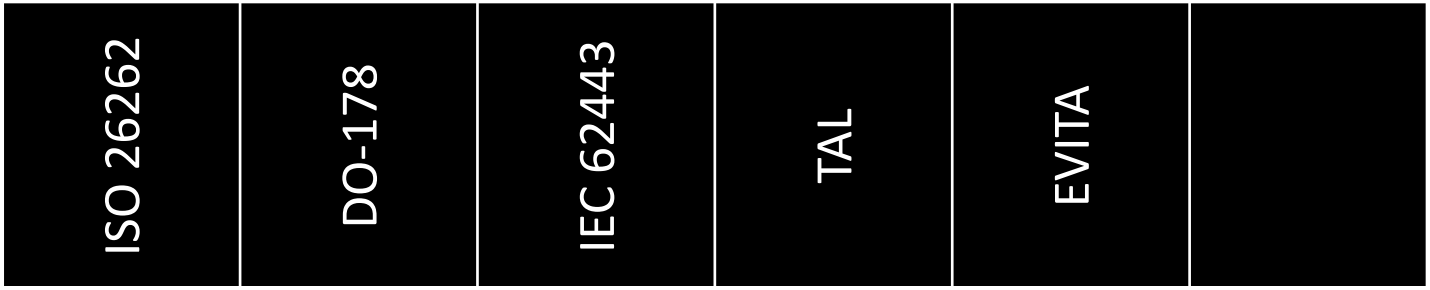
Reviewed Standards and Models



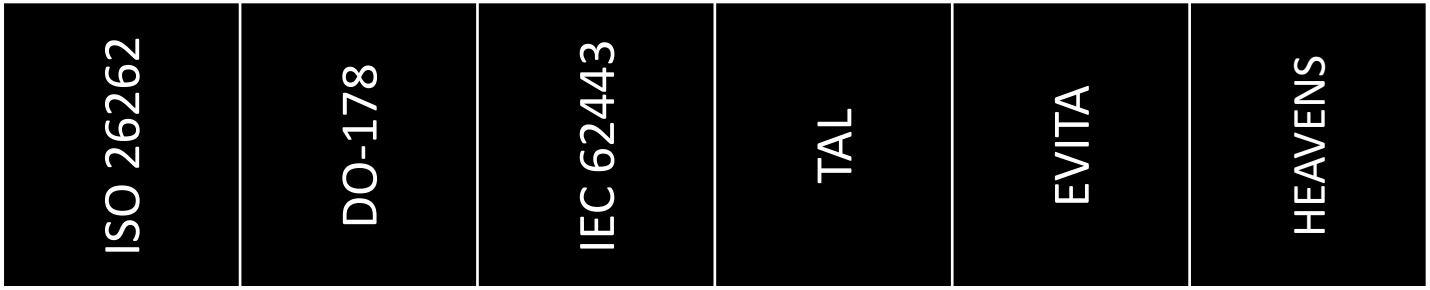
Reviewed Standards and Models



Reviewed Standards and Models



Reviewed Standards and Models



Reviewed Standards and Models

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Application	Safety	Safety	Security	Security	Security	Security

Reviewed Standards and Models

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Application	Safety	Safety	Security	Security	Security	Security
# SLs						
Vector Size						

Reviewed Standards and Models

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Application	Safety	Safety	Security	Security	Security	Security
# SLs	5	5	5	5	8	5
Structure / Vector Size	1	1	7	1	4	1[a]

[a] HEAVENS associates each threat/asset pair with a security level (SL)

Reviewed Standards and Models

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Application	Safety	Safety	Security	Security	Security	Security
# SLs	5	5	5	5	8	5
Structure / Vector Size	1	1	7	1	4	1[a]
System REQs						

[a] HEAVENS associates each threat/asset pair with a security level (SL)

Reviewed Standards and Models

	ISO 26262	DO-178	IEC 62443	TAL	EVITA	HEAVENS
Application	Safety	Safety	Security	Security	Security	Security
# SLs	5	5	5	5	8	5
Structure / Vector Size	1	1	7	1	4	1[a]
System REQs	(✓)[b]	–	✓	✓	–	–

[a] HEAVENS associates each threat/asset pair with a security level (SL)
[b] ISO 26262 provides recommendations for specific methods depending on the SL

Number of Security Levels

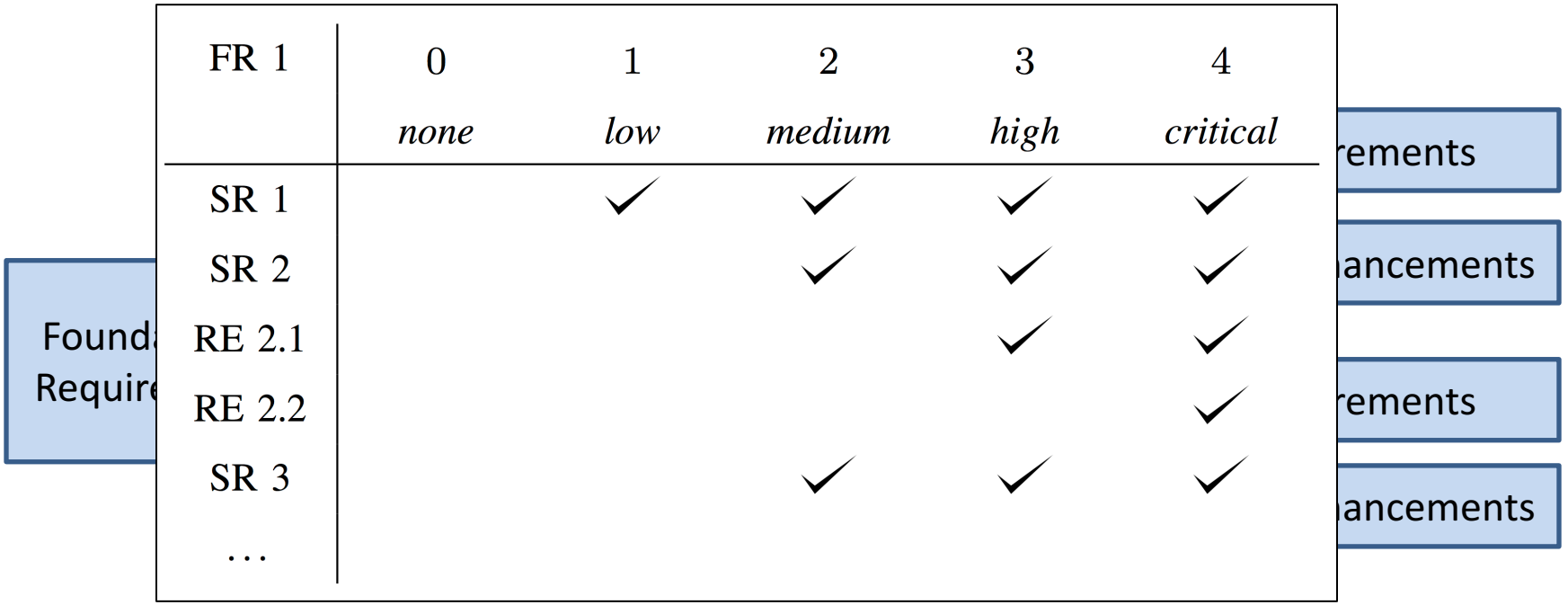
- Many levels increase the complexity
  - 8 levels – What is the difference between SL 6 and SL 7?
- Too few may lead to an overly secured system
  - 3 levels – Does my function need the highest possible security measure?
- 5 levels
  - Give enough detail to distinguish between the requirements

Structure of Security Levels

- Security is more complex than safety
- Representation as a vector is necessary

$$SL = \begin{bmatrix} \text{Authenticity} \\ \text{Integrity} \\ \text{Non-repudiation} \\ \text{Confidentiality} \\ \text{Availability} \\ \text{Authorisation} \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 1 \\ 0 \\ 2 \\ 1 \end{bmatrix}$$

Mapping to Requirements



Next Steps

- Investigate suitable mechanisms and design rules
- Assign these security mechanisms to security levels

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!