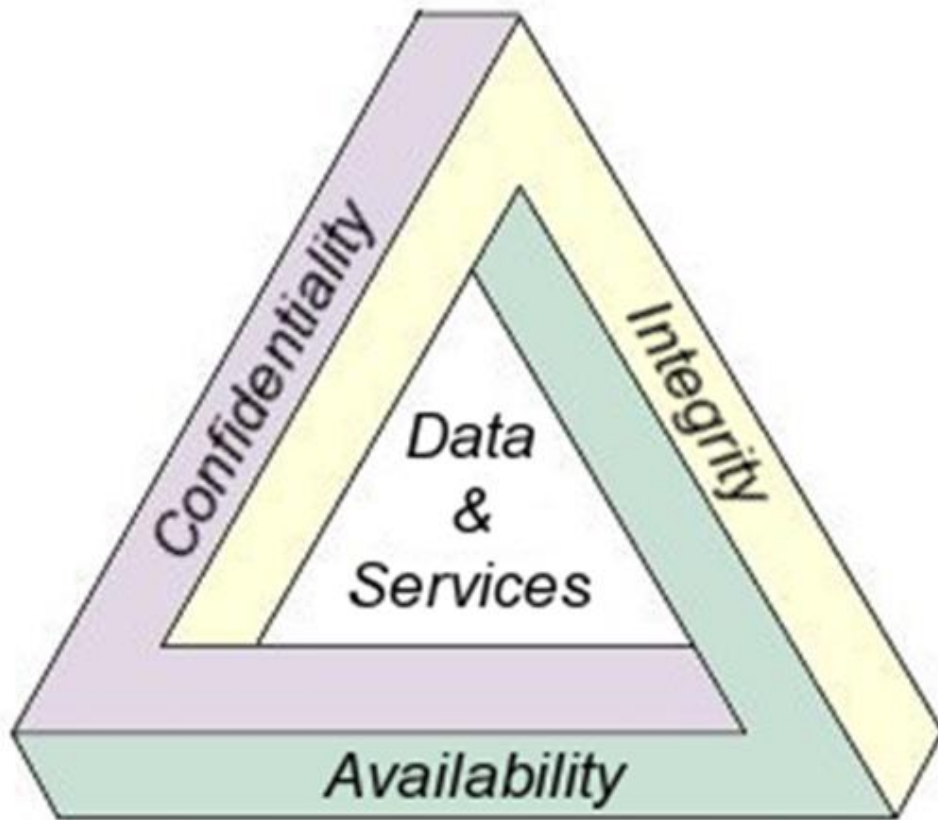# **Software Security**

WP29 / ITS

11-11-2015

Definition Security

Security = certain level of
- confidentiality
- integrity
- availability

Approval system principles

?

- E.g. ISO 26262 is used by manufacturers for software development

- Software Security is not yet included in testing/certification for type approval

Impact software security

- Security affects safety, environment and functionality
- Proper security serves Liability and Privacy

Security threat increases

- More internet connected cars (and infra)
- More wireless
- More networks within vehicle
- More connection with Nomadic Devices
- Better tools for breaking codes
- Faster communication of hacking methods
- **THERE IS AN INCREASING BUSINESS CASE**

Aspects for security

- Architecture (hardware & software)
- Security level components (chips e.a)
- Software Process (SDLC)
- Software Updates (OTA? While driving?))
- Memory capacity hardware
- Response time
- Quality level components and data
- Configuration management of parameters

Windows - Out of Virtual Memory

Your system is low on virtual memory. To ensure that Windows runs properly, increase the size of your virtual memory paging file. For more information, see Help.

OK

RDW

Proposal to proceed

- Decide that software security should be part of Type Approval requirements

- Develop a seperate (modular) Regulation for Software security

- Determine Security requirements, preferably based on existing standards

- Define a flexible process to support future developments/requirements

RDW

Considerations

- Find the right balance

Practical use   Assurance level

Function	Assurance level	Examples
Safety	High	ASIL C/D, EAL 6/5
Environment	Medium	ASIL A/B, EAL 4/3
Information (ie. Infotainment)	No requirement	-

- If software combines functions, the highest level should be realized

Considerations (2)

- Importance of data analysis (surveillance) will increase as part of approval

- How about "self-learning software"

Considerations (3)

SAE Level	Assurance levels for safety functions and components that could impact safety functions	Assurance levels for environmental functions
0-2	ASIL C/D, EAL 4/3	EAL 4/3
3-5	ASIL C/D, EAL 5/6	EAL 4/3

- Note: EAL Assurance levels could also depend on how "connected" a vehicle is
- Security should be considered for the complete system (vehicle & infra)

RDW

Thoses who surrender freedom for security will not have, nor do they deserve, either one
(Benjamin Franklin, 1706-1790)

Thank you for your attention

Peter Striekwold

RDW