A Survey on the Applicability of Safety, Security and Privacy Standards in Developing Dependable Systems

Lijun Shan, **Behrooz Sangchoolie**, Peter Folkesson, Jonny Vinter,

Erwin Schoitsch, Claire Loiseaux

EDCC 2019 19 Sept 2019 Naples, Italy

Safety-critical systems






Increasingly digitalised, networked and personalized

Ensure safety, security and privacy

Wide range of standards

From various standardization organizations

With different and interleaving subjects

Safety

- Existing standards for industrial sectors
- New standards on safety-security co-engineering

Security and privacy

- Existing standards from ICT domains
- New standards for industrial sectors

Practitioners in industrial sectors

- What standards are available and how they evolve?
- Which ones we should comply with and why?

Developers of standards

- How well the standards are accepted by the practitioners and other stakeholders?

A survey: target population

SECREDAS: EU ECSEL Joint Undertaking project

- Research subject: product security and safety for dependable automated systems in the domains of automotive, railway and health.

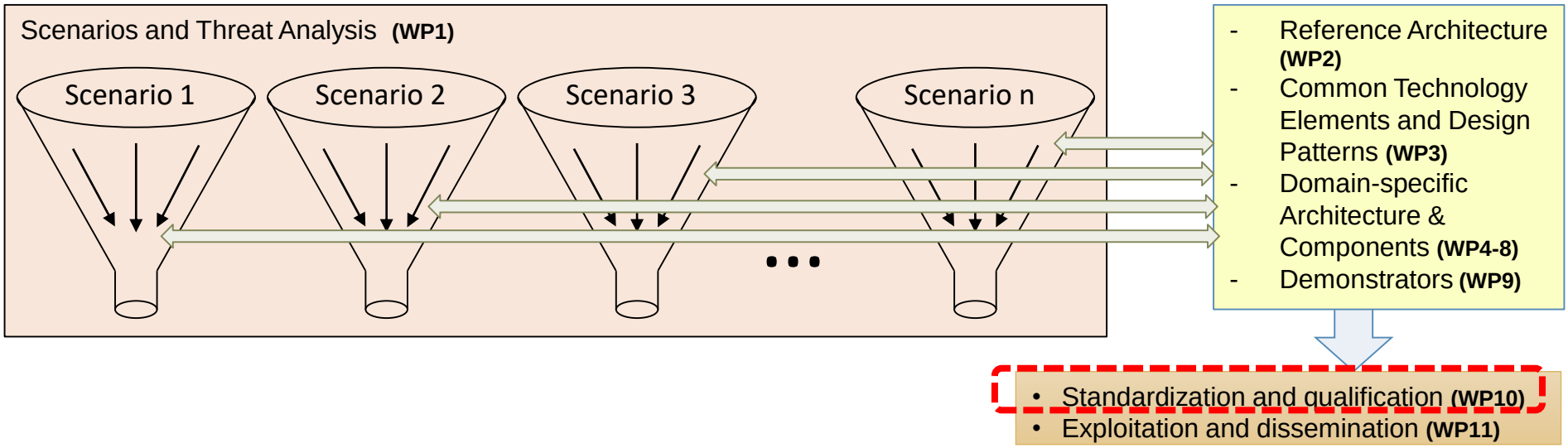
Consortium: 69 academic and industrial partners from 15 countries

- OEM/Tier 1/Tier 2 companies and IT companies: develop automated systems
- Research institutes and universities: provide supporting technologies, products or service

Partners' roles w.r.t. standards

- Practitioner of standards
- Developer of standards

SECREDAS research topics

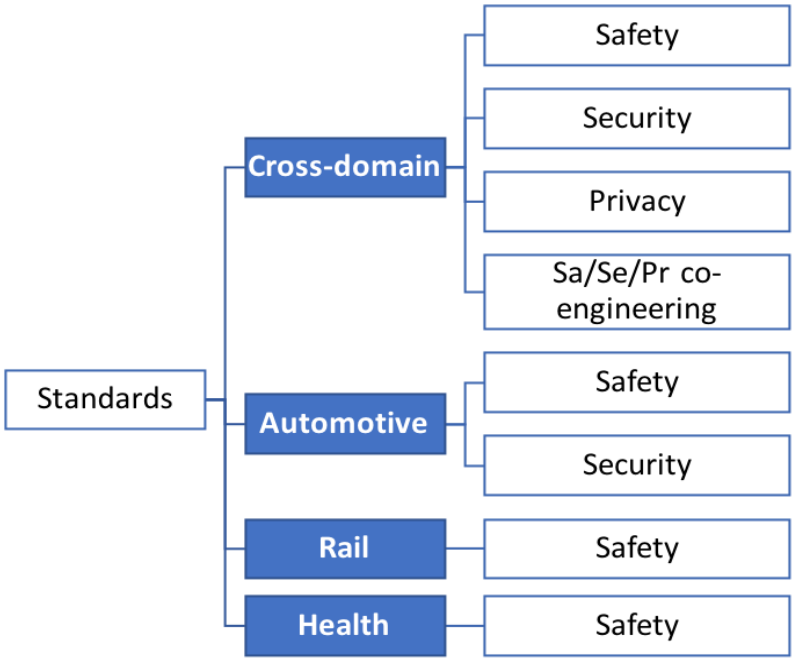


Objectives of WP10 include:

- Analyse the applicability of current standards and initiatives for the targeted domains: automotive, healthcare and railways.
- Support other work packages so they will comply with on-going standardization initiatives and identify possible contributions to ongoing standardization activities.

Questionnaire

8 categories of standards



Research questions

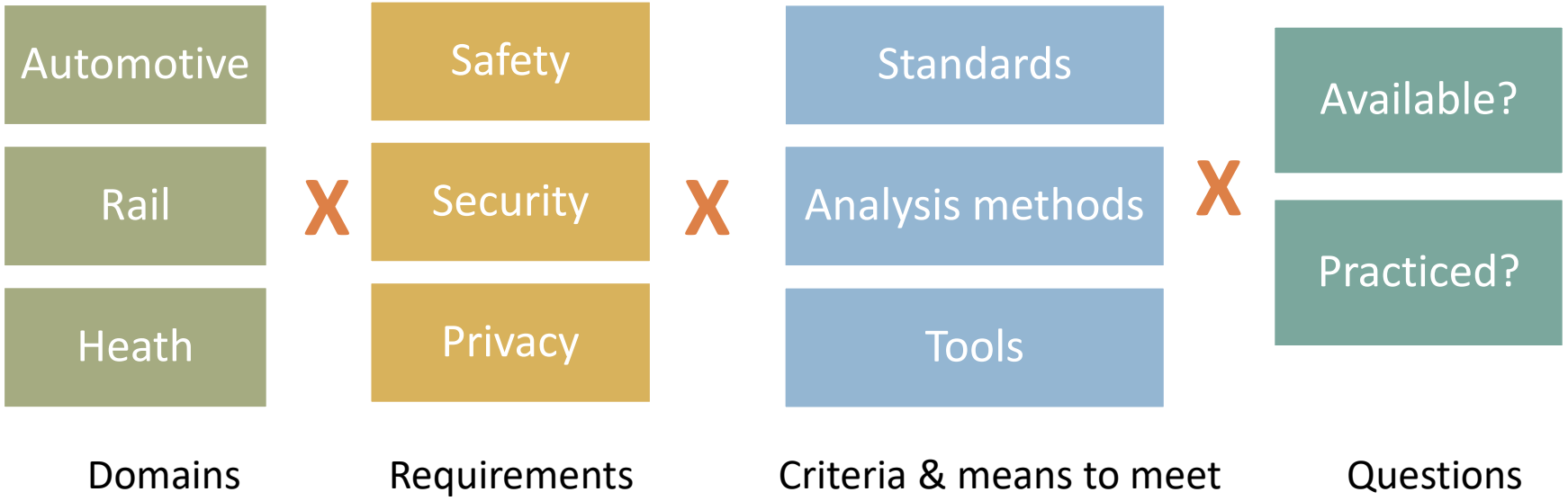
RQ1 What SSP standards are applicable?

RQ2 How are the SSP standards practiced?

RQ3 How do the practitioners follow the SSP analysis methodologies?

RQ4 How do the practitioners employ SSP engineering tools?

A questionnaire-based survey: themes



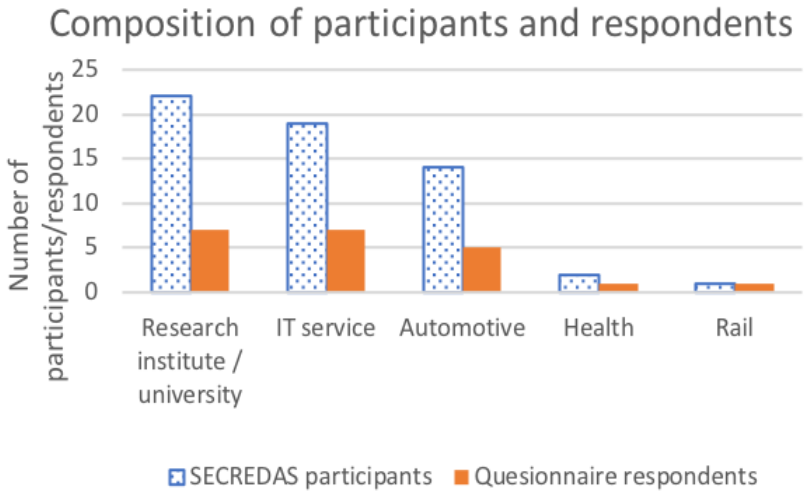
Survey design

Threats to validity

- Incomplete lists of standards/methods/tools
  - Mitigated by allowing respondents to complement
- Incomplete options to answers
  - Mitigated by allowing respondents to give any answer

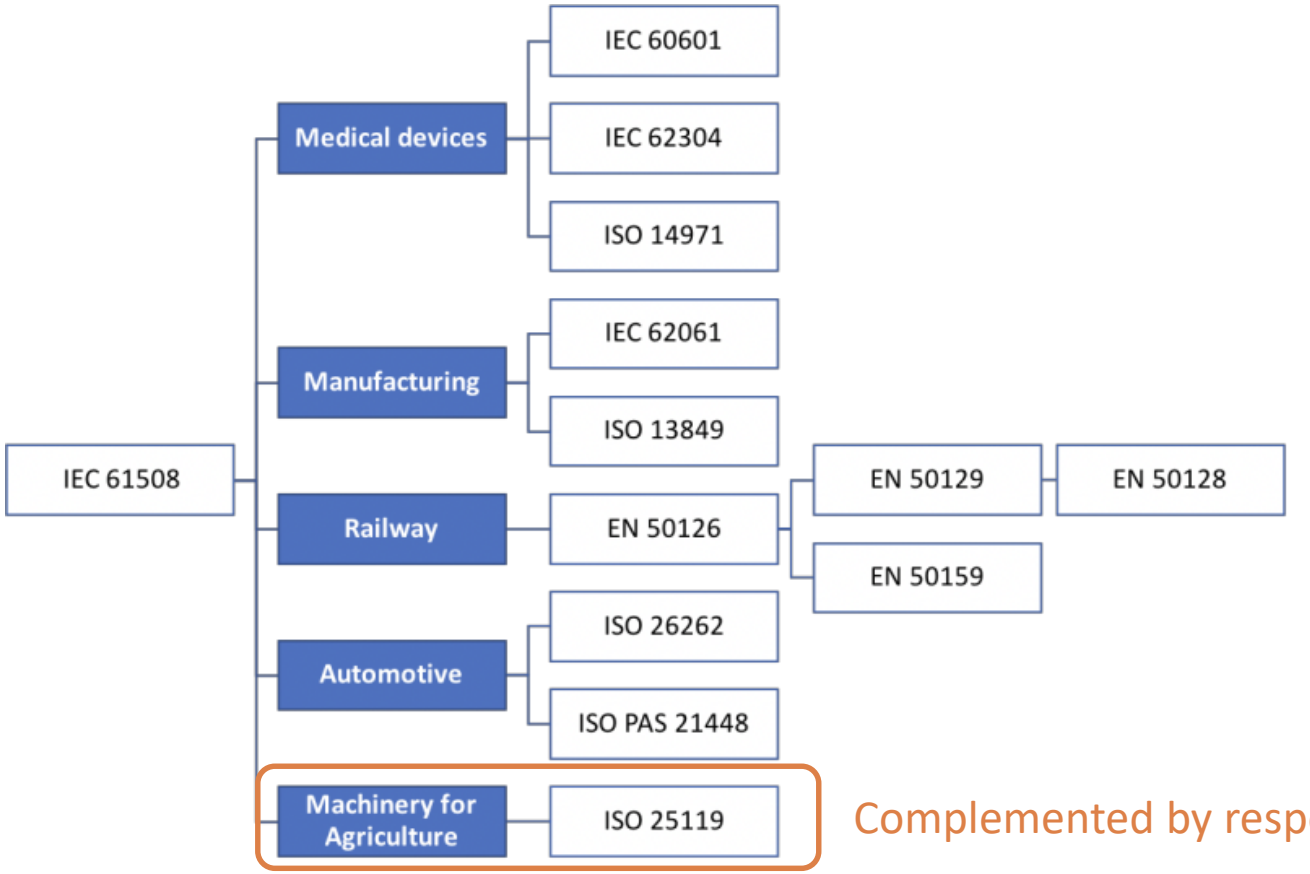
Data collection

- 05 Nov 2018 – 10 Feb 2019
- 21 responses



RQ1. What standards are applicable?

Safety standards



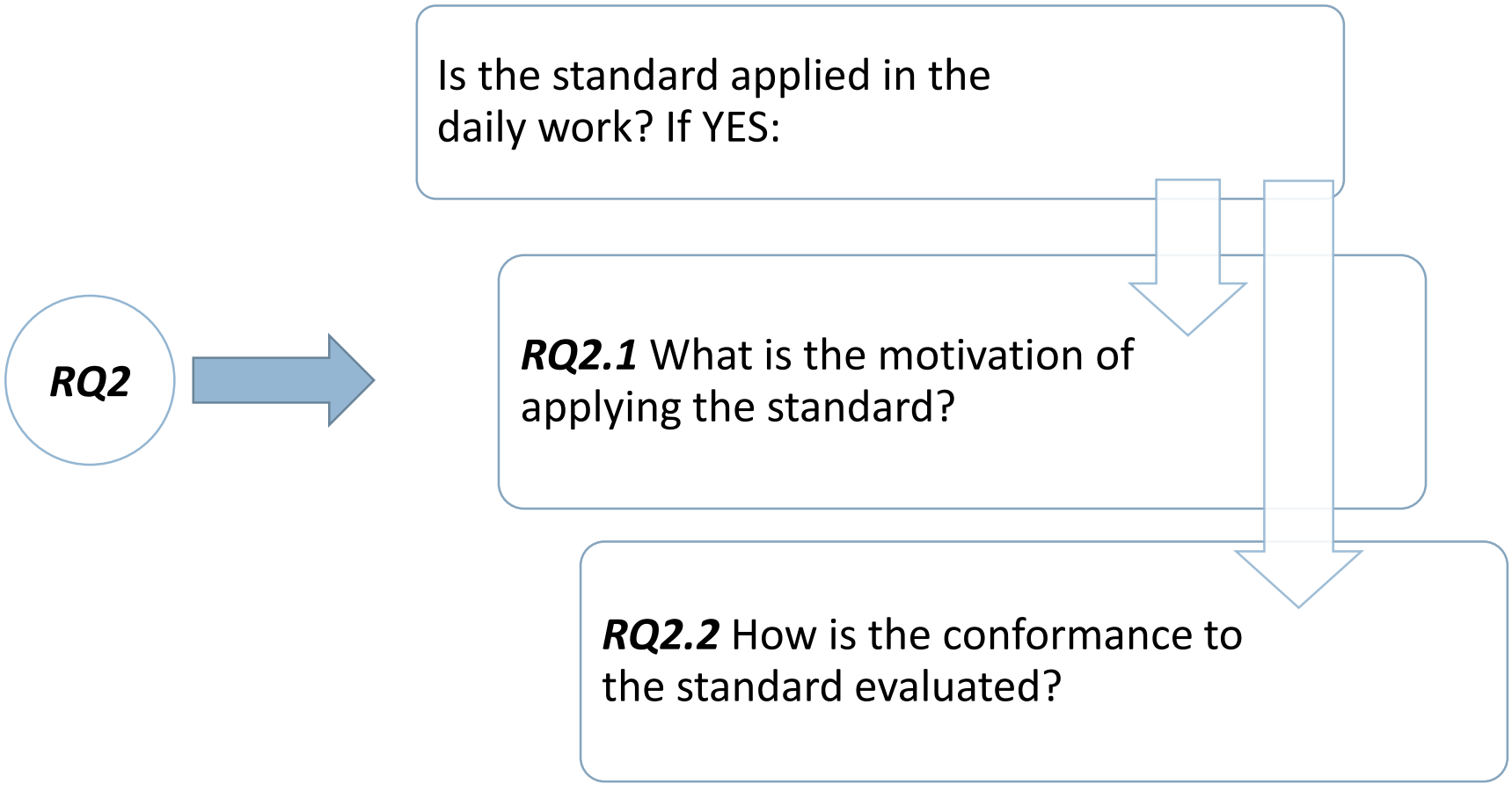
Complemented by respondents

RQ1. What standards are applicable? (cont.)

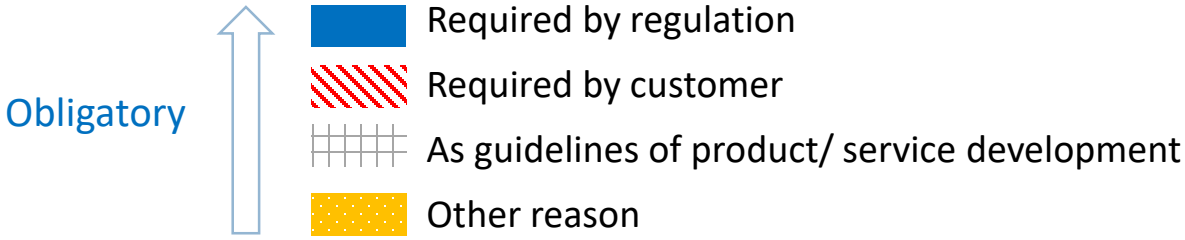
Security and Privacy standards

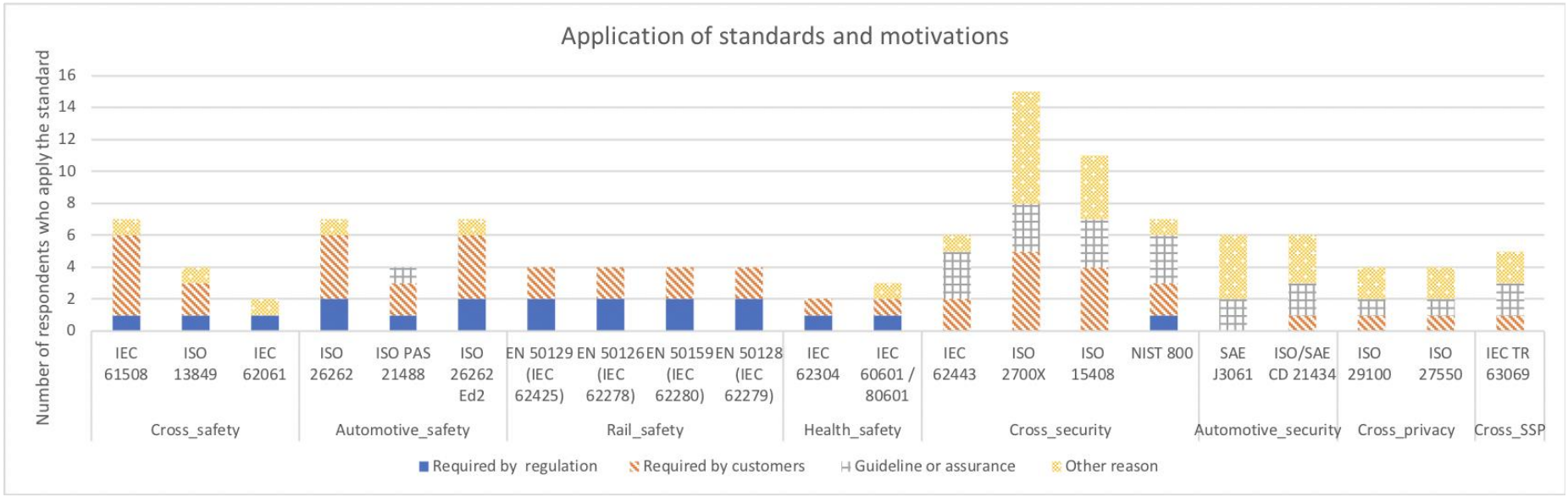
	Given	*Complemented*
Cross-domain (Security)	• IEC 62443 [11] • ISO 2700X [12] • ISO 15408 [13] • NIST 800 [14]	• GlobalPlatform specifications [15] • ETSI TS 101 733 [16]903 [17] • ETSI TS 102 204 [18] • eIDAS Security Regulation [19] • RFC cryptographic [20] • TISAX VDA ISA [21] • ETSI TS 103 532 [22] • BSI Grundschutz [23]
Cross-domain (Privacy)	• ISO 29100 [24] • ISO 27550 [25]	• GlobalPlatform Privacy framework [26] • ISO/IEC 19286 [27] • GDPR [28] • Standard Data Protection Model [29]
Automotive (security)	• SAE J3061 [3] • ISO/SAE CD 21434 [9]	-

RQ2. How standards are applied?



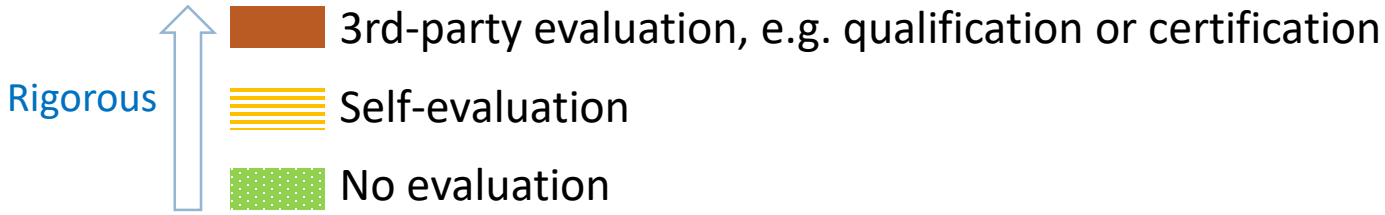
RQ2.1 Why apply the standard?

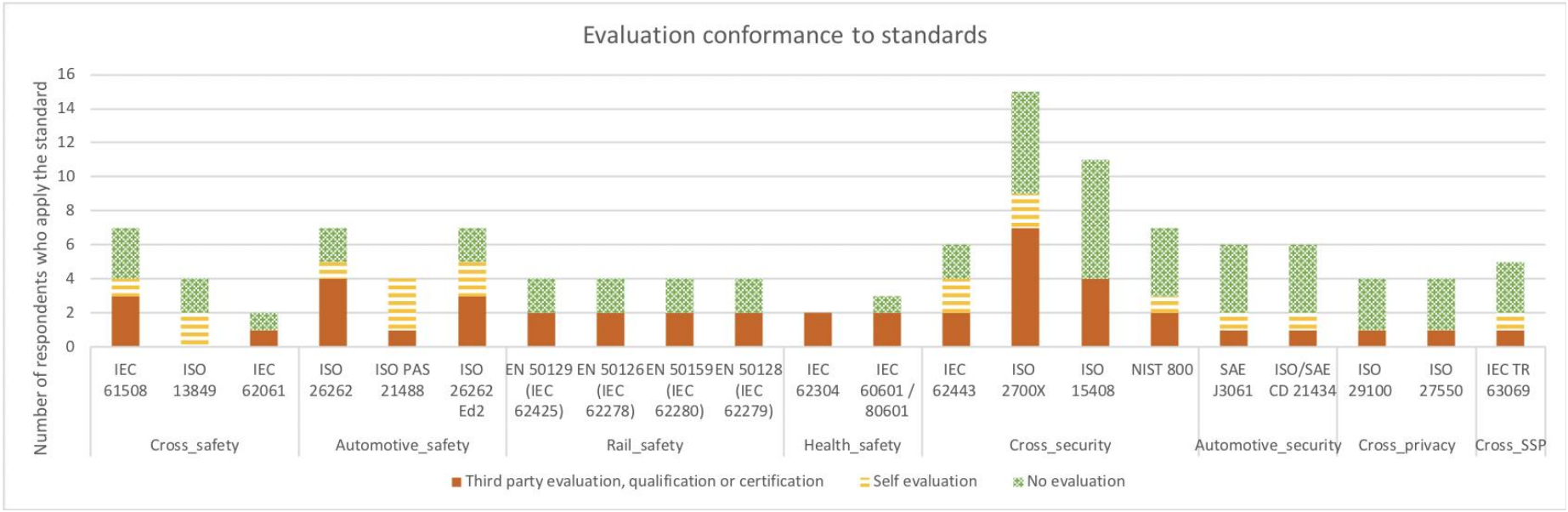




Safety standards is significantly more often imposed by regulations and customers than that of security/privacy standards.

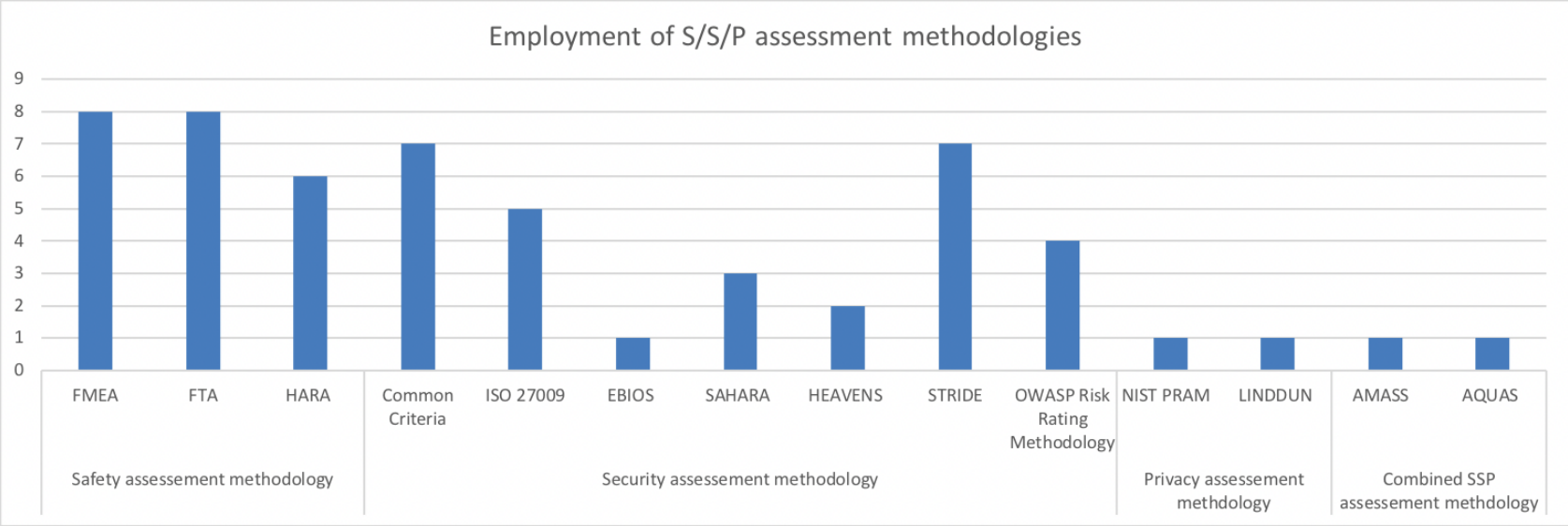
RQ2.2 How to evaluate conformance?





Conformance to safety standards is slightly more rigorously evaluated than that of security/privacy standards.

RQ3. How are analysis methods applied?



- Safety analysis: all the three methodologies are commonly used.
- Security analysis: more diverse methods are available and applied; ***STRIDE*** and ***Common Criteria*** are more commonly used.

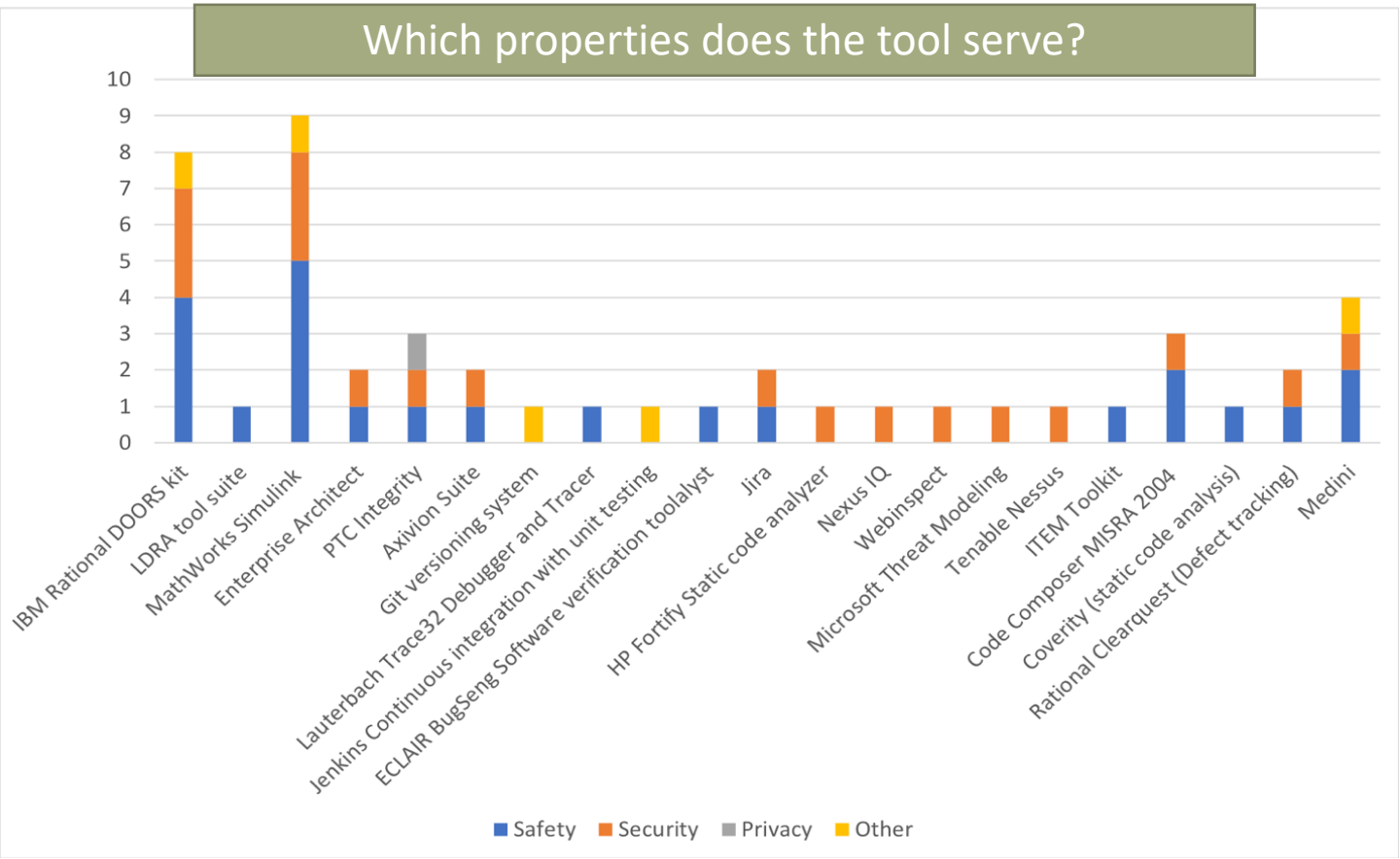
RQ4. How are tools used?

Tools given in the questionnaire:

Ansys SCADE code generators	Cadence Automotive Functional Safety
IBM Rational DOORS kit	Mentor Graphics
Veloce	Parasoft C/C++ test
LDRA tool suite	MathWorks Simulink

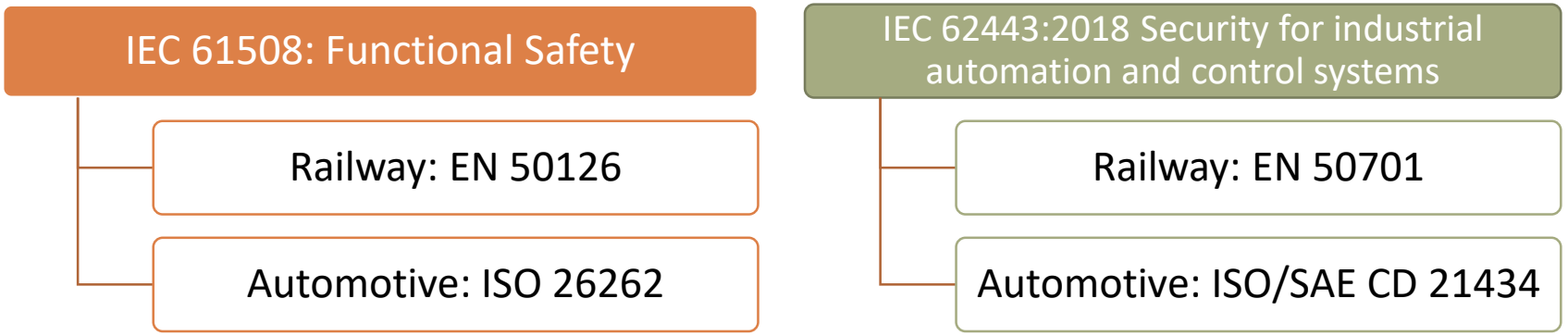
Tools complemented by respondents:

Enterprise Architect	Axivion Suite	Code Composer MISRA 2004	Coverity (static code analysis)
BugSeng ÉCLAIR	Git versioning system	HP Fortify Static code analyzer	ITEM Toolkit
Jenkins (unit testing)	Jira	Lauterbach Trace32	Debugger and Tracer
Medini	Microsoft Threat Modeling	Nexus IQ	PTC Integrity
Rational Clearquest (Defect tracking)	Tenable Nessus	Webinspect	



- 38% of the respondents employ some tools to support safety engineering, and 24% for security engineering.
- On privacy engineering, few tools are available and applied in practice.
- ***MathWorks Simulink*** and ***IBM Rational DOORS kit*** are the most used, both for safety and security engineering.

Evolution of standards: co-engineering



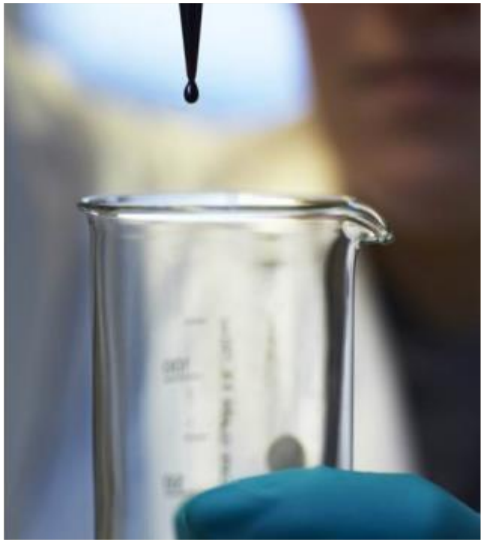
Safety standards latest versions include requirements to consider cybersecurity throughout the lifecycle

Security standards *complement* safety standards with concrete countermeasures

Future work:

- Safety Security Privacy co-analysis methods
- To motivate more awareness and participation to co-engineering standardization

?



Contact:

Behrooz Sangchoolie

Behrooz.sangchoolie@ri.se

+46 10 516 61 89

RISE Research Institutes of Sweden

RISE Safety and Transport Electronics