



Reconciling the ISO 26262-compliant and the Agile Documentation Management in the Swedish Context

Barbara Gallina¹

with contribution from and Mattias Nyberg²

1 Mälardalen University, Västerås, Sweden

barbara.gallina@mdh.se

2 Scania AB, Södertälje, Sweden

mattias.nyberg@scania.com

**Work supported by the Swedish Foundation for Strategic Research via the
SSF Gen&ReuseSafetyCases project**

Context and motivation

Focus on document management (work products), safety management



- ISO 26262
- Agile manifesto
- "Swedish" business/management culture

→ Conflicting requirements and characteristics
How can reconciliation be enabled?

Talk outline

- Background
 - ISO 26262
 - Agile manifesto
 - Swedish (business/management) culture
 - Safety culture and state of practice at Scania
 - Forces to be taken into consideration
- Challenge
- Soft and hard pieces of solutions
- Conclusion and future work

ISO 26262-compliant documentation management

Concept of “Work Product” is central.

Quoting from Part 8

- “The identification of a work product in ISO 26262 shall be interpreted as a requirement for documentation”
- “The **documentation process** shall be planned in order to make documentation available. The **documents should be**:
 - a) **precise and concise**,
 - b) **structured in a clear manner**,
 - c) easy to understand by the intended users, and
 - d) **maintainable**”



ISO 26262-compliant safety culture

- **Planning, coordinating and documenting** the safety activities of all phases of the safety lifecycle are key management tasks.
- The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety.
 - **Annex B → accountability is traceable; reward system; self-disclosure & disclosure; usage of diversity; defined, traceable and controlled process**
- The organization shall institute, execute and maintain **organization-specific rules** and processes to comply with the requirements of ISO 26262.



Agile Manifesto

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation;
- Responding to change over following a plan.

→radically informal and flexible

“Swedish” (business/management) culture

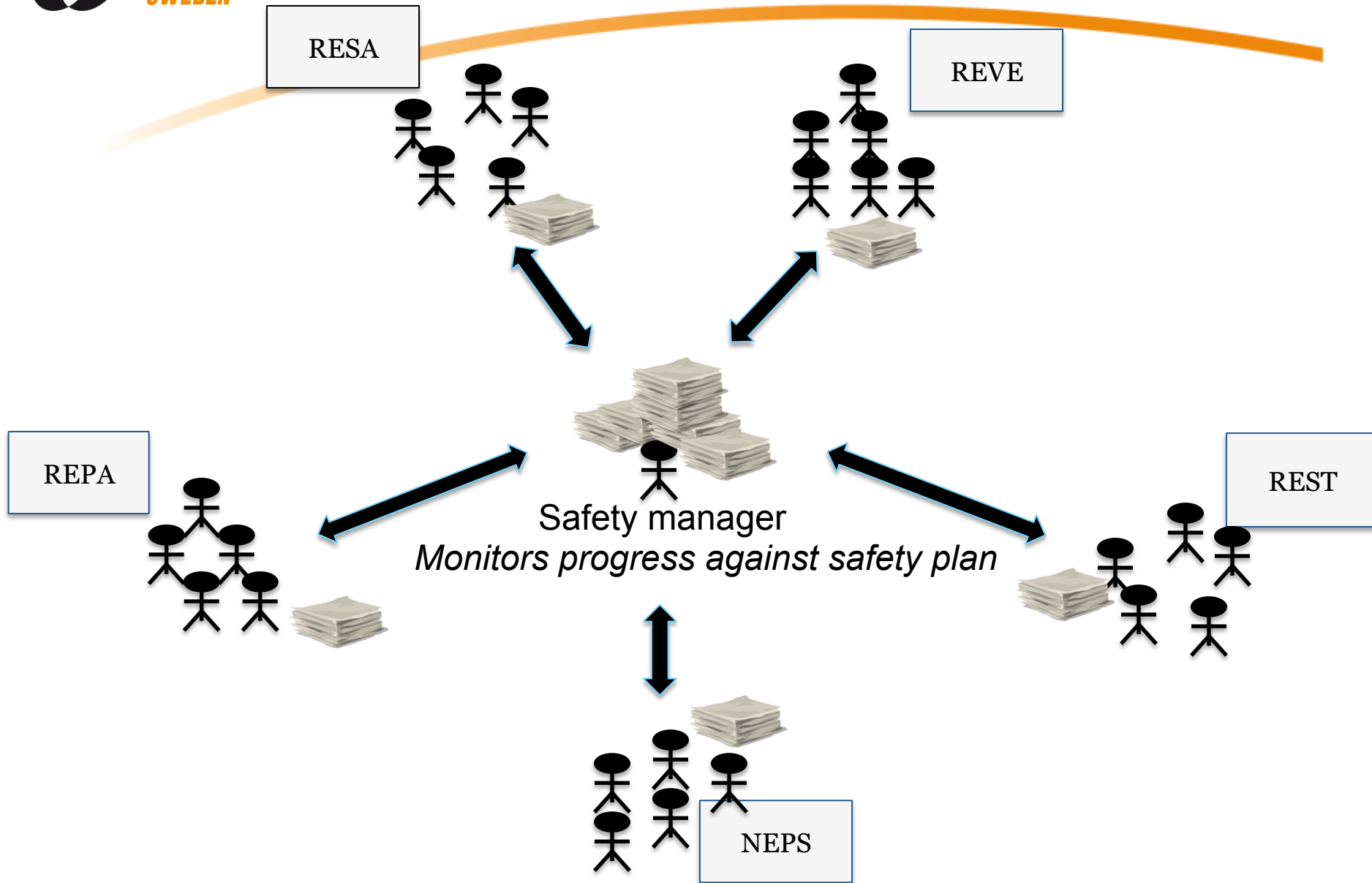
- from [8] and [9]

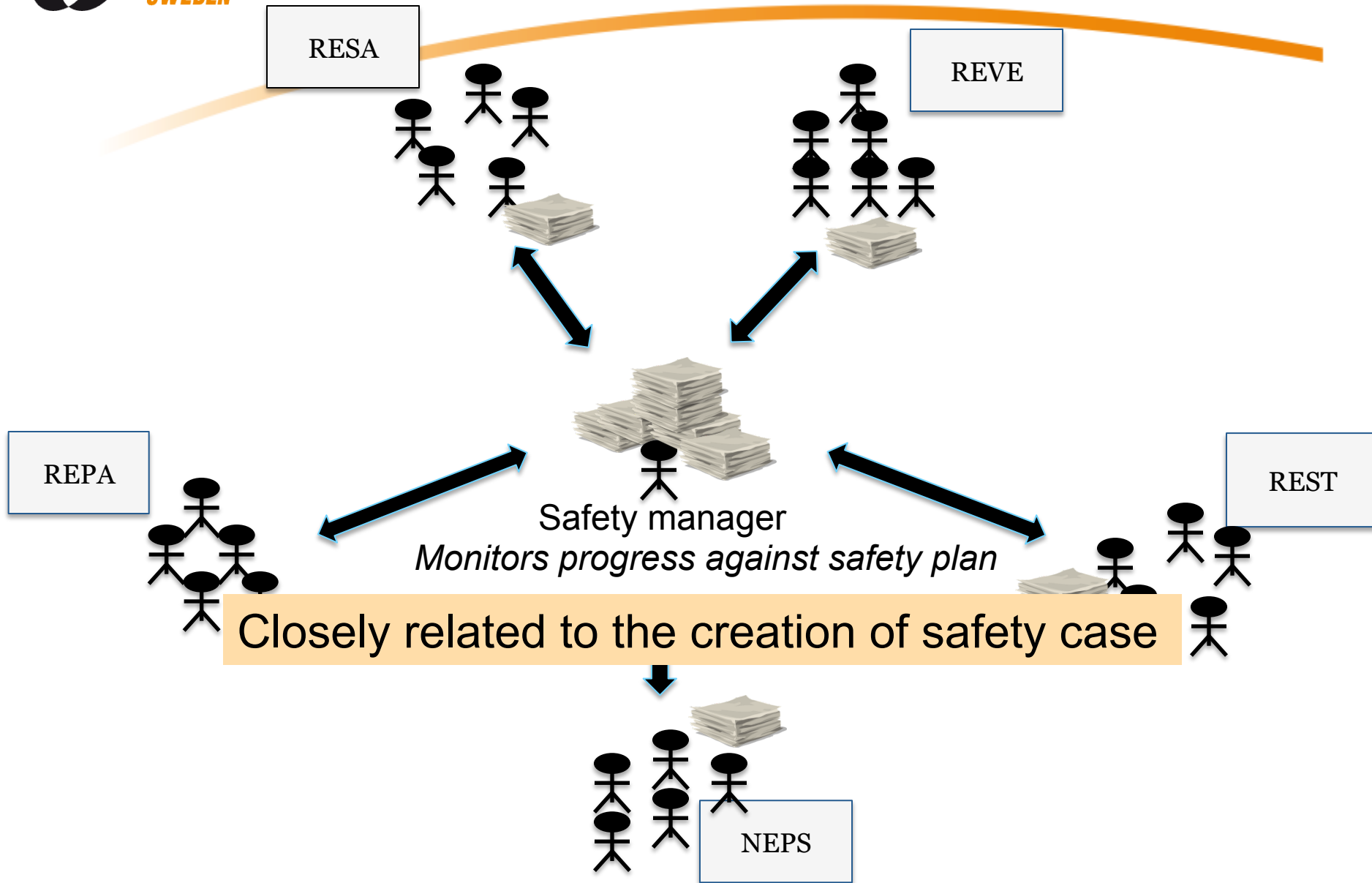
- Consensus-based informal decision making
- Flat hierarchy
- Trust
- Team-focused leadership
- “*Lagom*” – opinions are not strongly expressed
- and “*fika*” – informal communication

Safety culture and state of practice at Scania

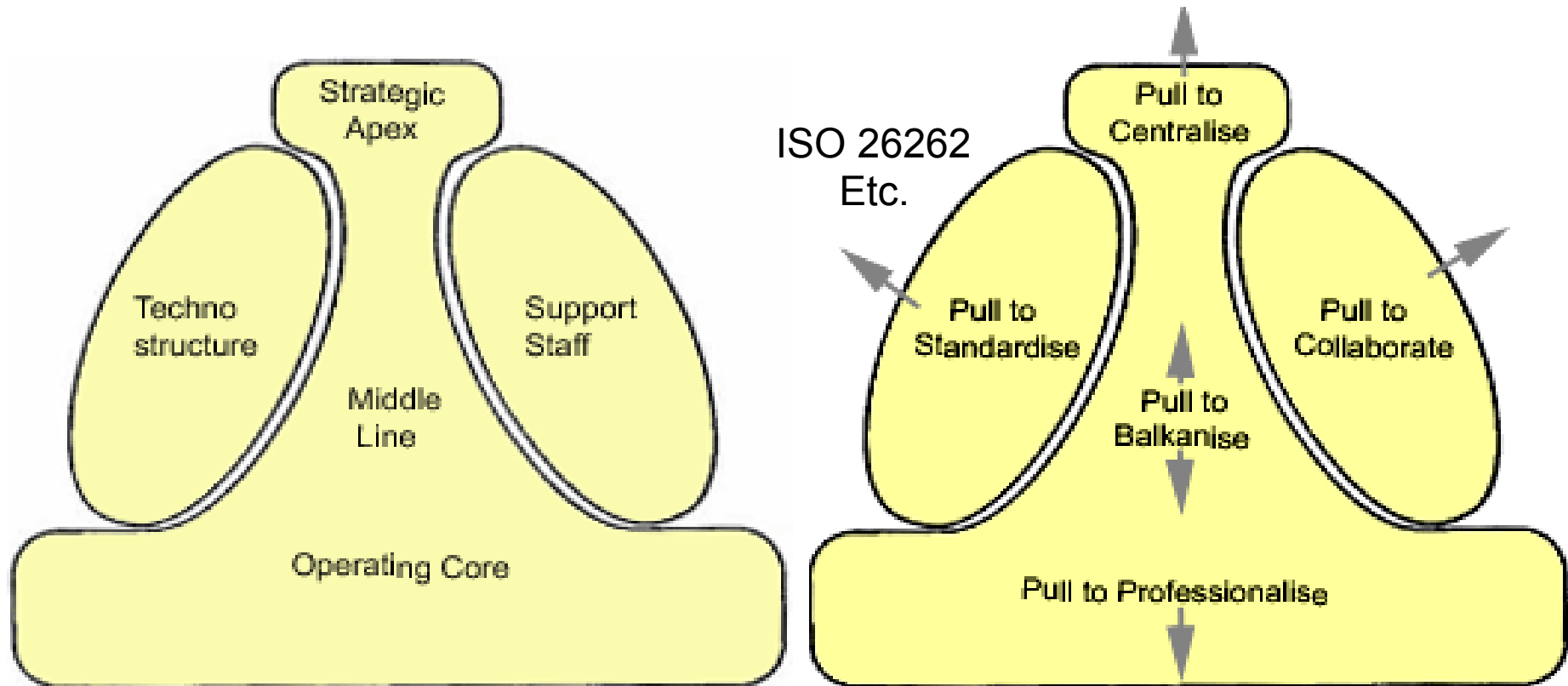
- “Respect for the individual”
- Imposed processes, assigned jobs, and *status rather than merit* are not so welcome.
- Roles are weakly defined
- Destructive interference is carefully avoided
- “Elimination of all forms of waste”.

→ commonalities with agile principles





Forces to be taken into consideration



http://www.lindsay-sherwin.co.uk/guide_managing_change/html_change_strategy/07_mintzberg.htm



Talk outline

- Background
- Challenge
- OSLC: overview
- OSLC-based soft and hard pieces of solutions
- Conclusion and future work



A true challenge

- ISO 26262
- Agile manifesto
- “Swedish” business/management culture
- Forces-balance

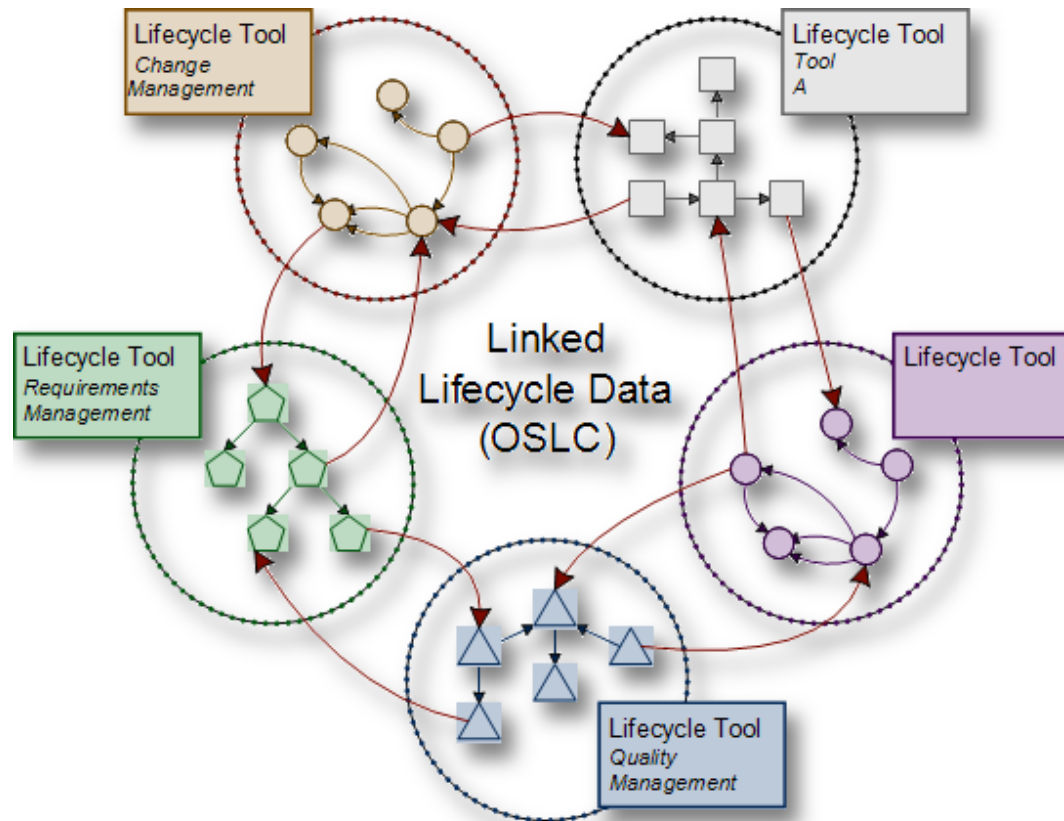
How can we reconcile?

OSLC – Open Services for Lifecycle Collaboration

- Standard that:
 - targets development tools used during a product's life cycle
 - enables tools integration and interoperability as well as traceability among their artifacts.
 - builds on top of Linked Data, Resource Description Framework, and HTTP protocol.

Remark: Each work product is described as an HTTP resource, identified via an URI. Work products are manipulated via HTTP methods.

OSLC – Open Services for Lifecycle Collaboration



OSLC Community - open-services.net, "Oslc diagram."



OSLC – Open Services for Lifecycle Collaboration

**In which way may OSLC be used to reconcile
agile and ISO 26262
in the Swedish context?**

Soft solution: Open-minded Teams for Lifecycle Collaboration

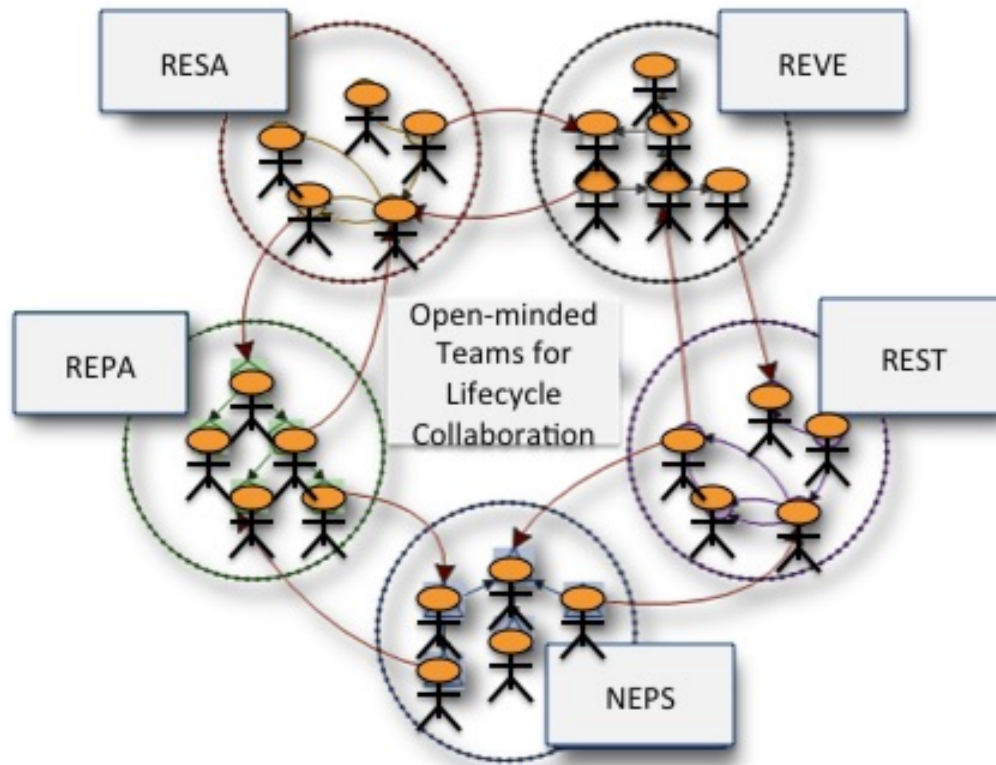
ISO26262:

safety manager can delegate tasks!

- Work performed by the different teams
- Replace safety manager by a safety case generator
- Avoid the introduction of additional hierarchical roles
- Flat hierarchy is preserved

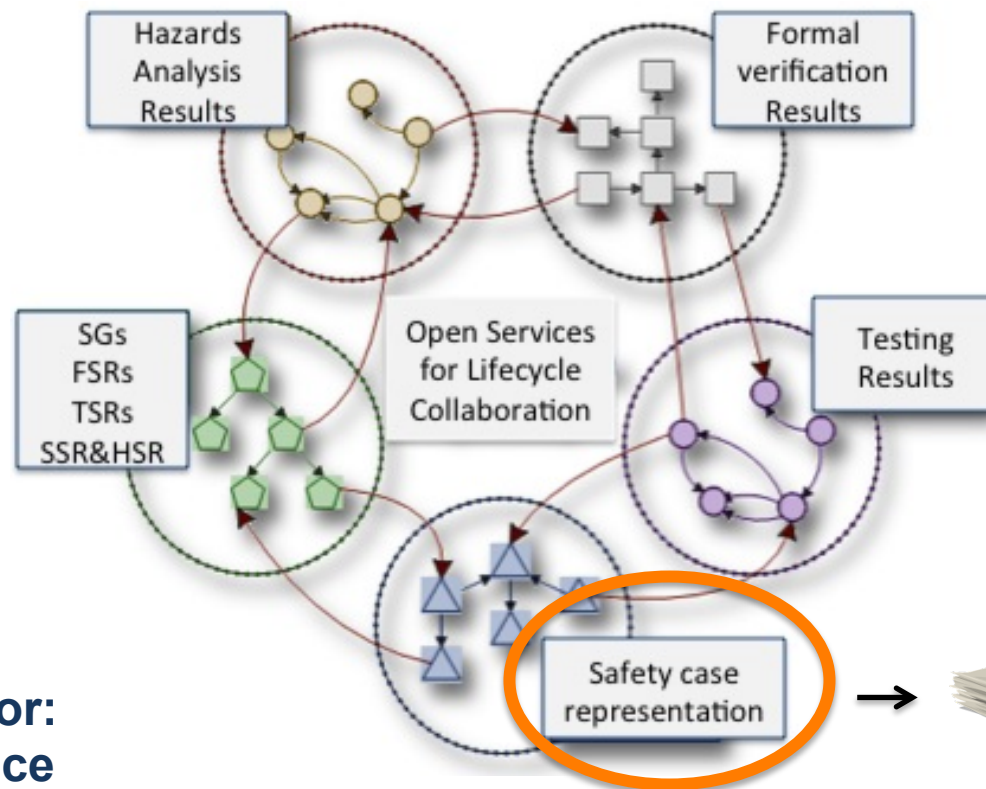
• A safety manager should be appointed to guarantee the continuous integration of best practices, which should be suggested to the various teams

A safety manager should be mindful and vigilant



Adapted from the original OSLC figure

Hard solution: OSLC-based interoperable tools



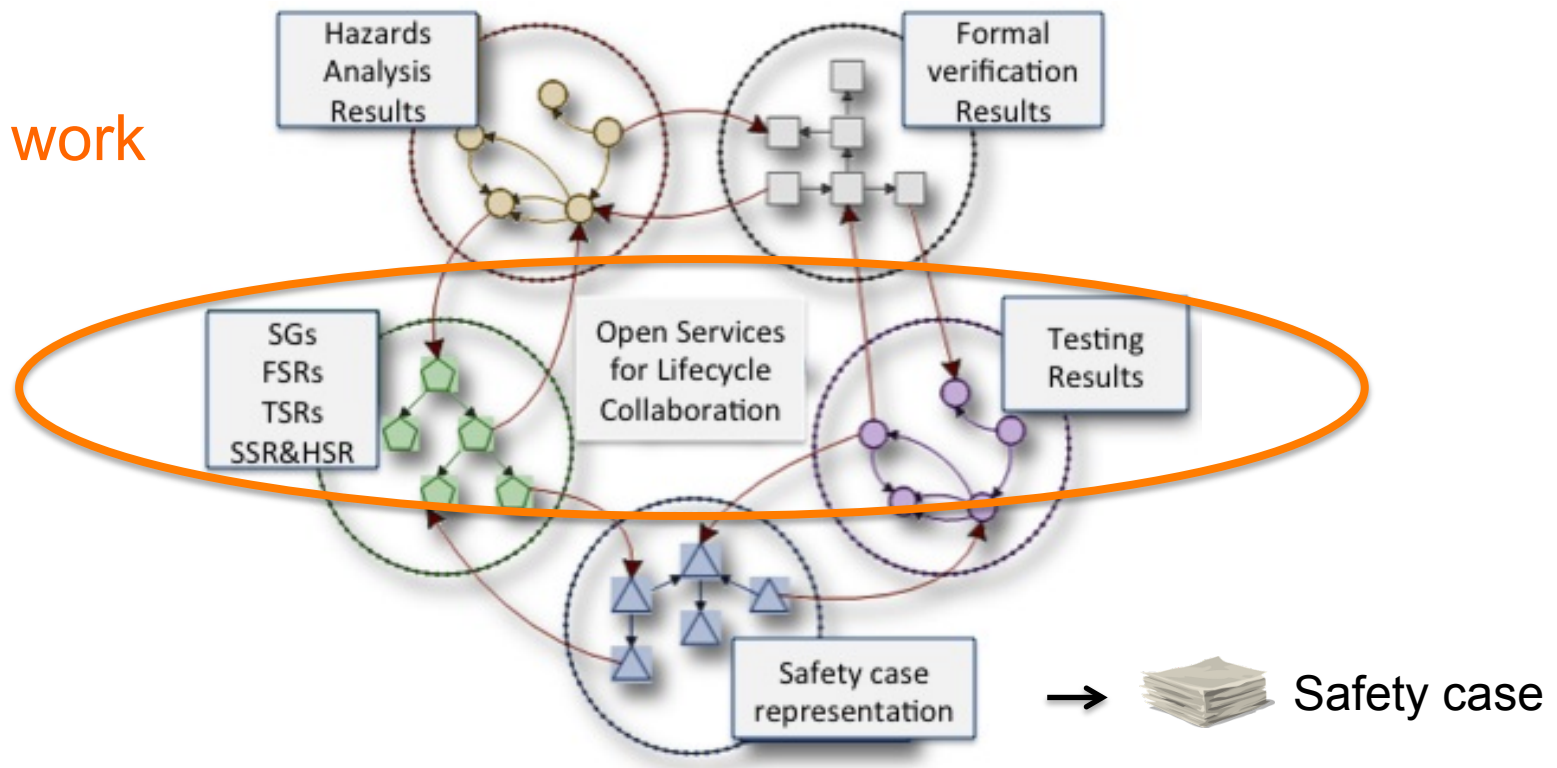
Safety-case generator:
Consumer of evidence

Producer of evidence-supported composable argument-fragments,
contributing to showing that the product is acceptable safe

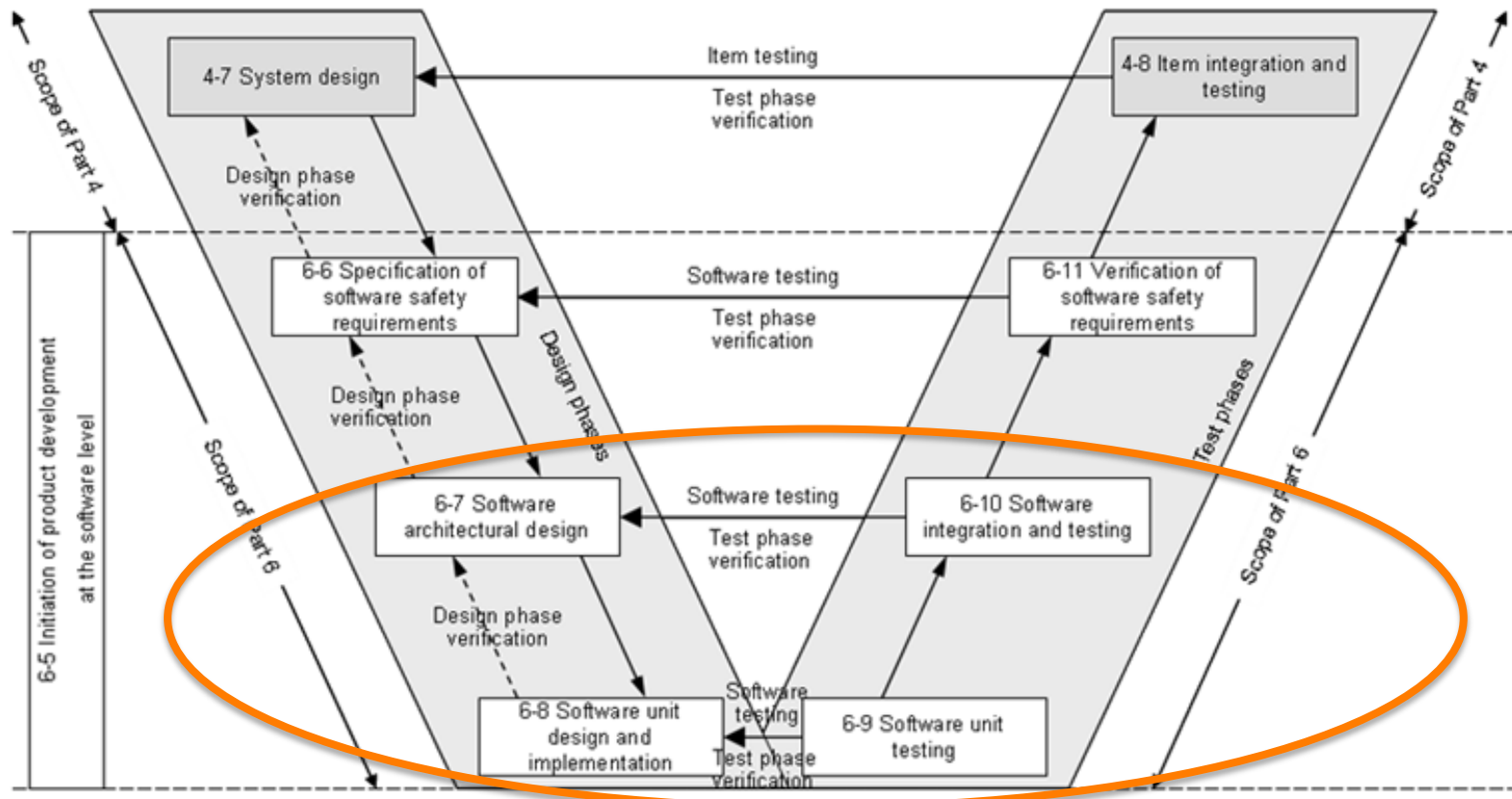
→  **Safety case**

Hard solution: OSLC-based interoperable tools

Ongoing work

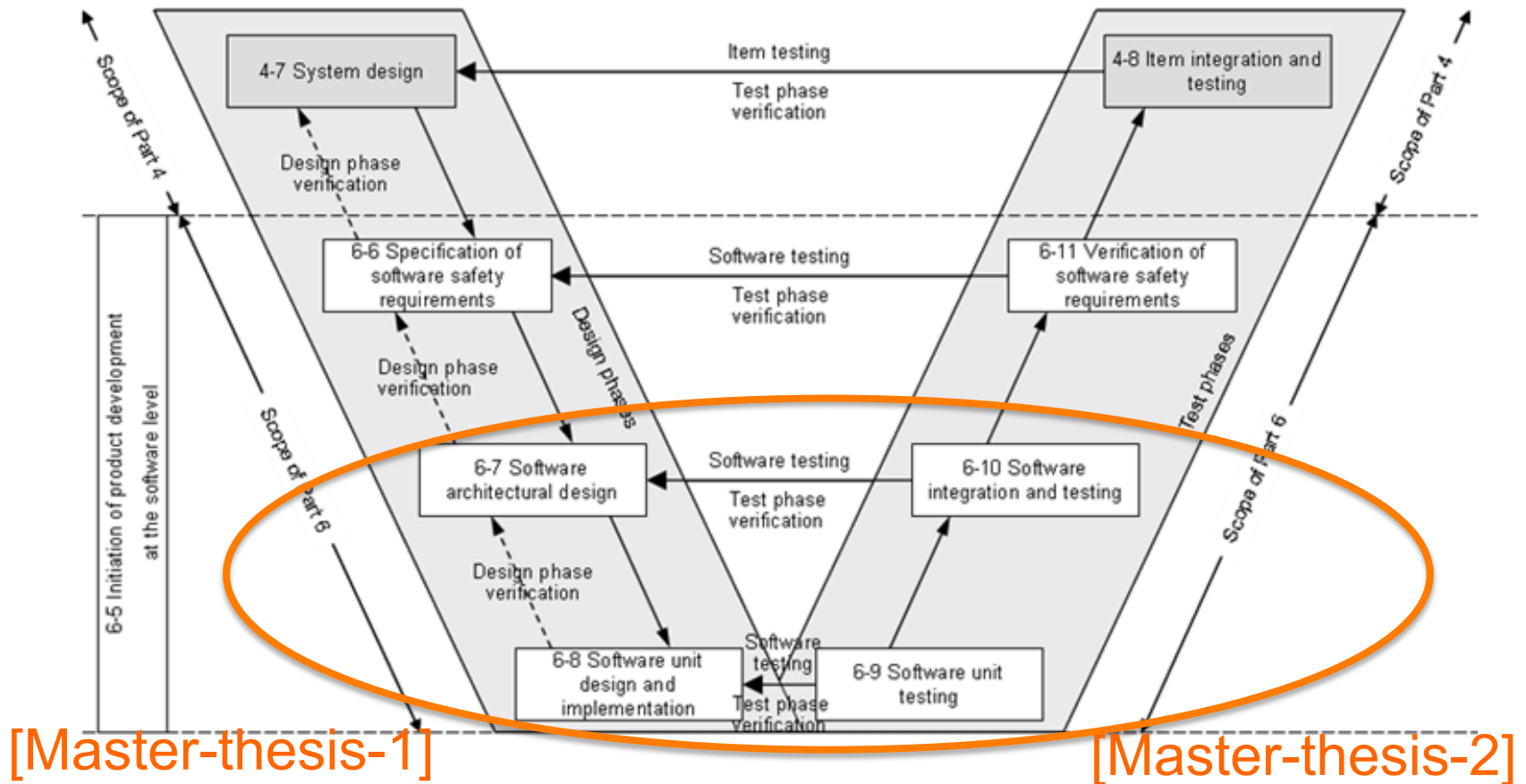


Hard solution: OSLC-based interoperable tools



Taken from ISO 26262 [ISO11]

Hard solution: OSLC-based interoperable tools



Hard solution: OSLC-based interoperable tools

- Current modeling:
 - OSLC-domains extension to include a subset of ISO 26262-Part 6 extended with Scania interpretation and tailoring

Conclusion and future work

- ISO 26262 in the agility- oriented Swedish context
- OSLC-based soft and hard solution

To be done:

- Further development of the proposed solution-towards a PoC aimed at demonstrating the (semi)automatic traceability and work-products compilation → towards a safety case
 - Via the ongoing and planned master theses
 - [Master-thesis-1]
 - [Master-thesis-2]
 - [Master-thesis-3]
 - [Master-thesis-4]
 - Via doctoral students → **AMASS**

References

- [Gallina et al. 2015] B. Gallina, M. Nyberg. Reconciling the ISO 26262-compliant and the Agile Documentation Management in the Swedish Context. Proceedings of the third Workshop on Critical Automotive applications: Robustness & Safety, joint event of EDCC-2015, Paris, France, September 8th, 2015.
- [ISO11] ISO 26262. Road vehicles – Functional safety. International Standard, November 2011.



Thank you for your
attention!

Discussion time...