Conflict as Software Levels Diversify

Fredrik Asplund, KTH Royal Institute of Technology

SCSSS 2019

Researcher in the System Safety Field

- Telecommunications Industry, 2003-2010
- PhD System Safety and Tool Integration, 2014
- PostDoc Rolls-Royce plc, 2015-2018
- Currently at KTH, Division of Mechatronics
- (And also at SAAB AB)

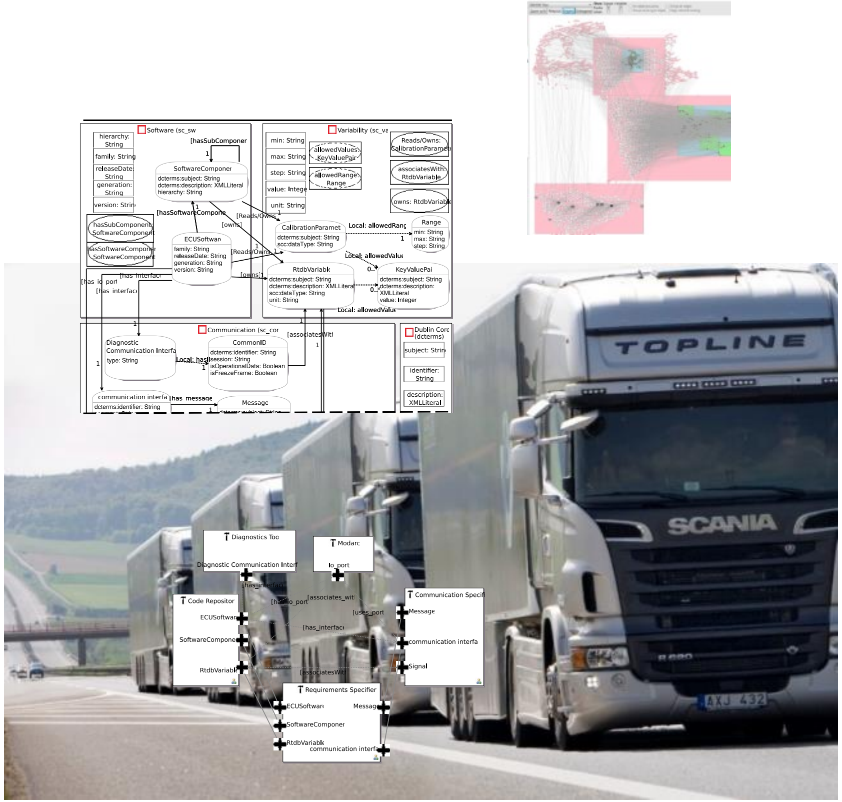
Division of Mechatronics?

Societal values
Energy and resource efficiency
Efficient concurrent engineering
Safe machines and systems
Competitive region
Better life

Model based methods and frameworks
Multi-domain optimization
Embedded systems architecting
Data and tool integration
Modelling languages
Design guidelines

Technical solutions
Vehicle prototypes
Open source tool integration software
Engineering tool prototypes
Energy optimal control strategies
Assistive device prototypes

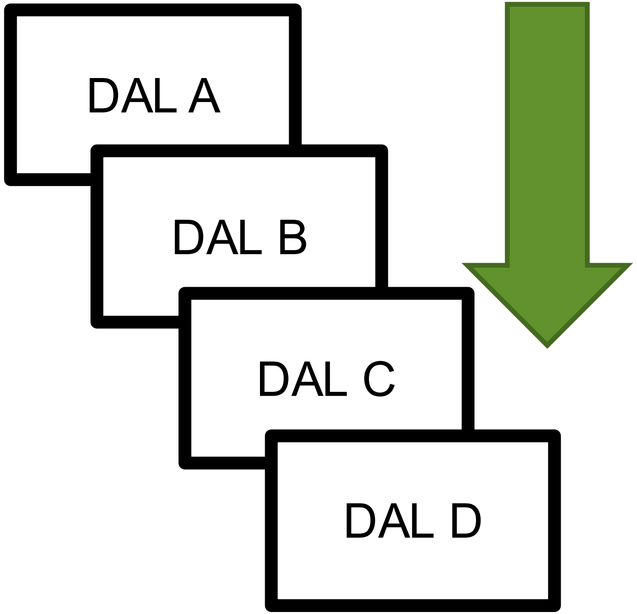
Professorial chairs
Embedded control systems
Mechatronics
Dependable control systems
Cyber-physical systems



This Presentation

- Software Levels, and the Influence by Safety-Related Standards?
- Conflict Centered on Software Levels
- Studies in Management / Cognitive Systems Engineering
- So What?

Software Levels – Changing Importance



- Some safety-relevant standards, like DO-178C, allow manufacturers to treat software components differently based on the components' relation to the safety of the end product.

- This is supposed to be a cost driver.

DAL Levels – Example Differences

- Higher levels require increasing independence between artefacts, and between those producing artefacts and those reviewing them.

- Higher levels require increasingly stringent handling of data through change reviews, tracking, traceability, etc.

- Higher levels require verification of the test coverage.

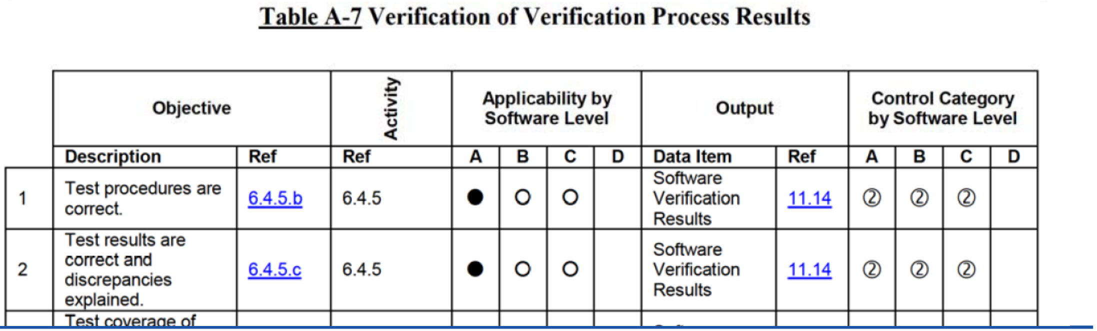
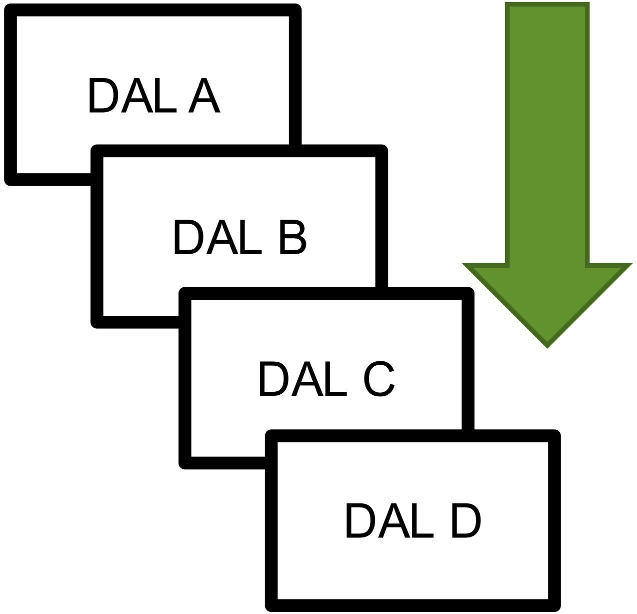


Table A-7 Verification of Verification Process Results

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref	Ref	A	B	C	D	Data Item	Ref	A	B	C	D
1	Test procedures are correct.	6.4.5.b	6.4.5	●	○	○		Software Verification Results	11.14	②	②	②	
2	Test results are correct and discrepancies explained.	6.4.5.c	6.4.5	●	○	○		Software Verification Results	11.14	②	②	②	
	Test coverage of												

Software Levels – Changing Importance



- Some safety-relevant standards, like DO-178C, allow manufacturers to treat software components differently based on the components' relation to the safety of the end product.
- This is supposed to be a cost driver.
- Lower levels are becoming increasingly important, as Artificial Intelligence and Predictive Maintenance are difficult to assure to higher levels.

Standards – The Holy Books of Engineers?

Exact step-by-step descriptions of practice

Vs

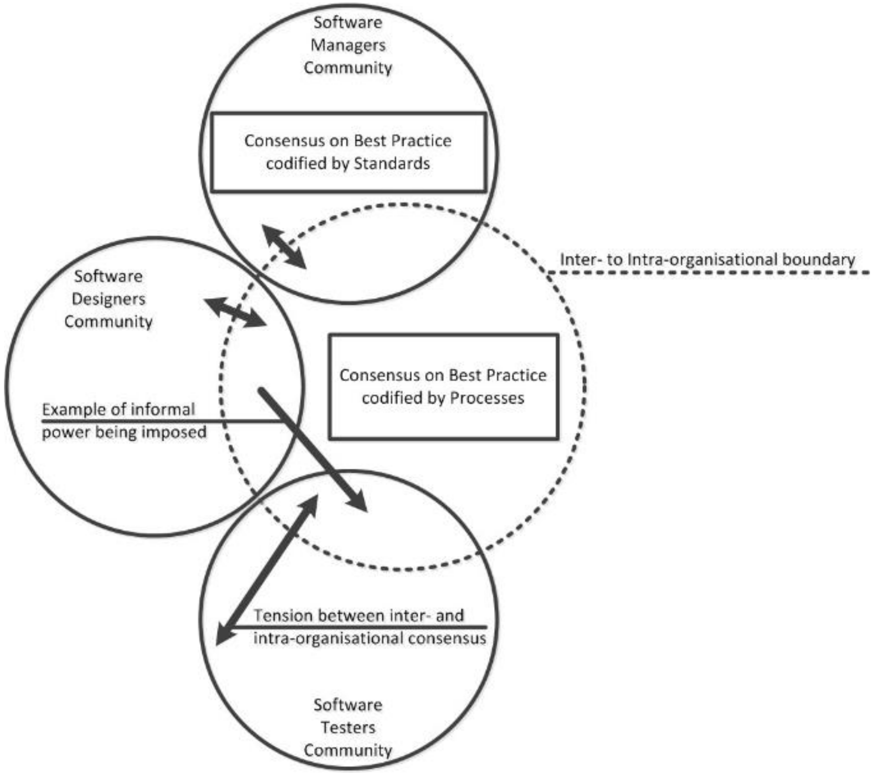
- *Part of a system of standards*
- *Implicit cause and effect*
- *High-level process descriptions*
- *Mainly for liability*

By [in NYC Wanderer (Kevin Eng)] - originally posted to Flickr as Gutenberg Bible, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=9914015

Communities of Practice

“groups of interdependent participants [that] provide the work context within which members construct both shared identities and the social context that helps those identities to be shared”

Software Communities of Practice in CPS Engineering

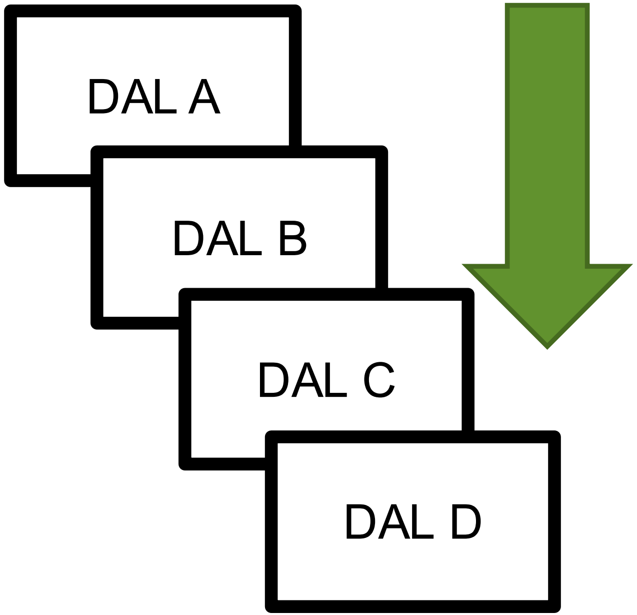


Software Managers Community
Consensus on Best Practice codified by Standards
Inter- to Intra-organisational boundary
Software Designers Community
Consensus on Best Practice codified by Processes
Example of informal power being imposed
Tension between inter- and intra-organisational consensus
Software Testers Community

- Software Managers
- Software Designers
- Software Testers

1. Standards as a way of influencing other communities *within* a firm.
2. Standards as a way of influencing those in the same community when adopting practices from *outside* a firm.

Changing Practice – A Risk?



DAL A

DAL B

DAL C

DAL D

- Software Managers
- Software Designers
- Software Testers

1. Standards as a way of influencing other communities *within* a firm.
2. Standards as a way of influencing those in the same community when adopting practices from *outside* a firm.

Conflict within the Software Designer Community

- Tactical Designers
  - Wants to **minimize the risk** of not delivering on time with the available resources.
  - As lower levels become more important, see it as an opportunity to drop some parts of existing practice.
  - Wants to diversify practice across levels.

- Strategic Designers
  - Wants to anticipate long-term needs, which means **dealing with the risk** of choosing between several uncertain paths on how to evolve the organization and products.
  - As lower levels become more important, see it as an opportunity to introduce new practice from external sources.
  - Wants practice to be uniform across levels.

No Objective Answer – Resolution by Mission Statement

- To discern whether elimination or transformation works best would require a significant amount of field data to establish.

- Other priorities such as liability play an important part.

- Resolved by the firm’s mission statement:
  - Majority likely to support tactical designers.
  - Early adopters likely to support strategic designers.

Risks Associated with Each Perspective

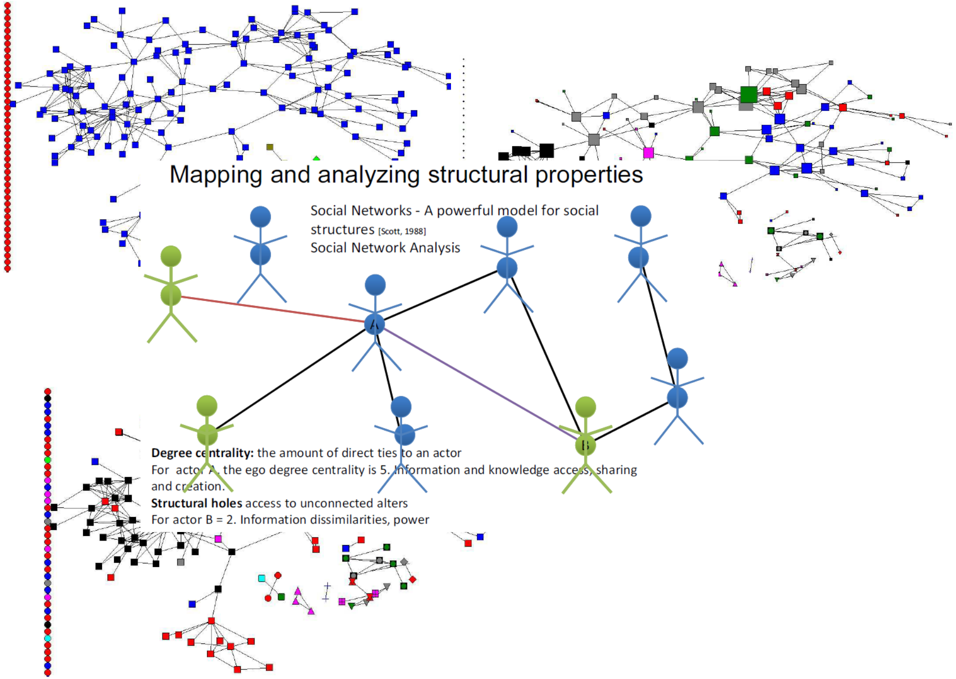
- Tactical Designers and the Majority
  - Risks splitting the software designer community into smaller parts, which have a difficult time communicating with each other.
  - Engineers working at higher levels of assurance will gain little experience from new techniques, such as artificial intelligence and predictive maintenance

- Strategic Designers and Early Adopters
  - Risk using techniques for which there is little guidance, and which require a broad competence to understand.
  - Not enough, or not the right, resources internally to the firm to investigate properly.

What to Do?

- Tacit Engineering Practice
- Different Communities
- Complex and Vague Standardization
- Non-technical Priorities (Liability, Value Creation, …)
- Organizational Values
- …

Studies in Management / Cognitive Systems Engineering



Mapping and analyzing structural properties

Social Networks - A powerful model for social structures [Scott, 1988]

Social Network Analysis

Degree centrality: the amount of direct ties to an actor

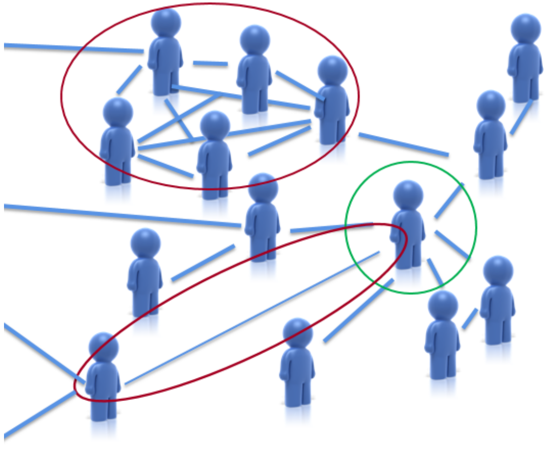
For actor A, the ego degree centrality is 5. Information and knowledge access, sharing and creation.

Structural holes access to unconnected alters

For actor B = 2. Information dissimilarities, power

CSE is an approach to the design of technology, training, and processes intended to manage cognitive complexity in sociotechnical systems.

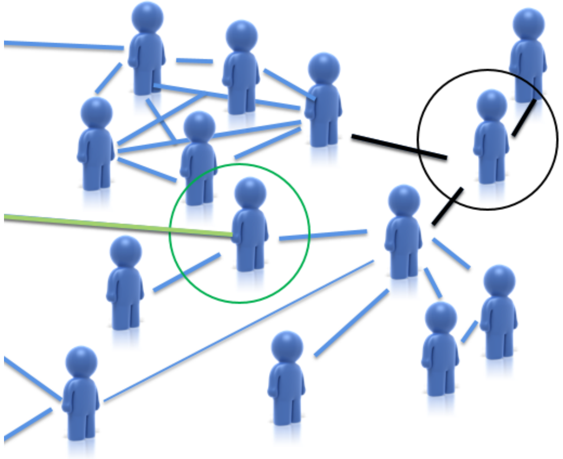
Management – Social Network Analysis



Highly connected individuals information advantage that positive influences innovation (Mehra et al., 2001; Tsai, 2001) and Ideation (Björk and Magnusson, 2009; Björk et al., 2011)

Dense network structures resource sharing benefits (Hansen, 1999; Ahjua 2000), knowledge development (Granovetter, 1973) positive for ideation (Björk et al., 2011)

The strength of weak ties (Granovetter, 1973) Creativity (Perry-Smith and Shalley, 2003, Perry-Smith, 2006) Radical innovations (Hemphäla and Magnusson, 2012)



•**Knowledge domain spanners** – individuals connected in different knowledge domains, have a positive relationship with ideation performance (Björk, 2012)

•Bridging **structural holes** (Burt et al., 2000; Burt, 2001; Björk et al;2011)

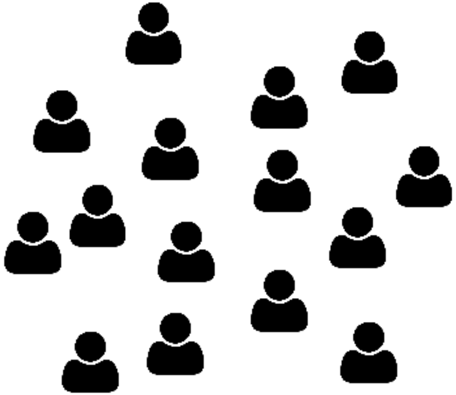
•Microprocesses and **Individual Strategic orientation**- Tertius Iugens (Obstfeld, 2005)

Cognitive System Engineering – Problem-driven

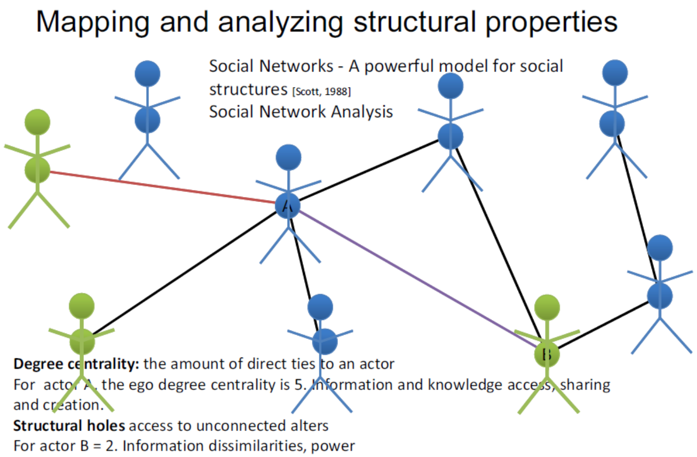
Font Awesome by Dave Gandy – http://fontawesome.io

- Operator and Machine perceived as one system.
- Problem-driven design

- The system to be analyzed can be an organization.



Who In Firm Networks Can Mitigate This Conflict?



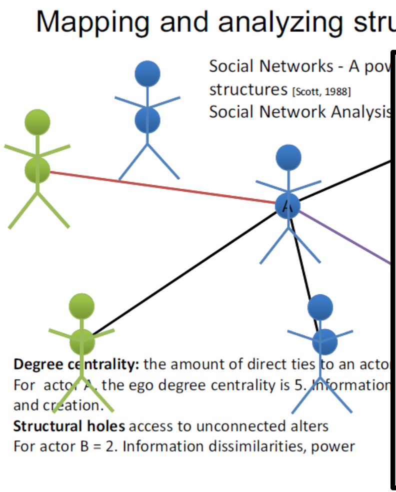
Mapping and analyzing structural properties

Social Networks - A powerful model for social structures [Scott, 1988]
Social Network Analysis

Degree centrality: the amount of direct ties to an actor
For actor A, the ego degree centrality is 5. Information and knowledge access, sharing and creation.
Structural holes access to unconnected alters
For actor B = 2. Information dissimilarities, power

- Analysis of an innovation platform
  - CPS development firm
  - Global reach
  - 23.000 users on platform
  - 4.500 active users on platform
  - 5.503 ideas submitted on platform
  - 80 ideas selected for implementation
  - Several types of ideas, ranging from technically complex to socially focused.
  - All firm functions active, ranging from secretarial to factory floor operators.

Who In Firm Networks Can Mitigate This Conflict?



Mapping and analyzing structural properties

Social Networks - A pow
structures [Scott, 1988]
Social Network Analysis

Degree centrality: the amount of direct ties to an acto
For actor A, the ego degree centrality is 5. Information
and creation.
Structural holes access to unconnected alters
For actor B = 2. Information dissimilarities, power

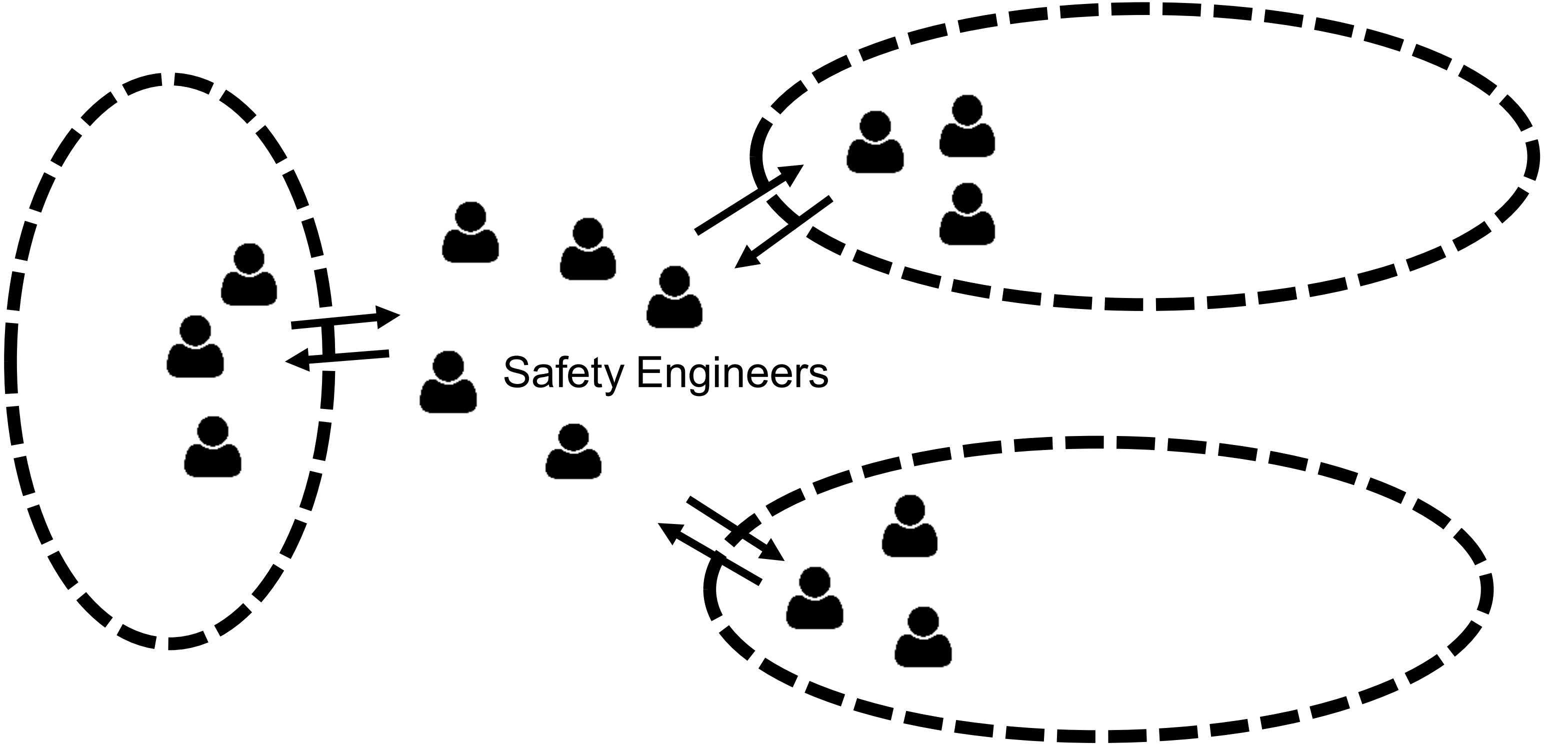
Which group is already supporting the organization by solving conflicts and improving the working context for engineers?

- Analysis of an innovation platform
  - CPS development firm
  - s on platform
  - users on platform
  - submitted on platform
  - ected for implementation
  - s of ideas, ranging from technically complex to socially focused.
  - All firm functions active, ranging from secretarial to factory floor operators.

Safety Engineers Emerge as Top Facilitators

- Safety engineers:
  - Were facilitators:
    - > *Commented significantly higher on successful ideas than other firm functions.*
    - > *Did not submit more or push through their own ideas.*
  - Focused on administrative innovations related to e.g.:
    - > *Non-technical safety issues*
    - > *Social interactions*
    - > *Communication*

Networking on Safety Culture



Conclusion

- Change is coming to our way of working with software levels.
- Risks will be difficult to grasp and will vary across firms.
- The mission of safety engineers (should) include safety culture. This can be a wider mission than ensuring adherence to processes.
- Emphasize the mediatory role of identifying required and viable changes to interactions between and within communities.