Faculty of Engineering Technology

Bruges Campus

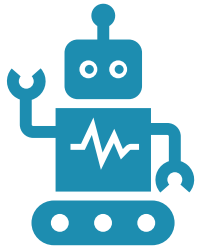
KU LEUVEN

STPA and Autonomy : Friends or foes? A case study analysis

TETRA project Safety Assurance 4.0: Management of Safety Risks in Industry 4.0 (HBC.2020.2088)

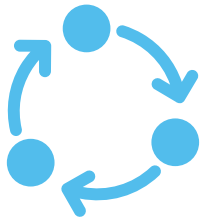
Ing. Laure Buysse
Ir. Manie Conradie
Prof. Dr. Ir. Davy Pissoort
Dr. Ing. Dries Vanoost

Background – Autonomous Systems



Autonomous and Collaborative Safety

Consideration of **automated and collaborative actions** within the system and between systems



Safety **through-life** in different environments and different situations (including maintenance, updates and more)

Inclusion of COTS, AI, ML and more

M. A. Ramos, C. Thieme, I. B. Utne en A. Mosleh, 2019, Autonomous Systems Safety - State of the Art and Challenges," in *International Workshop on Autonomous Systems Safety (IWASS)*, Trondheim, March 11-13.

Background – SA4.0

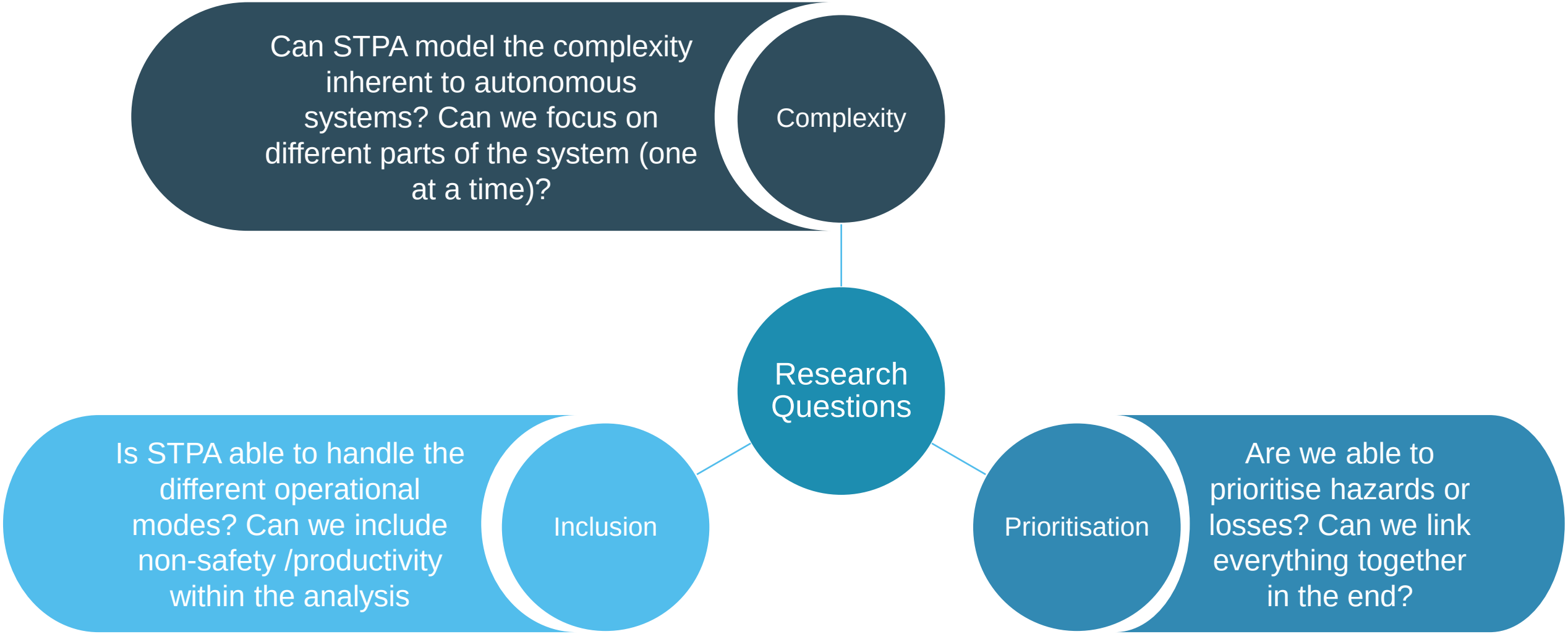
- **TETRA Safety Assurance 4.0** – Management of Safety Risks in Industry 4.0

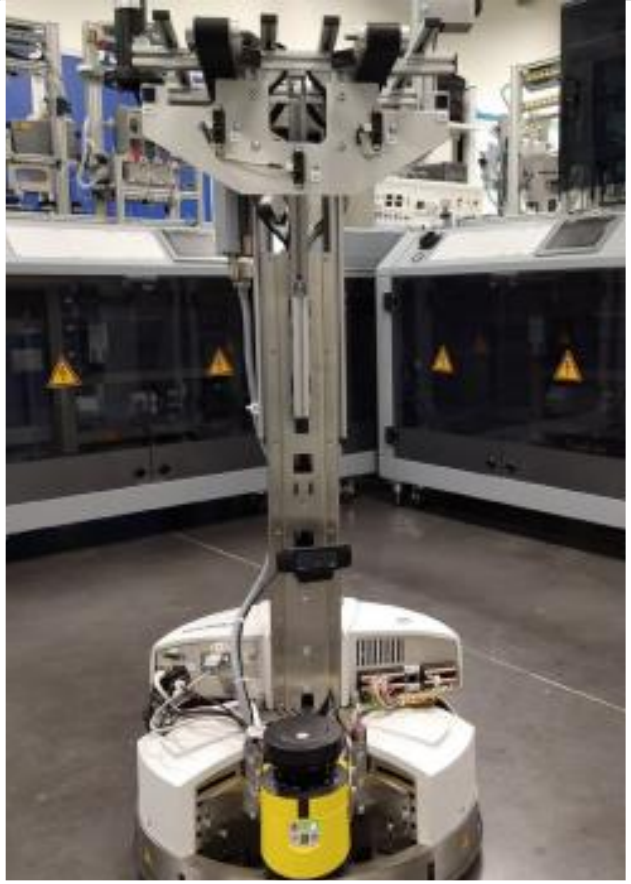
- **Technology Transfer** Project with a strong focus on Industry

How to ensure that cooperative / collaborative robots, AMR's, AGV's and autonomous systems can **operate safely without** having to be trapped in a **safety cage**?

Faculty of Engineering Technology KU Leuven. (2020). *Safety Assurance 4.0 – Management of Safety Risks in Industry 4.0. Retrieved from* https://iiw.kuleuven.be/onderzoek/m-group/research-and-projects/tetra_sa4.0

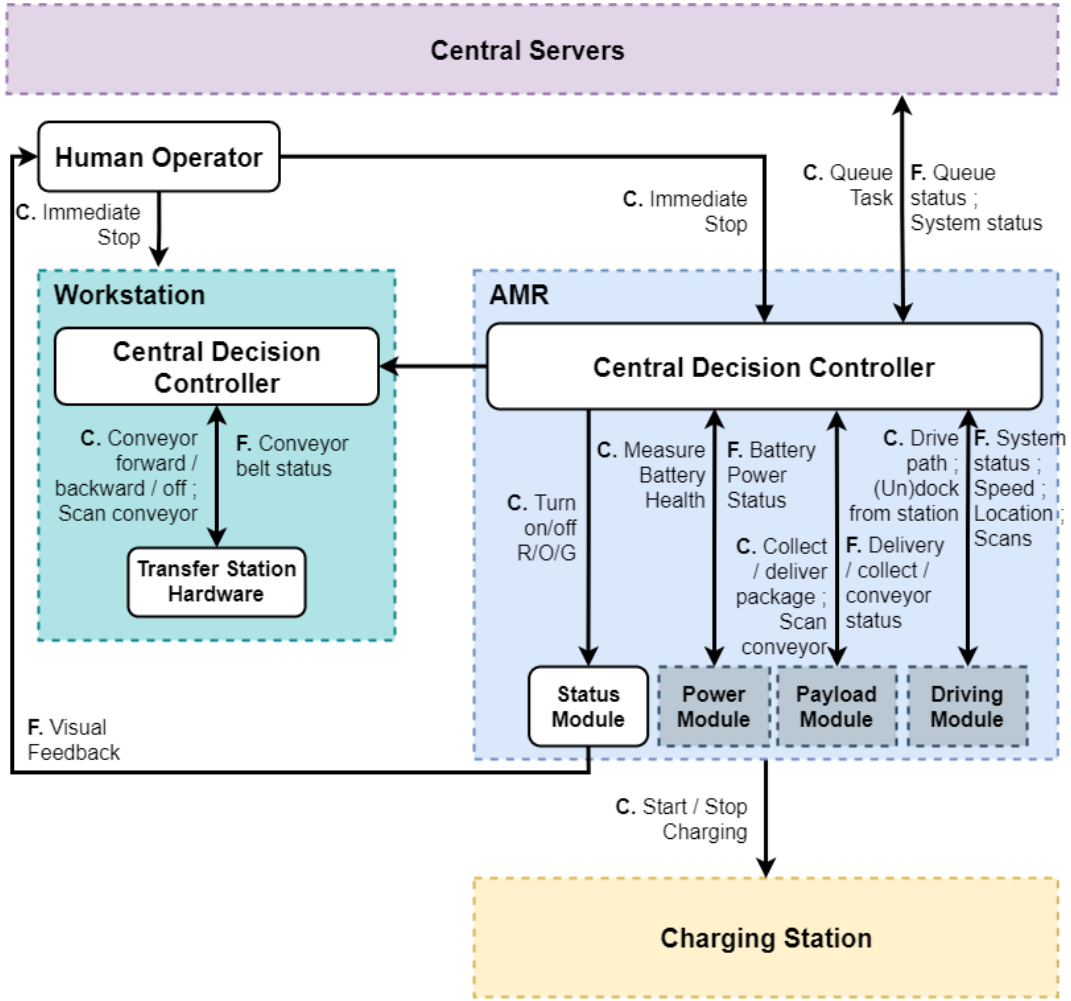
Research Questions



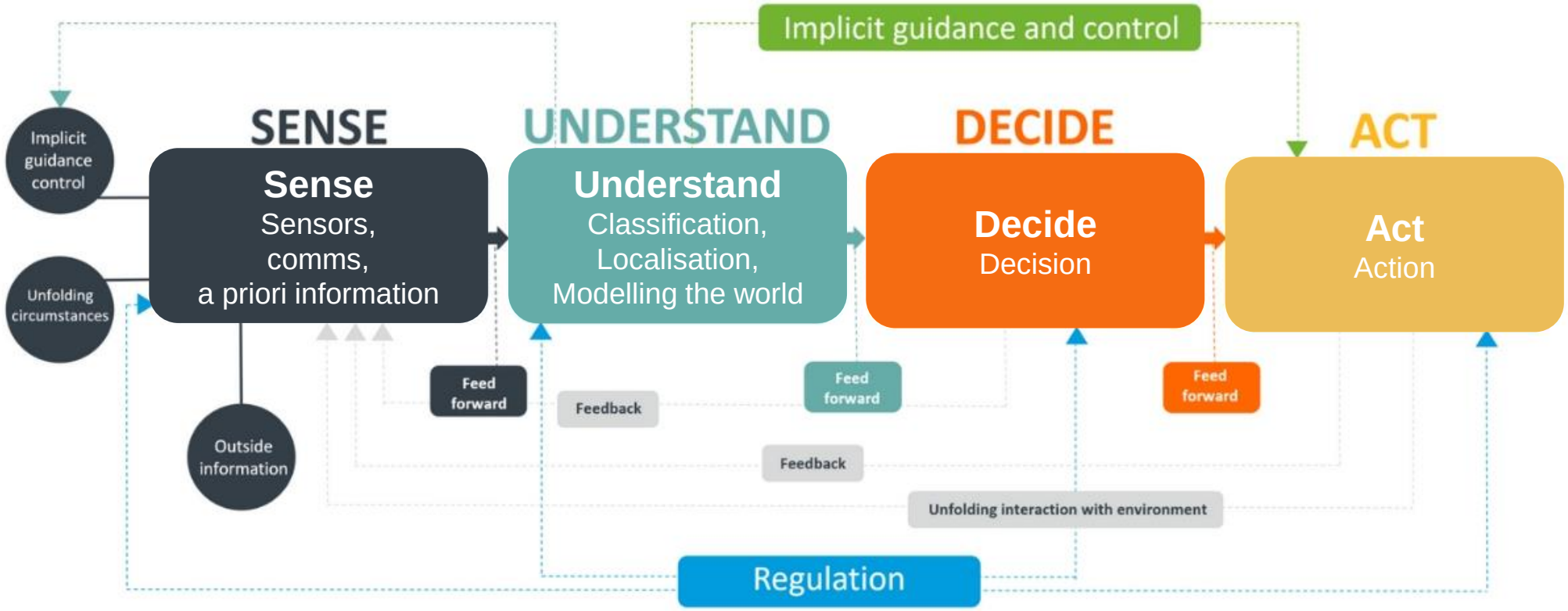
Background - Autonomous Mobile Robot

Results – Control Structure



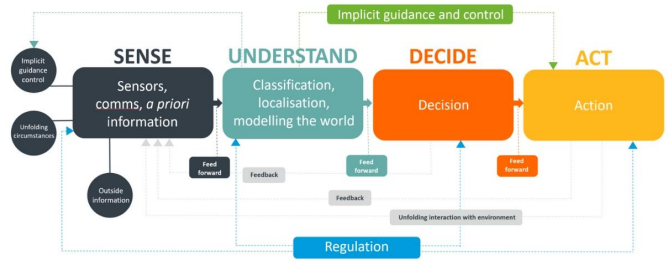
M. Nicholson, R. Hawkins , N. Johnson. (2019), "Workshop on Autonomy and AI" in *Safety Critical Systems Symposium (SCSS)*, Bristol, February 4.

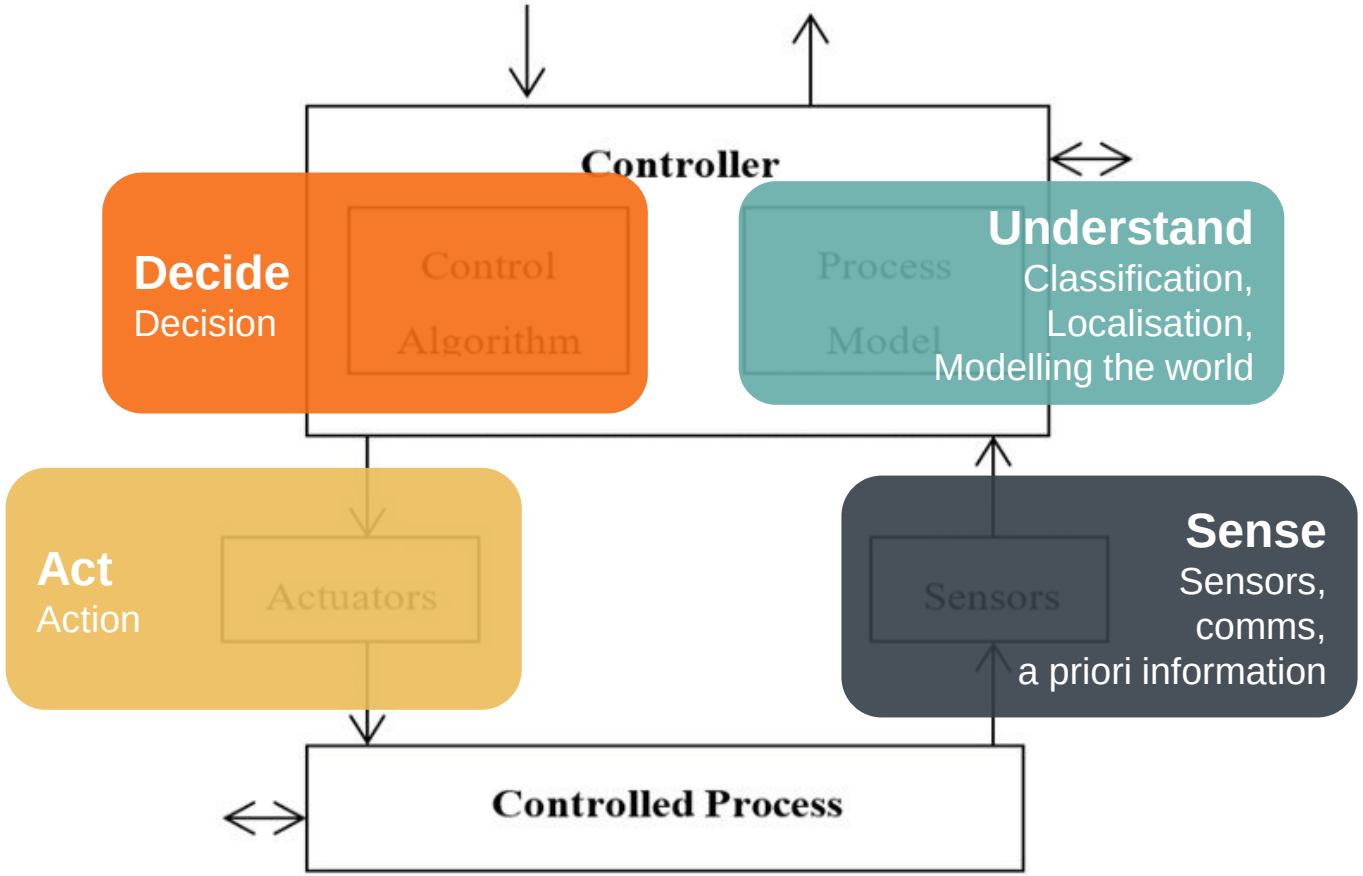
Results – SUDA Model



M. Nicholson, R. Hawkins , N. Johnson. (2019), "Workshop on Autonomy and AI" in *Safety Critical Systems Symposium (SCSS)*, Bristol, February 4.

Results – SUDA Model





M. Nicholson, R. Hawkins , N. Johnson. (2019), "Workshop on Autonomy and AI" in *Safety Critical Systems Symposium (SCSS)*, Bristol, February 4.

III. Results – Losses and Hazards

Losses

- Straightforward to identify losses
- Ability to include productivity within the losses

Hazards

- Not as straightforward for the industry
- Unable to use a manual or ISO guidelines to define hazards

International Organization for Standardization. *ISO 12100:2010 : Safety of machinery – general principles for design – Risk assessment and risk reduction*. (2010)

III. Results – Losses and Hazards

Losses
- Straightforward to identify losses
- Ability to include productivity within the losses

Hazards
- Not as straightforward for the industry
- Unable to use a manual or ISO guidelines to define hazards

Hazard according to ISO 12100:2010	Hazard within STPA
Moving elements	Violation of minimum separation rules between the AMR/infrastructure/humans/animals
Falling objects	Equipment under unnecessary stress

International Organization for Standardization. *ISO 12100:2010 : Safety of machinery – general principles for design – Risk assessment and risk reduction*. (2010)

Results – Unsafe Control Actions : Context

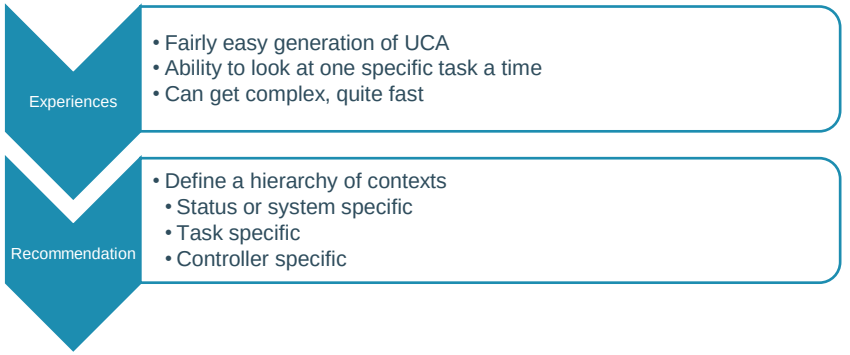
Experiences

- Fairly easy generation of UCA
- Ability to look at one specific task a time
- Can get complex, quite fast

Recommendation

- Define a hierarchy of contexts
  - Status or system specific
  - Task specific
  - Controller specific

Results – Unsafe Control Actions : Context



Status or system specific	
SA.C1	While standing still on standby
SA.C2	While in emergency mode

Task specific - Driving	
D.C1	When taking a sharp corner
D.C1	When driving from point A to point B

Controller specific – Navigation controller	
N.C1	When the global path isn't defined yet

Results – Unsafe Control Actions

Experiences

- Straight forward
- Have identified some previously unknown issues both in hardware and software requirements

Results – Unsafe Control Actions

Experiences

- Straight forward
- Have identified some previously unknown issues both in hardware and software requirements

<Driving controller> <[1]> <speed selection – speed zero > <while driving on a ramp>

- The AMR has no brakes.
  - Standing still / breakdown on a ramp is difficult or impossible.
  - Braking on the motor is possible, but not for steep descents.
  - Braking on the motor is way more intensive for the system.
  - At the moment, the AMR transport small, none-dangerous components. However, this might not always be the case. Brakes are definitely preferred.

Results – Unsafe Control Actions

Experiences

- Straight forward
- Have identified some previously unknown issues both in hardware and software requirements

<Driver controller> <[0]> <speed selection – backward> <when no other way to move, i.e. cornered>

- The AMR has only one LIDAR in front.
  - The distance sensors at the back are currently not (always) used
  - The distance sensors at the back have a smaller range and aren't able to detect objects which are too close (wrong data)

Results – Causal Scenarios

Experiences

- Huge **amount** of scenarios generated
- **Link** between the scenarios and the hazard (traceability) does allow to prioritize as well as “divide and conquer”

Recommendation

- Make **separate lists** (one for each category) for each controller in practice. This allows you to focus on one (smaller) task at hand with the right people present where needed. Similar scenarios can be deleted in a final list when needed.

Summary

Benefits

- We identified some previously unknown faults in the system
- Traceability and ability to prioritize
- Ability to analyse a system in parts and abstract or in detail
- Mapping to SUDA

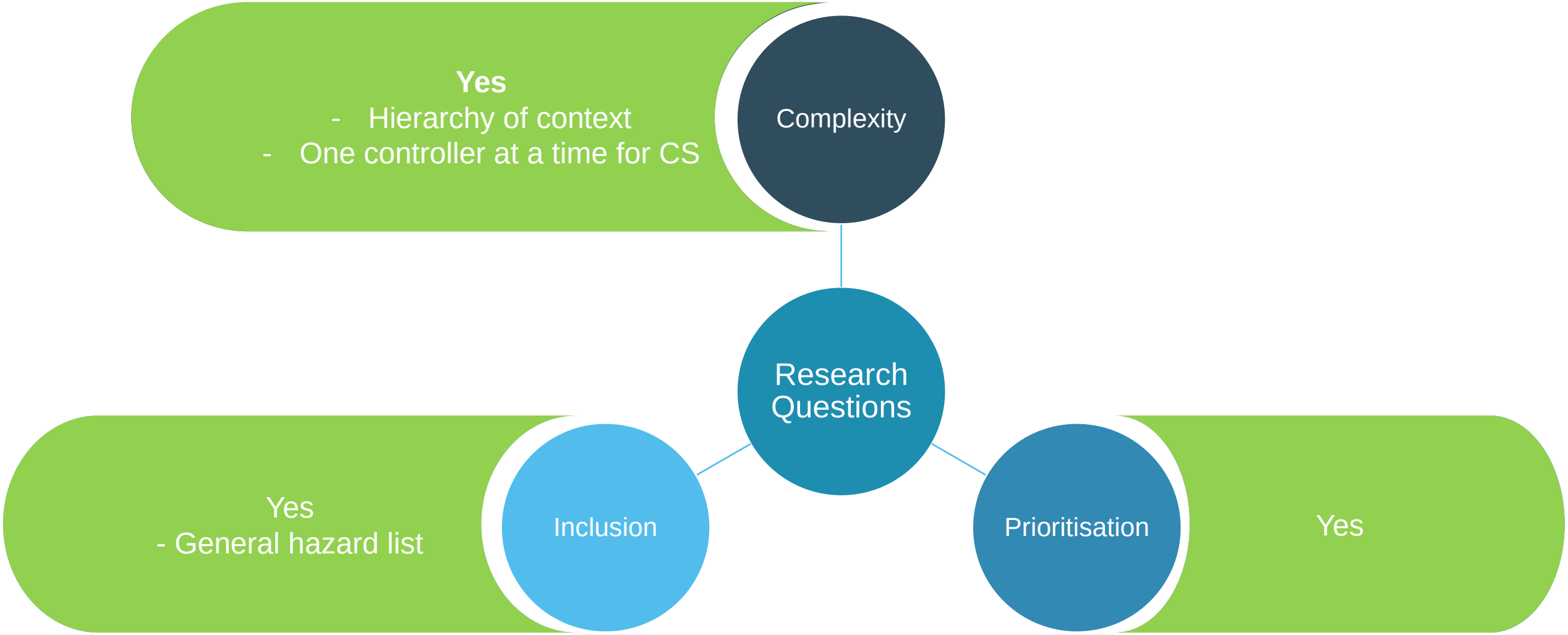
Drawbacks

- Size of the analysis
- Hazard definition
- No inclusion of risk calculations for the industry

Recommendations

- A STPA hazard list
- Hierarchy of context lists
- Causal scenario generation per controller

Research Questions



Thank you for your attention.
Questions?

Many thanks to S. Whiteley (Whiteley Aerospace Safety Engineering & Management Limited) for his help and insightful feedback during the process.