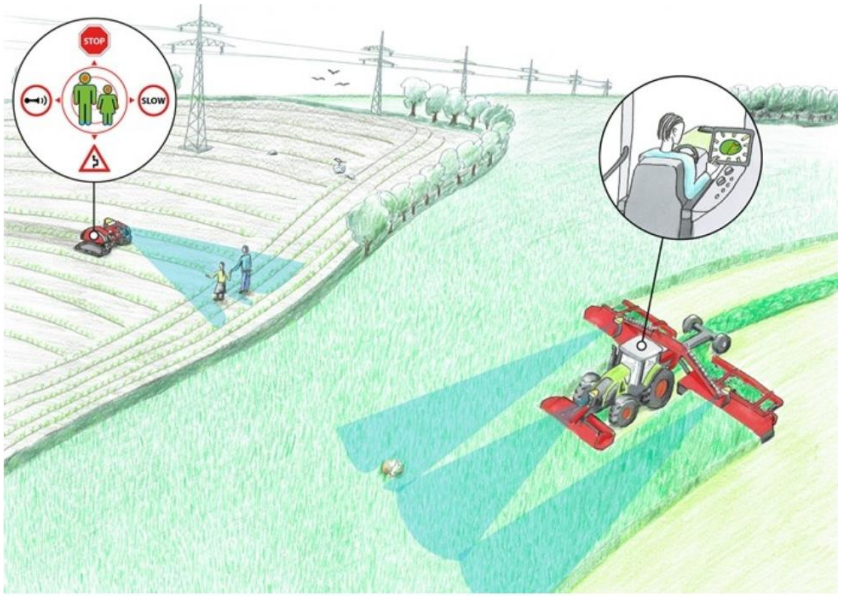
Towards Declarative Safety Rules for Perception Specification Architectures

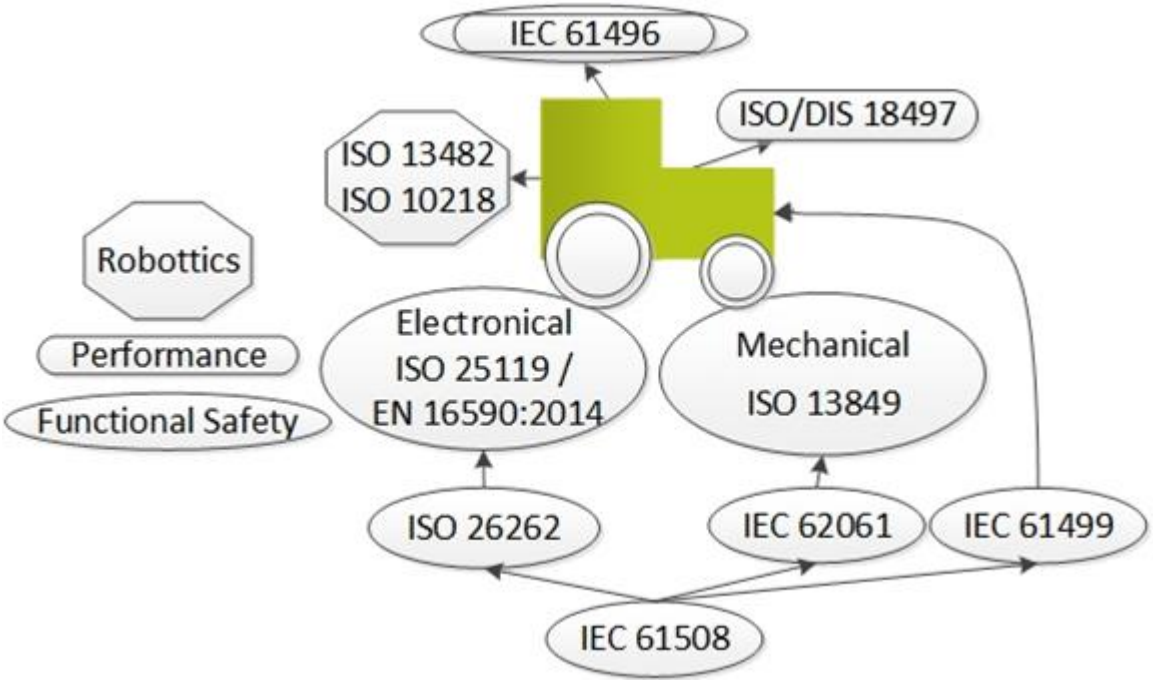
Johann Thor Mogensen Ingibergsson
MMMI, University of Southern Denmark
joint work with Ulrik Pagh Schultz and Dirk Kraft

Field Robots

- Why field robots?
  - Dangerous work.
  - Decreasing workforce.
  - Ecological Concerns.
- SAFE Project.



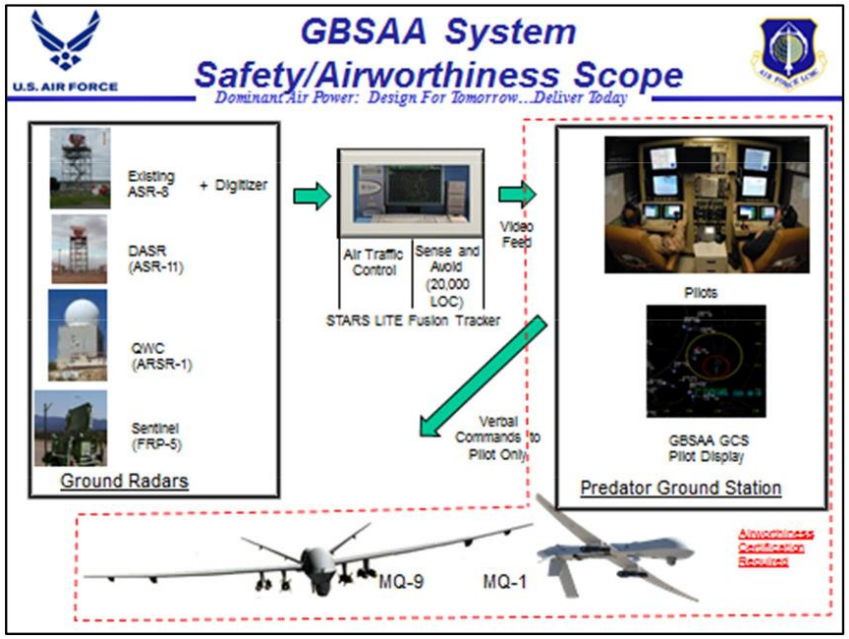
Context:
Safety Certification within Agriculture

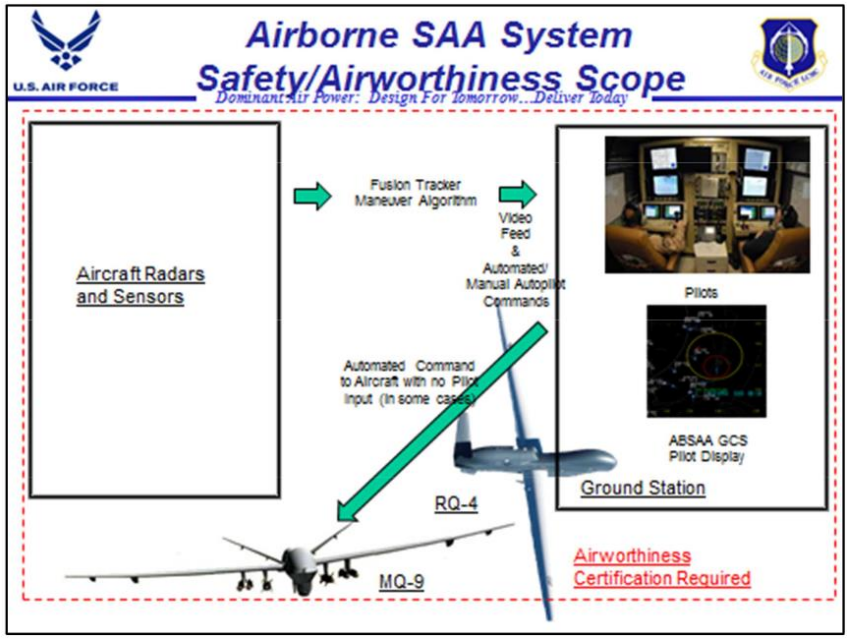


- Why certification? Liability!
  - Robot causes damage due to manufacturing defects.
  - Robot causes damage simply by acting or reacting.

How to Certify Field Robots?

- No standard is available.
- Other Industries? Avionics?
- Interpretation for agriculture and field robots.

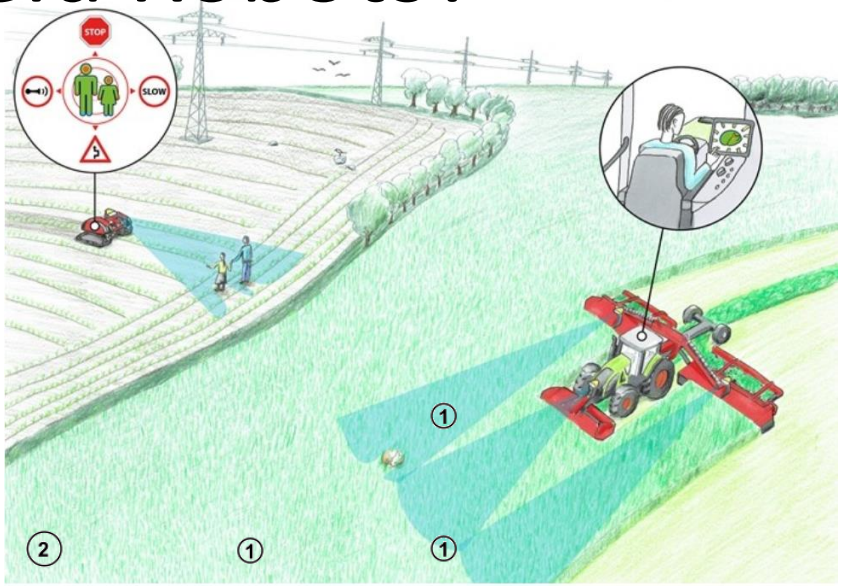


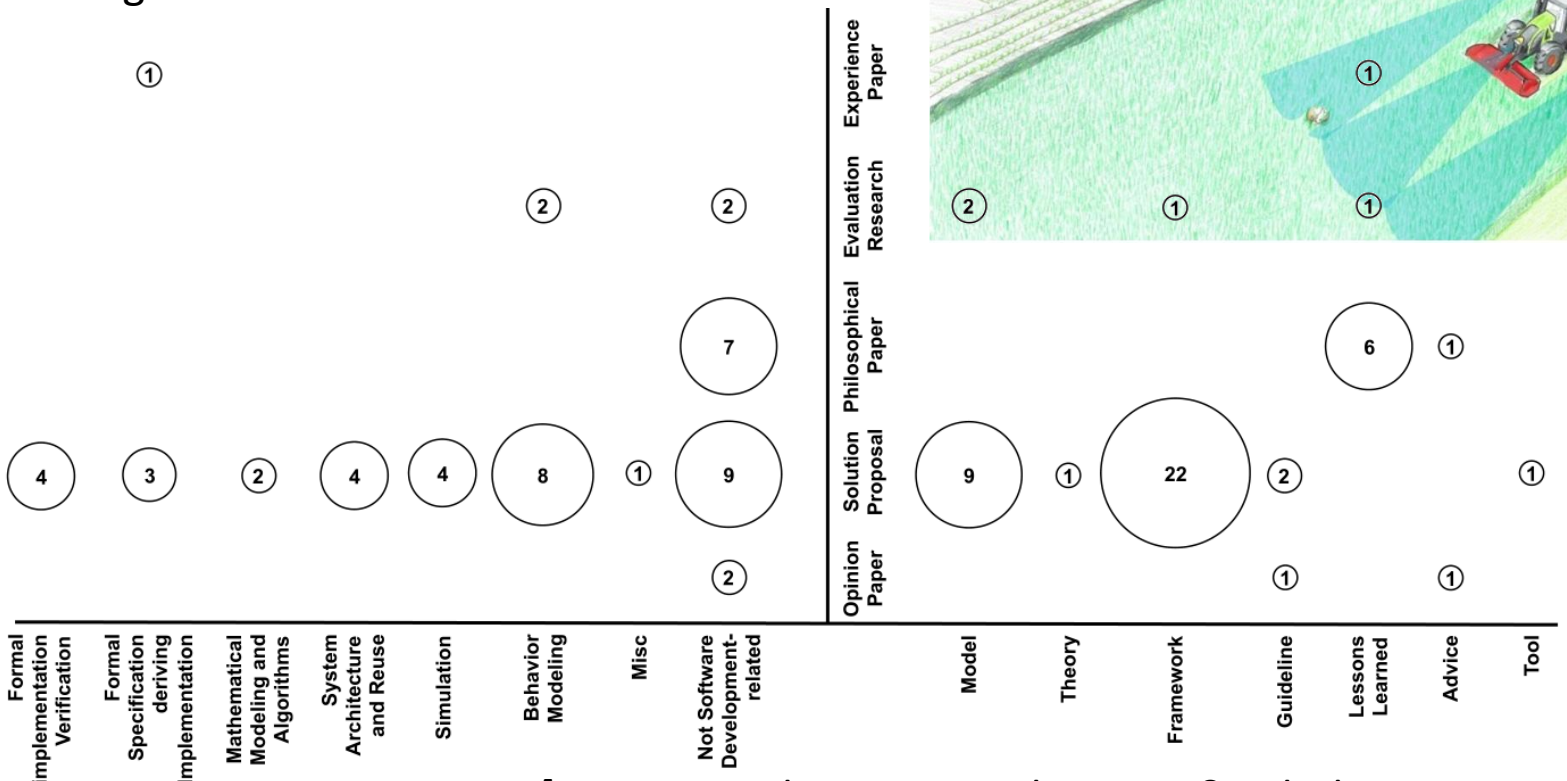


How is Certification Done within Software for Field Robots?

Issues with current standards.

- **Issue:** Research is solution driven.
- **Issue**: 20 papers in non-development-related, suggesting apporaches are investigated.

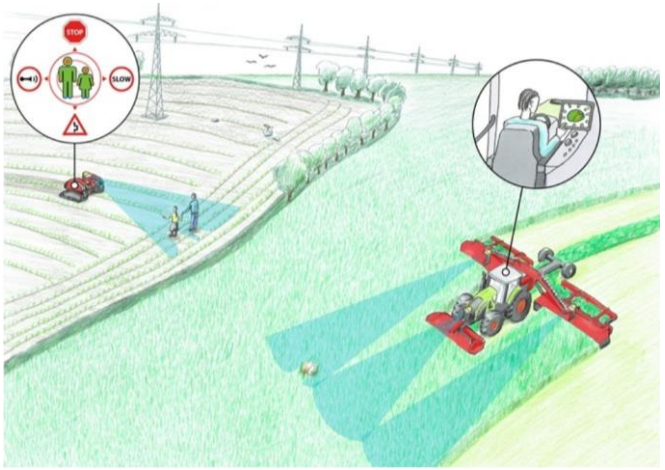




[Source: Ingibergsson, Kuhrmann & Schultz, PROFES2015]

How to Certify Field Robots?

- Issues with current standards.
  - **Issue:** Use of standards is limited.
  - **Issue:** Loose connection between development practices and standards.



Simulation	Formal implementation verification	Mathematical modeling and algorithms	System architecture and reuse	Misc	Behavior modeling	Formal specification deriving implementation	Not SW dev-related	
0	1	1	1	0	0	1	1	IEC 61508
0	0	0	1	0	0	0	2	ISO 13482
0	0	0	0	1	0	0	0	ISO 26262
0	0	0	0	0	0	0	0	ISO 10218
0	0	0	0	0	0	1	0	IEC 61499
0	3	2	0	0	1	0	2	Guranteeing safety - Not necessarily using a Standard approach
4	1	0	2	1	9	2	15	Non-Standard Approach
0	0	0	0	0	0	1	0	No standards available

Certifying Field Robots

Based on Interpretation

- **ISO 13482**

  Risk assessment

- **ISO 13849**

  Functional safety Mechanics.

- **ISO/DIS 18497**

  Performance

- **ISO 25119**

  Functional safety electronics.

- **IEC 61496**

  Electro-Sensitive Protective Equipment (EPSE).

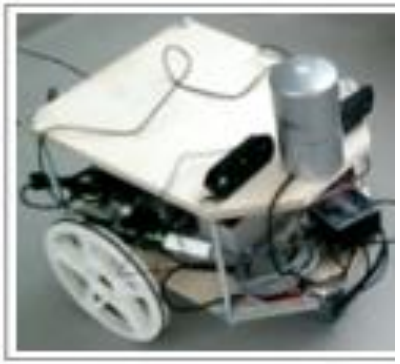
Safety functions of robots	PL
Emergency Stop	d
Protective Stop	e
Limits to workspace (incl. forbidden area avoidance)	e
safety-related speed control	e
Hazardous collision avoidance	e
Stability Control (incl. overload protection)	d

PL Definition : Average probability of dangerous failure per hour 1/h	PL
$\geq 10^{-5}$ *to* $< 10^{-4}$	a
$\geq 3 \times 10^{-6}$ *to* $< 10^{-5}$	b
$\geq 10^{-6}$ *to* $< 3 \times 10^{-6}$	c
$\geq 10^{-7}$ *to* $< 10^{-6}$	d
$\geq 10^{-8}$ *to* $< 10^{-7}$	e

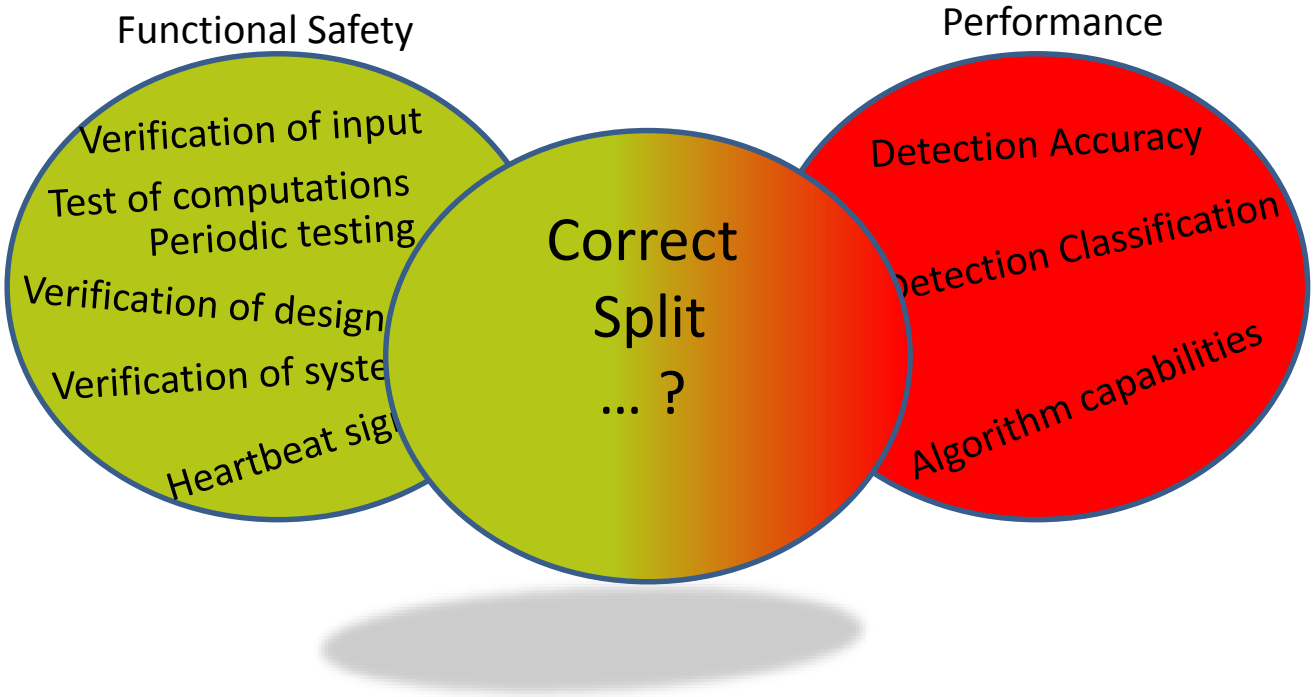
AgPL	B-3 : SRL				
a	1	B	B	B	B
b	2	1	B	B	B
c		2	1	1	1
d			2	2	2
e					3
	Cat B DC low	Cat 1 DC med	Cat 2 DC med	Cat 3 DC med	Cat 4 DC high

Key
Low $MTTF_{dc}$
Medium $MTTF_{dc}$
High $MTTF_{dc}$

Implications of Standards on Development of Field Robots in Practice?



Functional Safety vs Performance



ISO 26262-1:2011

Road vehicles -- Functional safety -- Part 1: Vocabulary

Abstract

Preview ISO 26262-1:2011

...
...
...

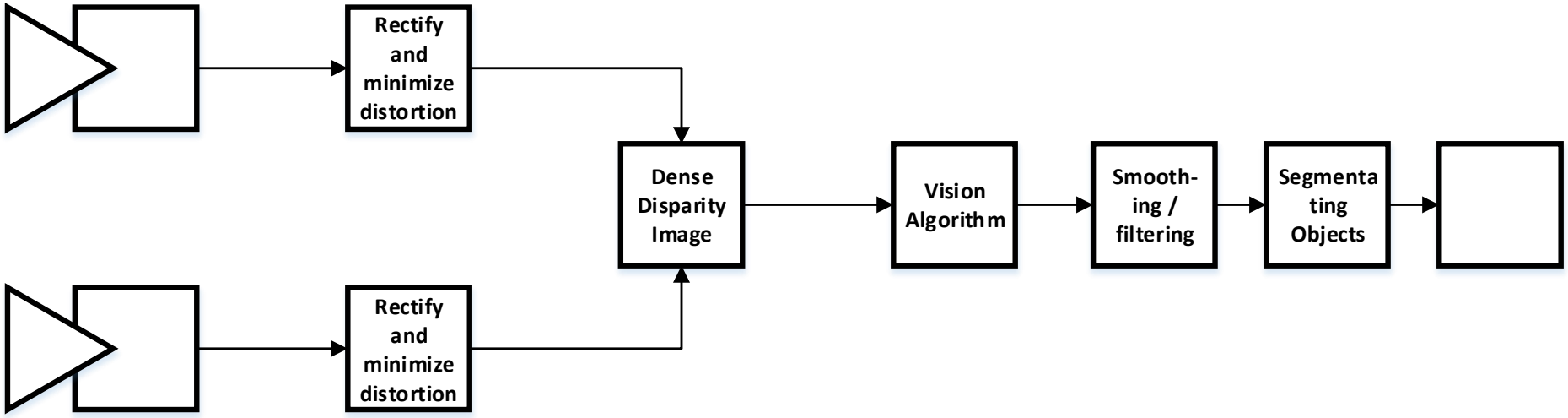
ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

ISO 25119-4:2010(en) Tractors and machinery for agriculture and forestry

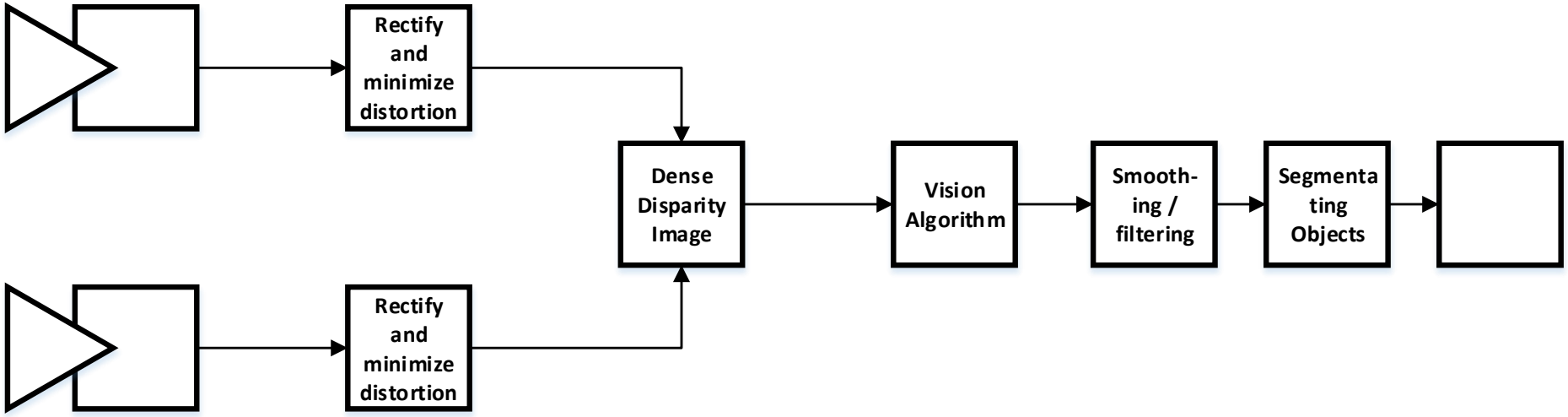
Introduction

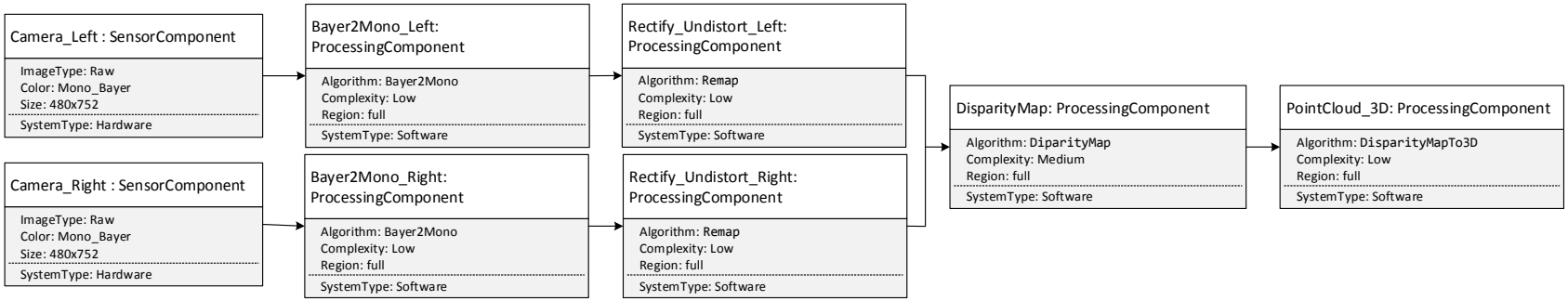
ISO 25119 sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant systems comprising electrical and/or electronic and/or programmable electronic components (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to municipal equipment. It covers the possible hazards caused by the functional behaviour of E/E/PES safety-related systems, as distinct from hazards arising from the E/E/PES equipment itself (electric shock, fire, nominal performance level of E/E/PES dedicated to active and passive safety, etc.).

Example: Simple Vision Pipeline



Vision Pipeline Described with RPSL





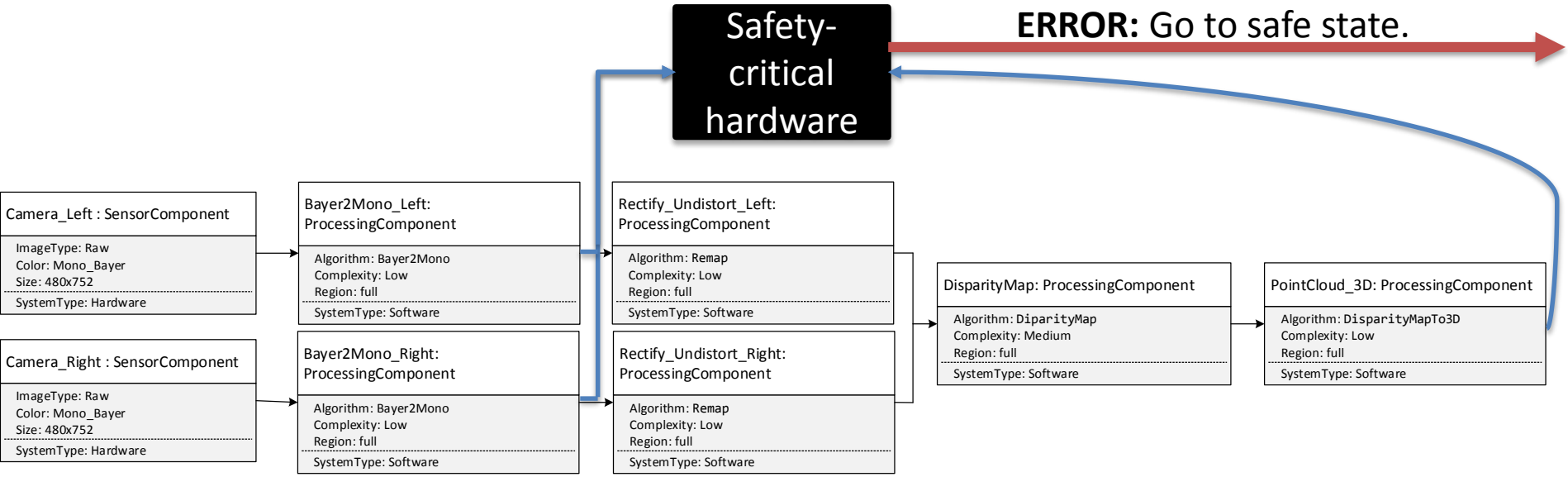
[Source: Hochgeschwender, Schneider, Voos & Kraetzschmar, SIMPAR2014]

How to Introduce Functional Safety

Based on Interpretation

- **ISO 25119** – Functional safety electronics.
  - Develop software and hardware according to the standard.
  - Software could be subjected to Misra, to create a foundation across standards.

- **IEC 61496** – Electro-Sensitive Protective Equipmen (EPSE).
  - **Fault:** Shall force the system to a safe-state, i.e. full stop.
  - **Multiple Faults:** Shall not influence the above reaction.
  - **Periodic tests:** Ascertain functionality.



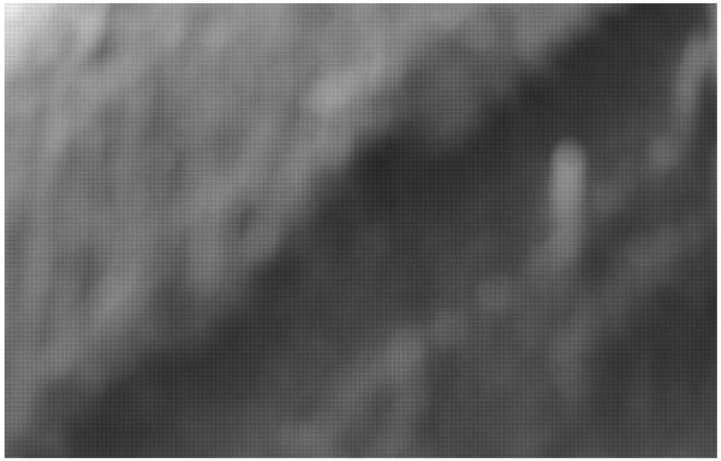
DSL Proposal

```
h=Bayer2Mono_Left.output.histogram;

length(nonempty(h.bins))/length(h.bins)>0.1;
max(h)-min(h)>1000p;


length(PointCloud_3D.output.inArea
   (Camera_Left_Landmark))>900 3D points;
```

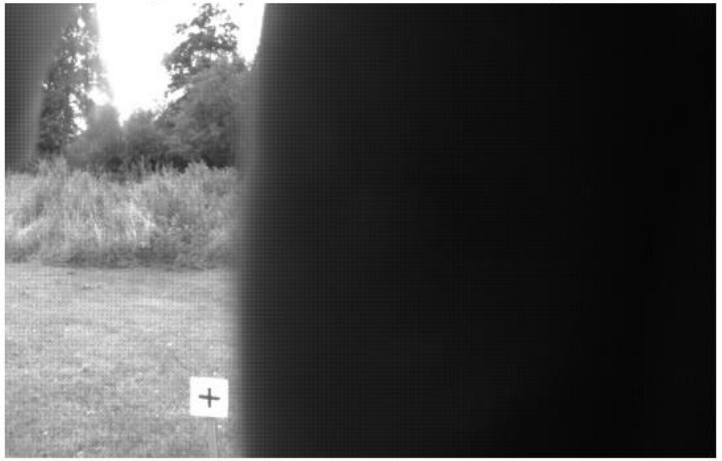
DSL Test images



(a) Left lens, covered.

(b) right lens, overexposed.

(c) Left lens, partial cover



(d) right lens, partial cover

Conclusion

Contributions

- Analysis of safety standards in the agricultural domain.
- Language concept for extending RPSL with safety annotations.

Future work

- Code generation for safety-critical hardware.
- Systematic evaluation of language design for the safety domain.
- Evaluation by safety experts.