Superposition and adaption of safety functions considering collaborating Systems

by Michael Kieviet
michael.kieviet@innotecsafety.com
innotec GmbH

Since 2011 the German automation industry talks about a new industrial era with the name “Industrie 4.0”.The “Industrie 4.0” shall be the fourth industrial revolution after mechanization, electricity and automation. It focuses the white range of the entire product lifecycle including a strong integration of smart system technology. In this context typical concepts of Cyber-Physical Systems (CPS) or the “Internet of the things” are placed in the same manner like sociological aspects for the collaboration between the human being and the machineries. The glue between these disciplines is the information exchange and the possibilities to access anytime and anywhere to all necessary data. The initial characteristics of Cyber-Physical System enclosures the data acquisition of physical processes by sensors, storing and managing of this data in virtual shared memory (cloud) and providing this data with the possibility of the world wide access. The new approach will be now the flexible adaption, situationally conditioned, of the provided data to the production processes.[1]

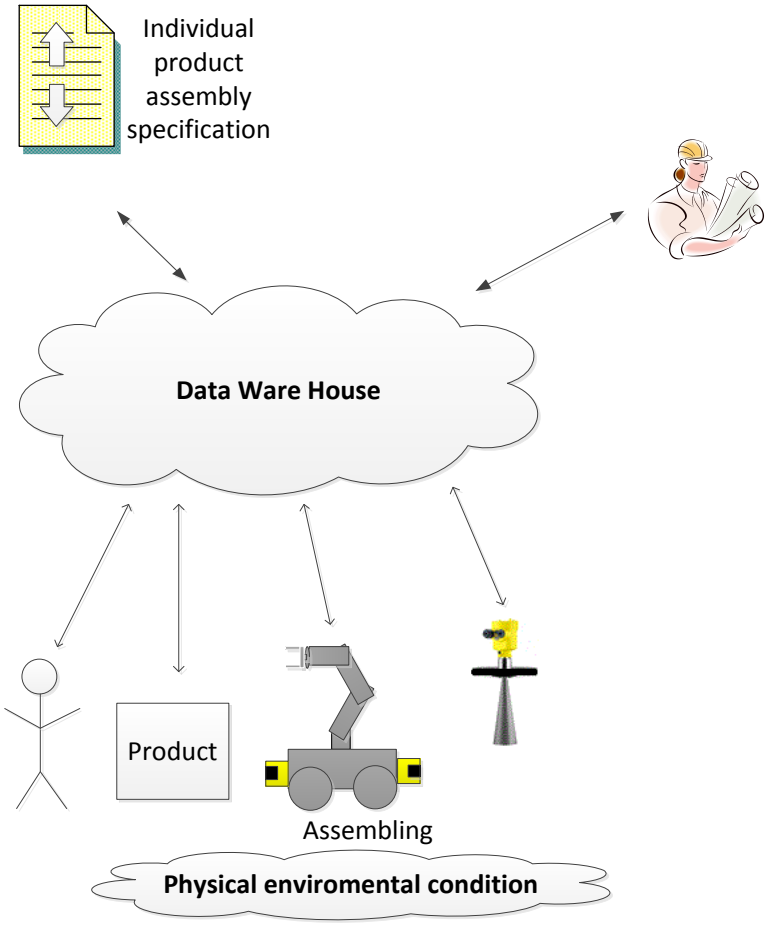


Figure 1 Concept of Cyber Physical System in a smart factory

[1] Bundesministerium für Bildung und Forschung, *Zukunftsbild „Industrie 4.0“*

Challenges for the Functional Safety

Due to the fact, that accesses from anywhere to safety functions brings a lot of new risks under IT-security aspects, also the aspects of flexibility adaption and collaboration will bring a new handling of risks. The adaption to a flexible collaboration between human beings and adaptive or mobile machines can hide a lot of unknown risks, which are not able to predict.

Nowadays, the risk analysis has a typical static view of the system and harms will be viewed just by the system itself. Of course it is required to analyze the entire life cycle for the risk analysis, but the process circumstance for each phase, are very constant.

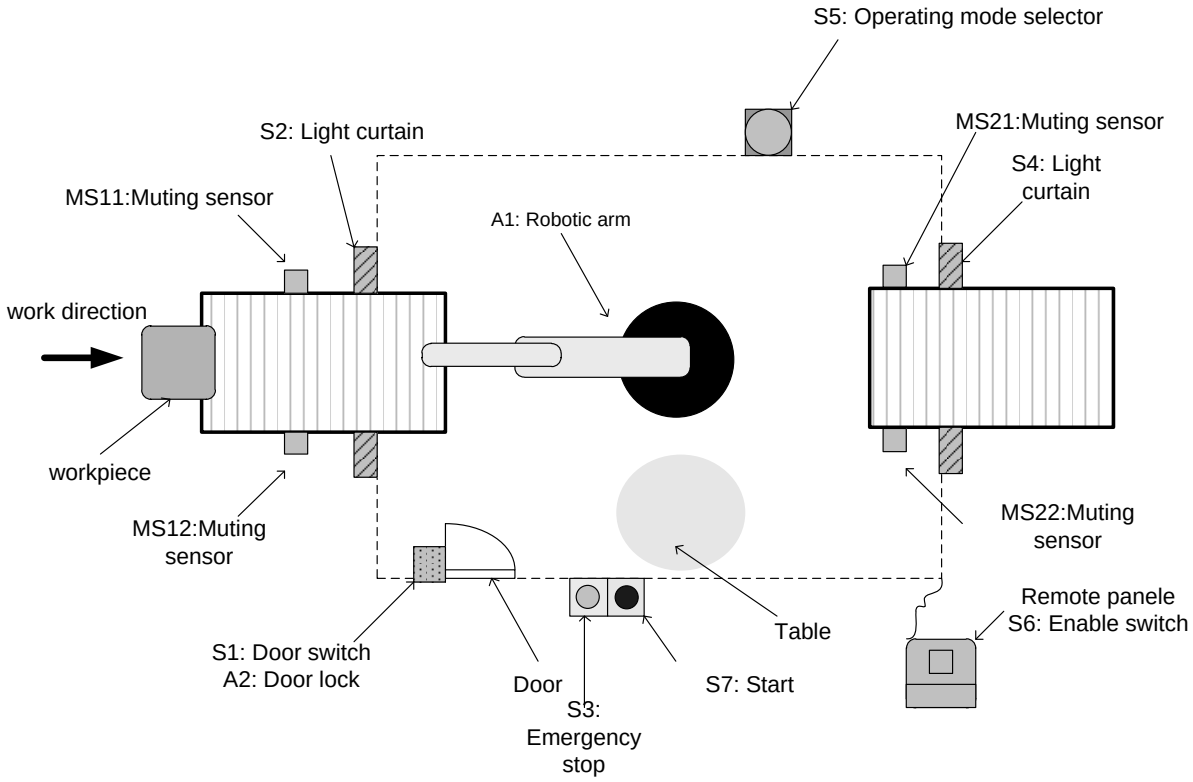


Figure 2 Typical work cell

The typical condition (Figure 2) has a lot of different safety functions in a fixed environmental. In the exampled case each safety function will be handled separated (Figure 3).

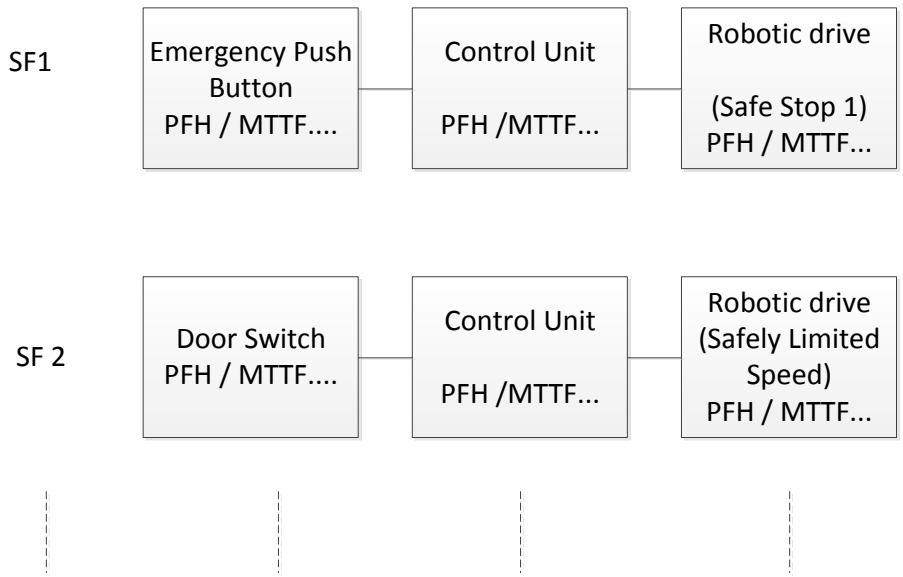


Figure 3 Separated safety functions

The variability will come usually from the variety of the products. Such cell is able to produce different kinds of modified products. The product information comes from the electronic product specification, normally identified with an RFID-Tag directly from the carrier. The robotic cell is able to load the assembly specification from the Data Ware House and start the assembling. It is also possible in this example to call for the safety parameter form the Data Ware House and adapt the safety functions according the related assembling specification. For example, according to the material dimension the parameter set of the light curtain will be modified or the speed limitation of the robotic arm must be adapted.

From the safety point of view this functionality is added with some technical risks which have not been present before. For instance:

- RFID –Tag will authorize the wrong assembling specification and also to the wrong safety parameter set.
- The access to the data ware house is enabled and the current safety parameter set isn't the right one for the product.
- The safety parameter set can be manipulated in the data ware house (conscious or unconscious).

But this cases do not change the safety functions just the parameter set of the safety functions will be changed.

Superposition in collaborated systems

The next example will upgrade the sophistication of the safety functions with combined and overlapped safety functions.

It starts with single mobile robotic (Agent).

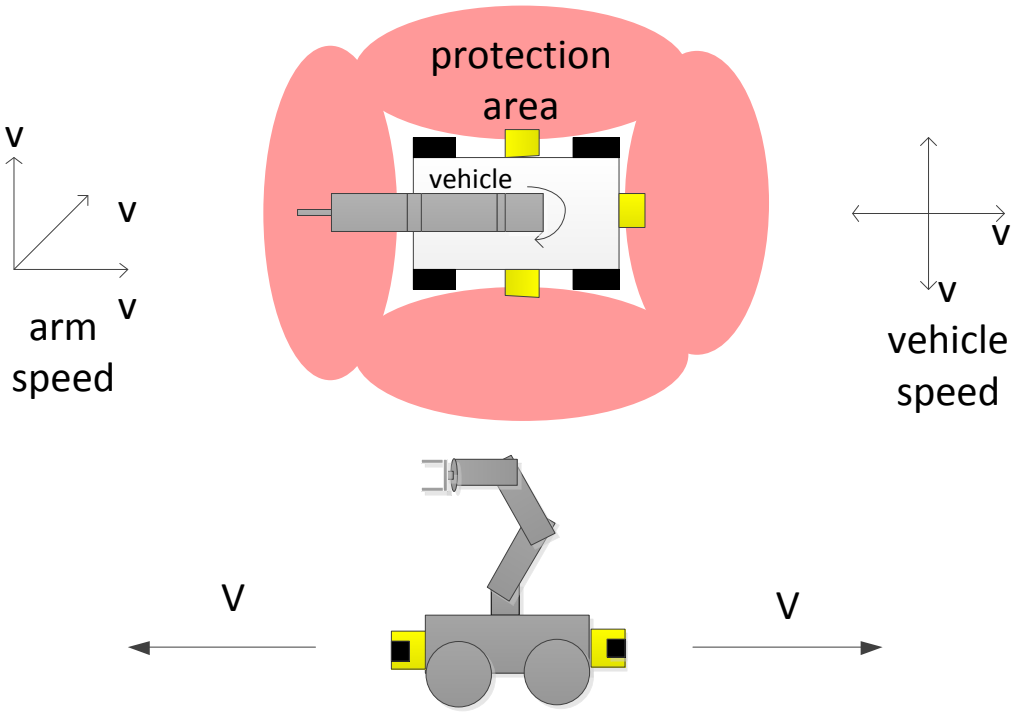


Figure 4 Mobile robotic (Agent)

The single agent has eight safety functions in this example. Each side is protected by a scanner system and will initiate the safely limited speed for the vehicle if an obstacle or a human being will be in the first protection area. If the obstacle will come in the second level area, the vehicle drives will change to safe operating stop (SOS).

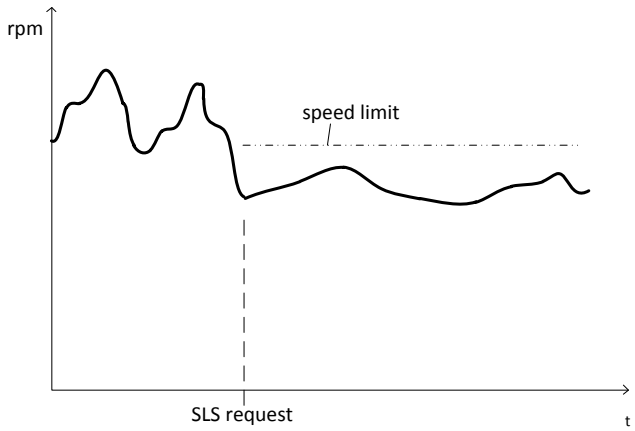


Figure 5: Safely limited speed

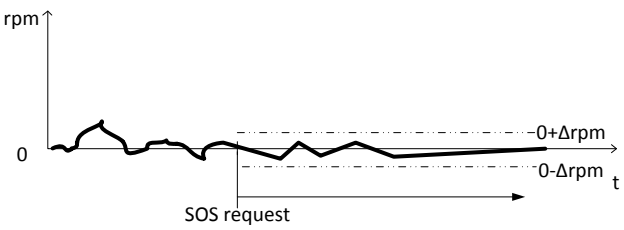
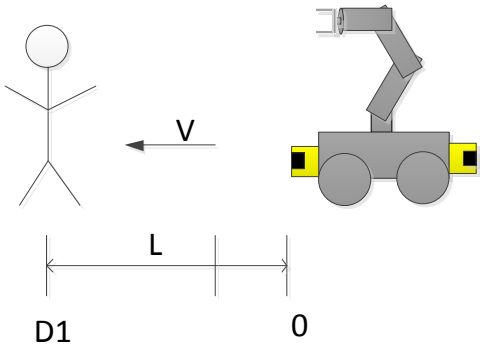


Figure 6: Safe operating stop

From the view of risk analysis of a single agent, the safety function seems very simple.



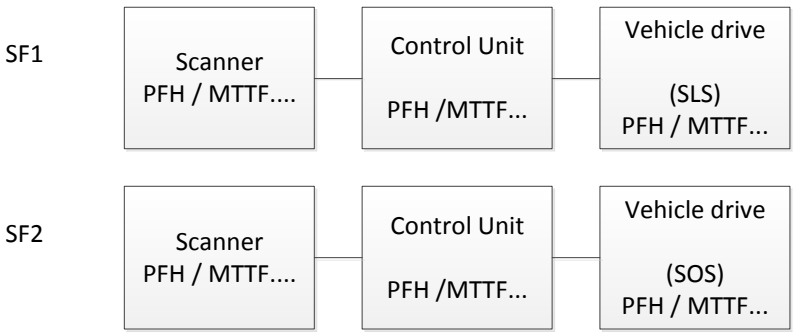
IF L <D1 then REDUCE $|\vec{v}|$

{

IF L< D2 then SET $|\vec{v}|$:=0

}

Figure 7: Single Agent view



SF1 ᵛ SF 2

Figure 8 Two independent Safety Functions

If more than one agent will collaborate with the human being the risk view must be changed. It was possible for the person to escape if the agent activated the SLS, in the first example.

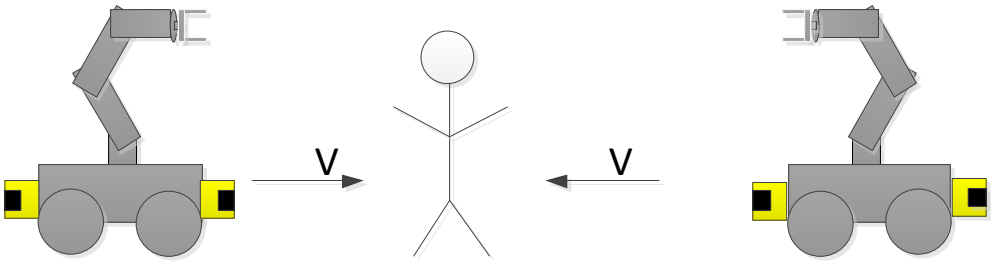


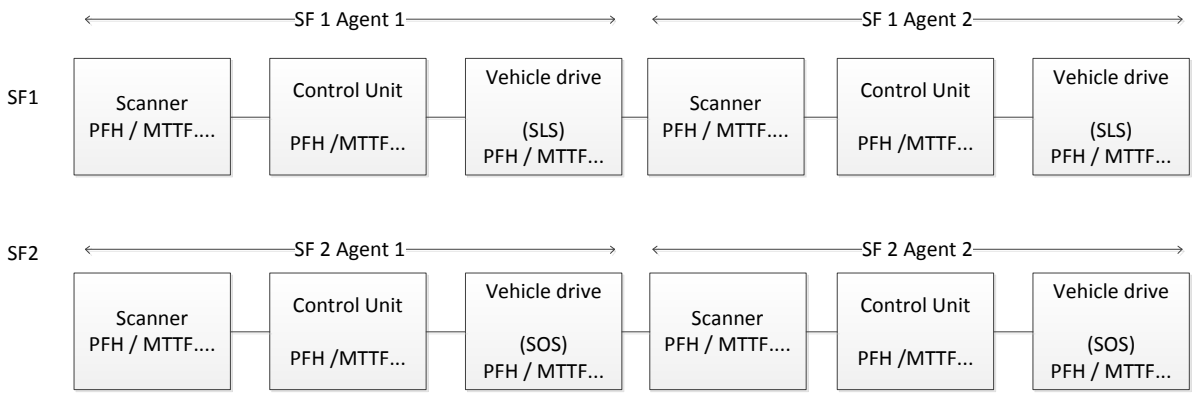
Figure 9: More than one Mobile System

Now it could happen that the person isn't able to escape. The space between the person and the agents will be reduced in the half of time, if we assume that the person is just able to move on the

same line as the movements of the agents. The energy which is affected to the human body is higher, because the body has to absorb the energy from both agents.

This deduced means different things:

- Each agent must have an environmental model. This means the knowledge about all other agents, about obstacles, about the own tools, work pieces and about the tools and work pieces of the collaboration partners.
- Each agent has to adapt the safety function in relation to the environmental model. This means it has to change the speed limits.
- The failure rates (PFH, $MTTF_d$) of the protection system will increase depending from the sum of collaborated agents.



Combinations of safety functions

SF1 A2 ^ SF2 A2
ᵛSF2 A2 ^ SF2A1
ᵛSF1 A1 ^ SF2A2
ᵛSF1 A1 ^ SF2A1

Figure 10 Possible combinations of safety functions with cluster of two agents and two basic safety functions

Conclusion

In cases where agents work in collaborated cluster it will be necessary that each agent has the total overviews of environmental reality. The flexibility and the dynamic of such networks require that safety critical values are available. The need is a compatible metadata model to exchange the data's between the agents. It is necessary to specify rules if different kinds of safety functions will be overlapped. The entry in and the leaving out of an agent from a collaborative cluster must be managed and all members of the collaborative network must be informed about. A cluster will be formed around a critical area (e.g. human beings).

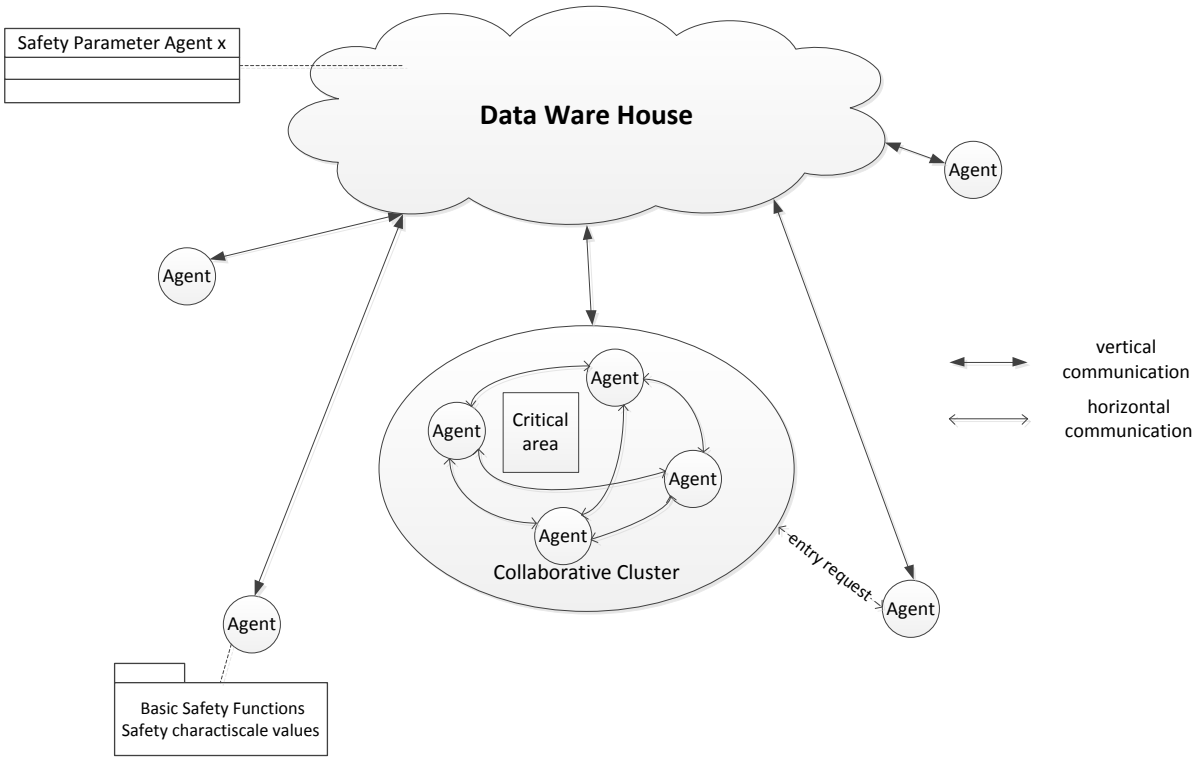


Figure 11 Model of agent based collaborative network

References

[1] Bundesministerium für Bildung und Forschung, *Zukunftsbild „Industrie 4.0", 2014*

[2] IEC 61800-5-2, Adjustable speed electrical power drive systems- Part 5-2, 2007

[3] Ladkin, Sieker, New Formal Methods for Human Machine Cooperative Tasks, 2009

[4] Wratil, Kieviet, Röhrs, Sicherheit für Maschinen und Anlagen, VDE-Verlag, 2010