Critique of the White Paper

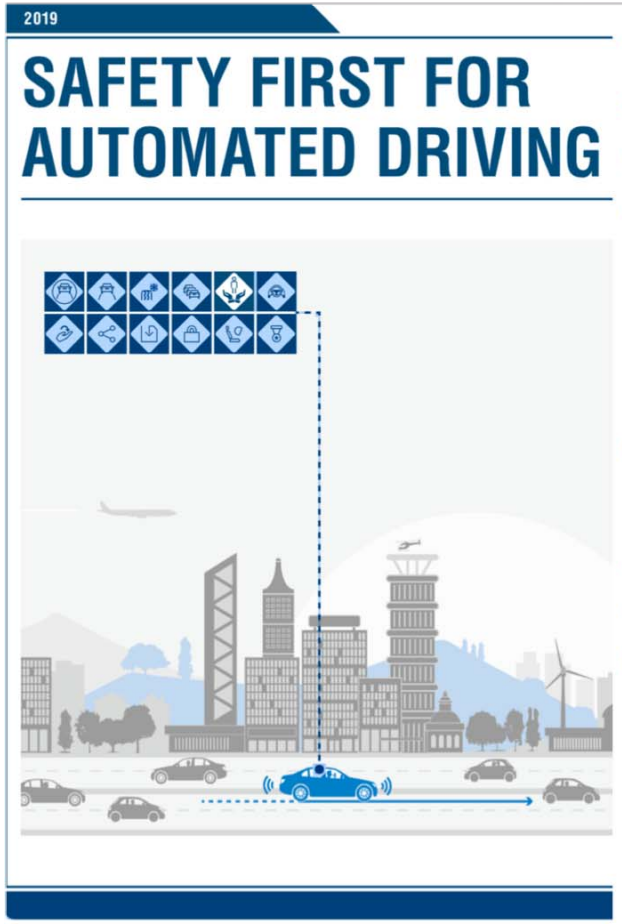
SAFETY FIRST FOR AUTOMATED DRIVING

H. Kopetz

Jan 2020

The *White Paper, July 2, 2019*

https://www.daimler.com/innovation/case/autonomous/safety-first-for-automated-driving-2.html



2019

SAFETY FIRST FOR AUTOMATED DRIVING

AUTHORS

APTIV
Matthew Wood, M.Sc.
matthew.wood@aptiv.com
Dr. Philipp Robbel
philipp.robbel@aptiv.com
Dr. Michael Maass
Dr. Radboud Duintjer Tebbens
Marc Meijs, M.Sc.
Mohamed Harb, M.Sc.
Jonathon Reach, B.Sc.
Karl Robinson

David Wittmann, M.Sc.
david.wittmann@audi.de
Toshika Srivastava, M.Sc.
Dr.-Ing. Mohamed Essayed Bouzouraa

apollo
Siyuan Liu, BS, MBA
liusiyuan01@baidu.com
Yali Wang, MA
wangyali05@baidu.com

Dr.-Ing. Christian Knobel
christian.knobel@bmw.de
Dipl.-Inf. David Boymanns
david.boymanns@bmw.de
Dr.-Ing. Matthias Löhning
Dr. Bernhard Dehlink
Dirk Kaule, M.Sc.
Dipl.-Ing. Richard Krüger
Dr. Jelena Frtunikj
Dr. Florian Raisch
Dipl.-Math. Miriam Gruber
Jessica Steck, M.Sc.
Dipl.-Psych. Julia Mejia-Hernandez

Continental
Dipl.-Ing. Sandro Syguda
sandro.syguda@continental-corporation.com
Dipl.-Ing. Pierre Blüher
Dr.-Ing. Kamil Klonecki
Dr. Pierre Schnarz

DAIMLER
Dr. Thomas Wiltschko
thomas.t.wiltschko@daimler.com
Dipl.-Inf. Stefan Pukallus
Dr.-Ing. Kai Sedlaczek

FCA
Neil Garbacik, M.Sc.
neil.garbacik@fcagroup.com
David Smerza, BSAE
Dr. Dalong Li
Dr. Adam Timmons
Marco Bellotti

here
Michael O'Brien, BS
michael.obrien@here.com
Michael Schöllhorn

Infineon
Dipl.-Ing. Udo Dannebaum
udo.dannebaum@infineon.com

intel
Jack Weast, BS, M.Sc.
jack.weast@intel.com
Alan Tatourian, BS

Volkswagen
Dr.-Ing. Bernd Dornieden
bernd.dornieden@volkswagen.de
Dr.-Ing. Philipp Schnetter
Dr.-Ing. Dipl.-Wirt.Ing. Philipp Themann
Dr.-Ing. Thomas Weidner
Dr. rer. nat. Peter Schlicht

*This publication summarizes widely known safety by design and verification and validation (V&V) methods of **SAE L3 and L4 automated driving**. This summary is required for maximizing the evidence of a positive risk balance of automated driving solutions compared to the average human driving performance.*
(from the abstract).

SAE *Autonomous Driving Levels* Taxonomy

ABS, ESP
Speed Control

Adaptive Speed
and Lane Control

“Eyes off”

“Hands off”






Focus of the *White Paper*

0	1	2	3	4	5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Some important Principles in the White Paper

SAFE OPERATION

DEALING WITH DEGRADATION

If safety-related functions or system components become hazardous (e.g. unavailable), the automated driving system shall:

- Be capable of compensating and transferring the system to a safe condition/state (with acceptable risk).
- Ensure a sufficient time frame for the safe transition of control to the vehicle operator.

FAIL-OPERATIONAL (limited to the safety-related function or component)

The loss of safety-related functions or system components shall not lead to a safety-related situation.

OPERATIONAL DESIGN DOMAIN

ODD DETERMINATION

As soon as system limits that restrict the safe functionality of the automated system are recognized, the system shall react to compensate or shall issue a driver takeover request with a sufficient time frame for the takeover.

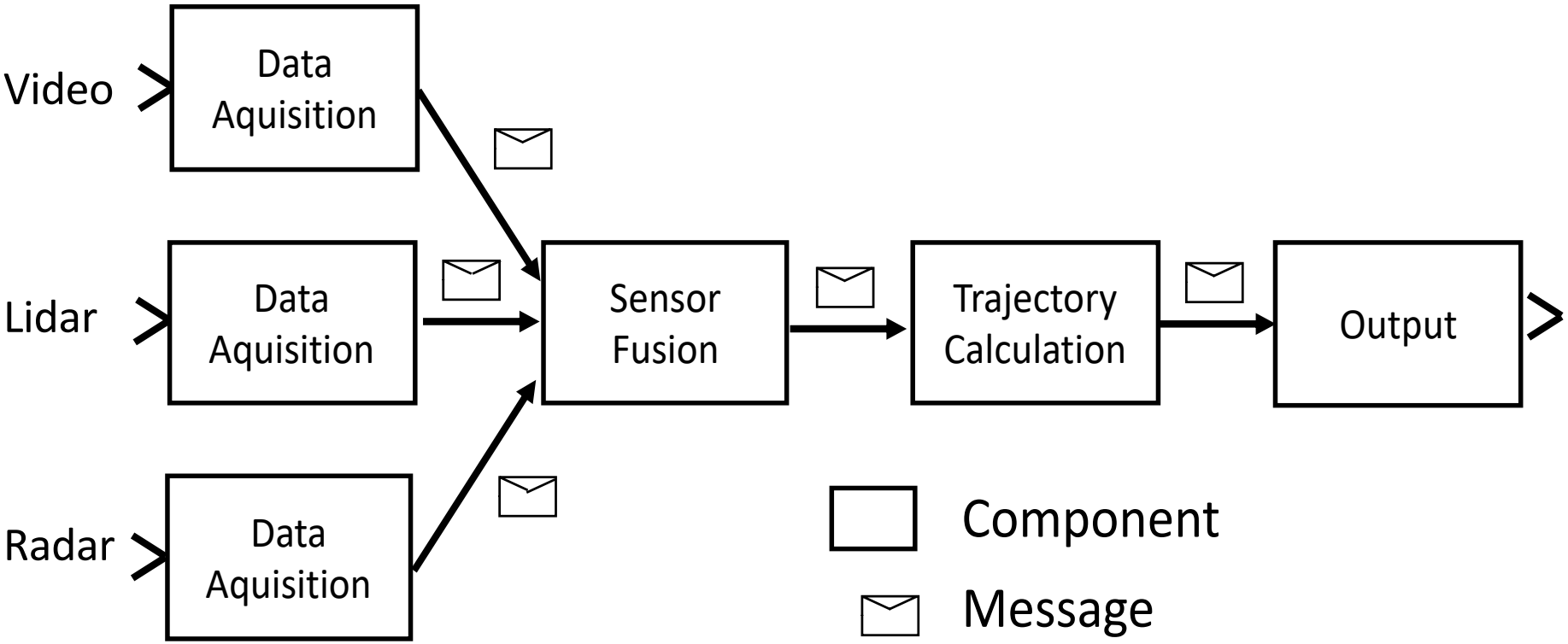
MANAGE TYPICAL SITUATIONS

The automated driving system shall take into account situations that can typically be expected in the ODD and address possible risks.

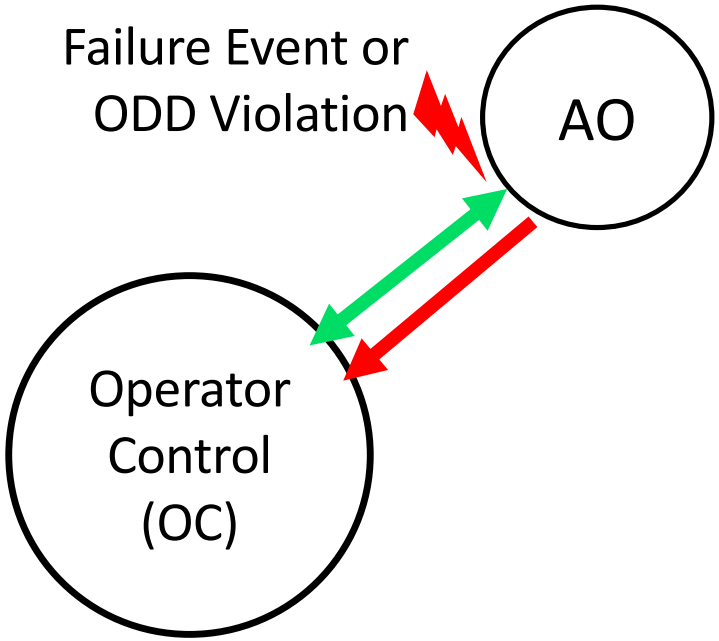
SECURITY

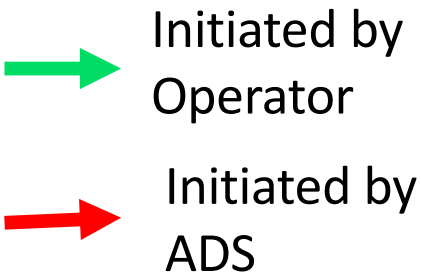
When providing an automated driving system, steps shall be taken to protect the automated driving system from security threats.

Current ADS Architecture for Level 2



State Transitions in Level 2 Autonomous Control



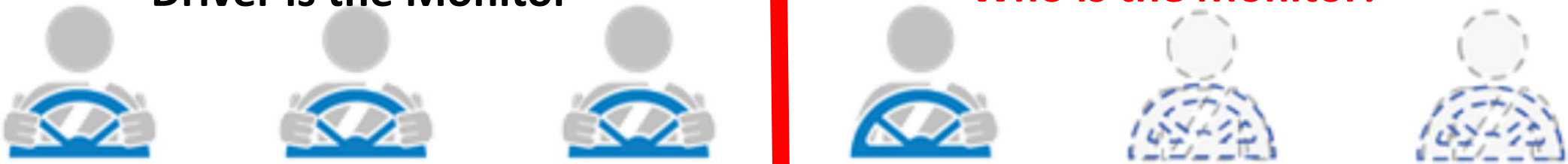


OC Operator Control
AO Autonomous Operation

SAE Autonomous Driving Levels—*the Role of a Monitor*

Supervised Autonomous Driving
Driver is the Monitor

Unsupervised Autonomous Driving
Who is the Monitor?



Focus of the *White Paper*

0	1	2	3	4	5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Comparison *Supervised* vs. *Unsupervised* Mode of ADS

In the supervised mode, **an independent system** with its own biological sensors and a mental model—**the human operator— functions as the monitor** that provides the following services:

- Detect ODD violations
- Monitor the ADS function and detect ADS failures.
- Initiate an immediate transition (less than 1 second) from the supervised mode to the driver mode of operation in case of an ODD violation or ADS malfunction.
- Minimal Risk Maneuver (MRM) to a safe state by the human driver.

In the supervised mode, a critical incident can only happen if a joint failure of both systems, the *ADS* and the *human driver*, occurs.

The Grand Challenge of Unsupervised Automation

In the *unsupervised* mode of an ADS, independent subsystems must implement the services that are provided by the human driver in the supervised mode.

Reliability:

- **Human Driver MTTF is about 10^6 to 10^7 hours**
- **Complex ADS Component MTTF at best 10^5 hours**

A single *flow of control in complex software* cannot achieve human reliability

Critique of the *White Paper (WP)*

The MTTF of a ***complex Software/Hardware Component*** can be assumed to be **at best 10^5** hours of operation due to the following faults

- transient faults in the hardware (e.g. SEU)
- undetected design faults in complex software

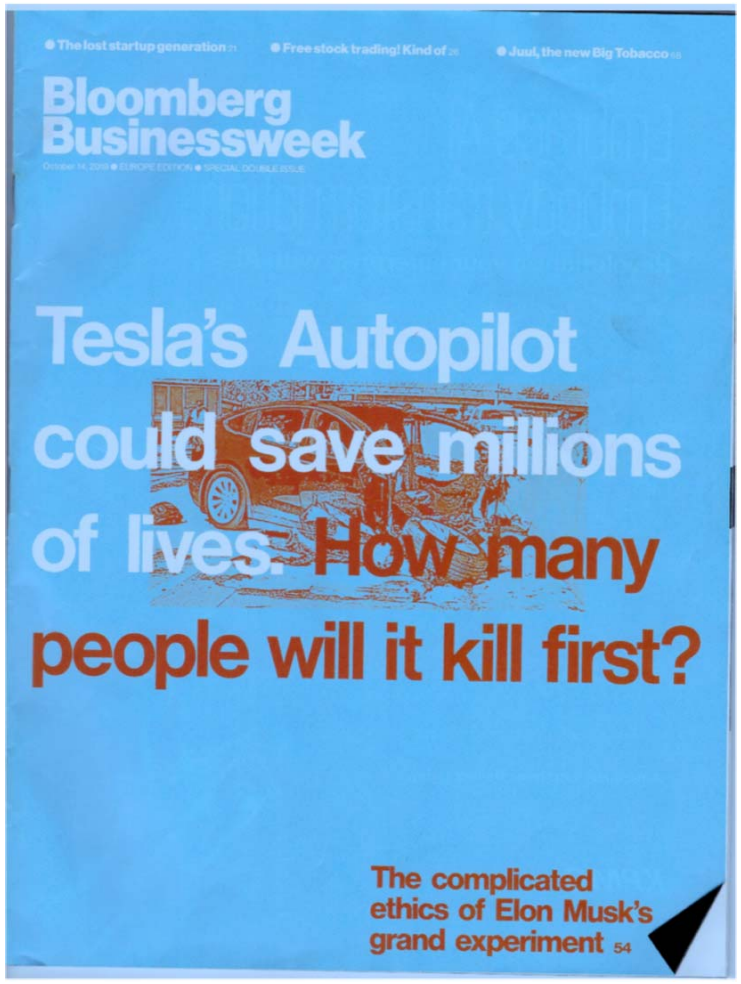
The required level of safety (MTBF of better than 10^8 hours w.r.t. fatal accidents) can only be achieved by the provision of redundant Fault-Containment Units (FCU) in a *well-defined safety architecture*.

Safety assessment of an *unsupervised ADS* requires a combination of structural analysis of this safety architecture and experimental evidence.

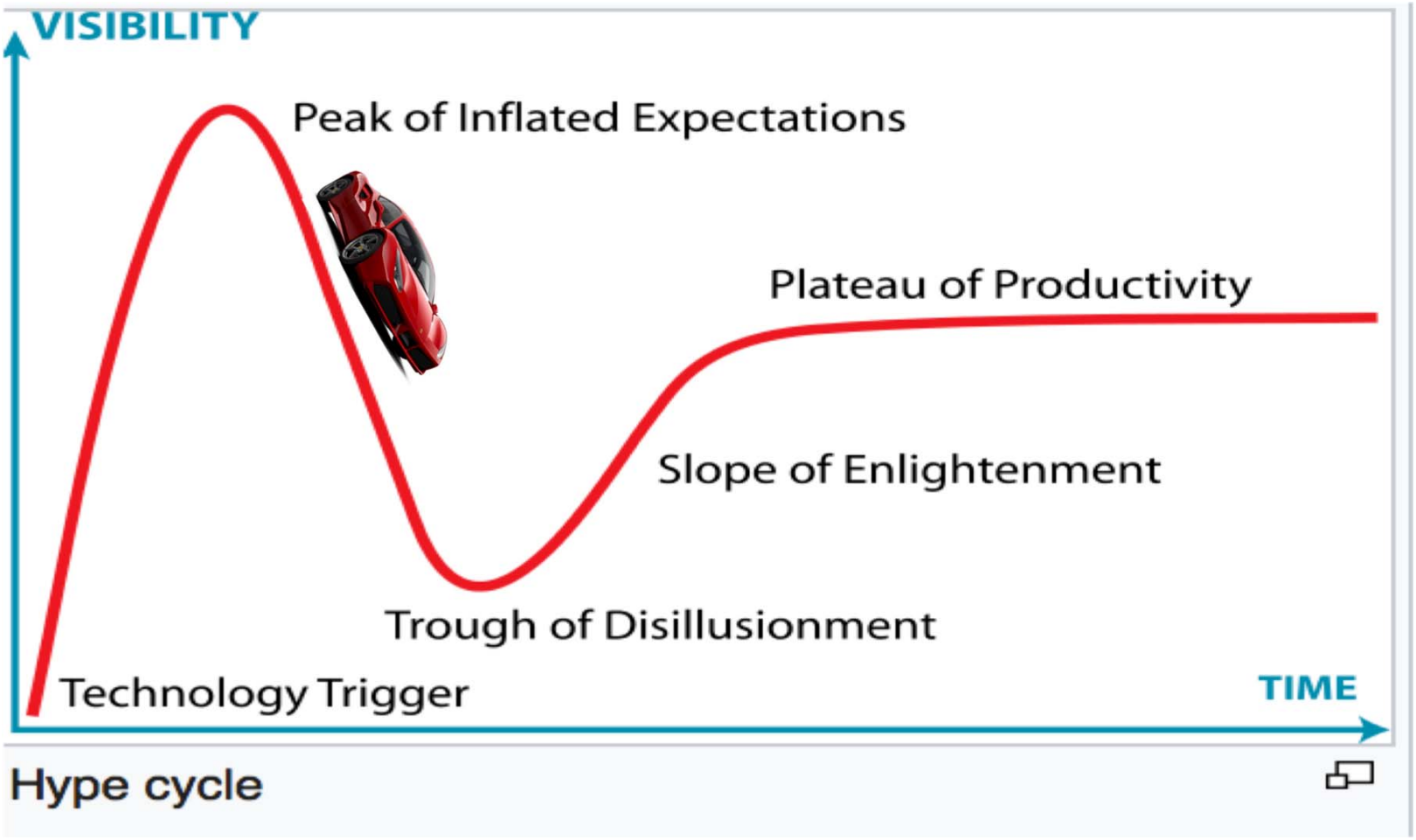
The White Paper (WP) does not seem to be aware that SAE levels 3 is fundamentally different from SAE level 2.

A *well-defined safety architecture*, based on FCUs, was not found in the WP!

Business Week, October 14, 2019

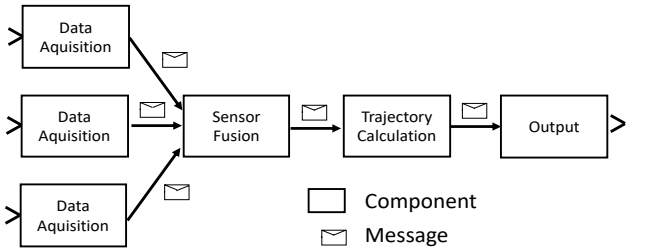


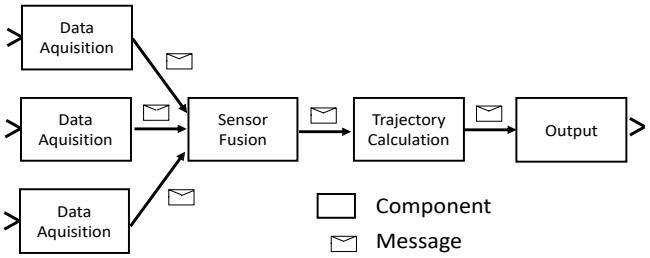
Hype Cycle of ADS

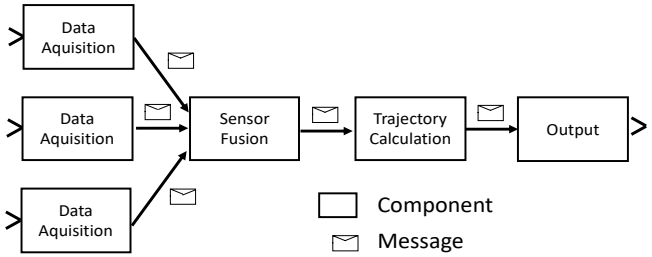


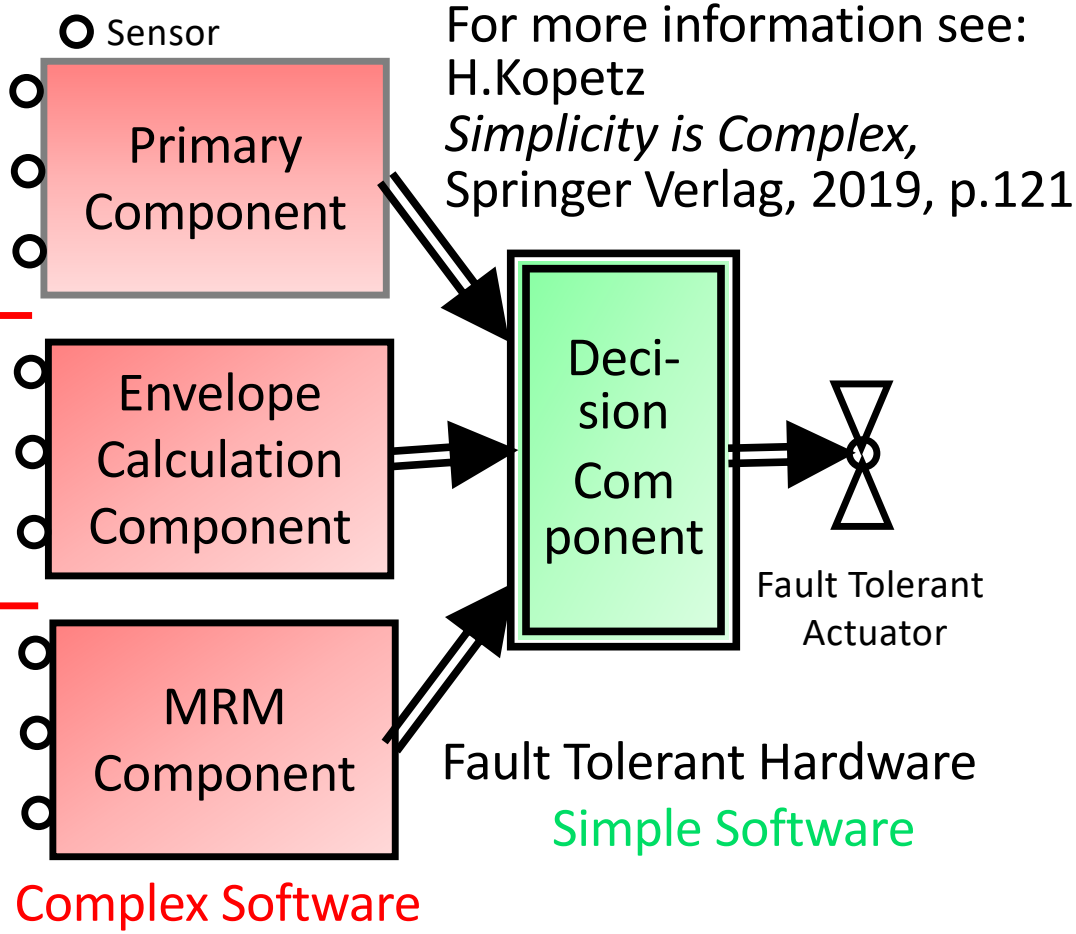
Sketch of an ADS for Unsupervised Autonomous Control

Three independent Subsystems with diverse Hardware, Software and Sensors









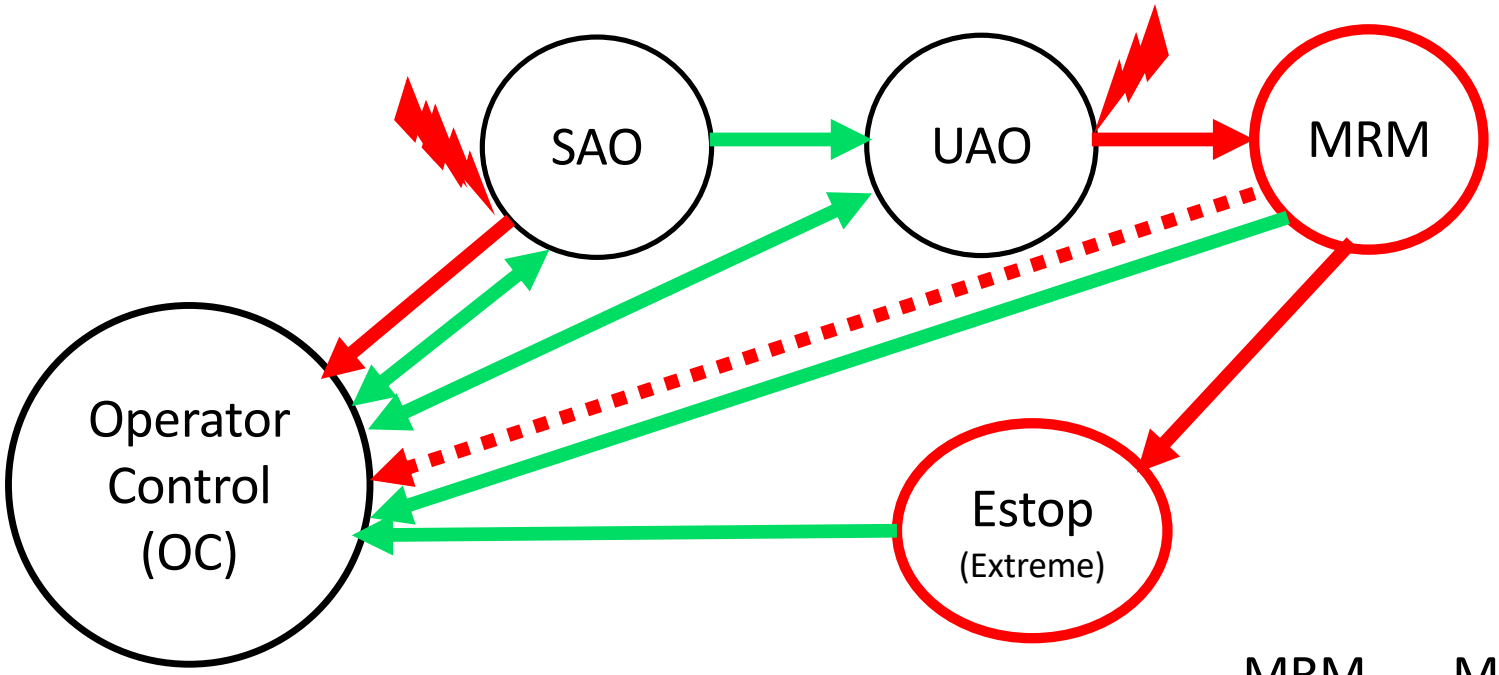
For more information see:
H.Kopetz
Simplicity is Complex,
Springer Verlag, 2019, p.121

Different Objectives justify *Independent Subsystems*

- Under normal conditions, the **Primary Component** drives the car autonomously *within the specified ODD*.
- The **Envelope Calculation Component** calculates independently a safety envelope in the ODD and thus provides the *reference for error detection*.
- Based on the results of the Envelope Calculation Component, the **Decision Component** (*simple software* on *fault-tolerant hardware*) decides whether the trajectory provided by the primary component is safe.
- In case of a failure or an ODD violation, the **Minimum Risk Maneuver (MRM) component** must bring the system—*immediately* or *deferred*, depending on the operational situation– from the current state to a safe state under *all possible conditions*.

The Minimum Risk Maneuver (RM) component must not fail due to an ODD violation or due to an intrusion.

State Transitions in Unsupervised Autonomous Control



State Transitions:

- Initiated by Operator
- Initiated by ADS
- Request to react from the ADS to the Operator

OC Operator Control
SAO Supervised Autonomous Operation
UAO Unsupervised Autonomous Operation

MRM Minimal Risk Maneuver
EStop Emergency Stop

Failure Event or ODD violation

Estop if there is no timely reaction of the driver to the request from the ADS

Conclusion

- The white paper elaborates on the issues that should be considered in the design and validation of an ADS.
- The *safety by design capabilities* and *elements and architectures* for safety critical ADSs are covered at a superficial level only.
- Accepted principles for the design of fault-tolerant systems, such as the introduction of independent fault-containment units (FCUs) and the formulation of a precise fault-hypothesis for these FCUs are not pursued.
- It is impossible to achieve the required level of safety without a well-defined fault-tolerant safety architecture.