Robotics & Embedded Systems

Autonomes Fahren

SS 2019

Automotive Safety, Development, Testing

Technische Universität München

How safe must autonomous vehicles be for permits?

Expert opinions from end of 2017:

- Prof. Dr. Raúl Rojas, Leiter des Dahlem Center for Intelligent Systems, Freie Universität Berlin
- Prof. Dr. Ortwin Renn, Wissenschaftlicher Direktor und Vorstand, Institute of Advanced Sustainability Studies e.V. (IASS), Potsdam
- Prof. Dr. Armin Grunwald, Leiter am Institut für Technikfolgenabschätzung und Systemanalyse, Karlsruher Institut für Technologie (KIT)
- Prof. Dr. Markus Maurer, Institut für Regelungstechnik, Technische Universität Carolo-Wilhelmina zu Braunschweig
- Prof. Dr. Philipp Slusallek, Wissenschaftlicher Direktor Agenten und Simulierte Realität, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Saarbrücken
- Prof. Dr. Volker Lüdemann, Wissenschaftlicher Leiter des Niedersächsischen Datenschutzzentrums, Hochschule Osnabrück
- Prof. Dr. Hermann Winner, Leiter des Fachgebiets Fahrzeugtechnik, Technische Universität Darmstadt

https://www.sciencemediacenter.de/alle-angebote/research-in-context/details/news/wie-sicher-muessen-automatische-autos-fahren-bevor-sie-zugelassen-werden/

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Raúl Rojas, Dahlem Center for Intelligent Systems, Freie Universität Berlin**
- Typical demand: drive millions of kilometers to enable statistically significant comparison with human performance. Can test 1000 cars instead of 1, drive 100.000 kilometers instead of 100 million, however both methods are very expensive.
- Another common challenge is the assumption of a „static world“, comparing autonomous vehicles with today‘s drivers.
- But AV technology is introduced incrementally, starting with driver assistance systems: automated emergency braking, lane keeping, lane change prevention if they would lead to an accident. These additions increase the gap between human and AV performance, by supporting the human driver with new safety functionality, i.e. giving each driver an intelligent computer-pilot.
- The incremental introduction into the vehicle a) saves lifes, b) allows modular testing of individual technology modules, or functions, with millions of individually driven kilometers.
- The core question should be, how many lifes can we save with driver assistance systems in the comming years, and can AVs get to the same level?
- ADAS provide the baseline and safe lifes, i.e. are a suitable introduction path for AV technology. In general traffic permits are granted quickly, as companies are in starting positions for the race.
- Vehicle-2-N (V2N) communication is sometimes neglected as well. Connected vehicles will further reduce accident occurances.

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Ortwin Renn, wissenschaftlicher Direktor und Vorstand, Institute of Advanced Sustainability Studies e.V. (IASS), Potsdam**

- Demonstrating that AVs are safer than humans is a statistical problem. Sufficient data available for human driving, but not enough for AV driving. Simultaneuously, accidents are very rare per driven kilometer, therefore a lot of data is required for significanct AV accidant probability studies.

- What‘s available are expert estimations and data from AV test vehicles in strongly limited areas, which is difficult to generalize to AV driving.

- Accident statistics depend on percentage of AV and human-driven vehicles in traffic scenarios. It could be expected that in a transition phase there are more accidents, as both vehicle system typeshave to adapt to each other.

- Even after verification there will be variance, and AV accidents will receive much more attention and scrutiny. Negative narratives could develop to increase permit difficulty, such as when accidents occur, where the human driver could have overruled the AV to prevent an accident, but did not, because he trusted the AV. This could negatively impact acceptance.

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Armin Grunwald, Leiter am Institut für Technikfolgenabschätzung und Systemanalyse, Karlsruher Institut für Technologie (KIT)**
- Comparing AV and human driver safety is currently only possible through plausibility evaluations and simulations.
- History shows that the introduction of complex new technologies into complex social constellations can often lead to new opportunities that nobody saw before.
- The evidence base for safety estimations needs to be extended incrementally through on-road tests in order to enable further learnings for future developments from the occuring scenarios.
- If statistical evidence is available even for small safety improvements due to AV introduction, then these small changes are enough to create ethical necessity for AV introduction.
- AV introduction considerations must consider the complete socio-technological scenario, beyond the safety question alone.

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Markus Maurer, Technische Universität Carolo-Wilhelmina zu Braunschweig**

- AVs are very complex software systems, facing many diverse scenarios, with other active participants, of whom many don‘t respect traffic rules. This very complex problem, also has a very complex solution, which leads to numerous uncertainties.
  - Computer vision creates a representation of the world from sensor signal interpretations, which can again and again lead to errors.
  - The intentions of other traffic participants are unknown. Even with perfect percetion, it is unclear what the environment will look like in 2 to 5 seconds. A child on a pedestrian walk way could keep walking in safe distance to the road, or run straight onto it.

- Complex softwaresystems cannot be fully tested yet. Even a complete specification of the requirements does not work flawlessly for general AV cases yet. Untested software components will remain, which can lead to undesired consequences.

- How safe must AVs be for society to accept them? Which human does the AV get compared against? The average driver or the 2% best drivers? Ethics commission for automated and connected driving in 2017 said that the question how much safer a technological system has to be statistically for society to accept it, remains open for future discussion.

- AVs might not just be better or worse than human drivers, but come with other strengths and weaknesses. How will these compare? How will you compare them statistically?

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Philipp Slusallek, wissenschaftlicher Direktor Agenten und Simulierte Realität, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH (DFKI), Saarbrücken**

- It would be false to think that only field experiments, i.e. on-road driving can improve AV safety.

- Traffic simulations can significantly improve safety, for example by simulating AV driving in critical traffic scenarios, allowing aimed optimization of AV driving in these scenarios.

- Incrementally a big test-scenario collection can be designed, collected, generated, which could serve as a driver‘s license test for AVs, for which passing it would become mandatory in order to gain traffic permits.

- Suggesting that only real driven kilometers can improve safety, would suggest that for example potential accidents during this testing would be accepted willingly, however loss of lifes should only be accepted where it is inevitable, which is not the case, when you could use simulations to improve safety.

- An often neglected problem: On-road driving swiftly leads to novelty saturation, where new driven kilometers provide very little new informatoin value, as most occuring situations have already been faced. Systematically testing critical situations is much more effective and effiecient in these cases.

How safe must autonomous vehicles be for permits?

- **Prof. Dr. Volker Lüdemann, wissenschaftlicher Leiter Niedersächsisches Datenschutzzentrum, Hochschule Osnabrück**
- Certain proof of AV safety superiority compared to humans is hardly possible before AV market introduction. Field tests take many years and simulation tests do not fully represent the complexity of the real world, making field tests necessary.
- Currently 90% of accidents are caused by human errors. When humans are replaced as drivers, new technology errors will replace some of the human errors.
- Technology is never error-free, especially not software-technology.
- Unpredictability of human traffic participants will remain at least partially. Even when all vehicles are AVs, pedestrians and bicycle drivers would remain in many places.
- New risks develop from hacking and cyber crimes.
- The legal and societal assesment of guilt in cases of accidents will have major impact on when AVs will become available.
- Utilitarian view: introduce AVs as soon as they cause less accidents than humans.
- Principaled view, focused on human responsibility: Fundamental issue when machines lead to human injuries.

How safe must autonomous vehicles be for permits?

incrementally release

- **Prof. Dr. Hermann Winner, Leiter des Fachgebiets Fahrzeugtechnik, Technische Universität Darmstadt**

- General problem titled as „Freigabefalle“ (~Permit-Trap): Requiring i.e. 10 billion kilometers for high statistic certainty to proof that a system, which is two times as safe, is actually safer for highway driving.

- There is a lack of altenative safety verification methods, allthough people work on it.

- It is not seen as possible, before releasing AV L3+ with regards to today‘s safety levels, to certainly predict that AVs will endanger less people than human drivers after initial release.

- Proposed was an incremental release of AVs, with continuous monitoring, to achieve an acceptable risk, enabling safety validation after release in field.

- Strategy is to grant permits for sufficient AVs to estimate the safety level after testing, but limited enough to dillute risks.

- Eventhough field tests are necessary for safety assessments, and a limited introductoin („dosierte Zulassung“) can be beneficial for safety evaluations, still as much as possible should be tested beforehand, in order to av oid preventable risks, which could lead to accidents, related backlash and stifle technology developments.

savety is not comparable with cost

Taxonomy and safety analysis methods for AV on-road safety

- Discuss a taxonomy of on-road safety of an Automated Driving System (ADS)
- Describe safety analysis methods applicable for requirements and early design stage of ADS development.
- Cover:
  - Driving Behavior Safety Assurance
  - Safety of The Intended Functionality (SOTIF) Assurance
  - Hazard Analysis and Risk Assessment (HARA)
  - Functional Safety
  - System-Theoretic Process Analysis (STPA).

Read-along and source material for the following excourse: On-Road Safety of Automated Driving System (ADS) - Taxonomy and Safety Analysis Methods. Technical Report · July 2018 DOI: 10.13140/RG.2.2.28313.93287, Czarnecki, University of Waterloo

Taxonomy and safety analysis methods for AV on-road safety

- **Taxonomy (Wiki):** Taxonomy is the practice and science of classification of things or concepts, including the principles that underlie such classification.
- Taxonomy covers key terms related to different types of on-road safety of ADS, in particular Driving Behavior Safety, Safety of The Intended Functionality (SOTIF), and Functional Safety (FuSa).
- **Scene, Situation, and Scenario:**
  - S. Geyer et Al. Concept and development of a unified ontology for generating test and use-case catalogues for assisted and automated vehicle guidance. IET Intelligent Transport Systems, vol. 8, no. 3, 2014
  - S. Ulbrich et Al. Defining and substantiating the terms scene, situation, and scenario for automated driving. In Proc. 2015 IEEE 18th International Conference on Intelligent Transportation Systems (ITSC), 2015

Taxonomy and safety analysis methods for AV on-road safety

- **Taxonomy (Wiki):** Taxonomy is the practice and science of classification of things or concepts, including the principles that underlie such classification.

- Taxonomy covers key terms related to different types of on-road safety of ADS, in particular Driving Behavior Safety, Safety of The Intended Functionality (SOTIF), and Functional Safety (FuSa).

- **Passenger car:** *A passenger car is a motor vehicle "designed and constructed primarily for the carriage of persons and their luggage, their goods, or both, having not more than a* ***seating capacity of eight, in addition to the driver****, and* ***without space for standing passengers****."*

- **Example AV tasks:** *ADS requesting a* ***fallback-ready user*** *to take over control and perform the* ***dynamic driving task fallback****.*

Taxonomy and safety analysis methods for AV on-road safety

- **On-road:** *“On-road” refers to* ***publicly accessible roadways****, including* ***parking areas and private campuses*** *that permit public access, and* ***private access roads and garages****, “that collectively serve users of vehicles of all classes and driving automation levels (including no driving automation), as well as motorcyclists, pedalcyclists, and pedestrians.”*

- **On-road safety:** *On-road safety is scoped to mean the* ***absence of unreasonable risk of transport crashes,*** *with the ADS of the subject vehicle being a causal or contributing crash factor.*

- ***Automated Driving System (ADS):*** *is an E/E system that performs level 3, 4, or 5 driving automation In particular, ADS performs the complete Dynamic Driving Task (DDT), which consists of operational and tactical aspects of driving, and potentially also performs parts of the strategic driving tasks (the latter is beyond the scope of SAE 3016 [LA]). A passenger car equipped with ADS that is subject to the safety analyses is referred to as subject vehicle.*

Taxonomy and safety analysis methods for AV on-road safety

- **Functional safety**: *is the absence of unreasonable risk from malfunctioning behavior caused by failures or unintended behavior with respect to design intent.*

- **Safety:** *ISO 26262 defines safety as "absence of unreasonable risk" of harm. This definition is in contrast to defining safety as freedom from harmful events; the absence of a harmful event may simply mean that the event has not yet occurred. Thus, safety is more adequately defined as the absence of unreasonable risk of harm.*

- **Harm***: defined as "physical injury or damage to the health of persons." Thus, ISO 26262 limits the definition of harm to personal injury; however, ANSI D.16.1 subdivides harm into (personal) injury and (property) damage.*

- **Risk:** *ISO 26262 defines risk as "combination of the probability of occurrence of harm and the severity of that harm." Unreasonable risk is defined as "risk judged to be unacceptable in a certain context according to valid societal moral concepts."*

Taxonomy and safety analysis methods for AV on-road safety

- **Hazard:** *A hazard is potential source of harm caused by (1) deficiencies in the specified behavior, (2) performance limitations of the intended functionality (3) malfunctioning behavior, (4) foreseeable misuse, or (5) security vulnerability. This definition extends the one from ISO 26262, which is focused on malfunctioning behavior due to failures or unintended behavior (case 1), with cases (2,4,5)*

- **Crash:** *A crash is "an unstabilized situation which includes at least one harmful event." An unstabilized situation is "a set of events not under human control." A harmful event is "an occurrence of injury or damage." Traffic safety literature suggest using the term "crash" rather than "transport accident" because the term "accident" emphasizes "randomness," obscuring the controllable causes such as human factors. In fact, editions of ANSI D16.1 prior to the eighth one have used the term "accident" in place of "crash".*

Taxonomy and safety analysis methods for AV on-road safety

- **Transport crash:** *is “a crash that involves a transport vehicle in-transport”´. The definition of a transport crash excludes situations resulting directly from cataclysms, but includes situations occurring after the cataclysm has ended, such as road obstruction by fallen trees, and situations resulting from natural events that are not cataclysms, such as tree branches falling on a motor vehicle in traffic.*
  - However, a branch falling on a motor vehicle parked legally is not a transport crash, because the vehicle is not in-transport.
  - On the other hand, an illegally parked vehicle being struck by a falling branch or another vehicle is considered a transport crash.
  - Thus, in the case an ADS parks a subject vehicle illegally and the parked vehicle is subsequently struck by another vehicle or a falling tree branch, the ADS would have contributed to the cause of the resulting transport crash.

- **Transport vehicle:** consists of “one or more devices or animals and their load [...].” Examples of transport vehicles are car, airplane, train, snowmobile, and horse and rider. When applied to motor vehicles, in-transport means “on a roadway or in motion within or outside [the public road.]” This definition includes vehicles in traffic on public and private roadways, and (possibly soft) shoulders; it also includes disabled vehicle on a roadway. It does not include vehicles parked legally in designated parking spaces; however, “in roadway lanes used for travel during some periods and for parking during other periods, a parked motor vehicle should be considered to be in-transport during periods when parking is forbidden.”

- **Cataclysm:** *Effects, such as a tornado or an earthquake*

Taxonomy and safety analysis methods for AV on-road safety

- **Transport crashes include:** motor vehicle crashes, railway crashes, and airplane crashes.

- **Motor vehicle crash:** is a transport crash “that involves a motor-vehicle intransport,” but does not involve aircraft or railway train in-transport.
  - In particular, a collision between a motor vehicle and a railway train in-transport is classified as a railway accident.

- **Road vehicle crash:** is “a transport crash that is either a motor vehicle crash or an other-road-vehicle crash.”
  - An example of an other-road-vehicle crash is a collision of a pedalcycle in-transport with a pedestrian on a public road.

- **Traffic crash:** is a road vehicle crash in which “(1) the unstabilized situation originates on a public road or (2) a harmful event occurs on a public road”.
  - Thus, a road vehicle crash that occurs on a private road, rather than a public road, is not a traffic crash.

Taxonomy and safety analysis methods for AV on-road safety

- A road vehicle crash is further classified by the type of its first harmful event: a collision crash and a noncollision crash.

- **Collision crash:** is a road vehicle crash in which the first harmful event is a collision of a road vehicle in-transport with another vehicle, pedestrians, or other objects.

- **Noncollision crashes:** are road vehicle crashes other than collision crashes, including overturning, jackknife, fire or explosion of any parts of road vehicle in-transport, immersion (such as driving into water), occupant falling from a road vehicle in-transport or being thrown against some part of the vehicle inside, and thrown or falling objects striking occupant or the road vehicle in-transport.

Taxonomy and safety analysis methods for AV on-road safety

- **Manifold safety approaches:**
  - **General:**
    - **System-Theoretic Process Analysis (STPA):** A general safety assurance method
  - **Specific hazard sources three methods targeting specific hazard sources in the context of automated driving:**
    - **Driving Behavior Safety Assurance**
    - **SOTIF Assurance, and the Hazard Analysis**
    - **Risk Assessment (HARA)**
- Industry standards providing guidance on safety assurance related to hazards caused by, respectively, (i) **limited performance of sensor technology** and **algorithms** and **foreseeable misuse** and (ii) **malfunctioning behavior**. Driving Behavior Safety Analysis focuses on hazards caused by **deficiencies in the specified driving behavior**, and is defined in this document.

Taxonomy and safety analysis methods for AV on-road safety

- **Industrial guidance and standard documentation:**

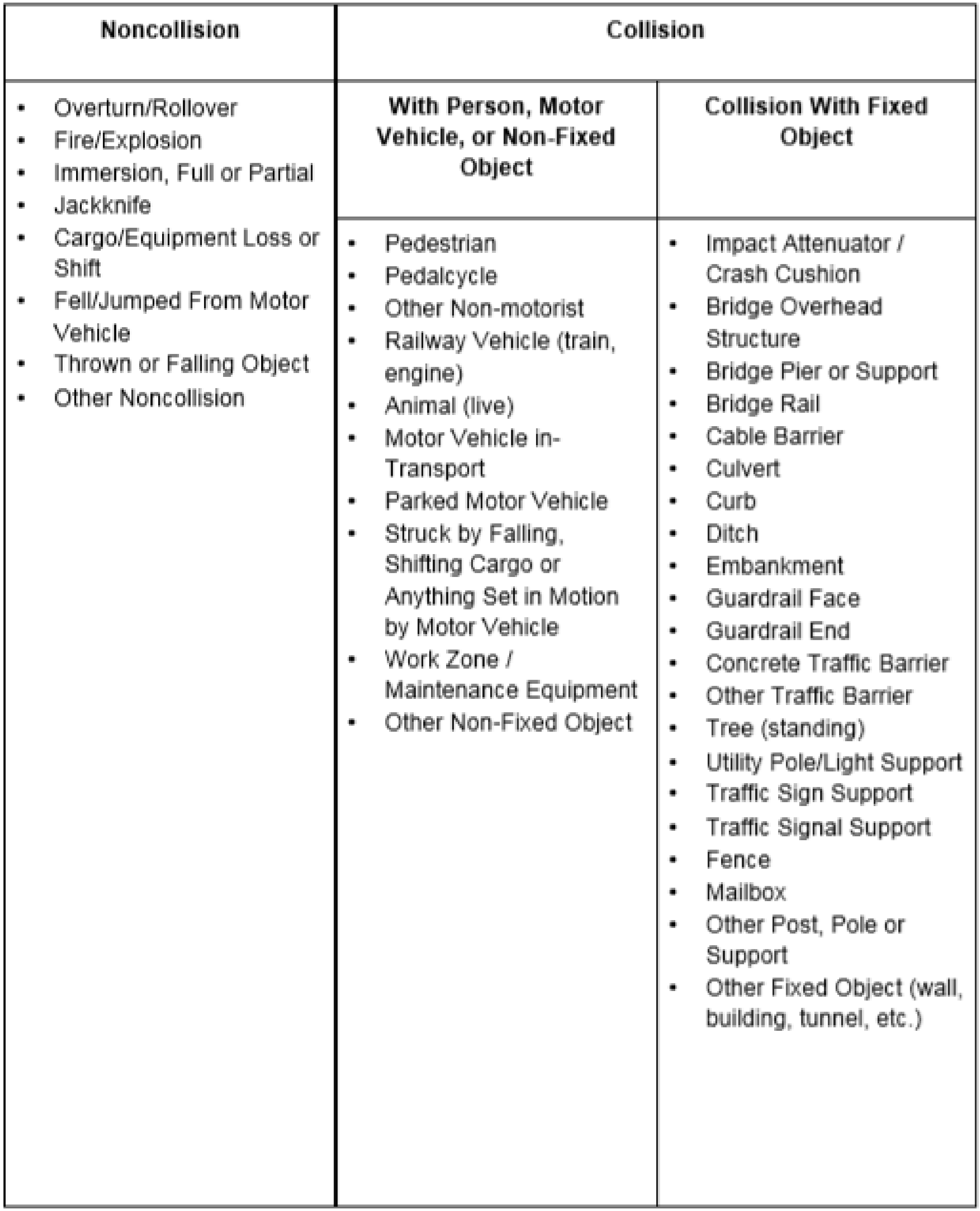
- **Model Minimum Uniform Crash Criteria (MMUCC) Guideline. Fourth edition, DOT HS 811 631, Governors Highway Safety Association (GHSA), July 2012**
  - This guideline provides a uniform schema for collecting, storing, and analyzing motor vehicle crash data in the United States. The classification schema is based on ANSI D16.1-2007.

- Defines a crash description schema to be used by reporters, classifiers, analysts and users of traffic crash data in the United States. Includes classification of crashes according to the first harmful event. Other MMUCC crash criteria include location of first harmful event (on roadway, shoulder, median, roadside, parking zone, etc.), impact type (front-to-rear, front-to-front, angle (includes front-toside), sideswipe in same or opposite direction, rear-to-side, rear-to-rear), weather conditions, light conditions, roadway surface conditions, contributing circumstances, road configuration, and temporary road structure.

- **Industrial guidance and standard documentation:**

- **Model Minimum Uniform Crash Criteria (MMUCC) Guideline. Fourth edition, DOT HS 811 631, Governors Highway Safety Association (GHSA), July 2012**
  - This guideline provides a uniform schema for collecting, storing, and analyzing motor vehicle crash data in the United States. The classification schema is based on ANSI D16.1-2007.

- Defines a crash description schema to be used by reporters, classifiers, analysts and users of traffic crash data in the United States. Includes classification of crashes according to the first harmful event. Other MMUCC crash criteria include location of first harmful event (on roadway, shoulder, median, roadside, parking zone, etc.), impact type (front-to-rear, front-to-front, angle (includes front-toside), sideswipe in same or opposite direction, rear-to-side, rear-to-rear), weather conditions, light conditions, roadway surface conditions, contributing circumstances, road configuration, and temporary road structure.



Noncollision	Collision	
	With Person, Motor Vehicle, or Non-Fixed Object	**Collision With Fixed Object**
• Overturn/Rollover • Fire/Explosion • Immersion, Full or Partial • Jackknife • Cargo/Equipment Loss or Shift • Fell/Jumped From Motor Vehicle • Thrown or Falling Object • Other Noncollision	• Pedestrian • Pedalcycle • Other Non-motorist • Railway Vehicle (train, engine) • Animal (live) • Motor Vehicle in-Transport • Parked Motor Vehicle • Struck by Falling, Shifting Cargo or Anything Set in Motion by Motor Vehicle • Work Zone / Maintenance Equipment • Other Non-Fixed Object	• Impact Attenuator / Crash Cushion • Bridge Overhead Structure • Bridge Pier or Support • Bridge Rail • Cable Barrier • Culvert • Curb • Ditch • Embankment • Guardrail Face • Guardrail End • Concrete Traffic Barrier • Other Traffic Barrier • Tree (standing) • Utility Pole/Light Support • Traffic Sign Support • Traffic Signal Support • Fence • Mailbox • Other Post, Pole or Support • Other Fixed Object (wall, building, tunnel, etc.)

Taxonomy and safety analysis methods for AV on-road safety

- On-road safety of ADS is concerned with crashes in which the subject vehicle is involved directly or indirectly while the subject vehicle is in-transport.

- Includes not only collisions of the subject vehicle with other vehicles or pedestrians, but also collisions with railway trains at level crossings or aircraft landing on a roadway in emergency.

- Also includes crashes of other road vehicles such as a car or a pedalcycle involving the subject vehicle indirectly, i.e., without contact between the subject vehicle and any vehicle directly involved in the crash. An example of such a crash would be an unsafe cut-in maneuver by the subject vehicle in intense traffic, which would cause subsequent vehicles to crash, without any contact with the subject vehicle. Another example would be a car colliding with roadside infrastructure because of its driver being blinded by high-beam headlights of the subject vehicle at night. In both examples the subject vehicle would be contributing to the cause of the crash as a noncontact vehicle.

Taxonomy and safety analysis methods for AV on-road safety

importand

- **Industrial guidance and standard documentation:**
- **Surface Vehicle Recommended Practice — Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. SAE J3016:Jul2018**
  - defines levels of driving automation and related concepts, including Automated Driving System (ADS).

Taxonomy and safety analysis methods for AV on-road safety

- **Industrial guidance and standard documentation:**

- **Road vehicles — Safety of the intended functionality. Working Document, ISO/WDPAS 21448.1:2017-11-15**
  - represents work in progress to develop an ISO Publicly Available Specification (PAS) providing guidance on design, verification and validation measures to achieve safety of the intended functionality, that is, avoid unsafe behavior that stems from technological and system definition shortcomings. The scope of the upcoming first edition of the PAS targets driving automation at levels 0, 1, and 2. While this first edition can be taken into account when developing driving automation at levels 3, 4, and 5, additional measures may be necessary. These will be addressed in future editions.

Taxonomy and safety analysis methods for AV on-road safety

- **Industrial guidance and standard documentation:**

- **Road vehicles — Functional safety. ISO 26262:2011**
  - This ISO standard defines terms and activities to be used in ensuring the functional safety of electrical and/or electronic (E/E) systems within motor vehicles. Functional safety is the absence of unreasonable risk from malfunctioning behavior caused by failures or unintended behavior with respect to design intent.

Taxonomy and safety analysis methods for AV on-road safety

- **Industrial guidance and standard documentation:**

- **Manual on Classification of Motor Vehicle Traffic Crashes. ANSI D16.1-2017**
  - This ANSI standard provides a taxonomy and guidance on classifying motor vehicle traffic crashes. It defines different types of transport crashes, including collision and noncollision crashes, to be used in collecting and analyzing data for crash databases.

Taxonomy and safety analysis methods for AV on-road safety

- **STPA introduction:**

- *N. Leveson. A New Approach to Hazard Analysis for Complex Systems. In Proceedings of International Conference of the System Safety Society, Ottawa, August 2003* provides a concise summary of the basic ideas behind STAMP and STPA.

- *N. Leveson. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2011* provides a comprehensive description of STAMP and STPA.

- *A. Abdulkhaleq et Al. A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles. In 4th European STAMP Workshop 2016, Procedia Engineering 179 (2017)* applies STPA to fully automated driving (levels 3, 4, 5). In particular, it provides a sample control structure for use in STPA.

Taxonomy and safety analysis methods for AV on-road safety

- **STPA introduction:**
- Hazard analysis technique based on the System Theoretic Accident Modeling Process (STAMP)
- Key idea: crashes occur because of inadequate control that takes a system outside of its safe envelope
- STPA focuses first on identifying safety constraints, rather than hazardous events and determining control actions that may violate the safety constraints
- STPA then examines the control structure of a system to determine the potential causes for the unsafe actions, and suggests improvements to eliminate, reduce, control, or mitigate these actions in design or operation.

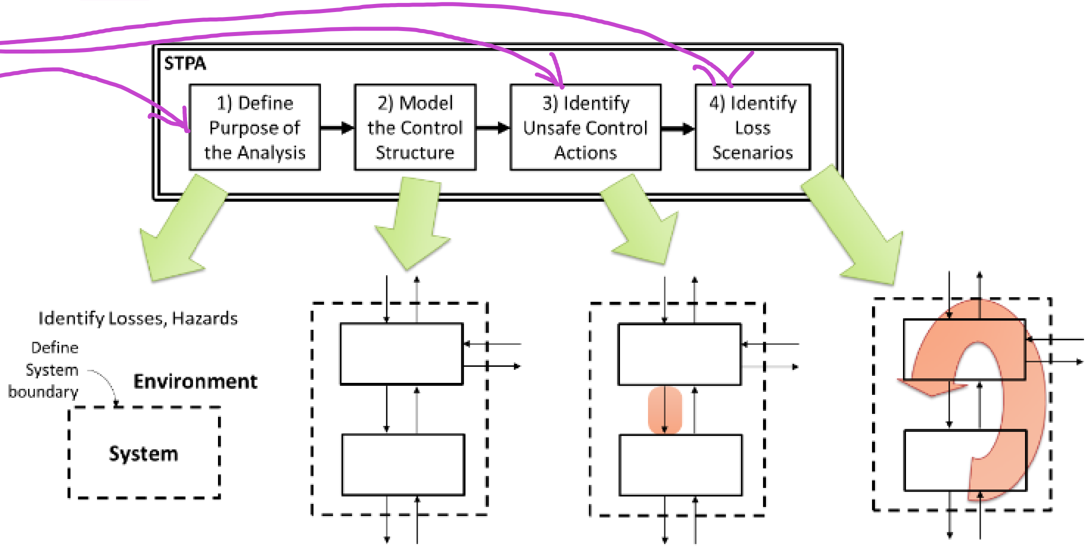
Taxonomy and safety analysis methods for AV on-road safety

- **STPA introduction:**

Assuming existence of a control structure:

- 1. Identify mishaps, hazards, and safety requirements
- 2. Identify hazardous control actions, that could lead to a hazardous state (violation of safety requirements)
- 3. Determine how each potentially hazardous control action identified previously could occur and eliminate, control, mitigate hazardous control actions in design or operation.

More extensive process (STPA handbook):


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

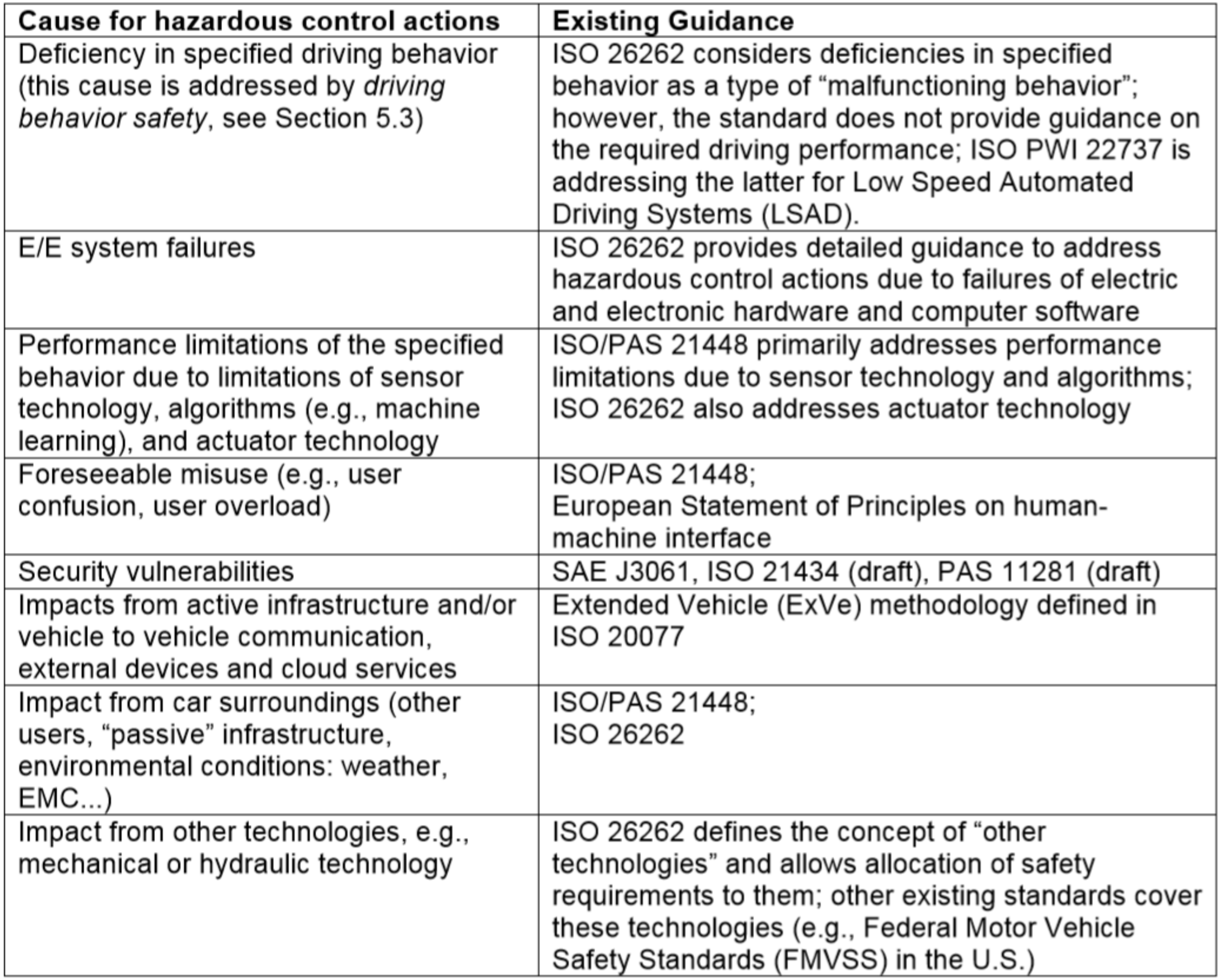
Taxonomy and safety analysis methods for AV on-road safety

- **STPA introduction:**
- 2. Identify hazardous control actions, that could lead to a hazardous state (violation of safety requirements):
  - a. A control action required for safety is not provided or not followed.
  - b. An unsafe control action is provided.
  - c. A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence.
  - d. A control action required for safety is stopped too soon or applied too long or at too high or too low intensity.

Taxonomy and safety analysis methods for AV on-road safety

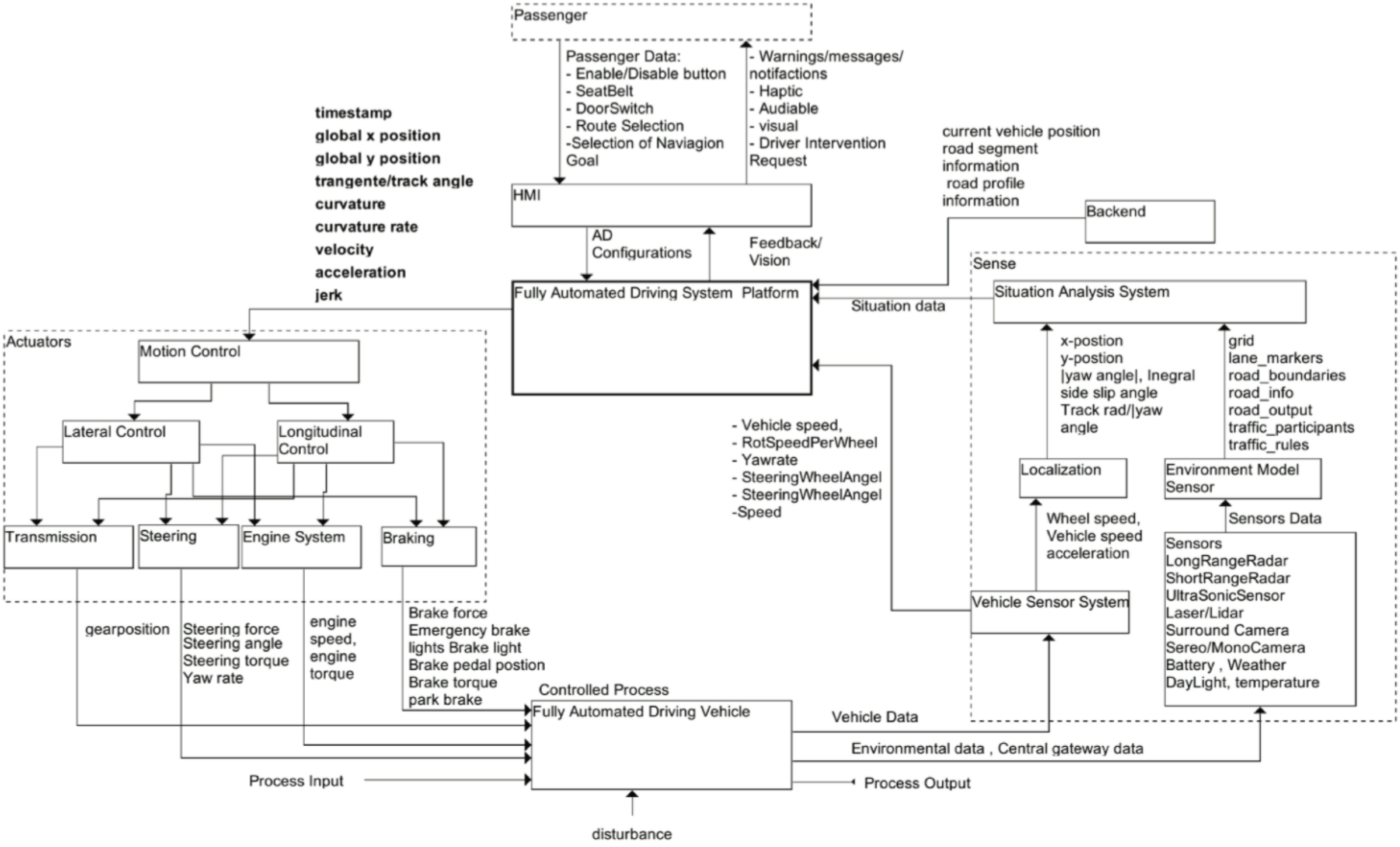
- **STPA introduction:**
- 3. Determine how each potentially hazardous control action identified previously could occur and eliminate, control, mitigate hazardous control actions in design or operation.
  - a. Consider the following potential causes for hazardous control actions when analyzing the control structure: inadequate enforcement of constraints in the controller part, including process model, algorithms, and coordination among controllers; inadequate execution of control actions (e.g., communication flaws, actuator problems, and time lags); and inadequate or missing feedback.
  - b. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design.
  - c. Consider degradation of the control structure over time and build protection, including change management, audits, and accident an incident analysis.

Taxonomy and safety analysis methods for AV on-road safety



Cause for hazardous control actions	**Existing Guidance**
Deficiency in specified driving behavior (this cause is addressed by *driving behavior safety*, see Section 5.3)	ISO 26262 considers deficiencies in specified behavior as a type of "malfunctioning behavior"; however, the standard does not provide guidance on the required driving performance; ISO PWI 22737 is addressing the latter for Low Speed Automated Driving Systems (LSAD).
E/E system failures	ISO 26262 provides detailed guidance to address hazardous control actions due to failures of electric and electronic hardware and computer software
Performance limitations of the specified behavior due to limitations of sensor technology, algorithms (e.g., machine learning), and actuator technology	ISO/PAS 21448 primarily addresses performance limitations due to sensor technology and algorithms; ISO 26262 also addresses actuator technology
Foreseeable misuse (e.g., user confusion, user overload)	ISO/PAS 21448; European Statement of Principles on human-machine interface
Security vulnerabilities	SAE J3061, ISO 21434 (draft), PAS 11281 (draft)
Impacts from active infrastructure and/or vehicle to vehicle communication, external devices and cloud services	Extended Vehicle (ExVe) methodology defined in ISO 20077
Impact from car surroundings (other users, "passive" infrastructure, environmental conditions: weather, EMC...)	ISO/PAS 21448; ISO 26262
Impact from other technologies, e.g., mechanical or hydraulic technology	ISO 26262 defines the concept of "other technologies" and allows allocation of safety requirements to them; other existing standards cover these technologies (e.g., Federal Motor Vehicle Safety Standards (FMVSS) in the U.S.)

Taxonomy and safety analysis methods for AV on-road safety



Passenger

Passenger Data:
- Enable/Disable button
- SeatBelt
- DoorSwitch
- Route Selection
-Selection of Naviagion Goal

- Warnings/messages/ notifactions
- Haptic
- Audiable
- visual
- Driver Intervention Request

HMI

AD Configurations

Feedback/ Vision

timestamp
global x position
global y position
trangente/track angle
curvature
curvature rate
velocity
acceleration
jerk

Fully Automated Driving System Platform

current vehicle position
road segment information
road profile information

Backend

Sense

Situation Analysis System

Situation data

x-postion
y-postion
|yaw angle|, Inegral
side slip angle
Track rad/|yaw angle

grid
lane_markers
road_boundaries
road_info
road_output
traffic_participants
traffic_rules

Localization

Environment Model Sensor

Wheel speed, Vehicle speed acceleration

Sensors Data

Sensors
LongRangeRadar
ShortRangeRadar
UltraSonicSensor
Laser/Lidar
Surround Camera
Sereo/MonoCamera
Battery , Weather
DayLight, temperature

Vehicle Sensor System

- Vehicle speed,
- RotSpeedPerWheel
- Yawrate
- SteeringWheelAngel
- SteeringWheelAngel
-Speed

Actuators

Motion Control

Lateral Control

Longitudinal Control

Transmission

Steering

Engine System

Braking

gearposition

Steering force
Steering angle
Steering torque
Yaw rate

engine speed, engine torque

Brake force
Emergency brake lights Brake light
Brake pedal postion
Brake torque
park brake

Controlled Process

Fully Automated Driving Vehicle

Vehicle Data

Environmental data , Central gateway data

Process Input

Process Output

disturbance

Taxonomy and safety analysis methods for AV on-road safety

- **STPA introduction:**
- 3. Determine how each potentially hazardous control action identified in step 1 could occur and eliminate, control, mitigate hazardous control actions in design or operation.
  - a. Consider the following potential causes for hazardous control actions when analyzing the control structure: inadequate enforcement of constraints in the controller part, including process model, algorithms, and coordination among controllers; inadequate execution of control actions (e.g., communication flaws, actuator problems, and time lags); and inadequate or missing feedback.
  - b. Design controls and mitigation measures if they do not already exist or evaluate existing measures if the analysis is being performed on an existing design.
  - c. Consider degradation of the control structure over time and build protection, including change management, audits, and accident an incident analysis.

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**
- 1. Identification of crash types and safety requirements on driving behavior
- 2. Verification that the specified driving behavior satisfies to the safety requirements on driving behavior
- 3. Validation of the safety of the specified driving behavior in real-life use cases
- 4. Assessment of residual risk due to specified driving behavior

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**

- **1. Vehicle stability:** Skid and roll stability is required for a vehicle to be controllable. Loosing control may result in colliding with other road users or objects, skidding off the roadway, and rollover.

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**
- **2. Assured clear distance ahead (ACDA):** ACDA is the path distance ahead of the subject vehicle that the ADS can assure to be clear for driving and within which the ADS can bring the vehicle to a halt. ACDA is the minimum standard of care in driving in common law. Measures of ACDA include different types of sight distances, which depend on road geometry and the executed maneuver, and the stopping sight distance.

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**

- **3. Minimum separation:** The ADS has to assure minimum separation between the subject vehicle and other dynamic and static objects. Multiple measures characterize separation, including distance gaps, time gaps, time to collision, and lateral clearance. Minimum separation has to include sufficient safety margin to accommodate perception, prediction, and control uncertainties. The target values for many of the separation measures are maneuver- and situation-specific. Violating minimum separation may lead to a crash, typically a collision.

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**

- **4. Traffic regulations:** Traffic regulations are formal traffic rules required by law in a given geographic area. The majority of traffic regulations are safety-related. They control traffic conflict resolution, such as yielding rules at intersections and passing rules, and prescribe how different road users use the roadway, such as specifying traffic direction, lane restrictions, and parking restrictions. Violating traffic regulations, such as running a STOP sign or a read light, may lead to a crash.

Taxonomy and safety analysis methods for AV on-road safety

- **Assuring driving behavior safety consists of the following steps:**

- **5. Driving best practices:** Driving best practices are informal traffic rules that refine and complement the formal rules. Examples include rules about how early to signal turns and how to respond to tailgating. Among others, an ADS-operated vehicle should use best practices to anticipate, recognize, and properly respond to likely mistakes of human road users such as those identified in the NHTSA pre-crash scenarios. Disregarding best practices may increase crash risk.

Taxonomy and safety analysis methods for AV on-road safety

- **Validation, Verification, Residual Risk Assessment:**
- **Verification:** assure that the specified behavior satisfies the safety requirements on driving behavior that were identified. The verification can be achieved using a range of methods, including inspections and walkthroughs, prototyping and testing of prototypes, and using formal methods.
- **Validation:** assure that the behavior specified by the safety requirements does not cause unreasonable risk of crashes in real-life use cases. This can be achieved using a combination of simulation, closed course, and field tests. Long-term field tests are of particular importance to validate the assumptions on the driving environment, including road user behavior.
- **Residual risk assessment:** review the previous behavior safety assurance steps and evaluate the acceptability of the residual risk considering the findings of these steps. The step could also include a statistical argument about the residual risk, such as using the validation targets and rare event theory.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**
- **Safety of The Intended Functionality (SOTIF)** is defined as "absence of unreasonable risk due to hazards caused by performance limitations of the intended behavior or by reasonably foreseeable misuse by the user."
- The SOTIF standard is an extension of ISO 26262 that targets unsafe actions due to performance limitation of the "intended behavior," which is the "specified behavior including interaction with other systems and functions".
- Performance limitations are insufficiencies of the implemented functions due to technology limitations, such as sensor performance limitations and noise, limitations of algorithms (e.g., machine learning), and limitations of actuator technology.
- Hardware and software failures are addressed by ISO 26262 and are out of scope of SOTIF.
- SOTIF also addresses unsafe actions due to foreseeable misuse by the user, such as user confusion, user overload, and user overconfidence.
- The current SOTIF standard targets automation levels 0, 1 and 2; it also states that the method can be applied to levels 3, 4 and 5, but additional measures may be necessary.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF assurance process starts with a functional description of the system as input, which includes:

- 1. The goals of the intended function
- 2. The description and behavior of the functions and functionalities
- 3. The dependencies on, and interaction with - other vehicle functions and systems; - the car driver and passengers; - relevant environmental conditions; - the interfaces with the road infrastructure
- 4. The use cases in which the system is activated
- 5. The concepts and technologies for the system and sub systems
- 6. The level of automation / authority over the vehicle dynamics
- 7. The limitations and their countermeasures
- 8. The system architecture supporting the countermeasures
- 9. The degradation concept
- 10. The warning strategies

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

1. Identification of hazardous events
2. Establishment of validation targets
3. Identification of triggering events
4. Evaluation of triggering events
5. Functional modification
6. Verification
7. Validation
8. Evaluation of residual risk

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

1) Identification of hazardous events: The first step is to identify hazardous events, which are combinations of hazards (or more precisely hazardous control actions) and driving situations. An example would be unintended emergency braking by the subject vehicle while being followed closely by another vehicle, which could lead to a rear-end collision. The hazardous events with severity other than S0 and controllability other than C0 are considered for further analysis (using the ISO 26262 classification of severity and controllability).

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

2) Establishment of validation targets: The purpose of this step is to establish performance targets for the analyzed function that would be used as acceptance criteria, such as the maximum acceptable probability of unintended braking per kilometer driven. The validation targets may be derived based on the performance of similar systems that are already in the field, human driver performance from traffic safety statistics, and expert judgment.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

3) Identification of triggering events: This step identifies scenarios that may trigger the unsafe action, such as emergency braking triggered by a radar reflection from a soda can on the roadway or missed emergency braking because of sun glare or missed detection by a perception algorithm. The standard provides a checklist of possible triggering events related to sensor technologies, algorithms, actuator technologies, and external conditions (such as bad weather or unusual traffic situation).

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

4) Evaluation of triggering events: The purpose of this step is to assess the likelihood of the triggering events and determine their acceptability by comparing their likelihood with the validation targets.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

5) Functional modification: For those triggering events whose likelihood does not meet the validation target, the functional specification needs to be modified, either by improving the function, e.g., increasing sensor or algorithm performance, or by restricting the ODD (Operational Design Domain) of the system.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

6) Verification: The purpose of this step is to verify that the system and the components perform as specified in the known potentially unsafe scenarios, and that they are covered sufficiently by the tests within the entire ODD. Verification uses a combination of unit and integration tests, requirements-based tests, robustness tests, and simulation and vehicle-level tests.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

7) Validation: The purpose of this step is to show that the system and the components do not cause an unreasonable level of risk in real-life use cases. Validation uses a combination of requirements-based tests, simulation, closed-course and longterm field tests.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

The SOTIF process consists of the following main steps:

8) Evaluation of residual risk: The purpose of this step is to review the SOTIF steps and evaluate the acceptability of the residual risk considering the findings of the SOTIF steps.

Taxonomy and safety analysis methods for AV on-road safety

- **SOTIF introduction:**

- The SOTIF process is iterative.

- Step 5 (functional modification) may be executed after the SOTIF evaluation (steps 1-4) and also after any of the steps 6, 7, and 8, if needed. Each functional modification triggers renewed SOTIF evaluation, followed by verification, validation, and evaluation of residual risk.

- Step 1 of SOTIF corresponds to step 2 in STPA. Steps 3-4 of SOTIF correspond to step 3.a in STPA. Finally, step 5 of SOTIF corresponds to step 3.b in STPA.

Taxonomy and safety analysis methods for AV on-road safety

- **STPA & SOTIF**

STPA:

1. Identify mishaps, hazards, and safety requirements
2. Identify hazardous control actions, that could lead to a hazardous state
3. Determine how each potentially hazardous control action identified in step 1 could occur and eliminate, control, mitigate hazardous control actions in design or operation.

~3a. Consider potential causes ~3b. Design controls and mitigation measures

SOTIF:

1. Identification of hazardous events
2. Establishment of validation targets
3. Identification of triggering events
4. Evaluation of triggering events
5. Functional modification
6. Verification
7. Validation
8. Evaluation of residual risk

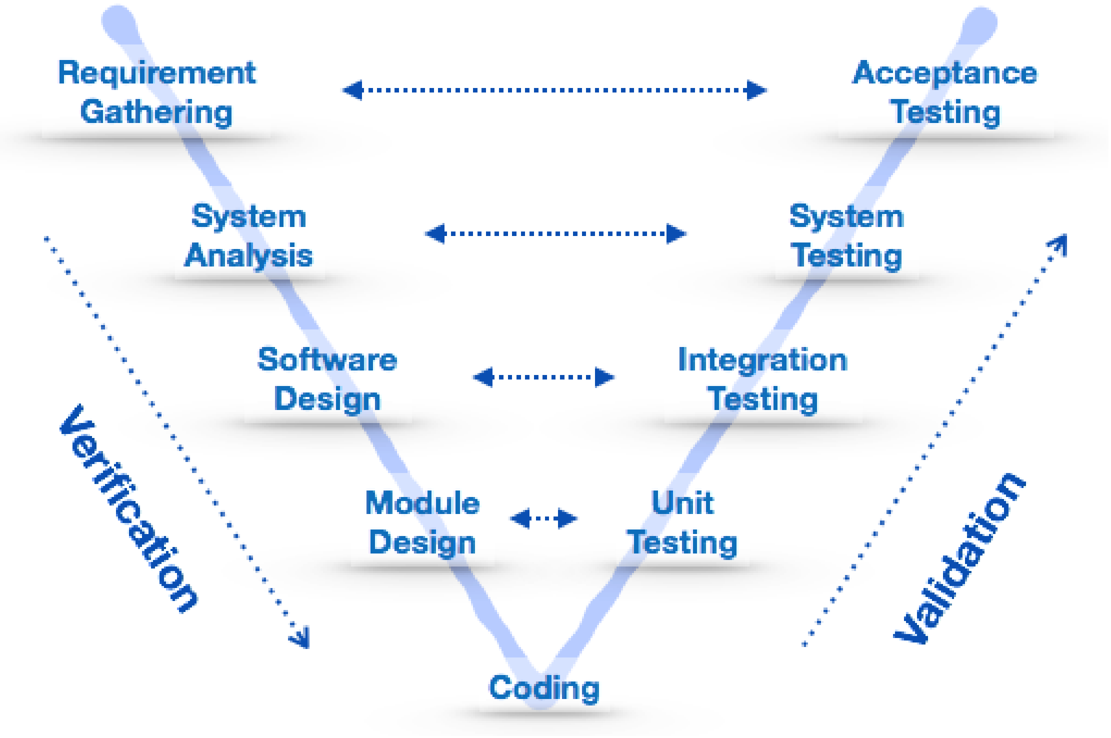
Taxonomy and safety analysis methods for AV on-road safety

V-Modell: Process model for software development organizing development and testing in phases.

Each development phase is connected with an associated testing phase.

Starting with a functional specification, the left side of the V-modell iteratively improves the depth to a technical specification, concluding in an implementation.

On the right side of the V-modell each previous component is systematically tested against.



https://www.tutorialspoint.com/software_engineering/software_development_life_cycle

Taxonomy and safety analysis methods for AV on-road safety

V-Modell XT:

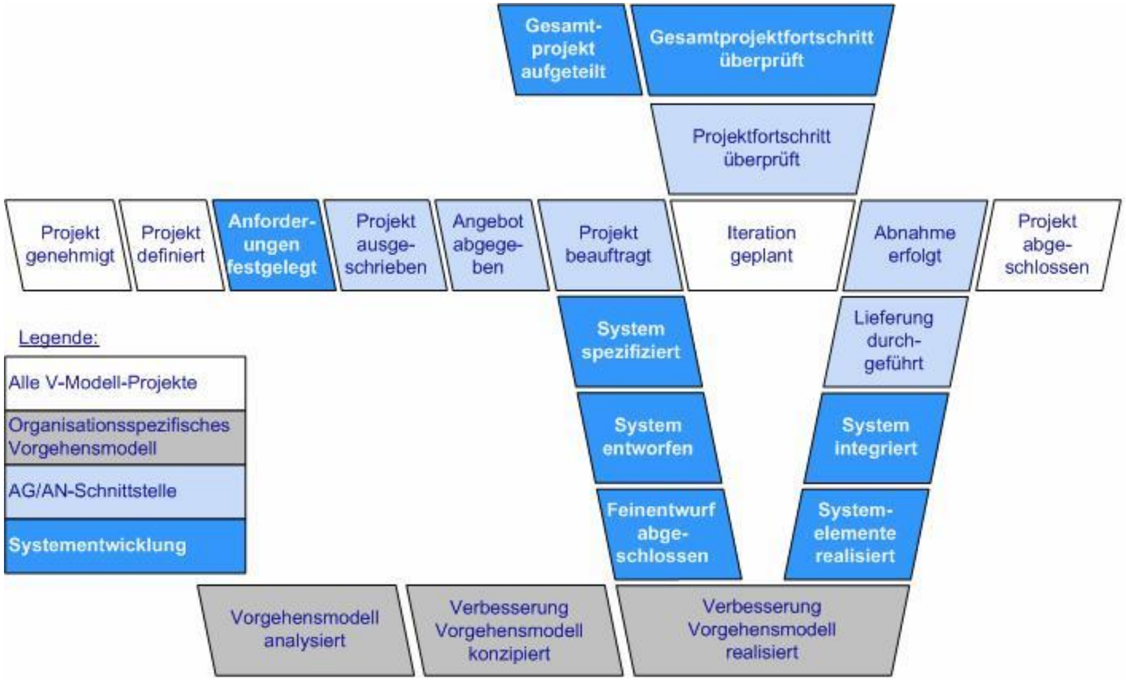
Main changes:

- V-Modell can be adapted to function specific challenges (Tailoring). Depending on project size components are required or can be neglected to avoid overhead.

- The customer is included.

- Increased modularity: Processblocks to be combined to create the project specific V-Modell (tailoring)

- More agile and incremental. No requirement for the time-order of the different process-blocks. Created products are the focus not the documentation.


Gesamt-projekt aufgeteilt
Gesamtprojektfortschritt überprüft
Projektfortschritt überprüft
Projekt genehmigt
Projekt definiert
Anforder-ungen festgelegt
Projekt ausge-schrieben
Angebot abgege-ben
Projekt beauftragt
Iteration geplant
Abnahme erfolgt
Projekt abge-schlossen
Legende:
Alle V-Modell-Projekte
Organisationsspezifisches Vorgehensmodell
AG/AN-Schnittstelle
Systementwicklung
System spezifiziert
System entworfen
Feinentwurf abge-schlossen
Lieferung durch-geführt
System integriert
System-elemente realisiert
Vorgehensmodell analysiert
Verbesserung Vorgehensmodell konzipiert
Verbesserung Vorgehensmodell realisiert

Example v-xt modell: http://www2.wiw.hs-albsig.de/ws1213/itpmv6/index.php/de/e-learning?view=featured&start=70

Taxonomy and safety analysis methods for AV on-road safety

- **Automotive SPICE** is a domain specific variation of the international standards ISO/IEC 15504 (SPICE).

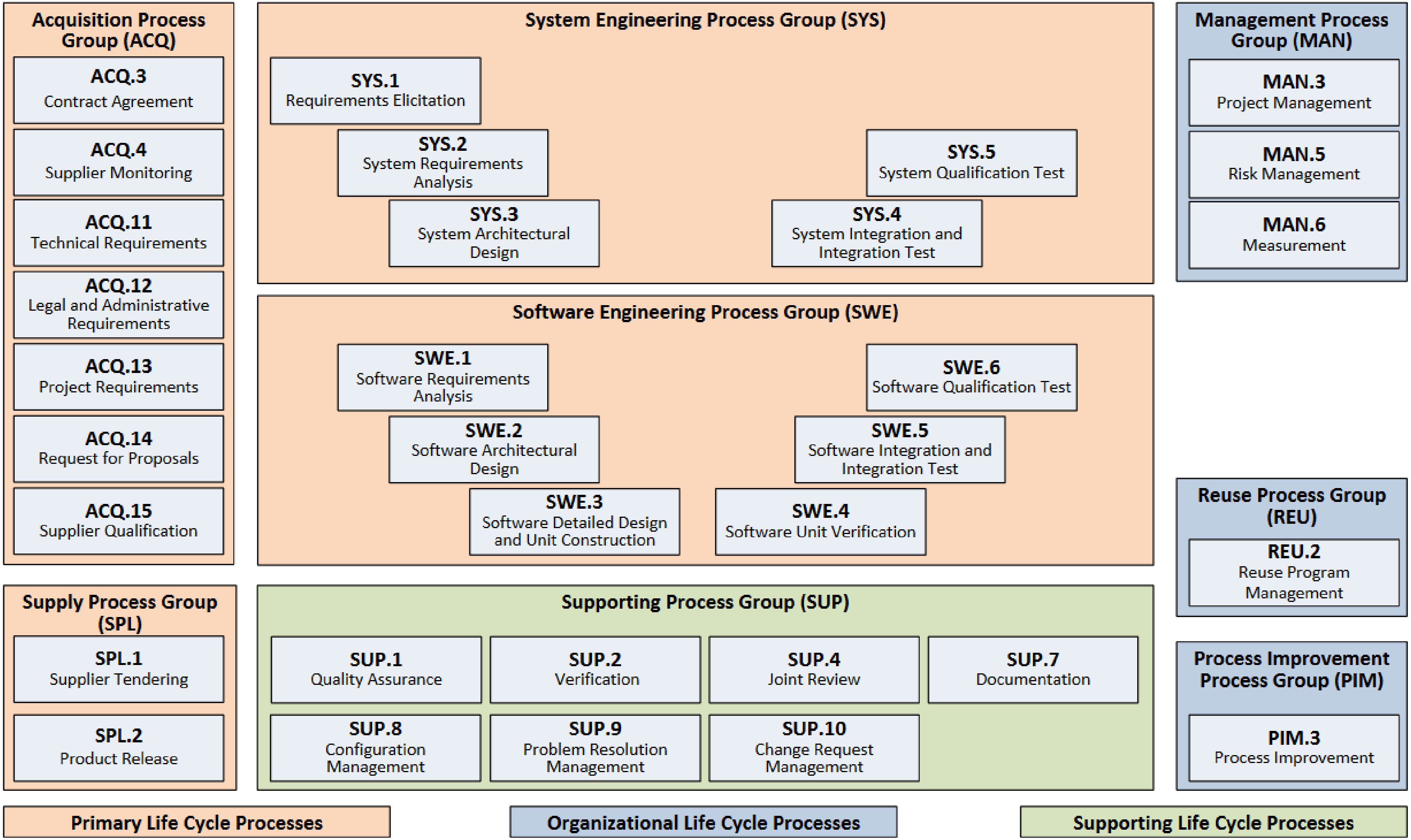
- The purpose of Automotive SPICE is the evaluation of the performance potential of the development processes of ECU suppliers inthe automotive industry.

- Automotive SPICE was developed in 2001 by AUTOSIG (Automotive Special Interest Group). AUTOSIG includes Audi, BMW, Daimler, Porsche, Volkswagen, Fiat, Ford, Jaguar, Land Rover, Volvo…

- For Automotive SPICE execution, the requirements of ISO/IEC 33020:2015 and relevant, such as competence of the leading assessor, created documentation, required action items.

Read-along & source: https://www.i-q.de/leistungen/iso-26262-fsm-und-fusi/fusi-asil-klassifikationen/

Taxonomy and safety analysis methods for AV on-road safety



Acquisition Process Group (ACQ)

- **ACQ.3** Contract Agreement
- **ACQ.4** Supplier Monitoring
- **ACQ.11** Technical Requirements
- **ACQ.12** Legal and Administrative Requirements
- **ACQ.13** Project Requirements
- **ACQ.14** Request for Proposals
- **ACQ.15** Supplier Qualification

System Engineering Process Group (SYS)

- **SYS.1** Requirements Elicitation
- **SYS.2** System Requirements Analysis
- **SYS.3** System Architectural Design
- **SYS.4** System Integration and Integration Test
- **SYS.5** System Qualification Test

Software Engineering Process Group (SWE)

- **SWE.1** Software Requirements Analysis
- **SWE.2** Software Architectural Design
- **SWE.3** Software Detailed Design and Unit Construction
- **SWE.4** Software Unit Verification
- **SWE.5** Software Integration and Integration Test
- **SWE.6** Software Qualification Test

Management Process Group (MAN)

- **MAN.3** Project Management
- **MAN.5** Risk Management
- **MAN.6** Measurement

Reuse Process Group (REU)

- **REU.2** Reuse Program Management

Supply Process Group (SPL)

- **SPL.1** Supplier Tendering
- **SPL.2** Product Release

Supporting Process Group (SUP)

- **SUP.1** Quality Assurance
- **SUP.2** Verification
- **SUP.4** Joint Review
- **SUP.7** Documentation
- **SUP.8** Configuration Management
- **SUP.9** Problem Resolution Management
- **SUP.10** Change Request Management

Process Improvement Process Group (PIM)

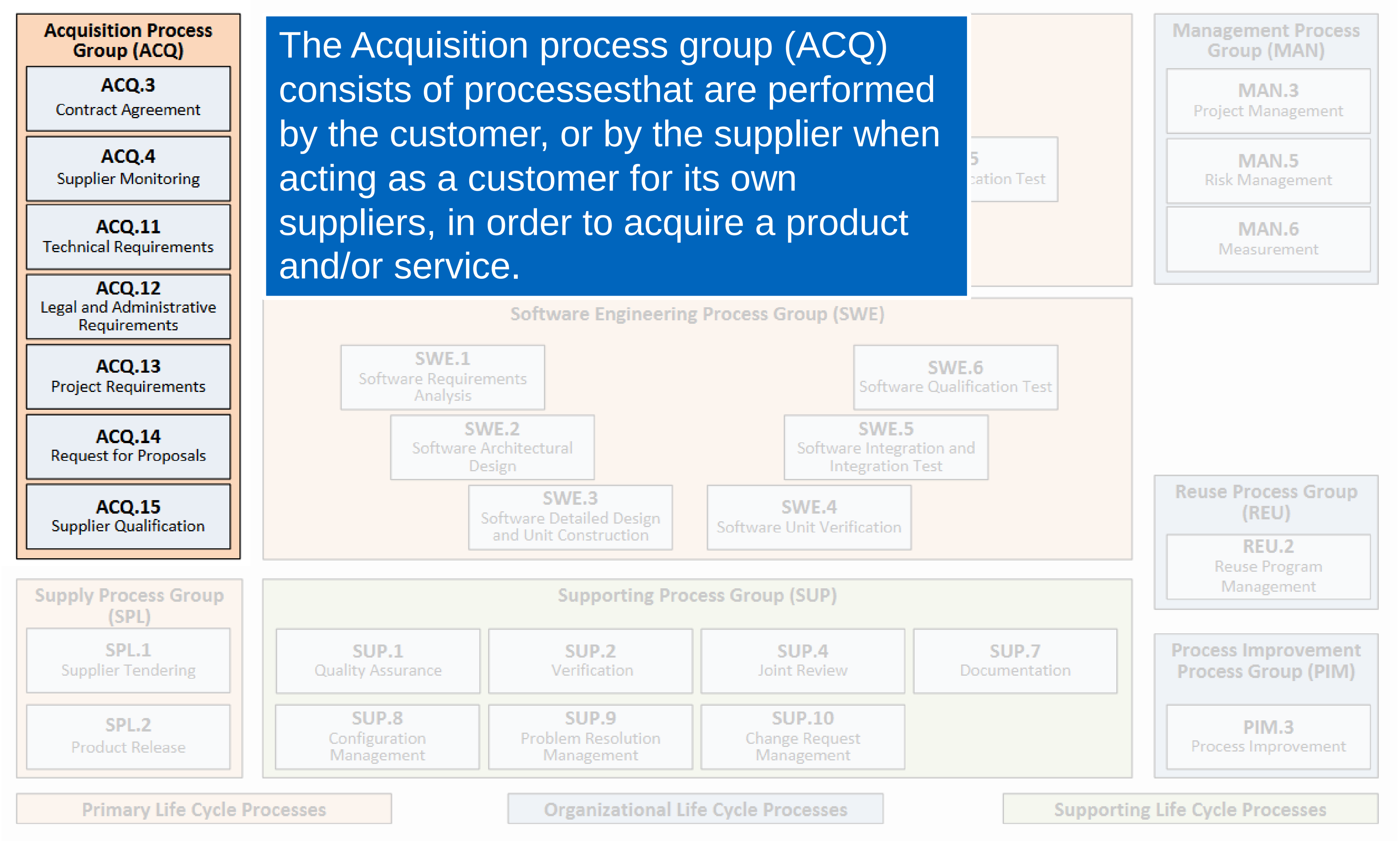
- **PIM.3** Process Improvement

Primary Life Cycle Processes | **Organizational Life Cycle Processes** | **Supporting Life Cycle Processes**

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety

The Acquisition process group (ACQ) consists of processesthat are performed by the customer, or by the supplier when acting as a customer for its own suppliers, in order to acquire a product and/or service.



Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

5 ation Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

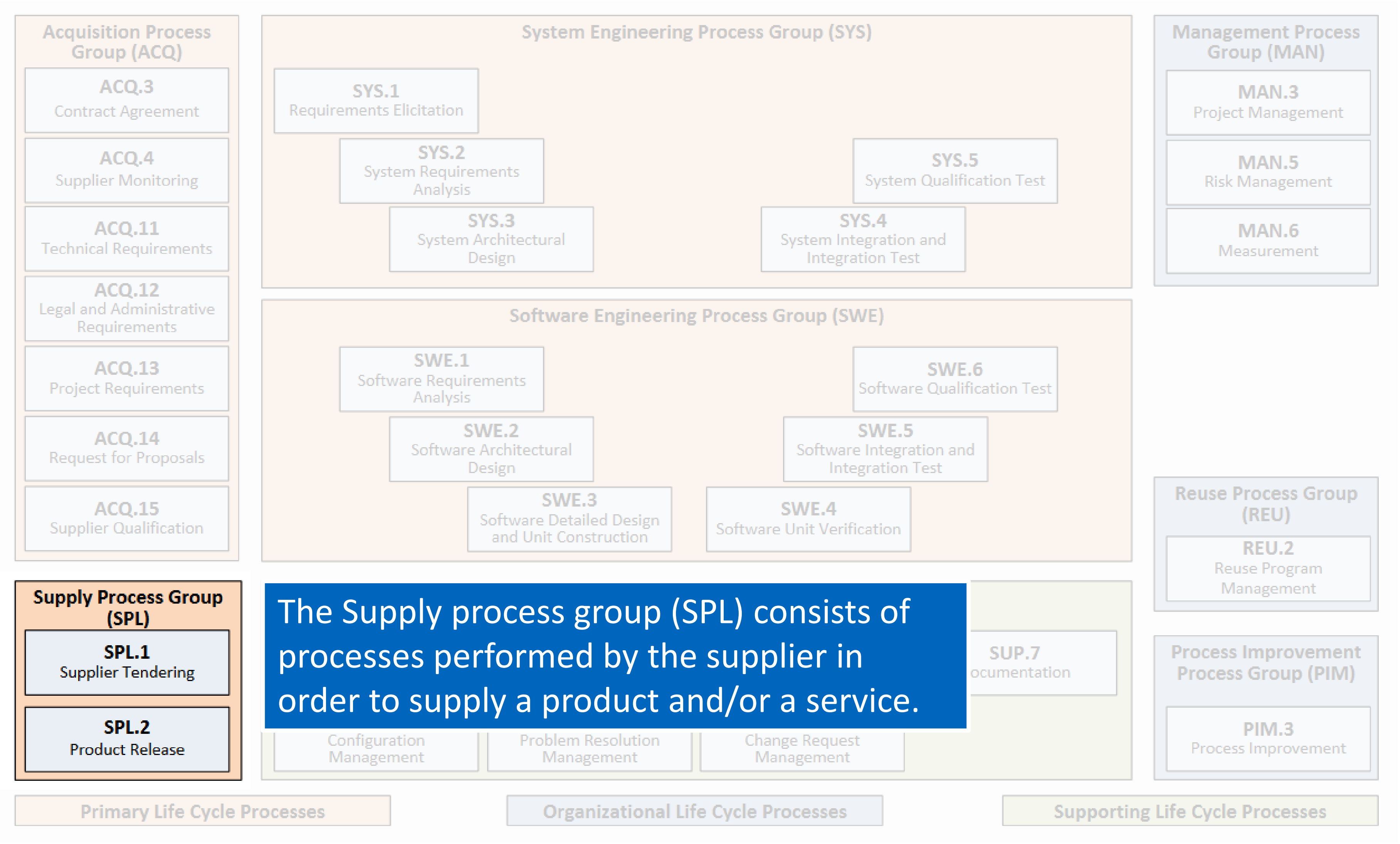
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety



Acquisition Process Group (ACQ)
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)
- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Management Process Group (MAN)
- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement

Software Engineering Process Group (SWE)
- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Reuse Process Group (REU)
- REU.2 Reuse Program Management

Supply Process Group (SPL)
- **SPL.1** Supplier Tendering
- **SPL.2** Product Release

The Supply process group (SPL) consists of processes performed by the supplier in order to supply a product and/or a service.

- SUP.7 ocumentation
- Configuration Management
- Problem Resolution Management
- Change Request Management

Process Improvement Process Group (PIM)
- PIM.3 Process Improvement

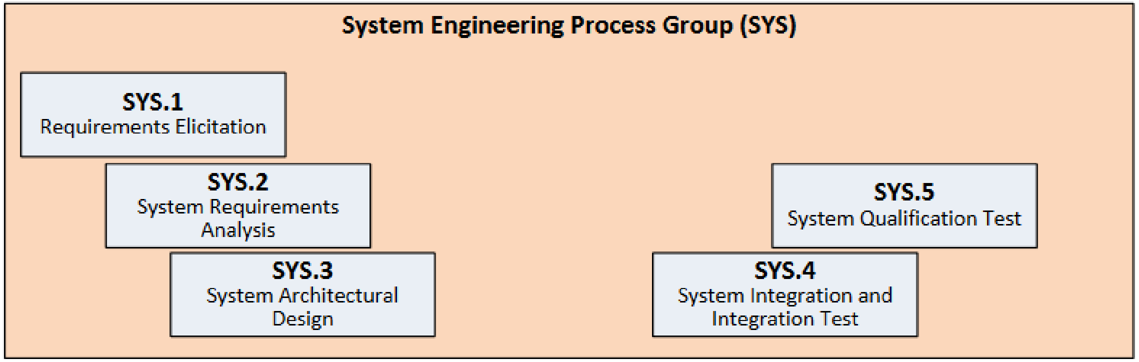
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety

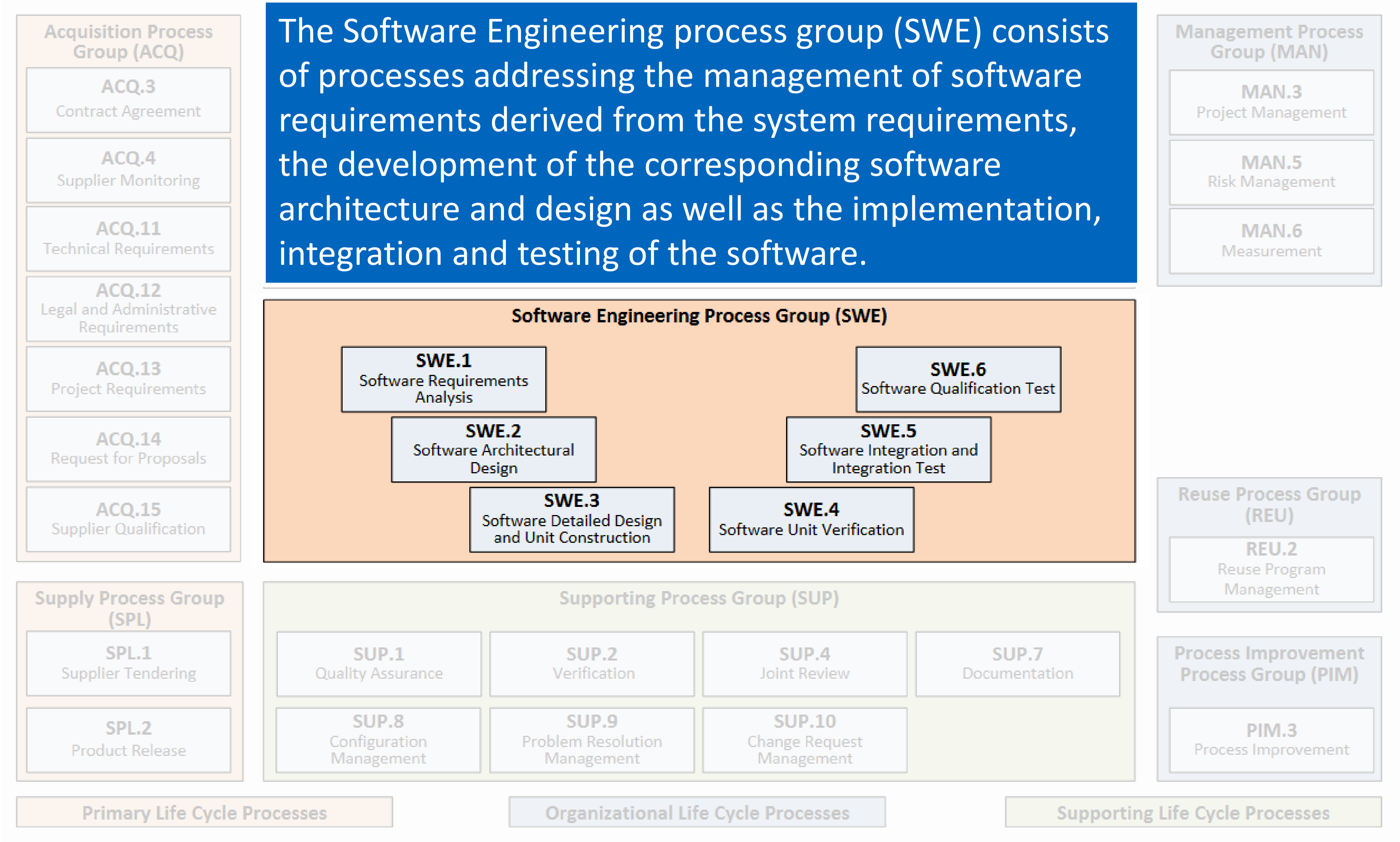

System Engineering Process Group (SYS)
SYS.1
Requirements Elicitation
SYS.2
System Requirements Analysis
SYS.3
System Architectural Design
SYS.4
System Integration and Integration Test
SYS.5
System Qualification Test

The System Engineering process group (SYS) consistsof processes addressing the elicitation and management of customer and internal requirements, the definition of the system architecture and the integration and testing on the system level.

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety

The Software Engineering process group (SWE) consists of processes addressing the management of software requirements derived from the system requirements, the development of the corresponding software architecture and design as well as the implementation, integration and testing of the software.



Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

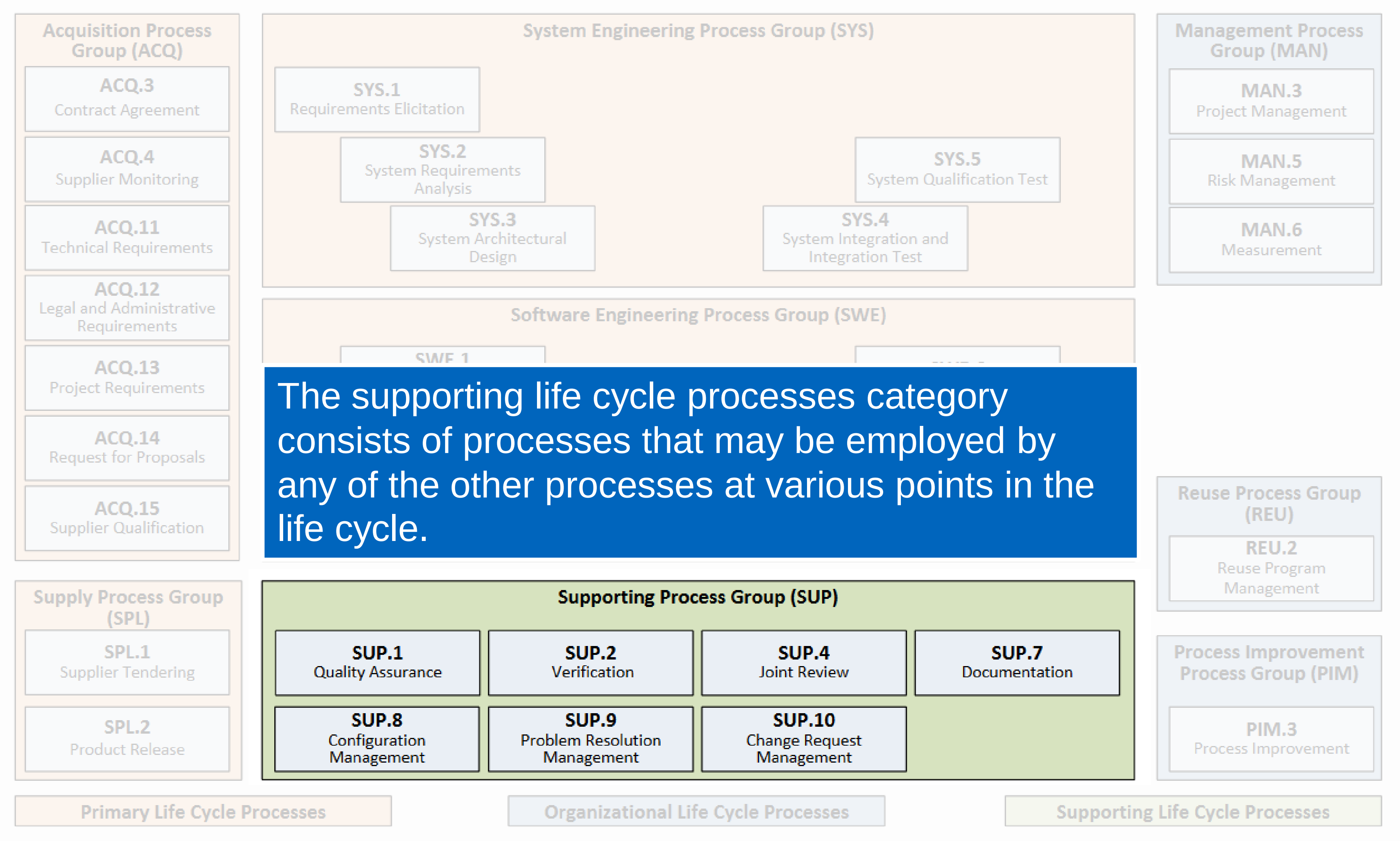
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

VDA Automotive SPICE 3.0

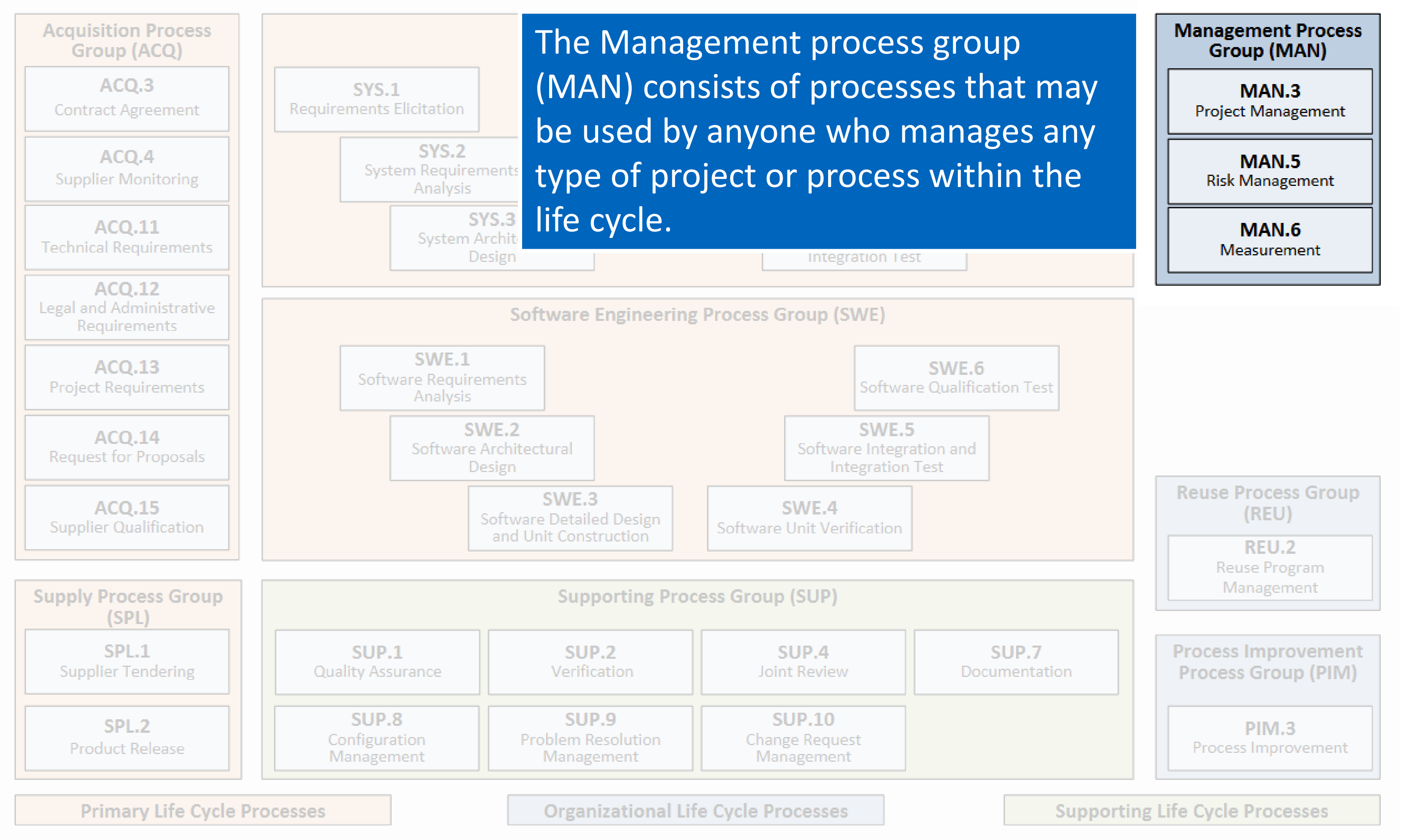
Taxonomy and safety analysis methods for AV on-road safety


Acquisition Process Group (ACQ)
ACQ.3 Contract Agreement
ACQ.4 Supplier Monitoring
ACQ.11 Technical Requirements
ACQ.12 Legal and Administrative Requirements
ACQ.13 Project Requirements
ACQ.14 Request for Proposals
ACQ.15 Supplier Qualification
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.3 System Architectural Design
SYS.4 System Integration and Integration Test
SYS.5 System Qualification Test
Management Process Group (MAN)
MAN.3 Project Management
MAN.5 Risk Management
MAN.6 Measurement
Software Engineering Process Group (SWE)
SWE.1
Reuse Process Group (REU)
REU.2 Reuse Program Management
Supply Process Group (SPL)
SPL.1 Supplier Tendering
SPL.2 Product Release
Supporting Process Group (SUP)
SUP.1 Quality Assurance
SUP.2 Verification
SUP.4 Joint Review
SUP.7 Documentation
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
Process Improvement Process Group (PIM)
PIM.3 Process Improvement
Primary Life Cycle Processes
Organizational Life Cycle Processes
Supporting Life Cycle Processes

The supporting life cycle processes category consists of processes that may be employed by any of the other processes at various points in the life cycle.

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety



The Management process group (MAN) consists of processes that may be used by anyone who manages any type of project or process within the life cycle.

Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

SYS.1 Requirements Elicitation

SYS.2 System Requirements Analysis

SYS.3 System Archit Design

Integration Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

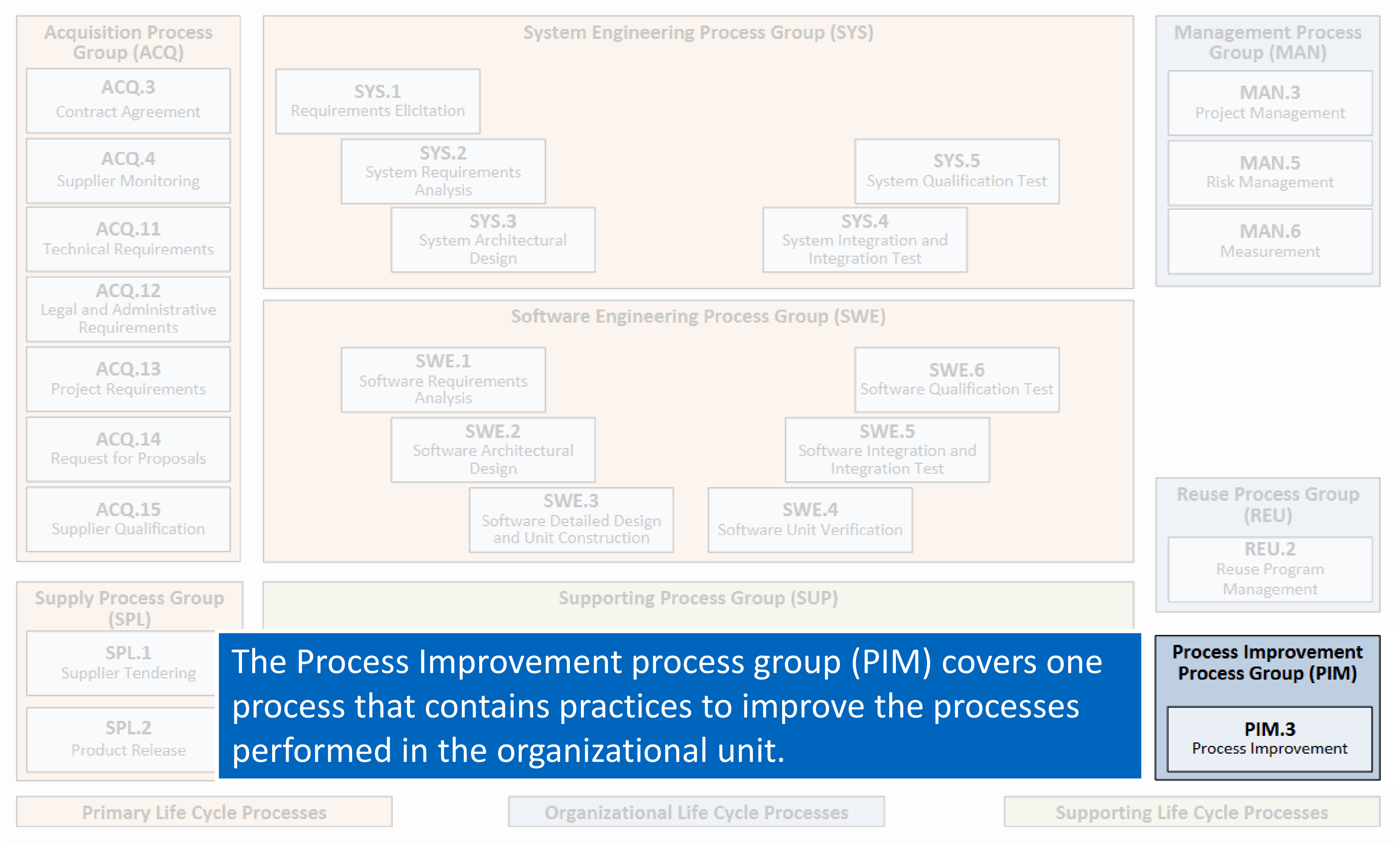
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety



Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)

SYS.1 Requirements Elicitation

SYS.2 System Requirements Analysis

SYS.3 System Architectural Design

SYS.4 System Integration and Integration Test

SYS.5 System Qualification Test

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural Design

SWE.3 Software Detailed Design and Unit Construction

SWE.4 Software Unit Verification

SWE.5 Software Integration and Integration Test

SWE.6 Software Qualification Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Group (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

Supporting Process Group (SUP)

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

Primary Life Cycle Processes

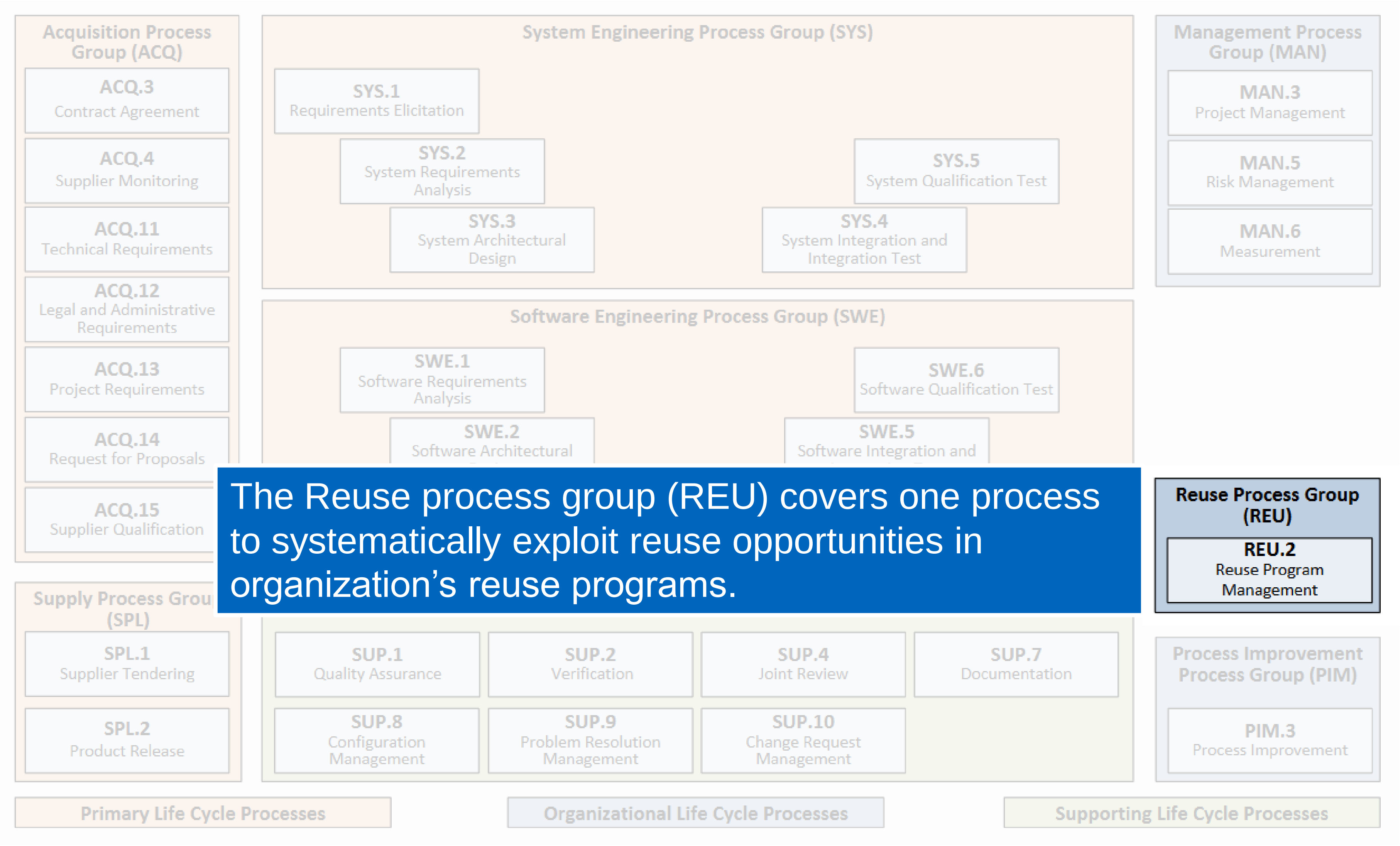
Organizational Life Cycle Processes

Supporting Life Cycle Processes

The Process Improvement process group (PIM) covers one process that contains practices to improve the processes performed in the organizational unit.

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety



Acquisition Process Group (ACQ)

ACQ.3 Contract Agreement

ACQ.4 Supplier Monitoring

ACQ.11 Technical Requirements

ACQ.12 Legal and Administrative Requirements

ACQ.13 Project Requirements

ACQ.14 Request for Proposals

ACQ.15 Supplier Qualification

System Engineering Process Group (SYS)

SYS.1 Requirements Elicitation

SYS.2 System Requirements Analysis

SYS.3 System Architectural Design

SYS.4 System Integration and Integration Test

SYS.5 System Qualification Test

Management Process Group (MAN)

MAN.3 Project Management

MAN.5 Risk Management

MAN.6 Measurement

Software Engineering Process Group (SWE)

SWE.1 Software Requirements Analysis

SWE.2 Software Architectural

SWE.5 Software Integration and

SWE.6 Software Qualification Test

The Reuse process group (REU) covers one process to systematically exploit reuse opportunities in organization’s reuse programs.

Reuse Process Group (REU)

REU.2 Reuse Program Management

Supply Process Grou (SPL)

SPL.1 Supplier Tendering

SPL.2 Product Release

SUP.1 Quality Assurance

SUP.2 Verification

SUP.4 Joint Review

SUP.7 Documentation

SUP.8 Configuration Management

SUP.9 Problem Resolution Management

SUP.10 Change Request Management

Process Improvement Process Group (PIM)

PIM.3 Process Improvement

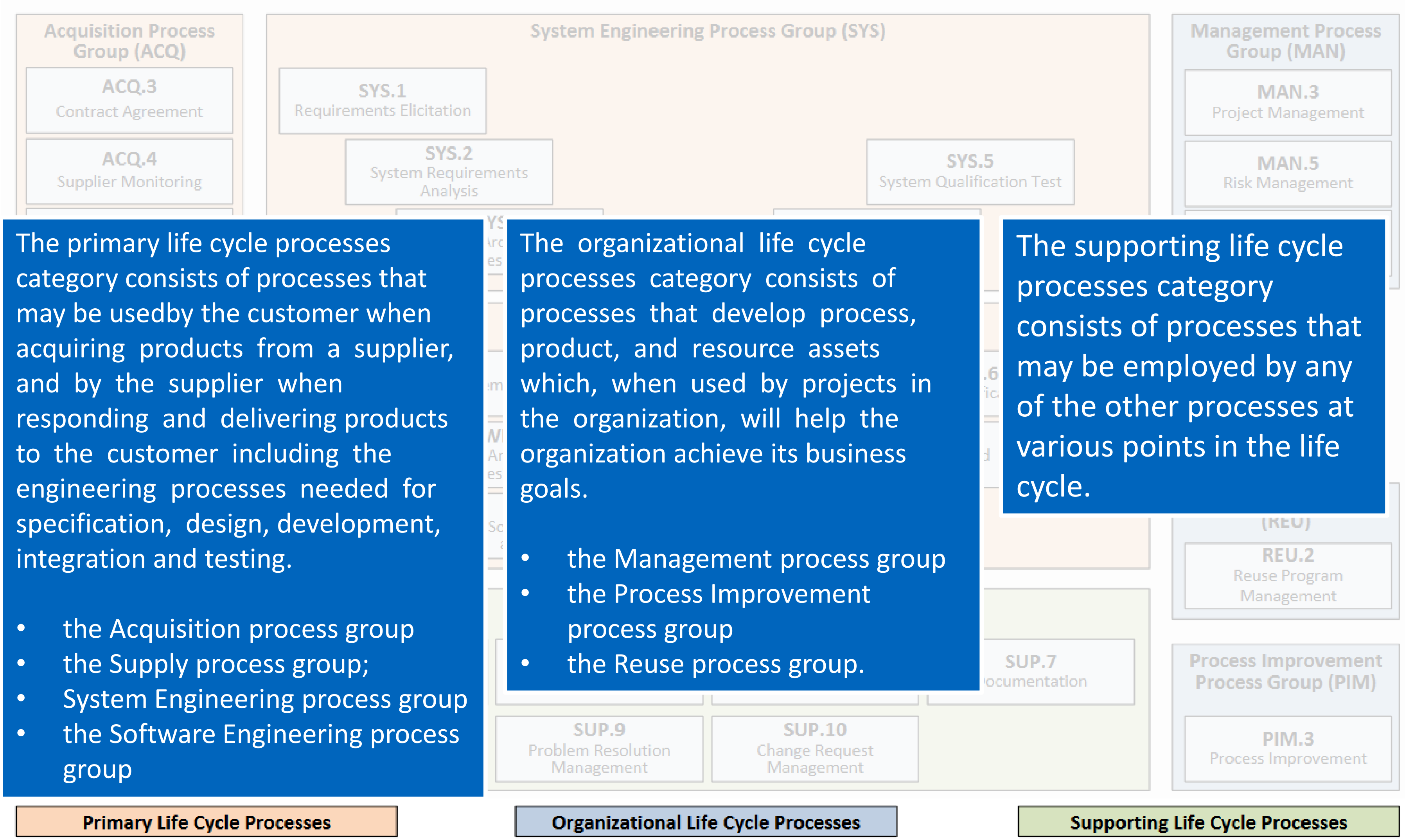
Primary Life Cycle Processes

Organizational Life Cycle Processes

Supporting Life Cycle Processes

VDA Automotive SPICE 3.0

Taxonomy and safety analysis methods for AV on-road safety


Acquisition Process Group (ACQ)
ACQ.3 Contract Agreement
ACQ.4 Supplier Monitoring
System Engineering Process Group (SYS)
SYS.1 Requirements Elicitation
SYS.2 System Requirements Analysis
SYS.5 System Qualification Test
Management Process Group (MAN)
MAN.3 Project Management
MAN.5 Risk Management
(REU)
REU.2 Reuse Program Management
SUP.7 Documentation
SUP.9 Problem Resolution Management
SUP.10 Change Request Management
Process Improvement Process Group (PIM)
PIM.3 Process Improvement
Primary Life Cycle Processes
Organizational Life Cycle Processes
Supporting Life Cycle Processes

The primary life cycle processes category consists of processes that may be usedby the customer when acquiring products from a supplier, and by the supplier when responding and delivering products to the customer including the engineering processes needed for specification, design, development, integration and testing.

- the Acquisition process group
- the Supply process group;
- System Engineering process group
- the Software Engineering process group

The organizational life cycle processes category consists of processes that develop process, product, and resource assets which, when used by projects in the organization, will help the organization achieve its business goals.

- the Management process group
- the Process Improvement process group
- the Reuse process group.

The supporting life cycle processes category consists of processes that may be employed by any of the other processes at various points in the life cycle.

VDA Automotive SPICE 3.0

ASIL Levels

- **Functional Safety / Funktionale Sicherheit (FuSi)**
- Introduction only, check exact standards when applying.
- **Severity S**
  - S0: No injuries (~unharmed)
  - S1: Light injuries to medium injuries (~injured body part)
  - S2: Serious injuriest, survival very likely (~lost body part)
  - S3: Critical injuries, survival unlikely (~lost head)

Read-along & source: https://www.i-q.de/leistungen/iso-26262-fsm-und-fusi/fusi-asil-klassifikationen/

ASIL Levels

- **Functional Safety / Funktionale Sicherheit (FuSi)**

- **Exposure E**

  - E1: rare event (car stuck on railroad crossing)
  - E2: sometimes occurs gelegentliches Auftreten (Driving with roof rack)
  - E3: happens often (vehicle refueling, wet road)
  - E4: happens all the time (acceleratingg, braking, steering)

  - Distinction according to duration (duration of occurance in driving situation) and frequency (frequency of the occurance of the according driving situation)

ASIL Levels

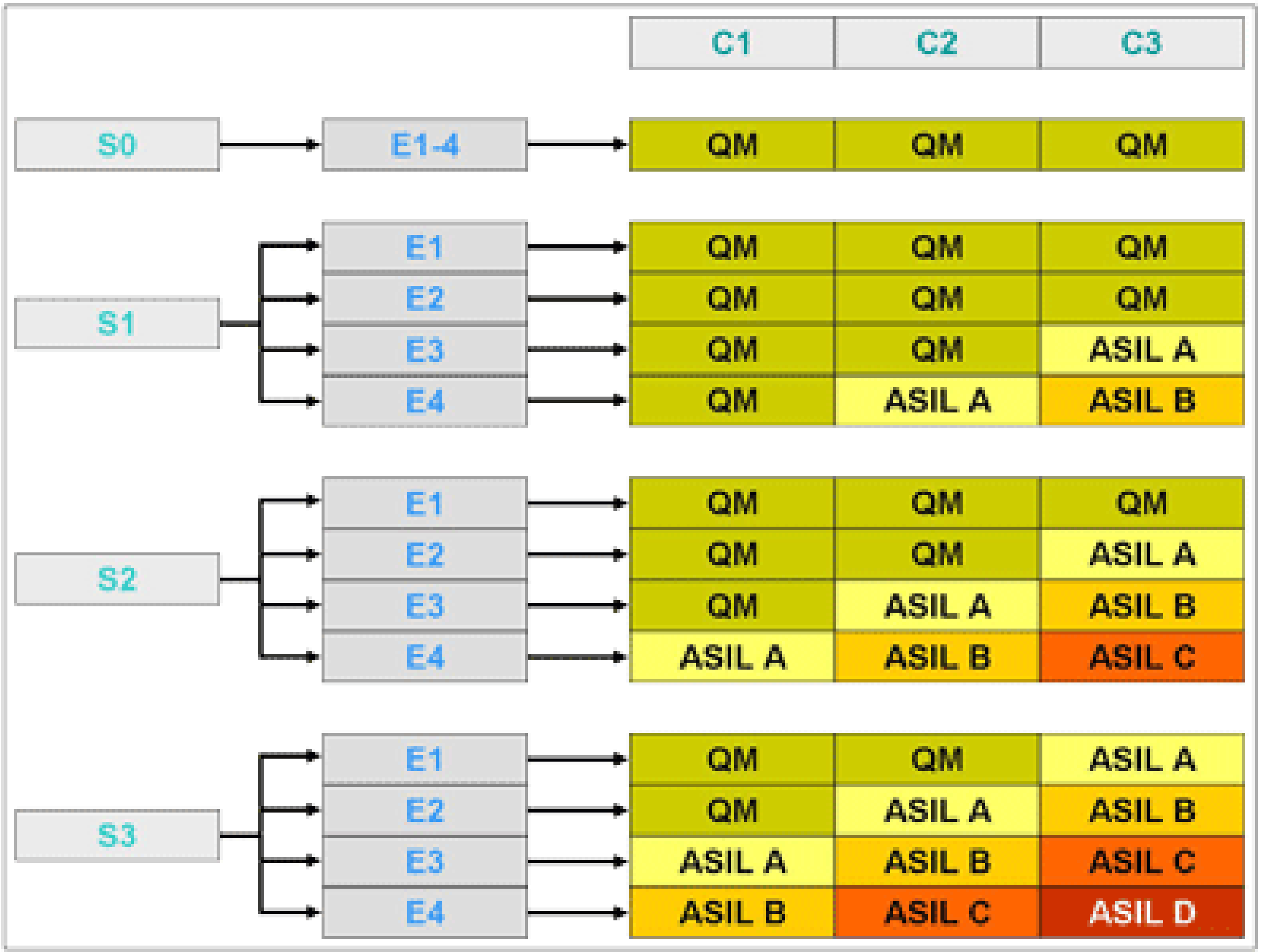
- **Functional Safety / Funktionale Sicherheit (FuSi)**

- **Controllabiolity C**

  - C0: safe control (Every driver can manage this situation, example: unintended increase of radio volume)
  - C1: simple control (more than 99% of the drivers can manage the situation, example: steering wheel being a little bit harder to turn during vehicle start)
  - C2: normal control (more than 90$ of the drivers can manage the situation, example: no ABS during emergency braking)
  - C3: difficult control (less than 90% of the drivers can manage the situation, example: suddenly occuring steering forces)

ASIL Levels

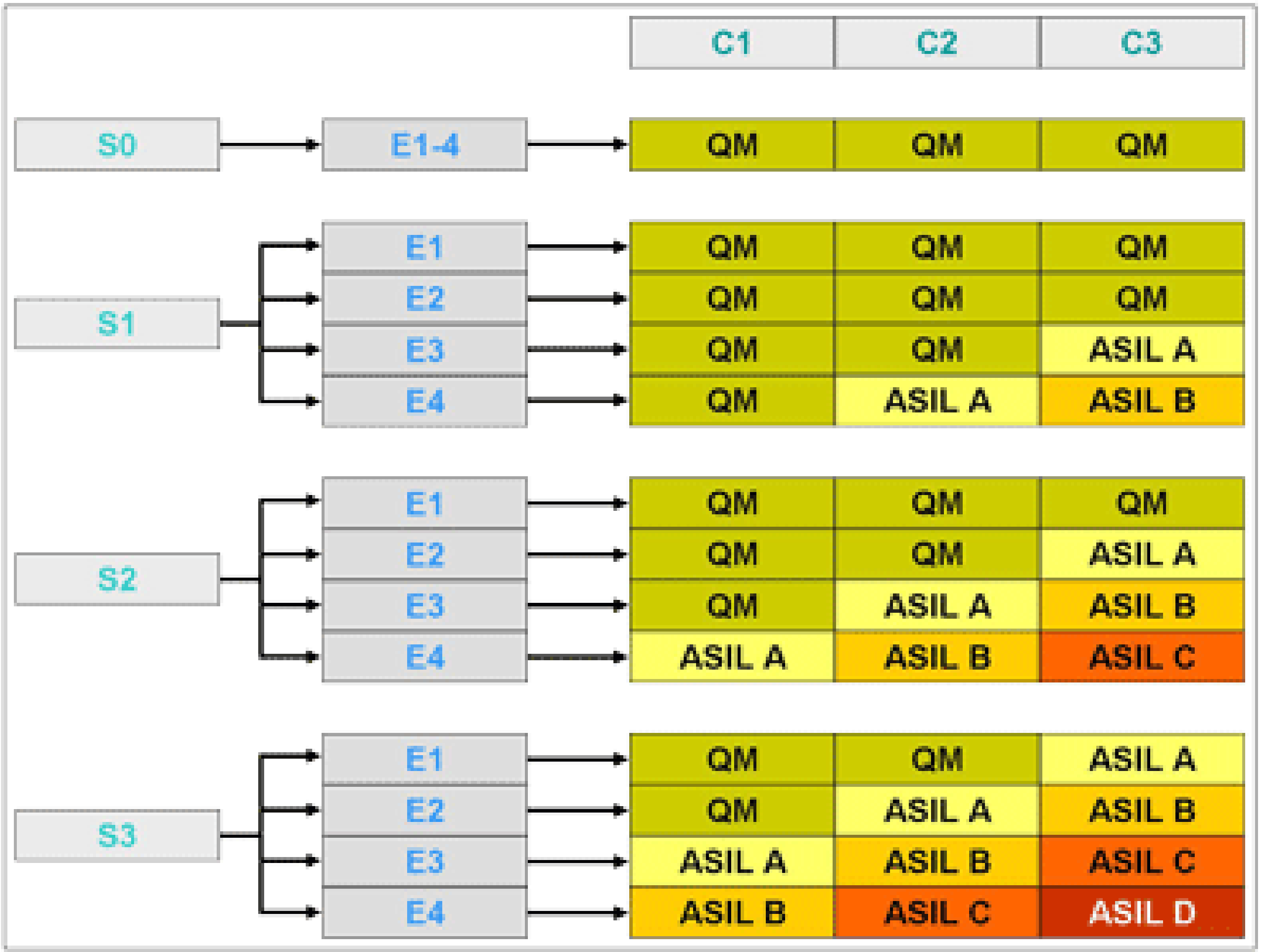
- Risk graph for choosing ASIL category.
- Choose sub categories and add numbers
  - S2+E2+C3 = 7 = ASIL A
  - Exception S0, as no injury does not indicate functional safety relevance
- 10 Points => ASIL D
- 9 Points => ASIL C
- 8 Points => ASIL B
- 7 Points => ASIL A
- QM: Quality management (ISO/TS 16949)



		C1	C2	C3
S0	E1-4	QM	QM	QM
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

ASIL Levels

- **ASIL A:** recommended failure probability less than 10E-6 / hour
- **ASIL B:** recommended failure probability less than 10E-7 / hour
- **ASIL C:** required failure probability less than 10E-7/hour
- **ASIL D:** required failure probability less than 10E-8 / hour
- Gap from B to C to dual channel requirements and requirement instead of recommendation.



		C1	C2	C3
S0	E1-4	QM	QM	QM
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

ASIL Levels

- **ASIL decomposition**

- **Asil decomposition:** *apportioning of safety requirements redundantly to sufficiently independent elements (1.32), with the objective of reducing the ASIL (1.6) of the redundant safety requirements that are allocated to the corresponding elements*

- Illustration:
  - QM (X) replace with 0
  - ASIL A(X) replace with 1
  - ASIL B(X) replace with 2
  - ASIL C(X) replace with 3
  - ASIL D(X) replace with 4

- Sum of decomposed elements must equal value of original.
  - ASIL D = ASIL A(D) + ASIL C(D) = 4 = 3 + 1
  - ASIL D = ASIL A(D) + ASIL A(D) + ASIL A(D) + ASIL A(D)

ASIL Levels

- **ASIL decomposition**

- ASIL A(D) is not ASIL A, but special requirements have to be realized

- Example: Decomposed elements using shared components require dependent error analysis to prevent systematic errors.
  - criteria for co-existence
  - freedom from interference
  - cascading failures (the failure of one or few parts can trigger the failure of other parts)
  - dependent failures
  - common cause failures

- Further requirements exist, compare standards.

Additional material: Politecnico di Milano: Dependent Failures

ASIL Levels

- **cascading failures**
  - the failure of one or few parts can trigger the failure of other parts)
  - several component share a common load
  - 1 component failure may lead to increase load on the remaining ones
  - increased likelihood of failure

Additional material: Politecnico di Milano: Dependent Failures

ASIL Levels

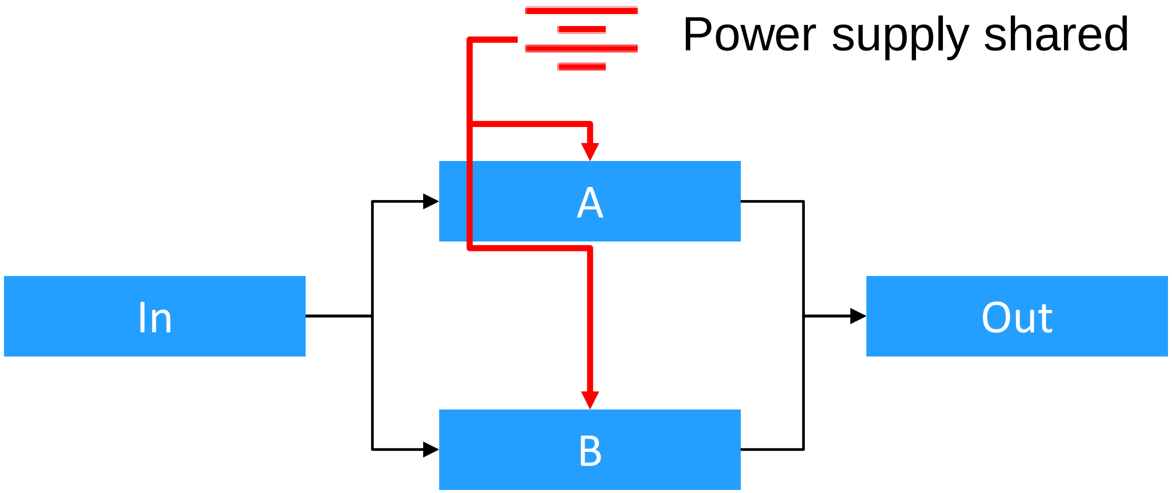
- **common cause failures (CCF)**
  - multiple failures that result directly from a common or shared root cause
  - Example: Extreme enviromental conditions
  - Example: Failure of a piece of hardware external to the system
  - Example: Human Error (operational or maintenance)

Additional material: Politecnico di Milano: Dependent Failures

ASIL Levels

Dependant failure example:

$$P(A \cap B) \neq P(A) \cdot P(B)$$



ASIL Levels

Dependant failure example:

$$P(A \cap B) \neq P(A) \cdot P(B)$$

Positive dependance: $P(A|B) > P(A)$ and $P(B|A) > P(B)$

Negative dependance: $P(A|B) < P(A)$ and $P(B|A) < P(B)$

ASIL Levels

- **ASIL decomposition vs monitoring**
- **Decomposition:** Both components can safely handle the scenario
- **Monitoring:** One module detects an error and informs other modules about it, but the monitoring module can not handle the scenario itself