excellence in dependable automation

Conduct safety assessment for autonomous driving car in Dubai

Bentley Lin

Managing Director

exida Safety Systems
(Shanghai) Co., Ltd

Bentley.Lin@exida.com

Sep 2019, Shanghai / China

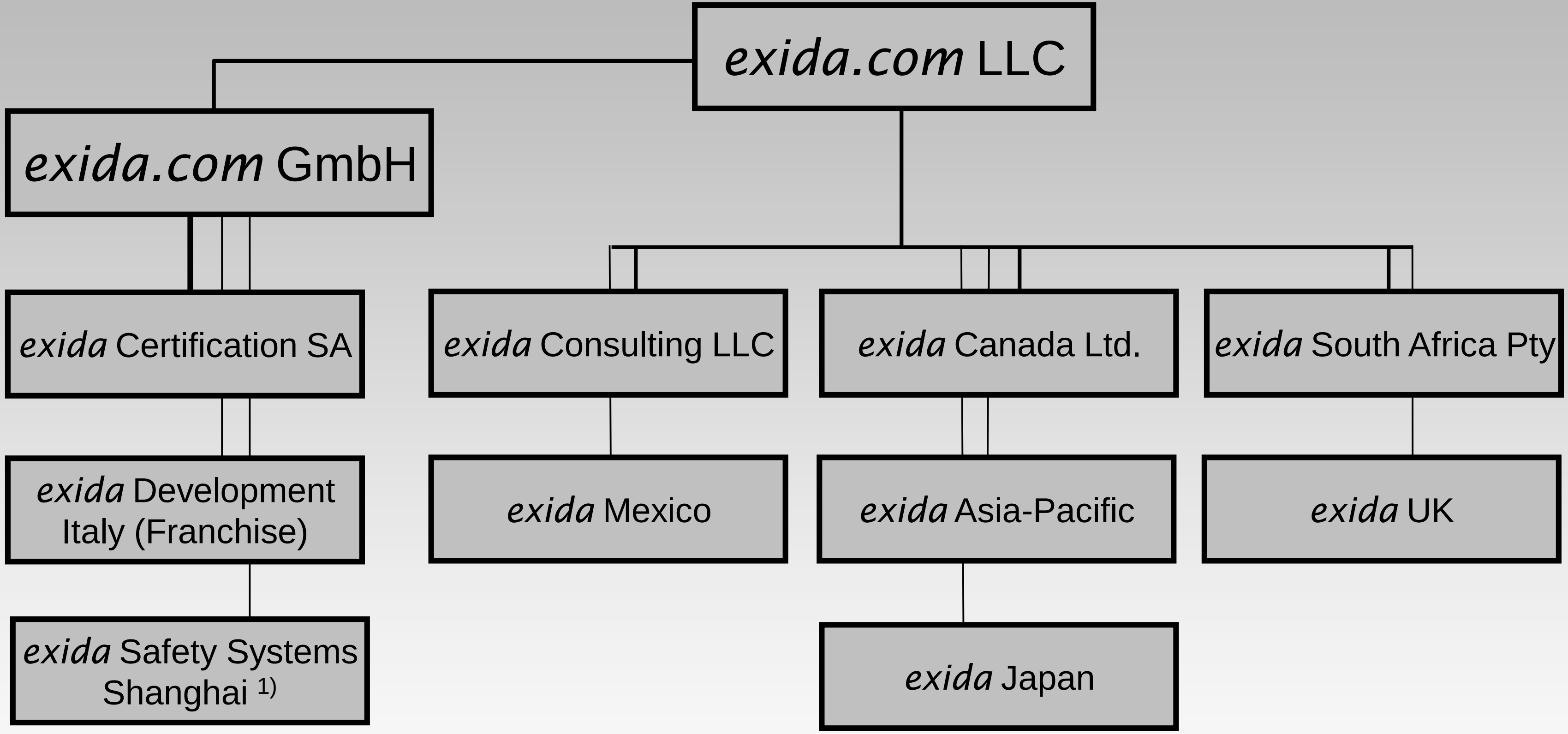
Outline

- *exida* – Company Introduction
- Autonomous Driving car application scenario in Dubai
- Why is safety assessment needed for autonomous driving car?
- Safety assessment for autonomous driving car, topics to be addressed
  - SOTIF
  - Functional Safety
  - Cyber security
  - Others
- Managing complexities of assessment- certified building block
- Deviation closures and pass of assessment
- *exida* strength in Safety

excellence in dependable automation

COMPANY INTRODUCTION

exida Company Structure



exida.com LLC

exida.com GmbH

exida Certification SA

exida Development Italy (Franchise)

exida Safety Systems Shanghai [1]

exida Consulting LLC

exida Mexico

exida Canada Ltd.

exida Asia-Pacific

exida Japan

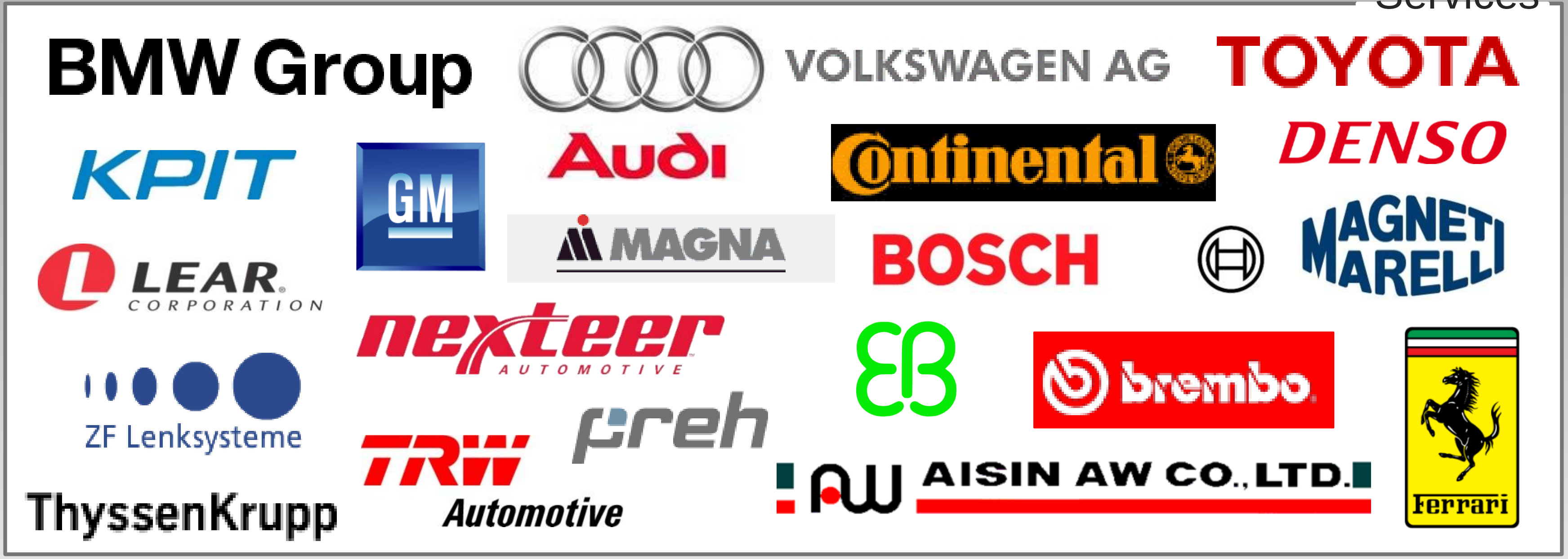
exida South Africa Pty

exida UK

[1] Company registration completed in Aug, 2016

exida Automotive Customers

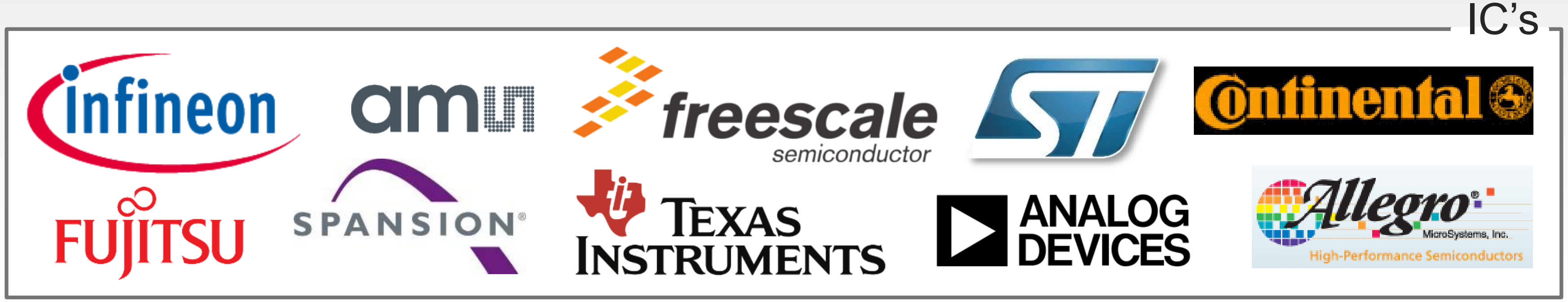
Services



Tools

DAIMLER
DENSO Japan
JasPar
CATARC

IC's



and more …

exida Automotive Customers

- Our experiences in Autonomous Driving
  - OEMs- complete vehicle functions and systems
  - T1s- Controlling box
  - T2s- Sensors, SW components, SOCs/ ASICs…etc

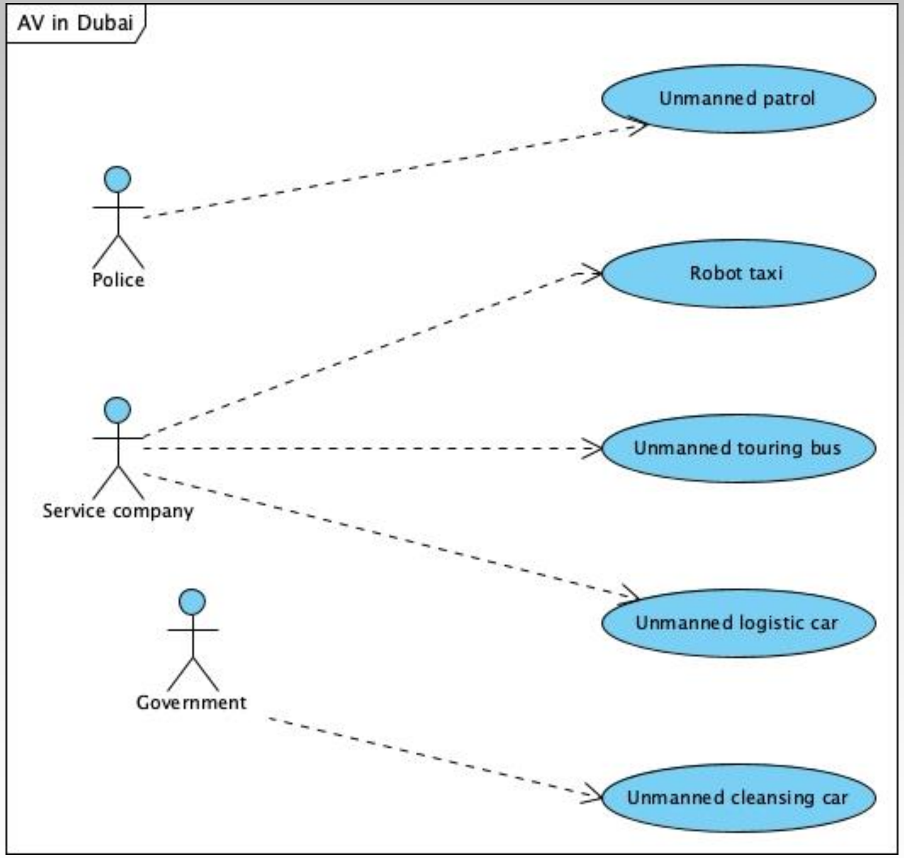
exida®

excellence in dependable automation

AUTONOMOUS DRIVING CAR APPLICATION SCENARIO IN DUBAI

Autonomous Driving car application scenario in Dubai

- There are several possible scenarios in deploying AV in Dubai:



Autonomous Driving car application scenario in Dubai

- New technologies, meaning:
  - New business opportunities for Dubai (e.g. service providers)
  - More convenient infrastructures set up for Dubai
  - More attractive features in Dubai for tourists
  - More organized and advance city images in Dubai
- BUT, This also implies increasing safety risks in Dubai due to new technologies

Who shall bear the safety liability?
How to minimize the safety liability?
How to ensure satisfactions in public safety?

exida®

excellence in dependable automation

WHY IS SAFETY ASSESSMENT NEEDED FOR AUTONOMOUS DRIVING CAR?

Why is safety assessment needed for autonomous driving car?

- Safety assessment:
  - Mandatory for public transportation including High Speed Rail; Aviation
  - More and more popular in Automotive industry
  - Especially critical for systems with below attributes:
    - High complexities- Plenty of dynamic behaviors and functional dependencies
    - Highly safety critical- for example, ASIL C/D system
- Safety assessment means:
  - “Technically competent” and “Sufficiently independent” assessors are needed (e.g. I1/ I2/ I3 definition in the ISO-26262 standard)
  - **ALL** developers have technical blind spot due to timing/ costs/ knowledge and experience level
  - Safety assessment is used to find out missing details and deviated direction (deviated from state of the art)

Why is safety assessment needed for autonomous driving car?

- About complexities-
  - Autonomous driving car is by far the most complicated automotive systems
    - Introduce new sensors and new technologies (e.g. fusion/ deep learning)
    - Require multi-core and multi-processors (similar to server) to achieve sufficient computation speed. Synchronization, pipelines and concurrency issues are significant
    - Engage almost all critical automotive actuators (e.g. EMS/ MCU/ EPS/ ESP/ TCU…etc)
    - Safety strategies in safety responsibilities allocation (between controller and actuator) is subtle and not obvious

exida®

excellence in dependable automation

SAFETY ASSESSMENT FOR AUTONOMOUS DRIVING CAR, TOPICS TO BE ADDRESSED

Safety assessment for autonomous driving car, topics to be addressed:

- SOTIF- Safety of Target Intended Function
  - Pure functional design, focus on how to ensure the safety when function operates correctly
  - Example: Braking force configuration for autonomous driving vehicle:
    - $\text{BrakeForce}_{\text{MAX}}$ different boundary value leads to different issues -> Front collision (0.5g)/ Rear collision (1g)
    - Brake force pattern (stage-wise force increase) engaged needs to balance:
      - Driver and passengers' comfort
      - Safety aspects- reasonable reaction time; possible consequences when unintended behaviors happen (this needs to interface with FuSa), which will impact controllability in hazardous event

Safety assessment for autonomous driving car, topics to be addressed:

- Functional safety
  - *Everything made by men will fail* – Typical mistake coming from developers: My product will not have issues because of XXX/ YYY
  - Functional safety deals with malfunction behaviors of E/E elements (Besides E/E?)
  - Example:
    - Unintended loss of deceleration (and hit the car in the front)
    - Cause:
      - Faults in sensors
      - Faults in communication bus
      - Faults in fusion algorithm
      - Faults in data storage
      - …etc
    - Safety concepts need to cover all fault sources to certain degrees, also its effectiveness needs to be quantified and evaluated (e.g. CRC length in different bus)

- Cyber security
  - Both of functional safety and cyber security might lead to same hazardous event, for example: Unintended steering
  - But functional safety and cyber security represent different failure cause:
    - Functional safety: hazardous event due to malfunction
    - Cyber security: hazardous event due to hacker attacks
  - A complete security lifecycle and security measures shall be implemented

Safety assessment for autonomous driving car, topics to be addressed:

- Others
  - HMI- Humane Machine Interface:
    - Is the warning message clear and noticeable? (Very critical aspect!)
    - Possibilities in leading foreseeable misuse?
    - Activation/ Deactivation process between humane and machine
    - …etc
    - Humane factor will be an important part for FMEA and safety analysis
  - Data recording
    - Traceable data if accidents happen, for debug and clarify belonging responsibilities
  - …etc (Could refer to Federal Automated Vehicles Policy)

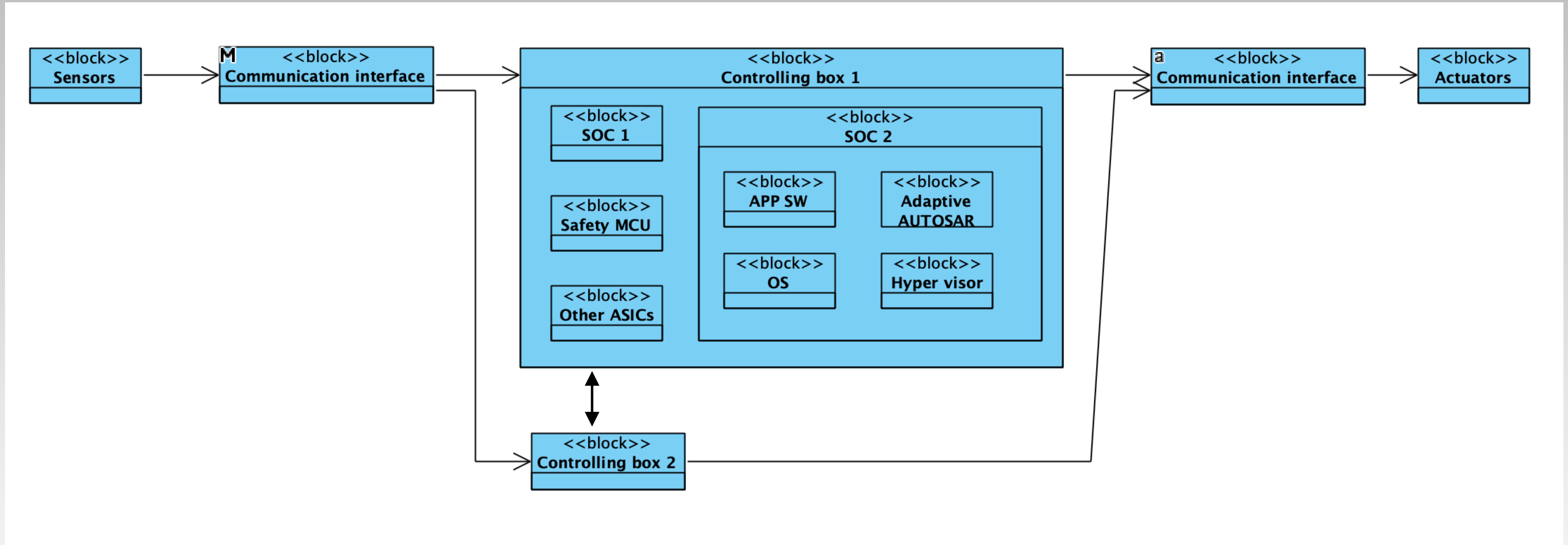
exida®

excellence in dependable automation

MANAGING COMPLEXITIES OF ASSESSMENT-CERTIFIED BUILDING BLOCK

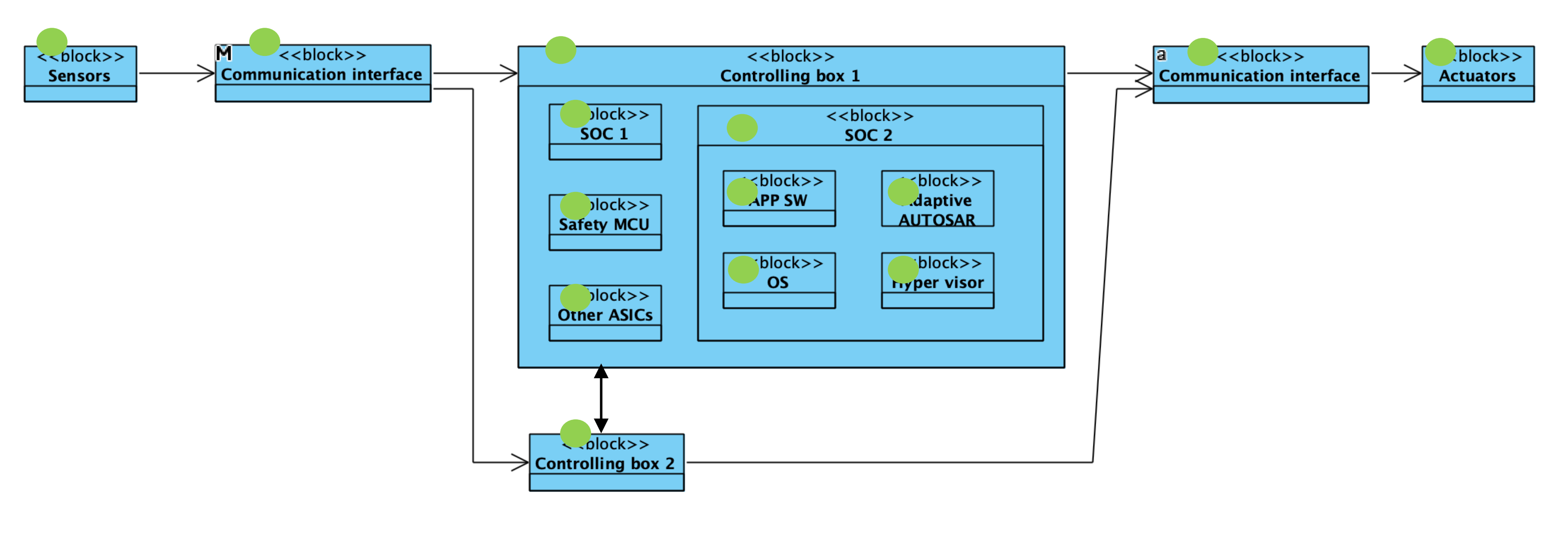
Managing complexities of assessment

- Example building blocks for autonomous driving:



Managing complexities of assessment

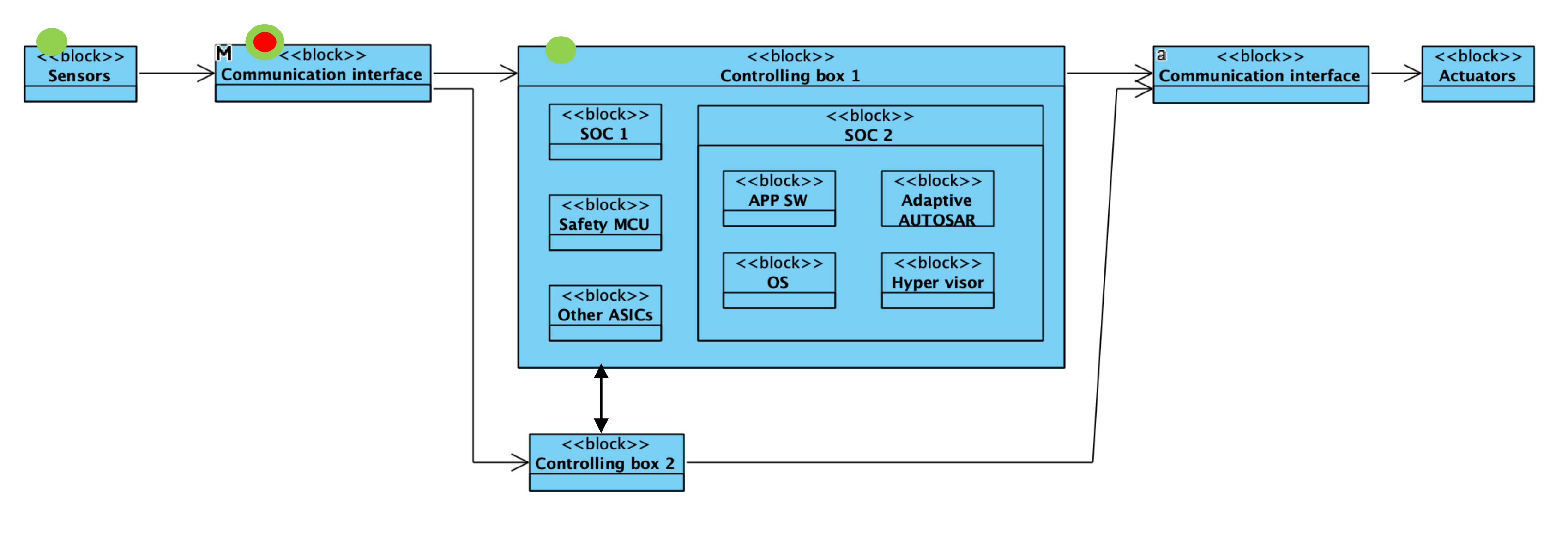
- Safety of the complete systems mean:



Or…

Managing complexities of assessment

- Safety of the complete systems mean:



Managing complexities of assessment

- For complexity management of safety assessment:
  - 60%- Choose certified/ assessed building block
  - 20%- Project-specific elements to be developed according to safety standards (e.g. ISO-26262)
  - 15%- Integration and interface check (Validate AoU of SEooC and external requirements between different elements)
  - 5%- Justification of safety protection for non- safety compliant element- similar to examples in previous page

exida

excellence in dependable automation

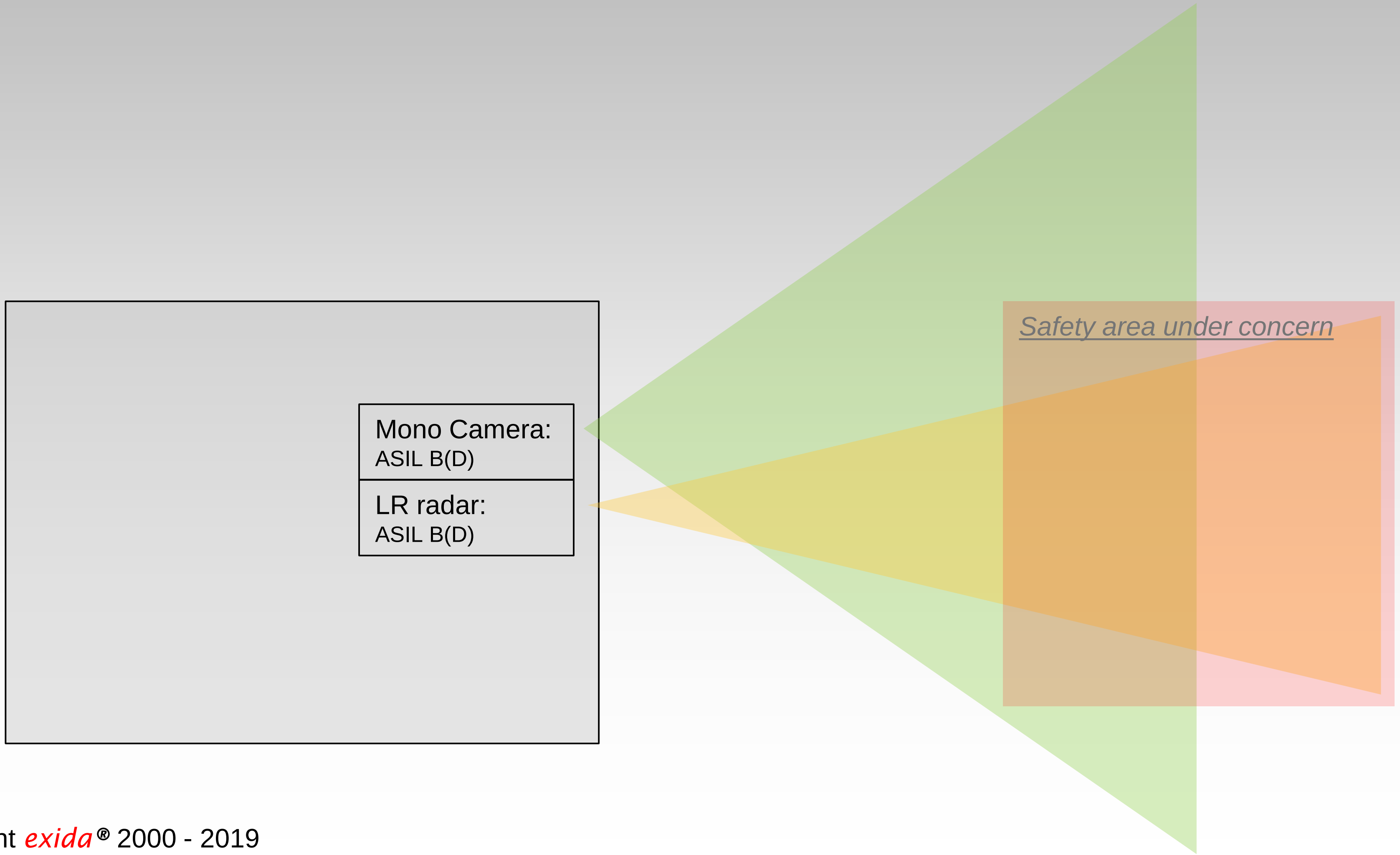
DEVIATION CLOSURES AND PASS OF ASSESSMENT

Deviation closures and pass of assessment

- Pass of assessment means: There is no any deviation from independent assessor’s point of view
- Deviation of assessment/ certification means:
  - Non compliant process/ methodology from existing standard (e.g. SOTIF/ FuSa/ Cyber security), e.g. Incomplete FSM
  - Technical concept is not logically safe or reasonable, e.g. Forbidden transition out of safe state; misleading safe state
  - Foreseeable systematic fault exiting (e.g. bugs in the implementation), e.g. If (conditions)… in the pseudo code are not complete from requirement perspective
  - Analysis or verification results don’t provide correct evidence to support safety design or argument, e.g. Risk matrix over limit in FMEA; existing cut-set 1 event in L3 system
  - Quantitative or qualitative targets are not met, e.g. SPFM/ LFM/ PMHF and other metrics for machine learning are not satisfied
  - Potential risk is above certain level, e.g. missing hazardous event in considering longitudinal control and lateral control together

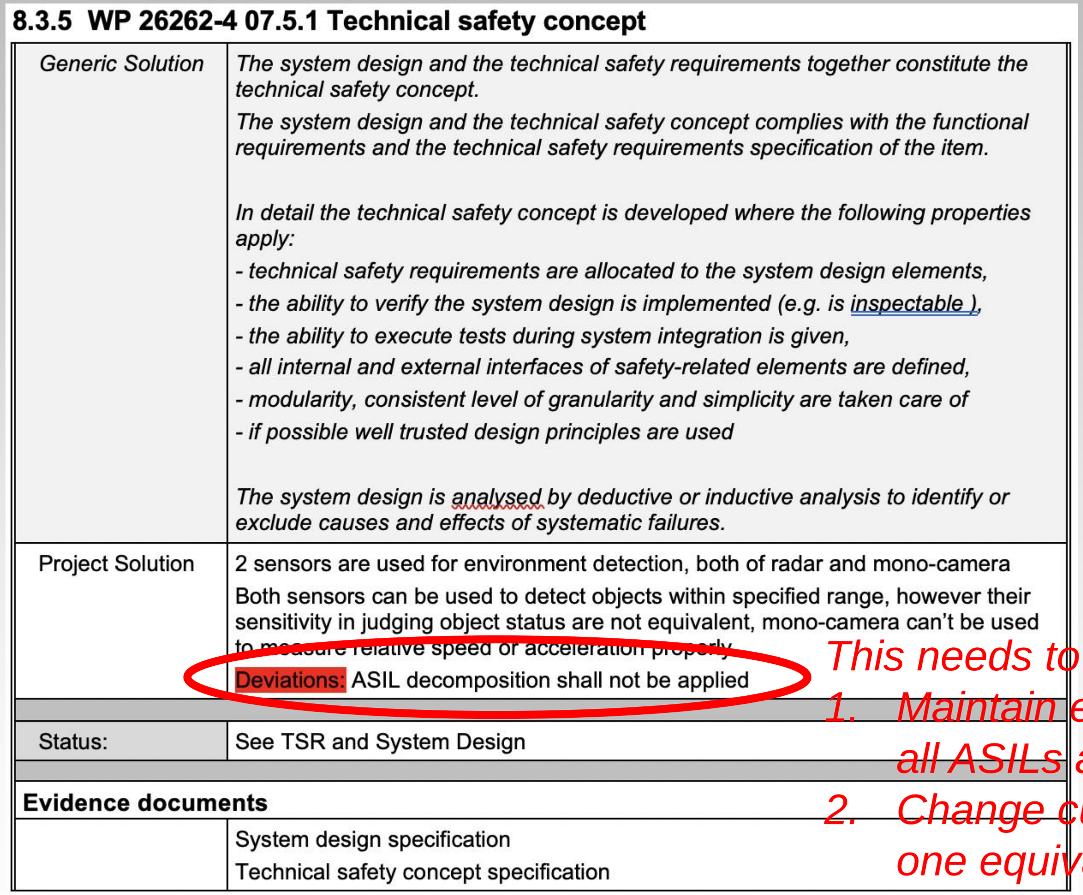
Deviation closures and pass of assessment

- Example case to be assessed- ASIL decomposition:



Deviation closures and pass of assessment

- Example assessment report:



8.3.5 WP 26262-4 07.5.1 Technical safety concept

Generic Solution	*The system design and the technical safety requirements together constitute the technical safety concept.* *The system design and the technical safety concept complies with the functional requirements and the technical safety requirements specification of the item.* *In detail the technical safety concept is developed where the following properties apply:* *- technical safety requirements are allocated to the system design elements,* *- the ability to verify the system design is implemented (e.g. is inspectable),* *- the ability to execute tests during system integration is given,* *- all internal and external interfaces of safety-related elements are defined,* *- modularity, consistent level of granularity and simplicity are taken care of* *- if possible well trusted design principles are used* *The system design is analysed by deductive or inductive analysis to identify or exclude causes and effects of systematic failures.*
Project Solution	2 sensors are used for environment detection, both of radar and mono-camera Both sensors can be used to detect objects within specified range, however their sensitivity in judging object status are not equivalent, mono-camera can't be used to measure relative speed or acceleration properly Deviations: ASIL decomposition shall not be applied
Status:	See TSR and System Design
Evidence documents	
	System design specification Technical safety concept specification

This needs to be solved, but how?

1. *Maintain existing design concept, but all ASILs are marked by ASIL D*
2. *Change current design concept, add up one equivalent sensors*

exida®

excellence in dependable automation

EXIDA STRENGTH IN SAFETY

exida strength in Safety

- Safety means: SOTIF/ Cyber Security/ Functional safety/ Other safety disciplines such as HMI factors
- *exida* focuses on engineering practices and is able to provide technical analysis and development support based on our engineering judgment:
  - For government:
    - We accept independent safety assessments/ evaluations of critical projects
    - We can help to investigate safety issues or incidents, if needed

exida strength in Functional Safety

- *exida* focuses on engineering practices and is able to provide technical analysis and development support based on our engineering judgment:
  - For OEM:
    - Evaluate suitability and effectiveness of safety goals based on knowledge of vehicle behavior
    - Verify correctness and consistency between safety goals and derived functional safety concept
    - Identify and joint-develop safety validation strategy

exida strength in Functional Safety

- *exida* focuses on engineering practices and is able to provide technical analysis and development support based on our engineering judgment:
  - For Suppliers:
    - Specify safety concept
    - Analyze or propose safety algorithms
    - Verify used signals and signal safety range for the target safety concept
    - Propose solutions in executing safe states
    - Detailed definition of H/W-S/W Interface (HSI) to fulfill safety functions and safety measures

exida strength in Functional Safety

- *exida* focuses on engineering practices and is able to provide technical analysis and development support based on our engineering judgment:
  - For Suppliers:
    - Jointly development of needed Safety Analyses (FMEDA, FTA, etc.)
    - DFA and define mechanism to achieve freedom from interference @ system, H/W and S/W level
    - Guidance in protection design (Safety Measures) at APP and LLS @ S/W level
- *exida* supports safety assessment in Chinese

excellence in dependable automation

Thank you

Bentley Lin
Bentley.Lin@exida.com