EUROPEAN STAMP WORKSHOP AND CONFERENCE (ESWC) 2020

WMG, THE UNIVERSITY OF WARWICK

21-22 OCTOBER 2020
Day 2

WMG, THE UNIVERSITY OF WARWICK

21-22 OCTOBER 2020

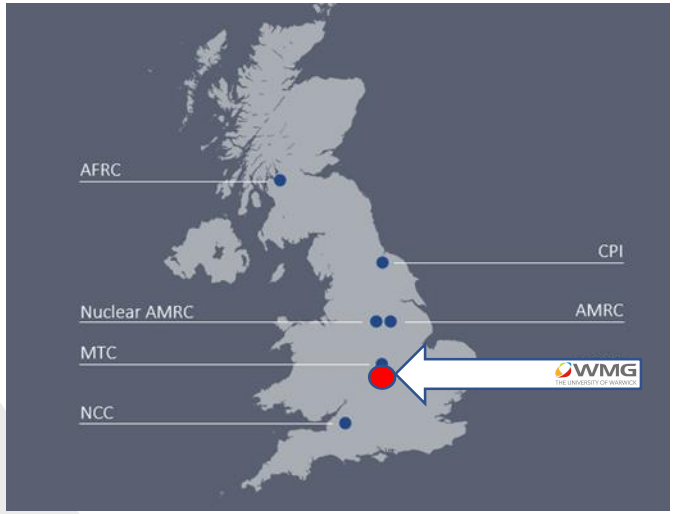
WELCOME TO DAY 2 AND INTRODUCTION TO WMG HVM CATAPULT

Alison Meir,
Head of Business Development,
WMG HVM Catapult

High Value Manufacturing Catapult

WHAT IS THE HVMC?

- A consortia of 7 world class research centres, part of UK Catapult network, working to:
  - **Drive growth in manufacturing**
  - **Accelerate and de-risk innovation**
  - **Provide access to world-class specialist capabilities and facilities**



- **12 Strategic Objectives** across major UK manufacturing sectors – making UK more competitive, efficient, and towards a greener, cleaner future

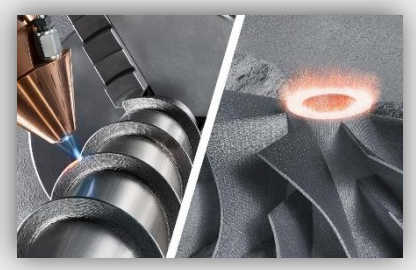
- Focus on manufacturing technology **TRLs 4-7** helping design, develop and deliver innovation, alongside policy and skills development

- Greater transparency for industry, sharing market intelligence and collective strategy; **cross-industry expertise delivering powerful solutions**

High Value Manufacturing Catapult

12 Strategic Objectives for HVMC

Increase Digital / Automation technologies for UK competitiveness



Establish global position in Additive Manufacturing

Develop/ secure leading capabilities in future Air Transport / Manufacture

Enable future technologies in Food / Drink

Accelerate Capabilities & Technologies for Zero Emissions Mobility

Support/ influence / deliver UK Nuclear Energy Policy and Strategy

Construction / infrastructure: transition product to process technologies

Healthcare Manufacturing: accelerate growth and technical innovation

Circular Economy: drive resource efficiencies = economic prosperity

Identify / develop / maximise UK capability in eCAM

Increase / augment TES & DfM: maximise performance / productivity

Position UK as global defence manufacturing nation

High Value Manufacturing Catapult

WMG as a part of HVMC:

Focus: Net Zero Emission Mobility

- WMG leads the **HVMC Strategy Team** on **Net Zero Transportation**
  - Inclusive of various transportation sectors: automotive, aerospace, maritime, rail and goods transit
  - Development across a range of propulsion technologies: hybridised/all electric, battery, and hydrogen

- WMG leads the **HVMC Technology Team on Digital Automation**
  - Focused on improving the development, design, and adoption across the UK
  - UK Supply Chain

- A key member in a number of diverse Sector Strategy Teams:

〉 **Energy**

〉 **Surface Transportation**

〉 **Aerospace / Defence**

〉 **eCam**

〉 **Digital Engineering**

〉 **Healthcare**

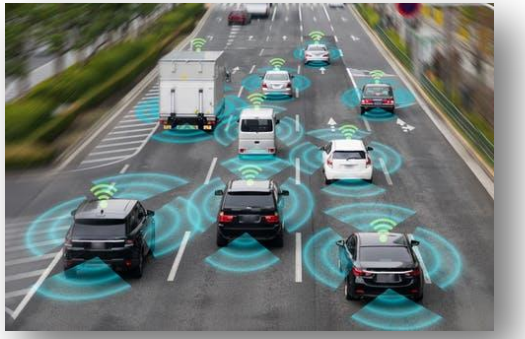
〉 **Circular Economy**

〉 **Through-life Engineering**

High Value Manufacturing Catapult

WMG HVMC supports STAMP – Technology for a Safer World

- Dynamic, systems approach to safety analysis and accident causality, a key focus in complex technology landscapes
- Provisions levels of granularity and control structures contributing to significant overall system understanding
- Application multi-sector as widening technology arenas require increasingly robust analysis. Design defensively
- Particular validity in net zero transportation where safety and system architecture plays a critical role
- Contribution to regulatory and policy development, aligns with WMG and role as a Catapult



TEST SCENARIO GENERATION USING STPA (AUTOMATED DRIVING SYSTEM CASE STUDY)

Dr Siddartha Khastgir,
Head of Verification & Validation,
Intelligent Vehicles
WMG, University of Warwick, UK

WMG, THE UNIVERSITY OF WARWICK

21-22 OCTOBER 2020

Test scenario generation using STPA:
(Automated Driving System case study)

Dr Siddartha Khastgir CEng MIMechE
Head of Verification & Validation, Intelligent Vehicles
WMG, University of Warwick, UK
UK Technical Representative – ISO TC204/WG14, ISO TC22/SC33/WG9

European STAMP Workshop and Conference
22 October 2020

Agenda

- Challenges in testing Automated Driving Systems
- Motivation
- STPA: Systems Theoretic Process Analysis
- Test Scenarios – STPA extension
- Conclusions

Some Challenges for CAVs: In numbers

11 Billion miles[1]

To demonstrate with 95% confidence that AVs are 20% better than human drivers

1 N. Kalra and S. M. Paddock, “Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?,” *Transp. Res. Part A Policy Pract.*, vol. 94, no. December, pp. 182–193, 20163

WMG
THE UNIVERSITY OF WARWICK

Some Challenges for CAVs: In numbers

11 Billion miles[1]

To demonstrate with 95% confidence that AVs are 20% better than human drivers

100,000 lives[2]

Saved (in the next 30 years) if AVs which are 10% better than human drivers are introduced

[1]N. Kalra and S. M. Paddock, “Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?,” *Transp. Res. Part A Policy Pract.*, vol. 94, no. December, pp. 182–193, 2016
[2]N. Kalra and D. G. Groves, *The Enemy of Good*. 2017

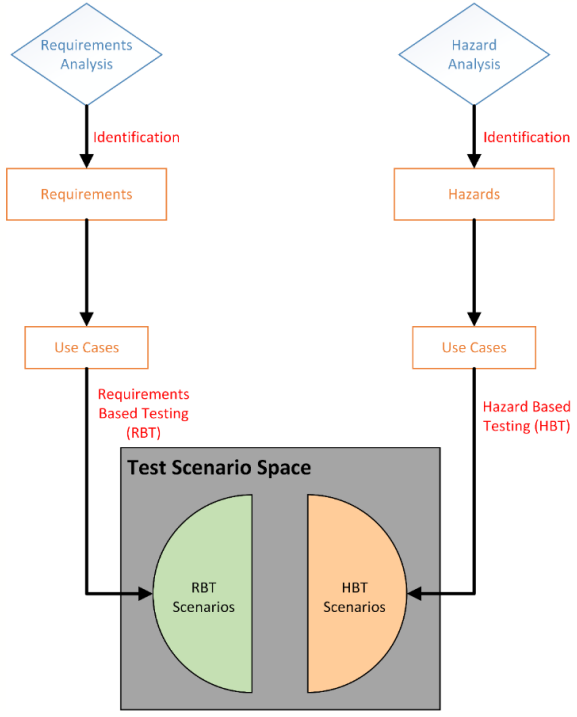
WMG
THE UNIVERSITY OF WARWICK

Motivation: Identifying test scenarios

- Semi-structured interview study of Verification and Validation (V&V) experts in the industry from USA, Sweden, Germany, India, UK and Japan (across the automotive supply chain)

- Key findings [3]:
  - For ADAS and ADS: we need to test *"how a system fails"* as compared to *"how a system works"*
  - Need for a structure way to define test scenarios and test cases

- Proposed Hazard Based Testing



[3] Khastgir, S. et al., "The science of testing: an automotive perspective," SAE World Congress Experience 2018

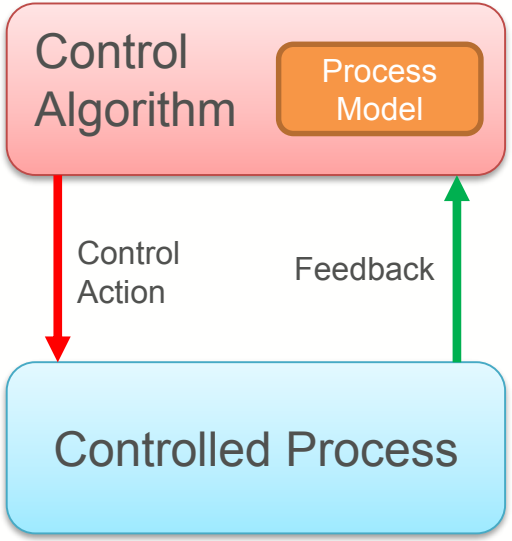
Hazard Based Testing

Three step process:

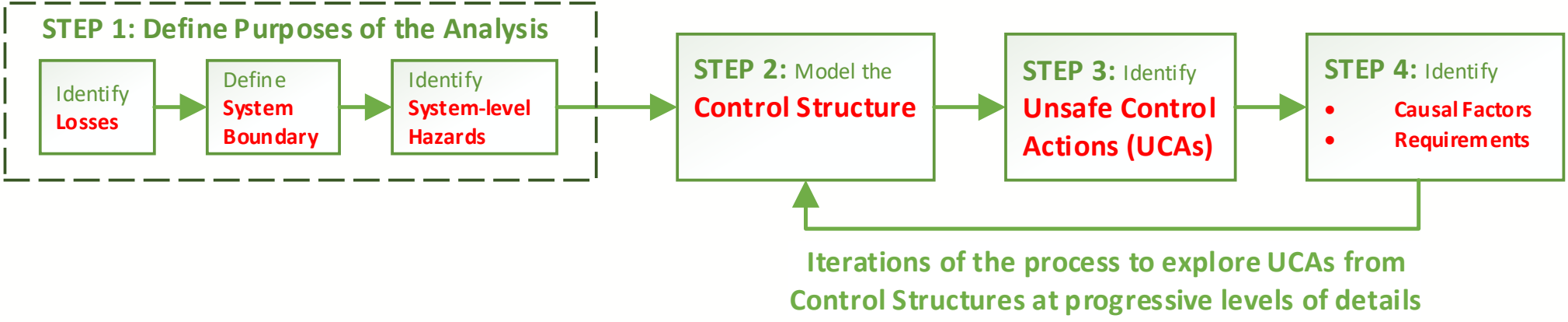
- Identification of hazards
- Creating test scenarios for the identified hazards
- Pass criteria for the created test scenarios

Systems Theoretic Process Analysis (STPA)

- After going through literature, we found STAMP/STPA the most exhaustive list of hazards capturing system interactions
- STAMP/STPA is based on Systems Engineering and considers system safety as a control problem
  - *Safety* is a control problem (property of a system as a whole, not individually)
  - Breach of control laws (constraints) cause accidents
- Basis of STAMP:
  - Constraints, control loops and process models, and levels of control



STPA: Four step process



System Definition

- Fully autonomous low-speed shuttle (SAE Level 4)
- Limited ODD
- Sensor suite
- Remote dispatcher
- Electric propulsion

STPA: Step 1: Losses and Hazards

Losses	
L1	Collision with objects outside the vehicle or damage to vehicle
L2	Not completing the journey with passenger and cargo
L3	Time of journey being too long, i.e., service target not met
L4	Loss of life or serious injury to people

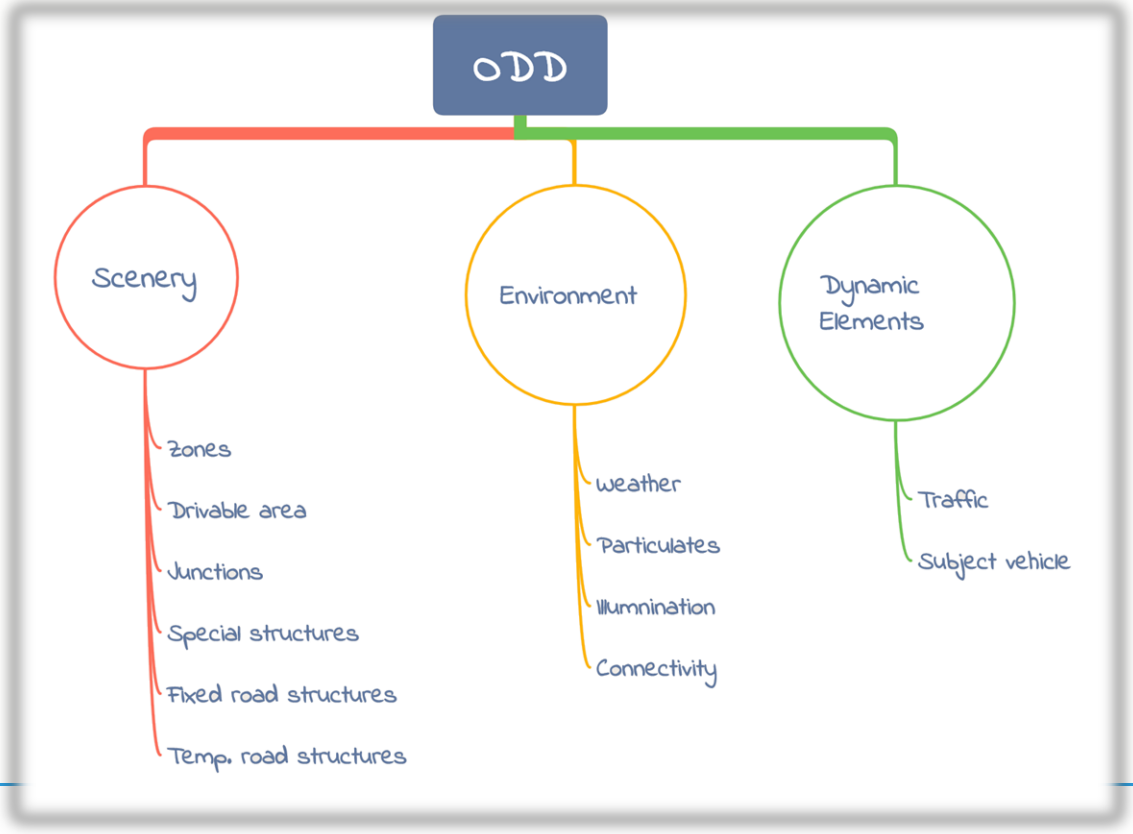
Hazards	
H1	Vehicle does not maintain safe distance from nearby objects - L1
H2	Vehicle enters dangerous area/region – L1
H3	Vehicle exceeds safe operating envelope for environment (speed, lateral/longitudinal forces) - L1, L2, L3
H4	Vehicle occupants exposed to harmful effects and/or health hazards (e.g. fire, excessive temperature, inability to escape, door closes on passengers, etc.) – L4
H5	Vehicle does not follow an efficient, complete path to destination – L2, L3

STPA: Step 1: Losses and Hazards

Losses	
L1	Collision with objects outside the vehicle or damage to vehicle
L2	Not completing the journey with passenger and cargo
L3	**Time of journey being too long, i.e., service target not met**
L4	Loss of life or serious injury to people

Hazards	
H1	Vehicle does not maintain safe distance from nearby objects - L1
H2	Vehicle enters dangerous area/region – L1
H3	Vehicle exceeds safe operating envelope for environment (speed, lateral/longitudinal forces) - L1, L2, L3
H4	Vehicle occupants exposed to harmful effects and/or health hazards (e.g. fire, excessive temperature, inability to escape, door closes on passengers, etc.) – L4
H5	**Vehicle does not follow an efficient, complete path to destination – L2, L3**

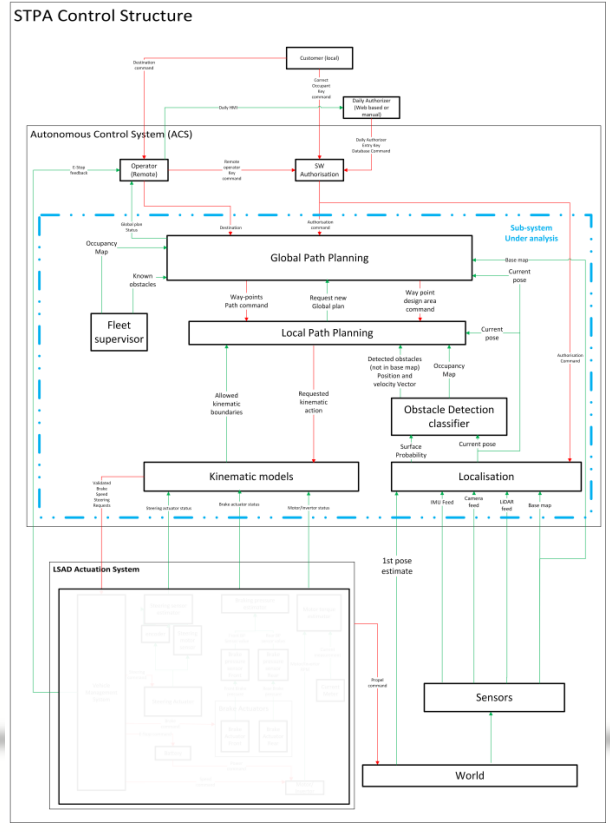
STPA: Step 1: Define the ODD



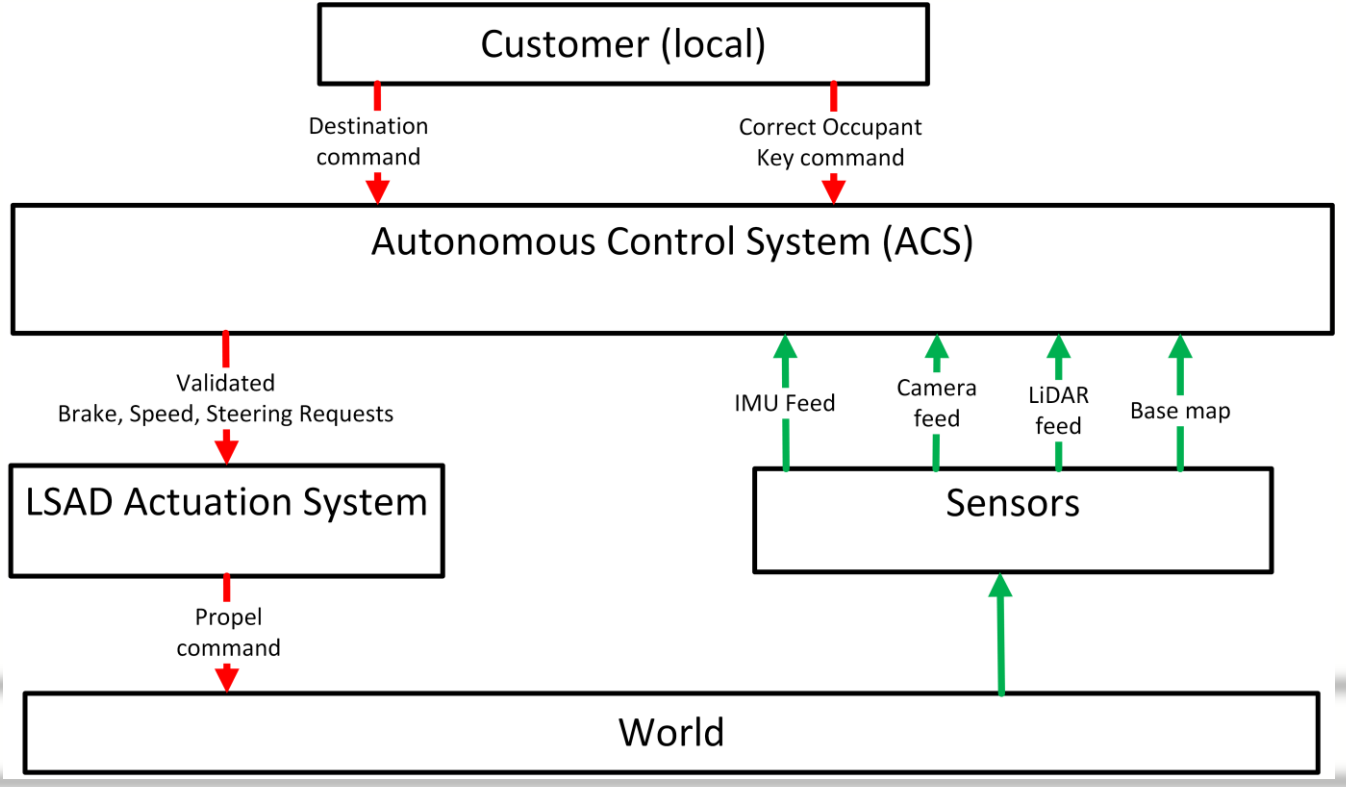
ODD Taxonomy as per BSI PAS 1883

STPA: Step 2: Control Structure

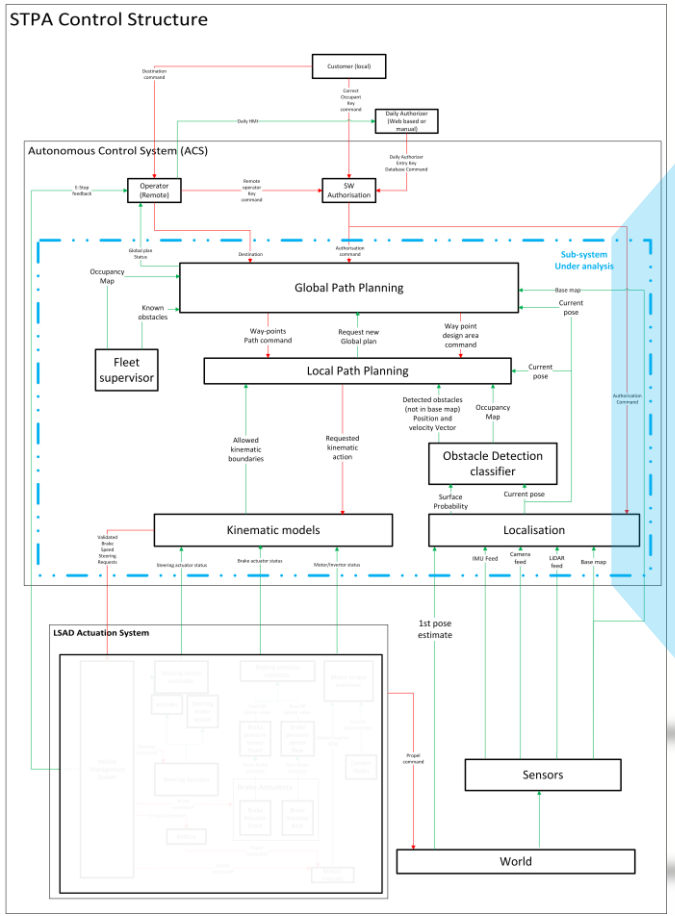
- Identify a control structure for the system with control actions and feedback
- Control structure can be at various abstraction levels
- Control structure for fully autonomous vehicle (pod)
  - Red = control action
  - Green = feedback

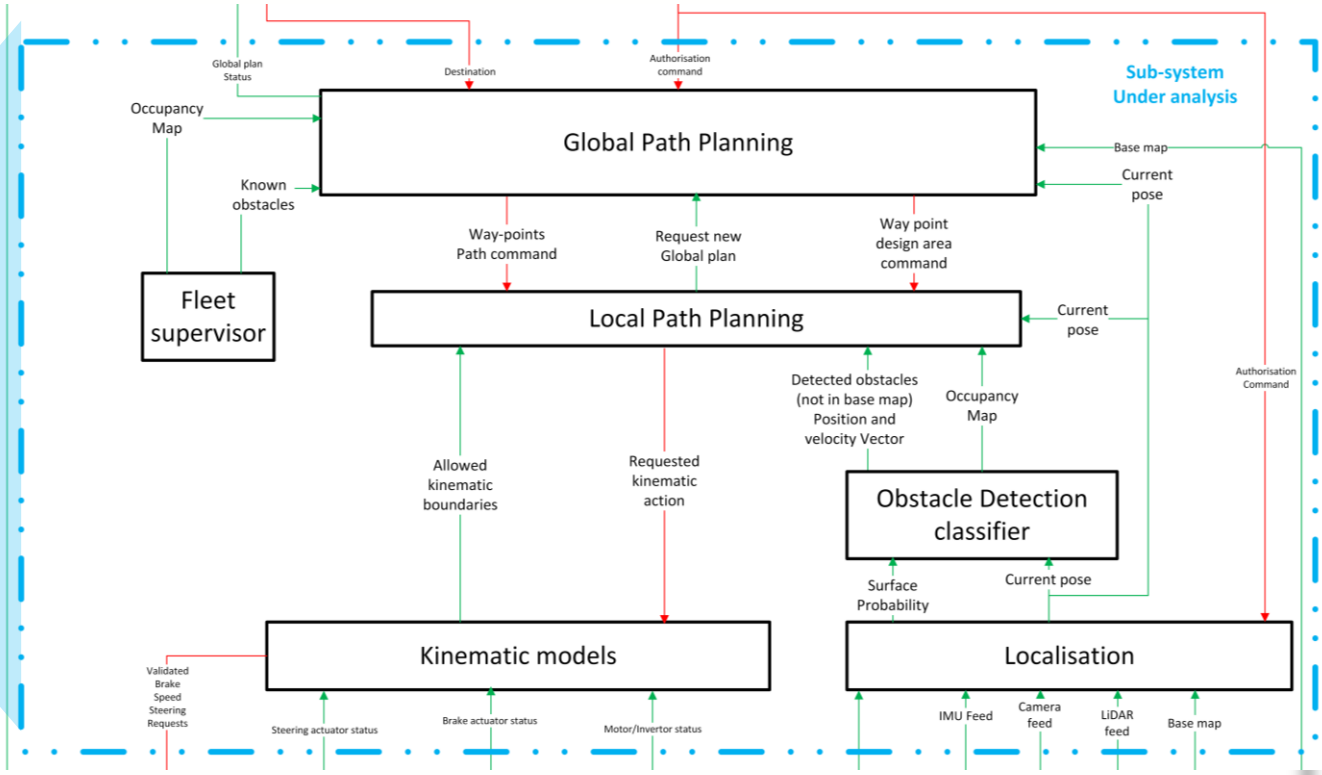


STPA: Step 2: Control Structure (high level)



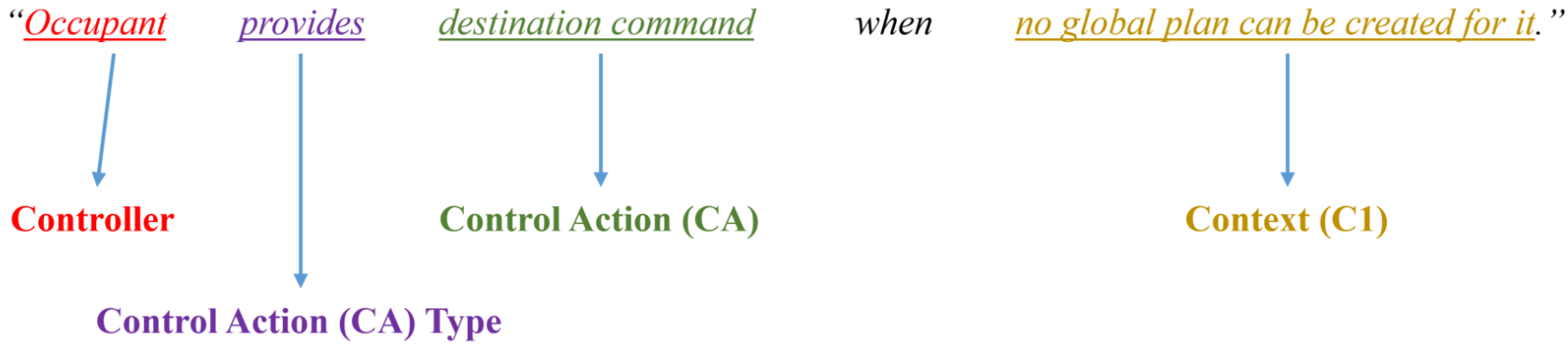
STPA: Step 2: Control Structure





STPA: Step 3: Unsafe Control Actions

- 12 Control Actions led to 70 Unsafe Control Actions
- Essential to maintain the UCA structure

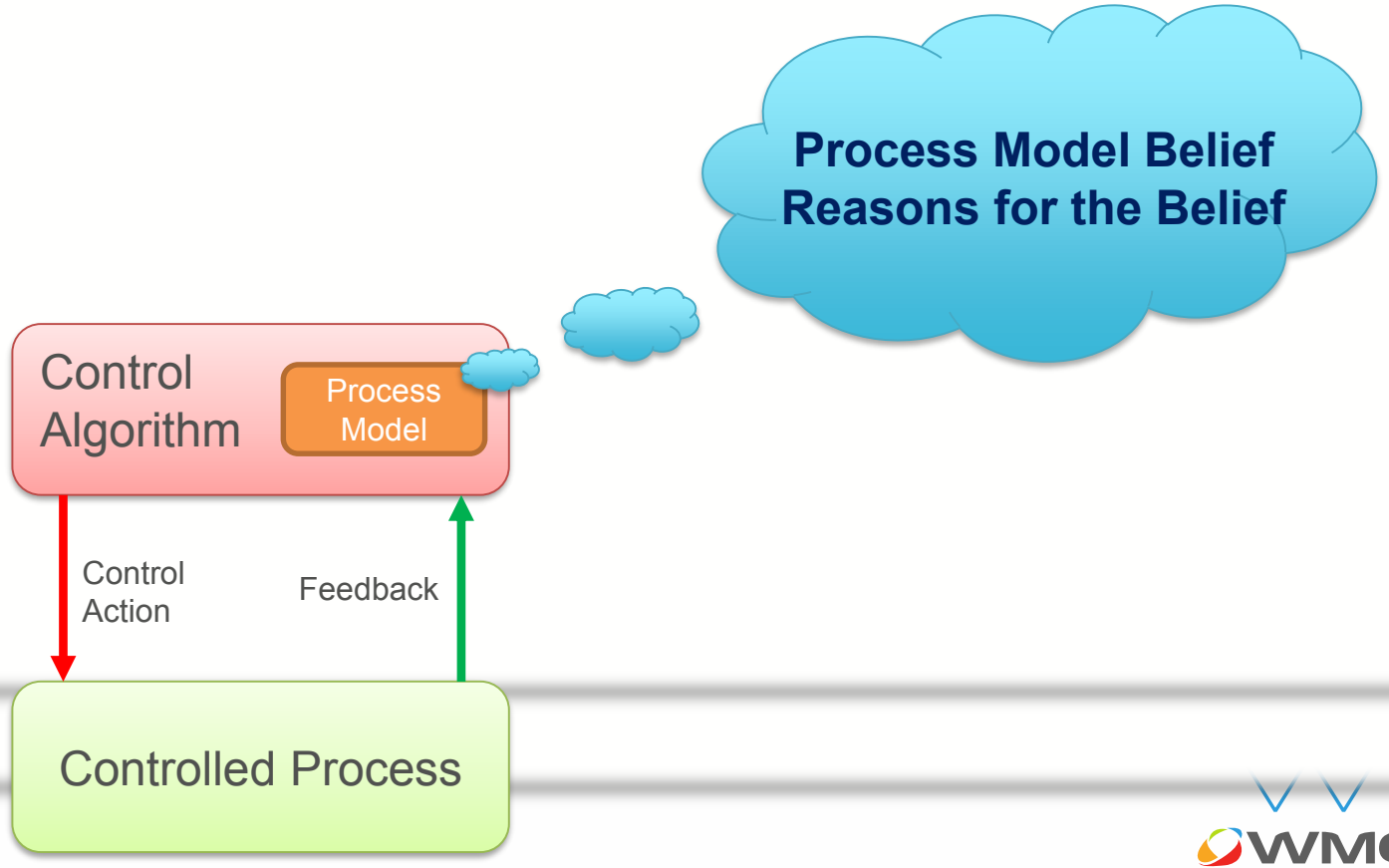


STPA: Step 3: Unsafe Control Actions

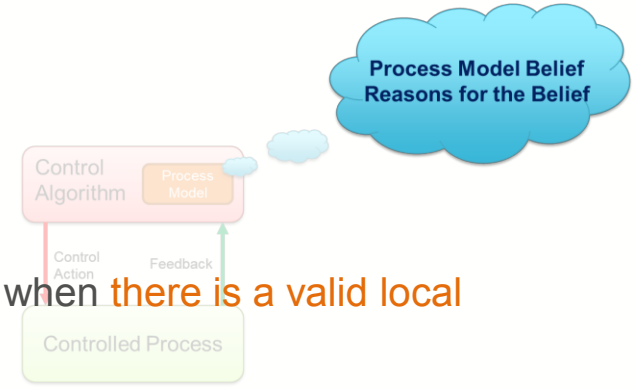
- 12 Control Actions led to 70 Unsafe Control Actions
- Essential to maintain the UCA structure

Control Action	Not Providing causes a loss	Providing causes a loss	Too early, too late, out of sequence causes a loss	Stopped too soon or applied too long causes a loss
Requested kinematic command	[UCA# 15a] Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front. – [H1, H2, H4, H5]	[..]	[UCA# 15c1] LPP provides kinematic action (braking) too late after conflict is unavoidable when there is an obstacle in front and pod is moving. – [H1, H2, H3]	[..]
	[..]		[..]	

STPA: Step 4: Loss Scenarios

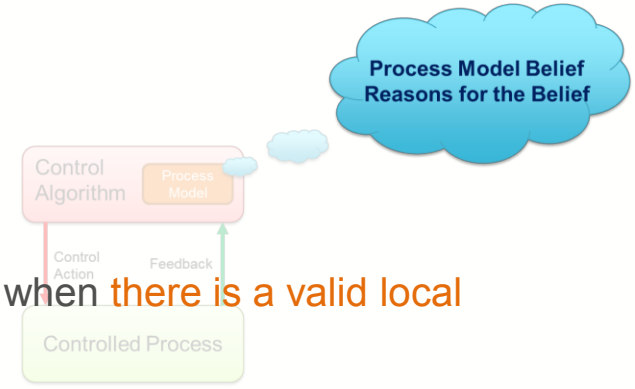


STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

STPA: Step 4: Loss Scenarios

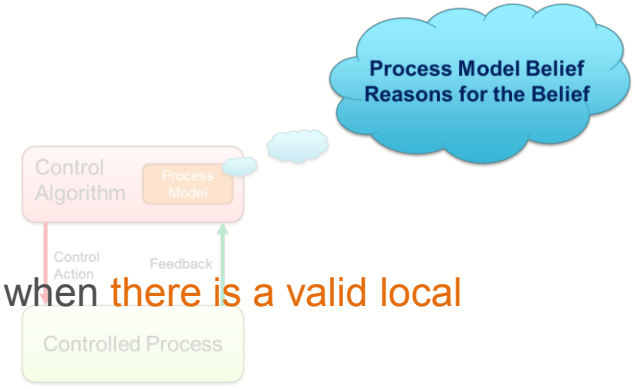


UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

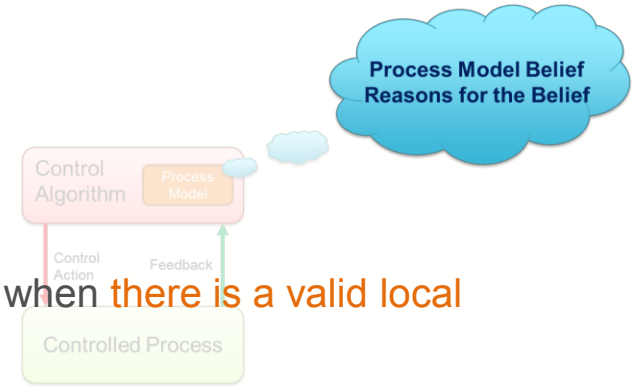
Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

Causal Factors

- This could be because historical data of the pose and the surface probability shows no collision and the Covariance Error is low (i.e., sensor data is coherent). This could be because all sensor feeds are delayed in time leading to a low covariance error as they are coherent.

STPA: Step 5: Extension: Test Scenario creation

STPA: Step 5: Extension: Test Scenario creation

***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

Controller: Local Path Planning (LPP)

Control Action (CA) Type: doesn't provide

Control Action (CA): kinematic action (braking)

Context (C1): there is a valid local path and the pod is moving and there is an obstacle in front

STPA: Step 5: Extension: Test Scenario creation

- Every test scenario will have:
  - Scenery
  - Environmental conditions
  - Dynamic elements

  } Library

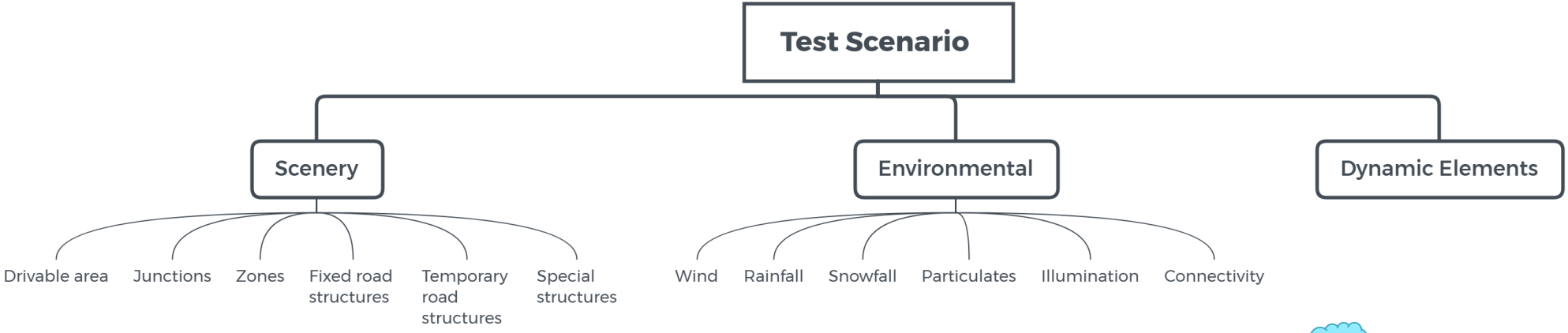
  - Depend on ODD, a library of base sceneries, env. conditions and dynamic elements have been created

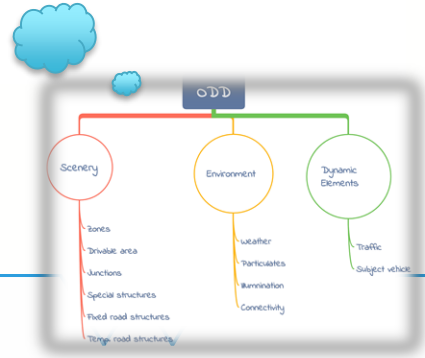
Additional Context:

- Parametrise the “context element” (of UCA)
- Parametrise the “causal factors” (step 4)

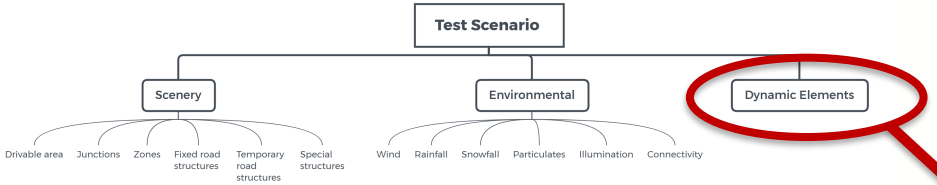
- Pass criteria

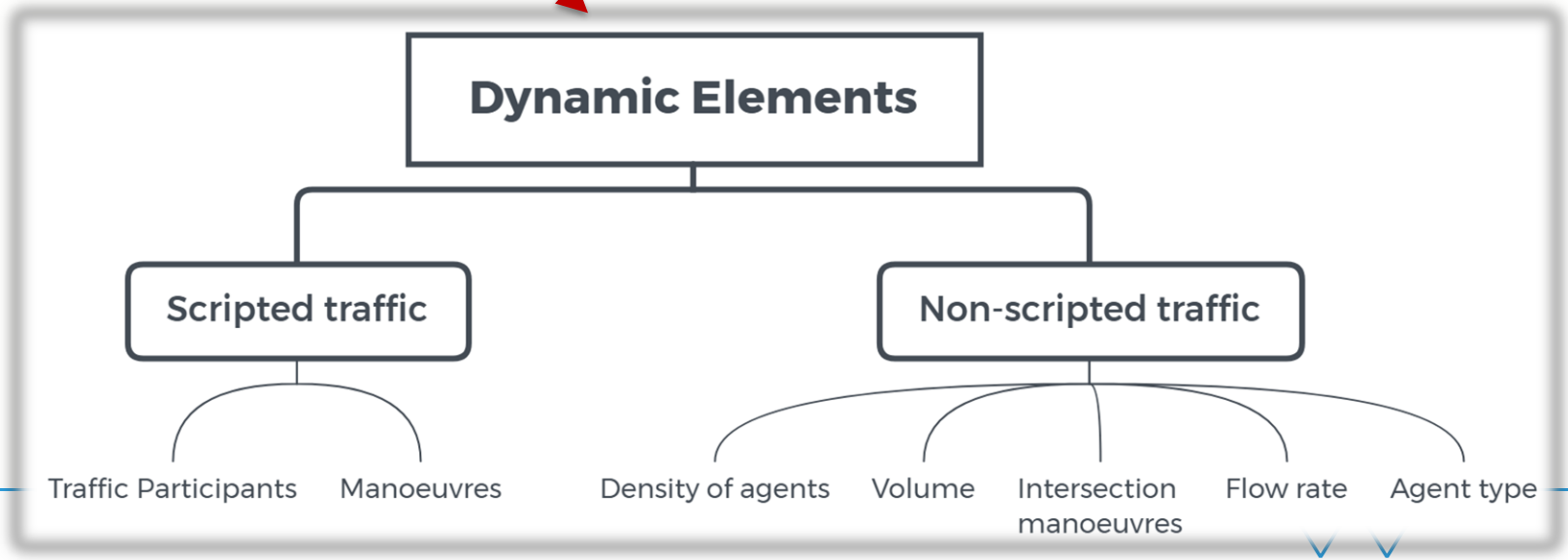
Test Scenarios structure





Test Scenarios structure





STPA: Step 5: Additional Context

***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

STPA: Step 5: Additional Context

***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

- Parametrise the "context element" (of UCA)
  - *there is a valid local path and the pod is moving and there is an obstacle in front*
  - Parameters: Velocity, obstacle position

STPA: Step 5: Additional Context

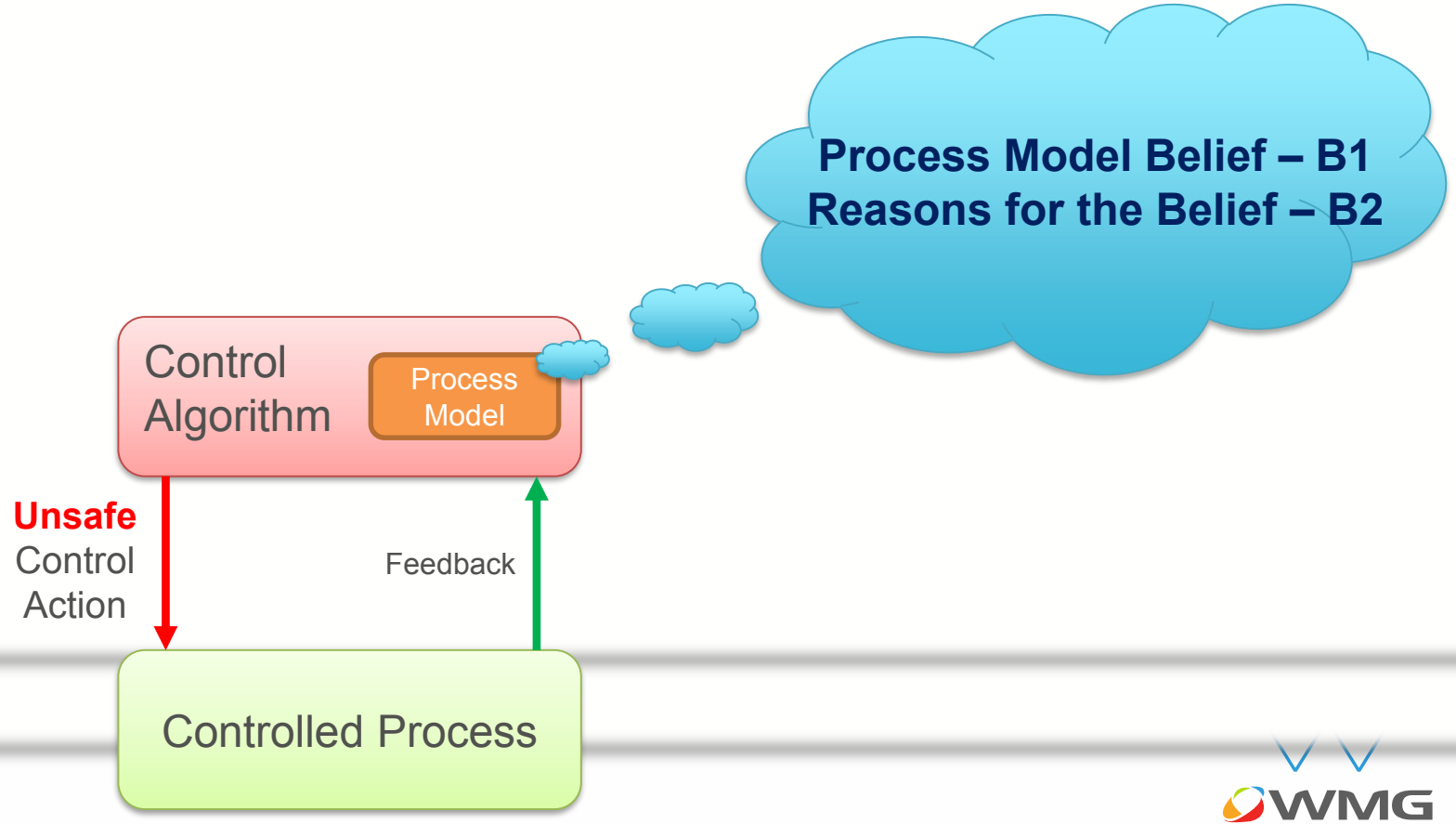
***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

- Parametrise the "context element" (of UCA)
  - *there is a valid local path and the pod is moving and there is an obstacle in front*
  - Parameters: Velocity, obstacle position

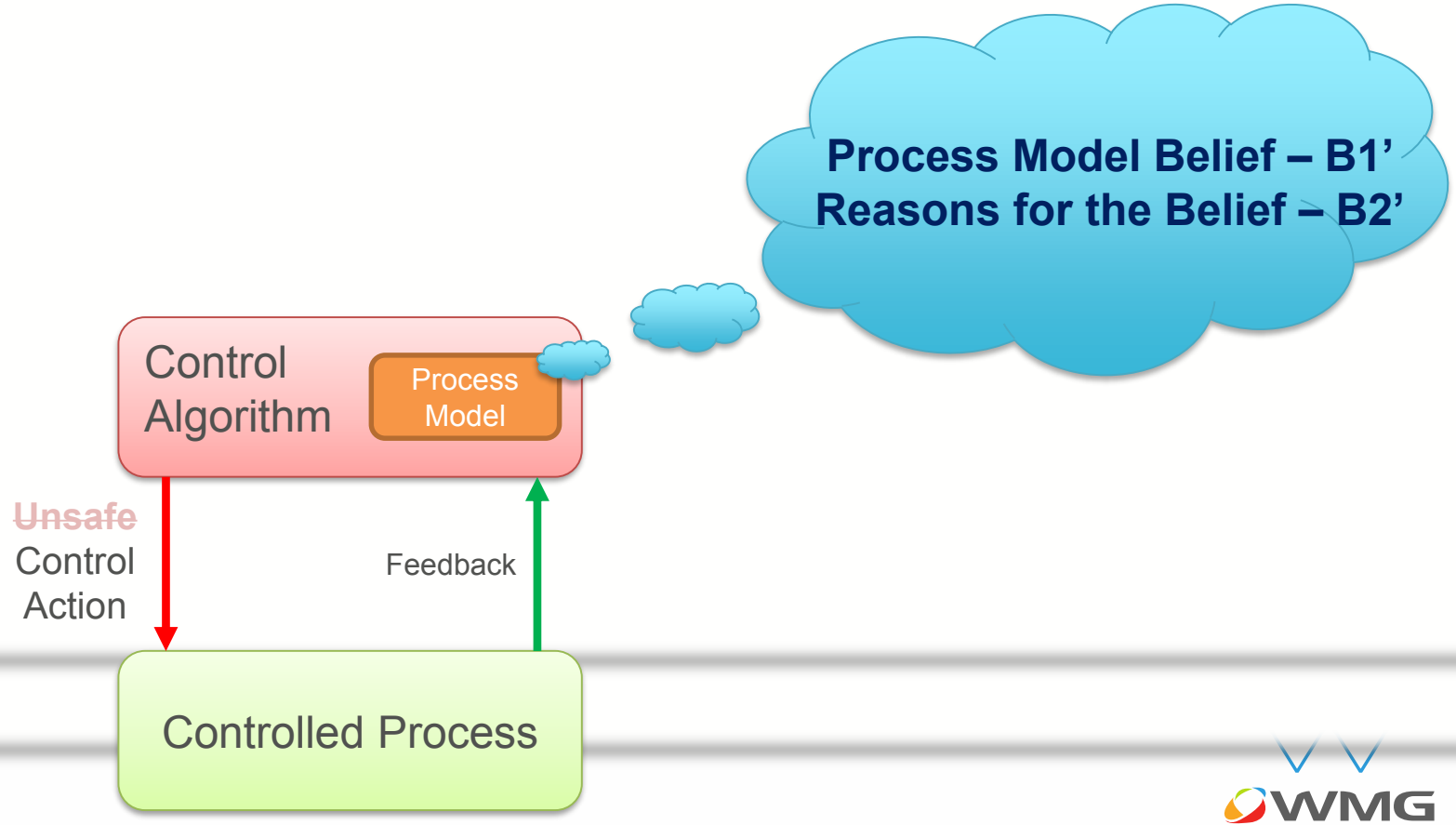
- Parametrise the "causal factors" (step 4)
  - This could be because all sensor feeds are delayed in time leading to a low covariance error as they are coherent.
  - Parameters: Delay time, type of sensor feed

STPA: Step 5: Pass criteria

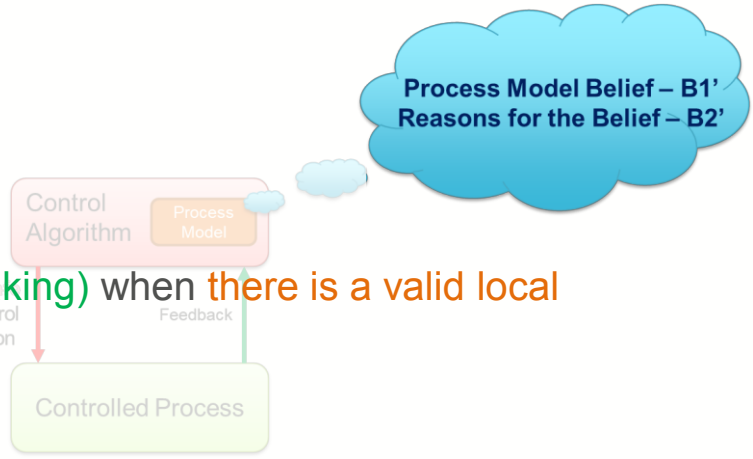
STPA: Step 5: Pass criteria



STPA: Step 5: Pass criteria

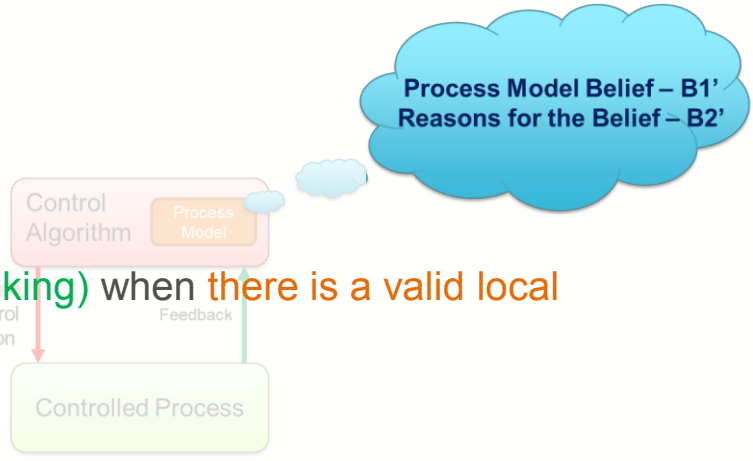


STPA: Step 5: Pass criteria



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

STPA: Step 5: Pass criteria



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

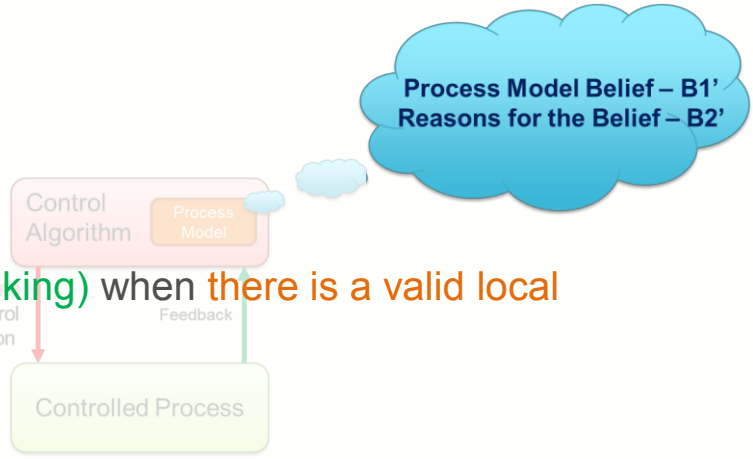
Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

STPA: Step 5: Pass criteria



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

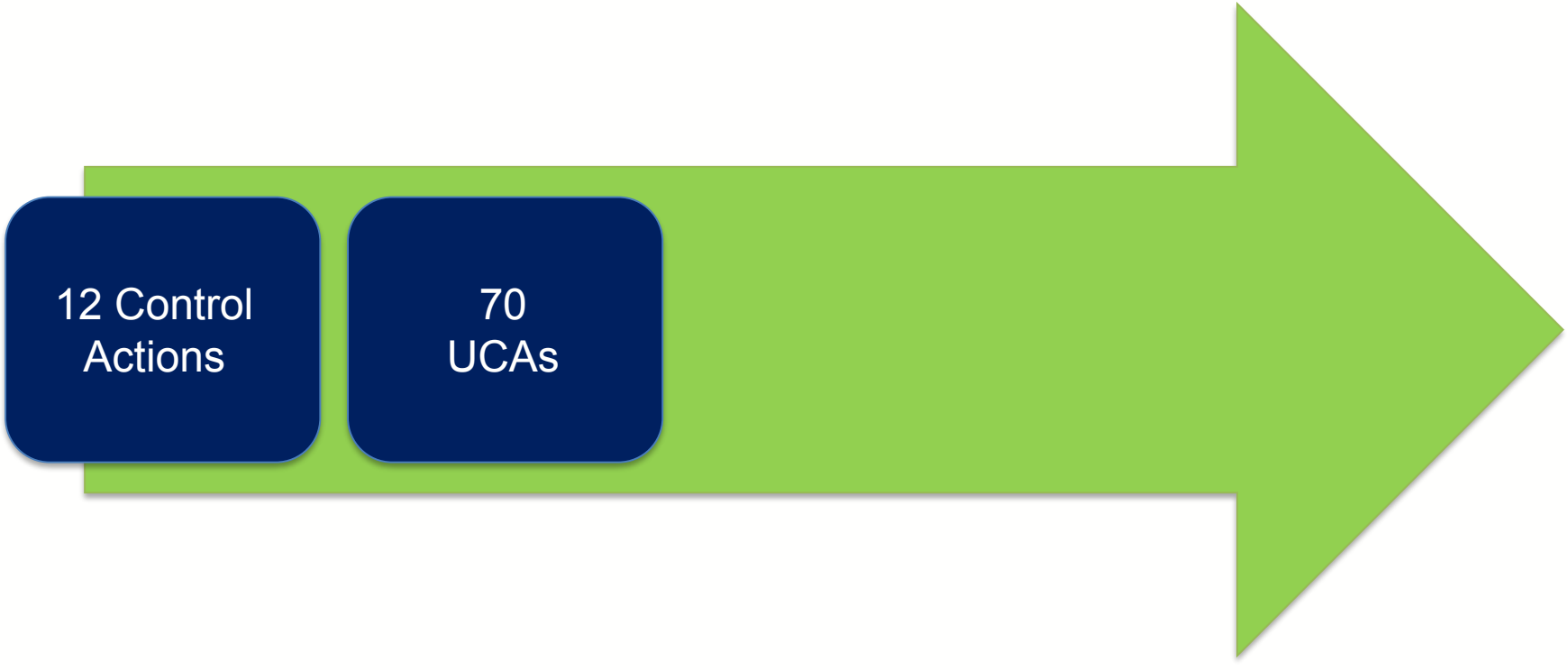
- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

Pass criteria 1 (B1'): LPP believes that obstacles are ~~not~~ in vehicle trajectory

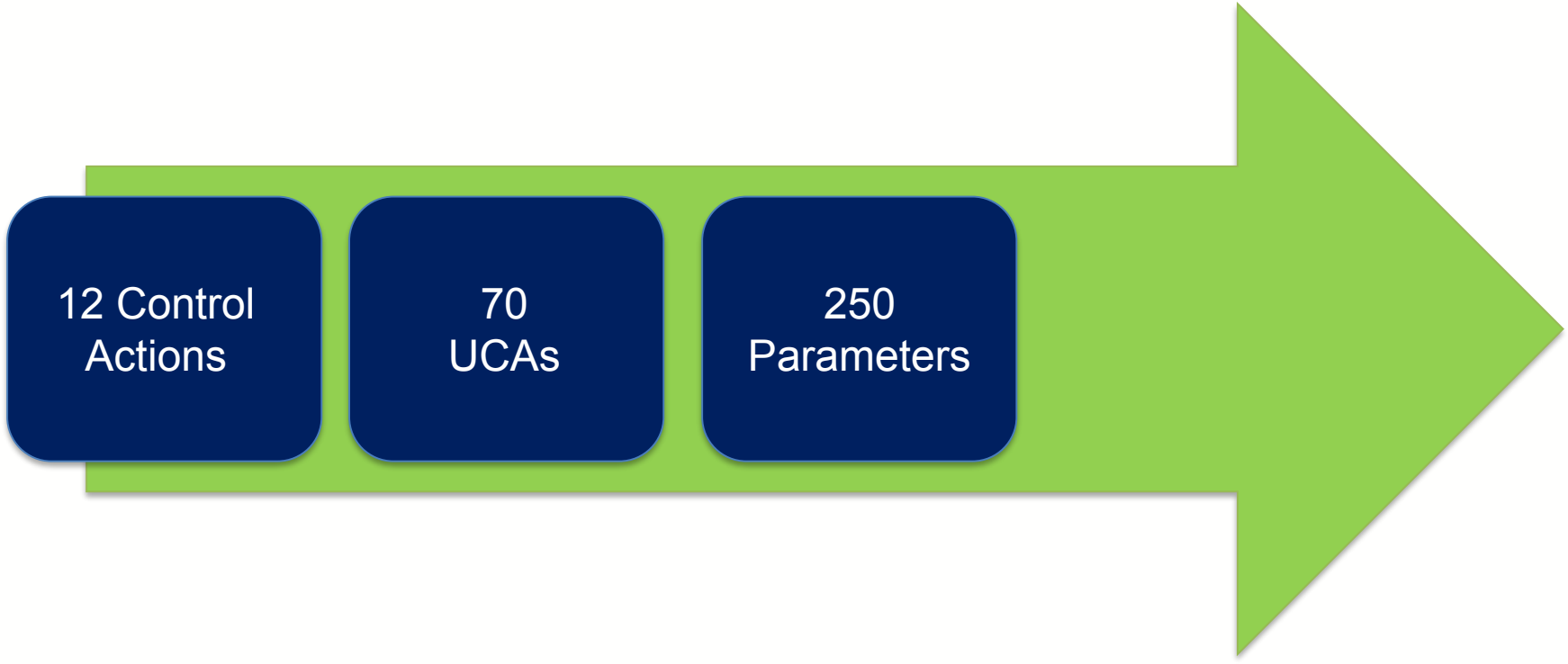
Pass criteria 2 (B2'): Obstacle Detection Classifier ~~doesn't~~ provides detected obstacles vector when obstacle is in vehicle trajectory

Case study overview: STPA & extension

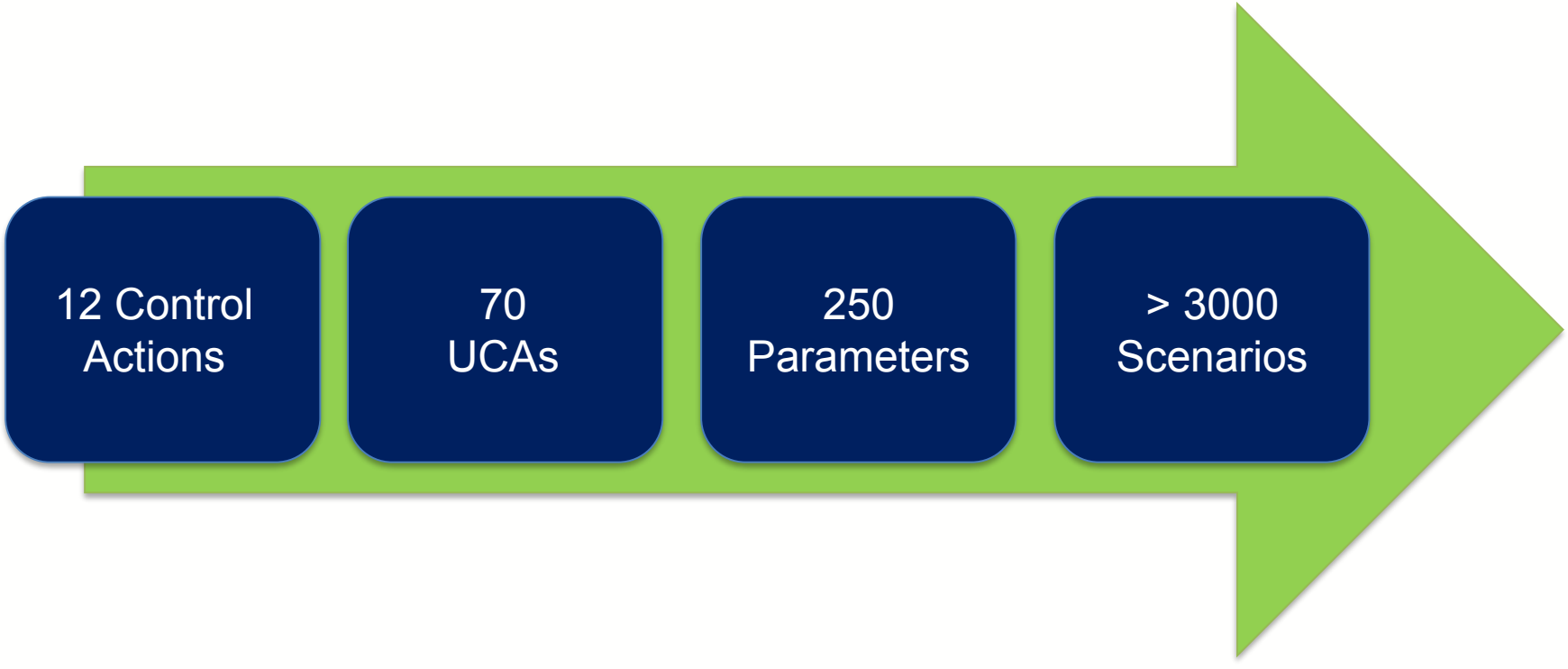
Case study overview: STPA & extension



Case study overview: STPA & extension

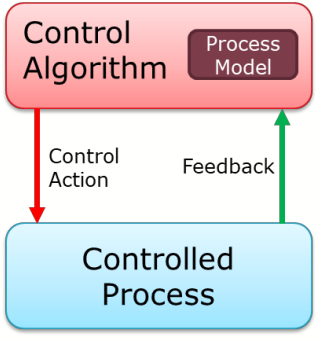


Case study overview: STPA & extension



STPA: Extension: An overview

1-2. Identify control actions, feedback and high level losses



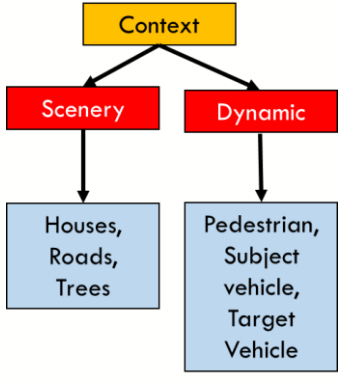
3. Identify Unsafe Control Actions

1) Not providing a control action
2) Not providing a control action
3) Providing a control action too late, too early or out of sequence
4) Control action stopped too soon or applied too long.

4. Identify the causes of Unsafe Control Action

- Process Model Belief
- Reason for the belief
- Negate this to obtain pass criterion

5. Extension: Provide context to obtain bounds on the scenario



- Test Scenario Parameters
- Pass Criteria

Acknowledgement

Centre for Connected & Autonomous Vehicles

AURRIGO

WMG THE UNIVERSITY OF WARWICK

MIT

UKRI Future Leaders Fellowships

For more details, upcoming publication: Siddartha Khastgir, John Thomas, Simon Brewerton and Paul Jennings

Summary

For Automated Driving, It is not about the number of miles, but about the number of *"smart"* miles...

Hazard based testing to identify the *"interesting"* scenarios

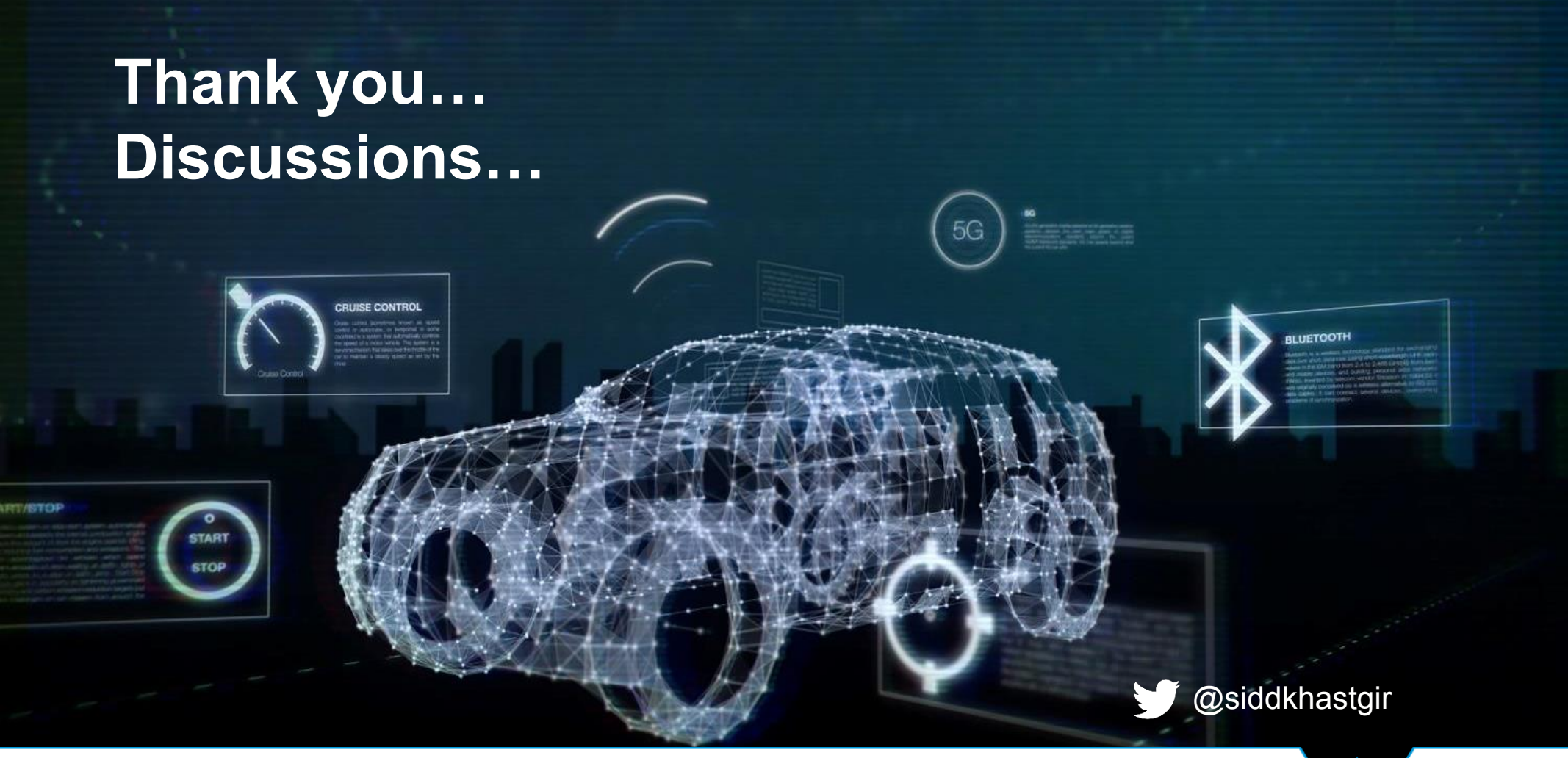
STPA facilitates Hazard Based Testing. STPA applied on a SAE Level 4 system

An extension to STPA proposed to solve two key challenges: test scenarios and pass criteria

STPA identifies the parameters to be fuzzed along with the pass/fail criteria for the test case

WMG
THE UNIVERSITY OF WARWICK

Thank you…
Discussions…



@siddkhastgir

Dr Siddartha Khastgir CEng MIMechE
S.Khastgir.1@warwick.ac.uk

WMG
THE UNIVERSITY OF WARWICK

CATAPULT High Value Manufacturing

WMG THE UNIVERSITY OF WARWICK

WMG, THE UNIVERSITY OF WARWICK

21-22 OCTOBER 2020

SOTIF AND FUSA STPA FOR A HIGHWAY PILOT FUNCTION OF A PASSENGER CAR

Nino Gabriel,
Senior safety expert,
ANSYS, Germany

SOTIF and FuSa STPA for a Highway Pilot Function of a passenger car

Nino Gabriel, Senior Safety Expert

Eckhardt Holz, Head Safety Expert Team

Ansys

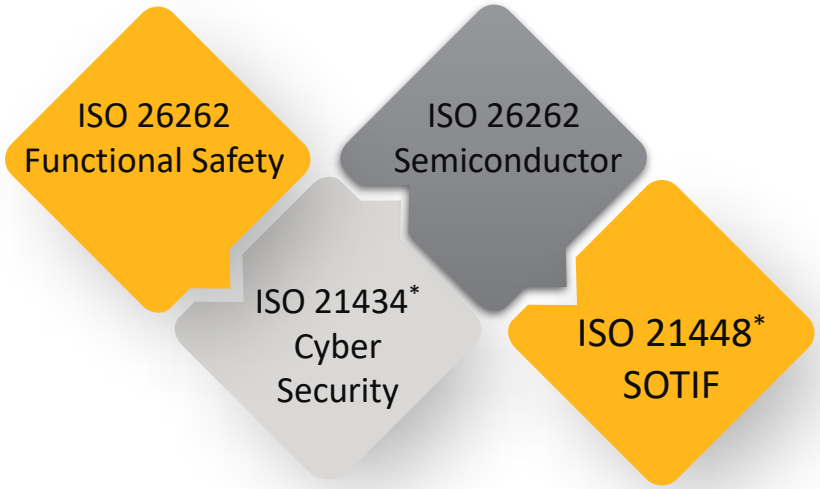
ANSYS medini analyze

Integrated solutions for Functional Safety, SOTIF, Cybersecurity and Reliability Engineering

Model-based approach covering the entire life cycle, supporting safety analysis at the conceptual, system, software, PCB, and chip level to ensure traceability and consistency

Best Practices for meeting safety standards and integration in existing tool landscape

Compliant to state-of-the-art safety & cybersecurity standards – ISO 26262, ISO 21434, ISO/PAS 21448



* ongoing standardization

300+ Customers

SAIC 上汽集团 SAIC MOTOR · BYD · 新能源汽车 引领者 · TESLA · GM · DAIMLER · MAGNA · PSA GROUPE · MASERATI · JOHN DEERE · Ford · NISSAN · FOTON · ZF · Volkswagen · TOYOTA · TRW · MANDO · Valeo · Audi · deedone · Hanma · Panasonic · DAESUNG · Continental · RICARDO · DENSO · BOSCH · GEELY · McLaren · DELPHI · nexteer · NEAR EARTH AUTONOMY · FCA · TUPOLEV · ANALOG DEVICES · NXP · SANYO · Allegro · COMAC · HARLEY-DAVIDSON

ANSYS medini analyze

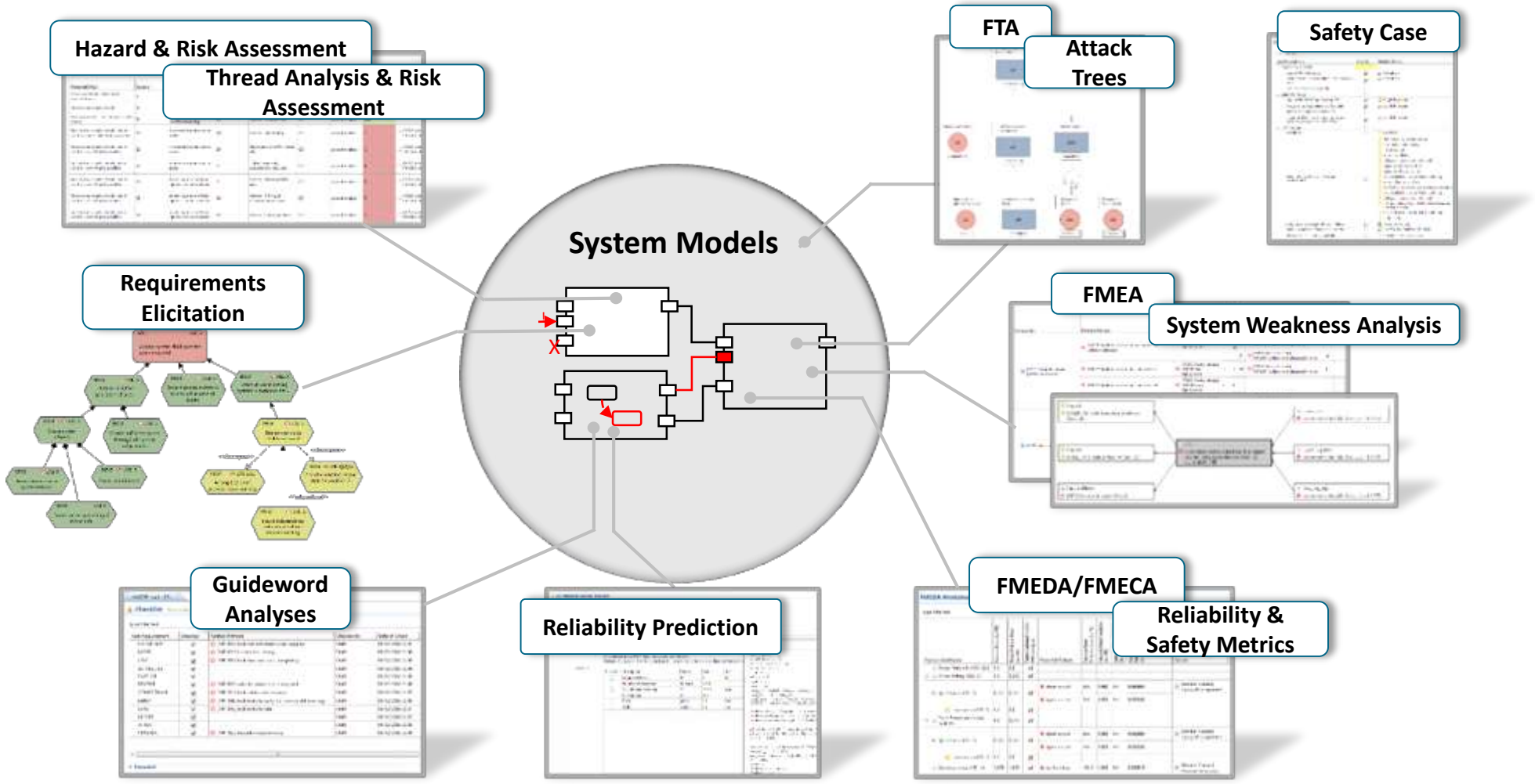
What we are doing ….

- Develop and supply tools for various safety, security and reliability analyses
- Extend the capabilities of our tools by further methods/techniques
- Extend the usage of our tools to new domains and use cases
- Guide our customers in applying methods for safety & security analyses

…. and what not

- Develop safety critical products/systems
- Perform in-depth safety analyses

ANSYS medini analyze



Model-based approach ensures unrivalled level of consistency, traceability and efficiency

We add STPA to the feature set …

… because our customers ask for it 

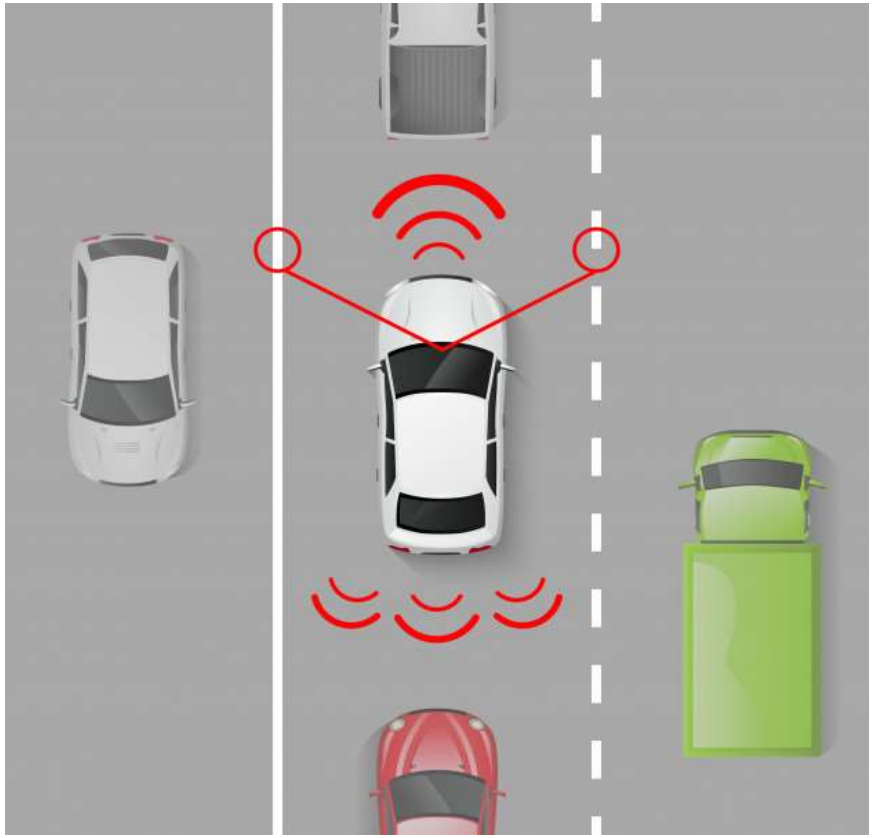
But also because the development of ADAS & autonomous vehicles has new challenges

- *A systemic view is required to cover also human, organizational, regulatory and other factors, e.g.*
  - Reasonably foreseeable human attempts to influence vehicle behavior in good faith
  - Reasonably foreseeable human non-compliance
  - Hazards caused by insufficient specification of autonomous functions resp. insufficient AI training
  - …
- *Need to address emergent factors as early as possible in the engineering*
  - Reduce the number of the *unknown-unsafes* as early as possible
  - Testing (by simulation and driving) can not be done in a full way without guidance
  - …
- *Need to provide traceable evidence for design decisions for the final safety case*
  - From safety analyses to requirements to system architecture to final system realization

… this applies to automotive as well as aviation and for safety as well as for cybersecurity

Sample application: *Highway Pilot*

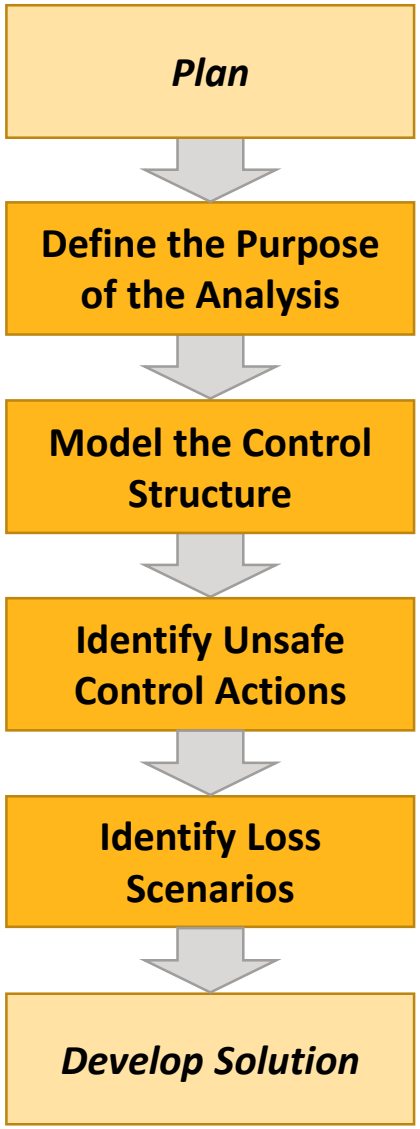
- *What is the system to be analyzed?*
  - A Highway Pilot Function of a passenger car featuring
    - Lane Keep Control
    - Adaptive Cruise Control
    - Automatic Emergency Braking
- *What is the system boundary?*
  - Given by an Operational Design Domain (ODD) definition
    - highway and the environment of a highway is in scope
- *The scope of the analysis*
  - Potentially hazardous behavior of the intended function due to
    - Performance Limitations and related Triggering Conditions
    - Misuse and other human related topics
    - Specified behavior that is dangerous (specification insufficiencies)
    - Failures of electric/electronic and SW components and (sub)-systems

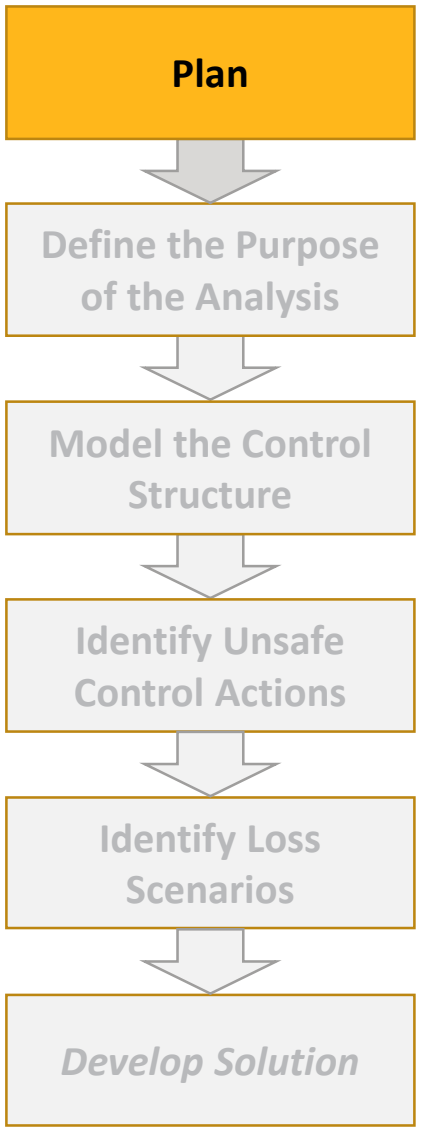


picture from https://www.freepik.com

STPA workflow

1. Define Purpose of the Analysis
   - Identify Losses
   - Identify System-Level Hazards
   - Identify System-Level Constraints
2. Model the control structure
   - Identify Control Elements
   - Identify Control Actions
   - Identify Feedback
3. Identify Unsafe Control Actions
   - Identify Unsafe Control Actions (UCA)
   - Identify Safety Constraints
4. Identify Loss Scenarios
   - Identify Controller Process Models
   - Identify Loss Scenarios
     - Identify Causes of Unsafe Control Actions
     - Identify Improper Execution of Control Actions





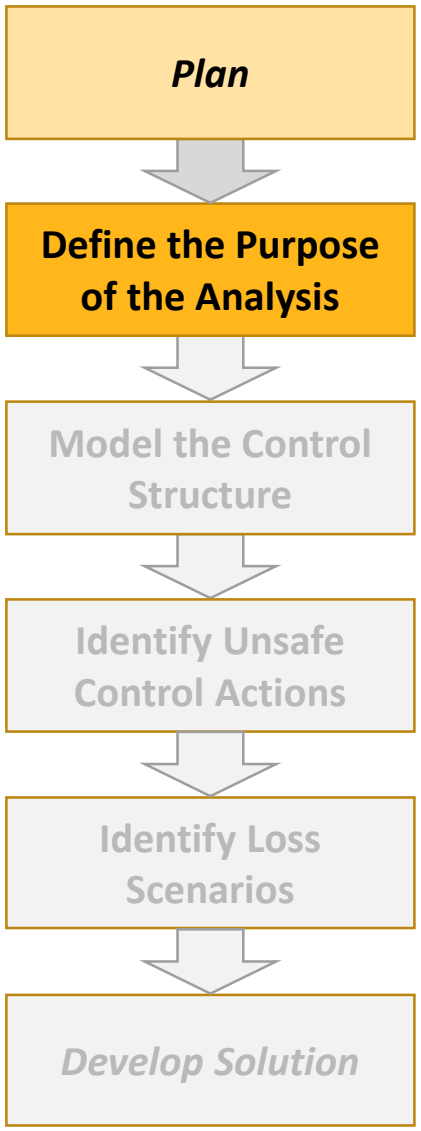
Include the tasks and activities for STPA in the safety plan:

- What?
- When?
- Who?
- Status?
- Trace expected and achieved work products

STPA

type filter text

Task/Requirement	Checked	Related Artifacts	Checked By	Date of Check	Note
Define the purpose of the analysis	☐				
Identify losses	☑	Losses	ngabriel	11.07.20 14:55	
Identify system-level hazards	☑	Hazards	ngabriel	11.07.20 14:55	
Identify system-level constraints	☑	System-Level Constraints	ngabriel	11.07.20 14:55	
Model the control structure	☐				
Identify control elements	☐	Control Structure			
Identify Control actions	☐	Control Structure			
Identify Feedback	☐	Control Structure			
Identify unsafe control actions	☐				
Identify dangerous Control actions	☐	Identify unsafe control actions			For each control action use guidewords to analyse the
Identify Safety Constraints / Requirements	☐	Safety Constraints			For each unsafe control action define one Safety Const
Identify loss scenarios	☐				#Usability# Please consider using the "Failure Net" for
Identify controller process models	☐	Controller Process Model Steering Controller Process Model Braking Controller Process Model Acceleration			
Identify loss scenarios	☐	Causes of a Unsafe Control Action Causes for improper execution of a Control Action			Identify scenarios that lead to unsafe control actions &



- Definition of System Boundary
  - Based on the typical functional item definition according to ISO26262 extended by SOTIF information about environment (ODD)
  - Optionally add information about Stakeholders and their interests
- Identification of Losses

Losses

type filter text

ID	Loss	Stakeholder
L-001	Loss of Life/ Serious Injury	• Driver & passengers • Other people in environment
L-002	Material Damage (Vehicle/ Environment)	• Car owner • Other people in environment

- Identification of hazards

Hazards

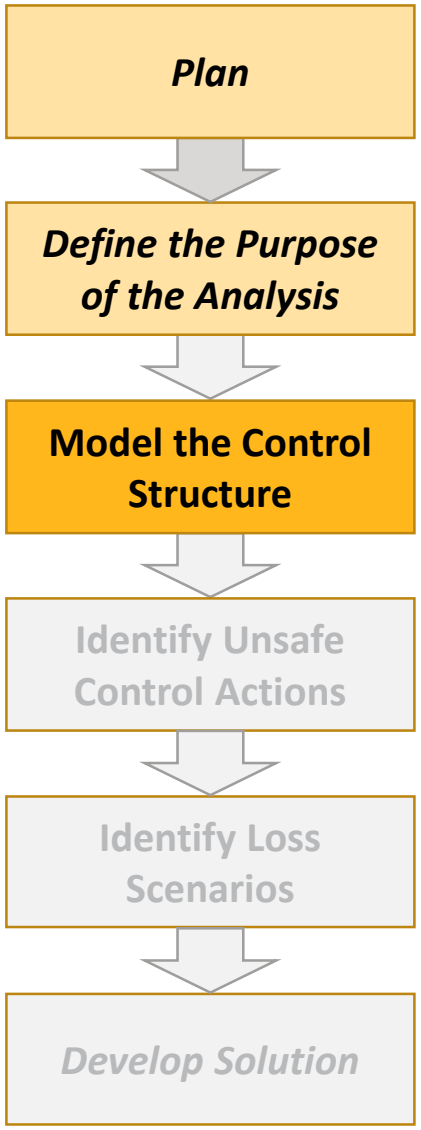
type filter text

ID	Hazard	Loss
H-001	Vehicle does not stay in lane	[L-001] Loss of Life/ Serious Injury [L-002] Material Damage (Vehicle/ Environment)
H-002	Vehicle impedes other road users in their movement	[L-001] Loss of Life/ Serious Injury [L-002] Material Damage (Vehicle/ Environment)
H-003	Vehicle violates safe distance to other road users	[L-001] Loss of Life/ Serious Injury [L-002] Material Damage (Vehicle/ Environment)

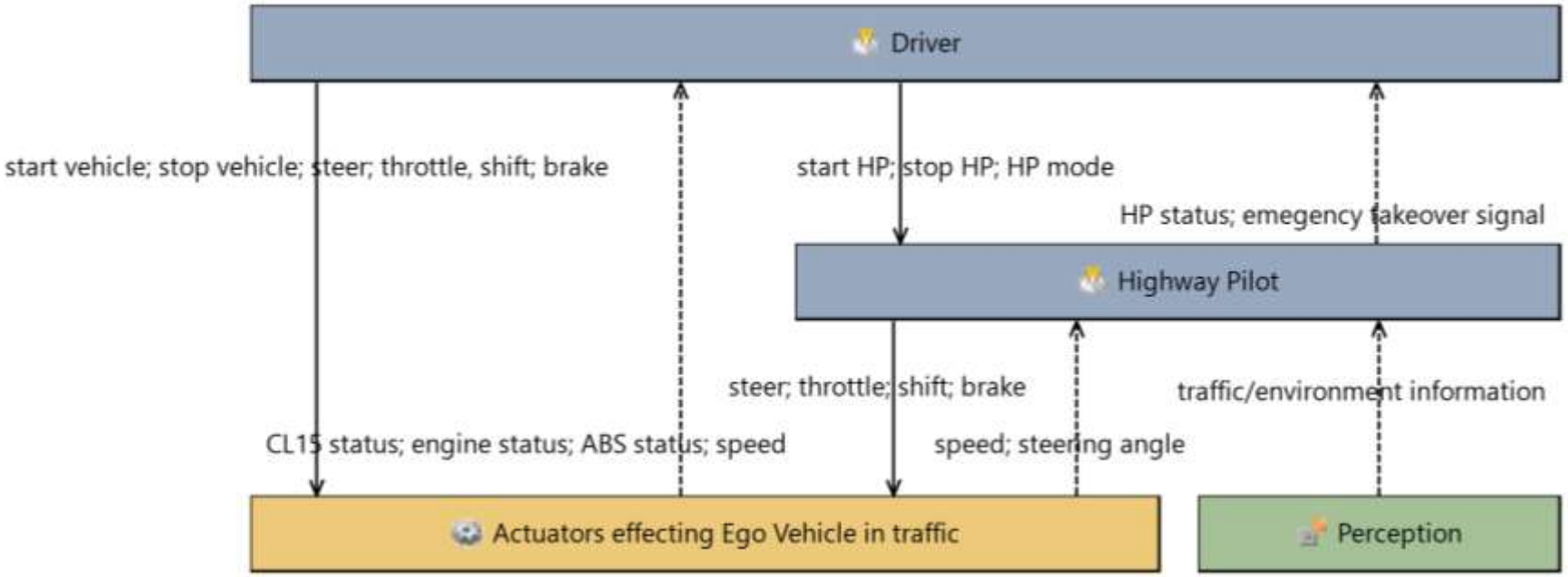
- Identify System-Level Constraints

Hazards	ID	System-Level Constraints
[H-001] Vehicle does not stay in lane	SLC-001	Highway Pilot shall keep vehicle in lane
[H-002] Vehicle impedes other road users in their movement	SLC-002	Highway Pilot shall prevent vehicle to impede other road users in their movement
[H-003] Vehicle violates safe distance to other road users	SLC-003	Highway Pilot shall prevent vehicle to violate safe distance to other road users

➔ *Losses, hazards and System-Level Constraints can be defined for FuSa and SOTIF at the same time an allocation to either domain could be done if necessary*

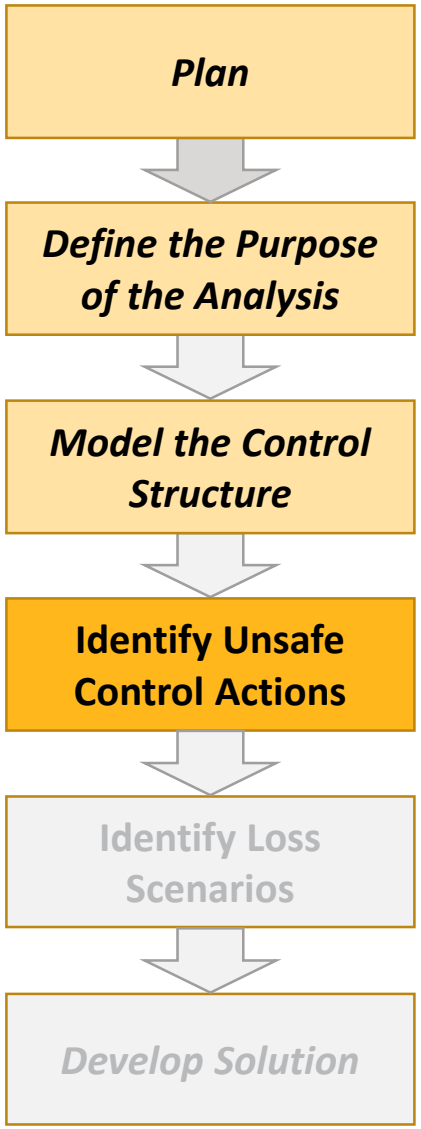


- Identify Control Elements
- Identify Control Actions
- Identify Feedback

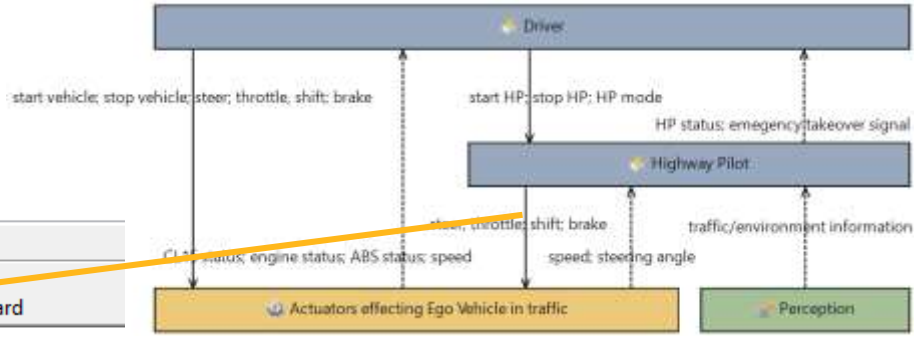


➔ *The same STAMP control structure applies for analyses and design decisions with respect to FuSa and SOTIF*

➔ *Being complementary to the physical/architectural models enables to focus on the right information for the safety analyses*



- Identify UCAs by applying guideword analysis



Control Action	Control Path	Not providing causes hazard	Providing causes hazard
[F-010] steer	Highway Pilot ↔ Actuators effecting Ego Vehicle in traffic	[UCA-001] Highway Pilot does not provide steering command while Highway Pilot enabled	[UCA-002] Highway Pilot does provide steering command while Highway Pilot disabled

- … trace them to hazards

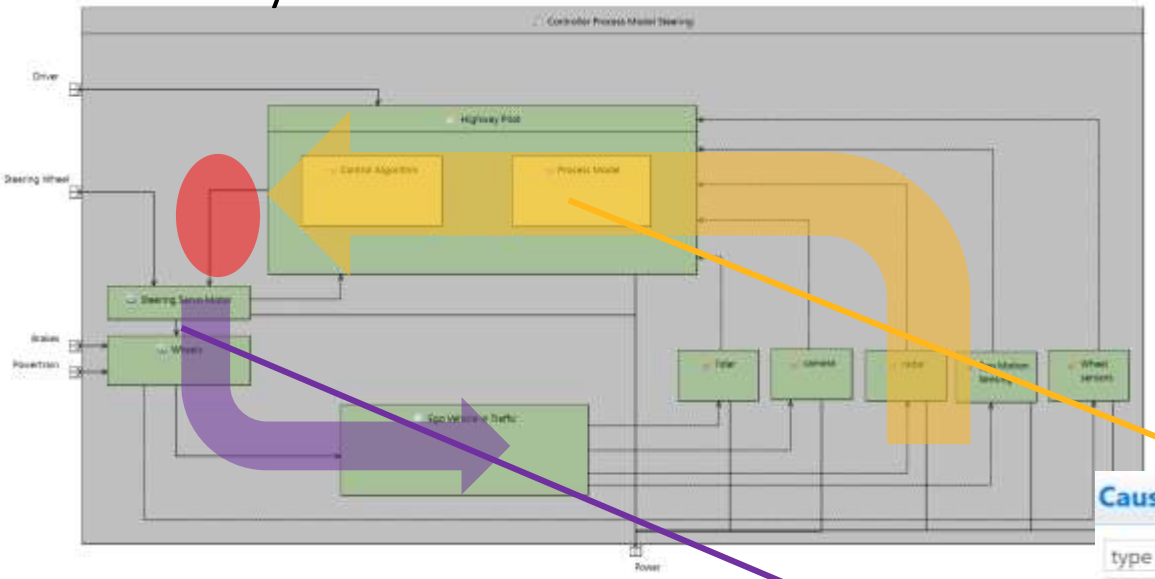
- … and derive safety constraints

Unsafe Control Action	ID	Safety Constraints
[[F-010] steer] [UCA-001] Highway Pilot does not provide steering command while Highway Pilot enabled	SC-001	Mitigate Highway Pilot not providing steering command while Highway Pilot is enabled

➔ *In case of a joined FuSa and SOTIF analysis most if not all UCAs and Safety Constraints should be the same for both disciplines*

- *Plan*
- *Define the Purpose of the Analysis*
- *Model the Control Structure*
- *Identify Unsafe Control Actions*
- **Identify Loss Scenarios**
- *Develop Solution*

- Identify Controller Process Model



- Identify Causes of Unsafe Control Actions

Causes of a Unsafe Control Action

type filter text

ID	Loss Scenario
LS-001	Highway Pilot's Process Model falsely recognizes the lane change as incomplete due to missing lane marking leading to UCA-5

- Identify improper execution of Control Actions

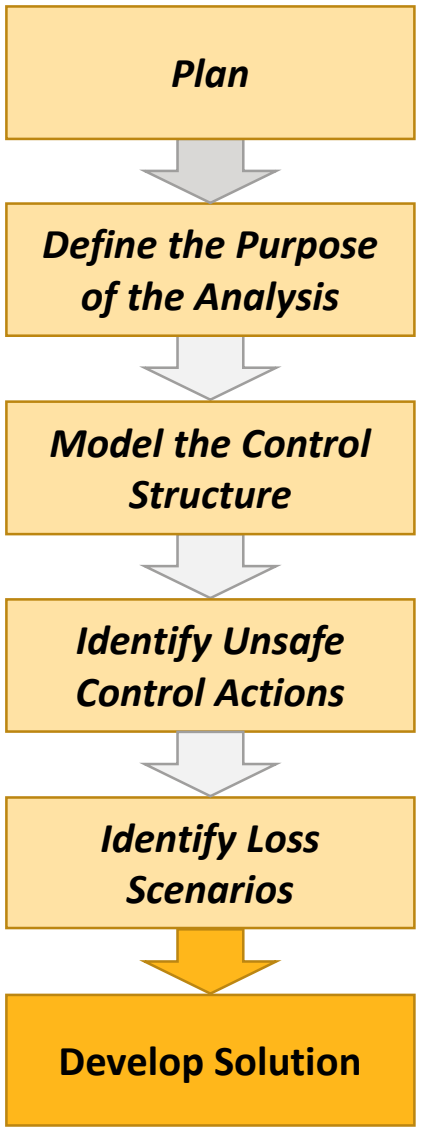
Causes for improper execution of a Control Action

type filter text

ID	Loss Scenario
LS-071	Steering Servo Motor fails to change angle of wheels due to the failure of power source leading to UCA-5

➔ The more detailed look on the controlled processes allows for a more detailed analysis compared to other methods which stop at the parts level, this higher level of detail is needed for SOTIF and allows for more detailed FuSa analysis

➔ The found Loss Scenarios can be allocated to FuSa or SOTIF or both



To be compliant to e.g. ISO26262 it is necessary to fullfill HW metrics like SPF metrics, to address this need use the inherent information of Loss Scenarios

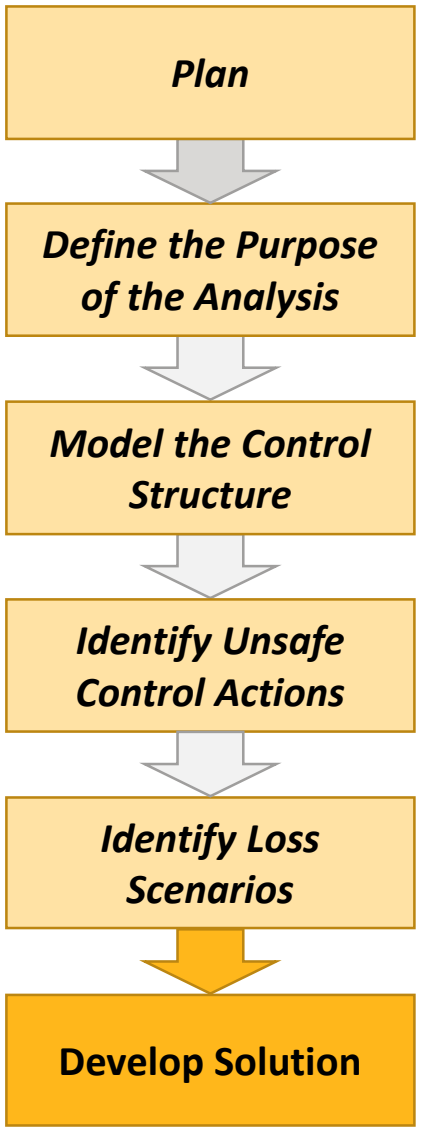
Causes for improper execution of a Control Action

type filter text

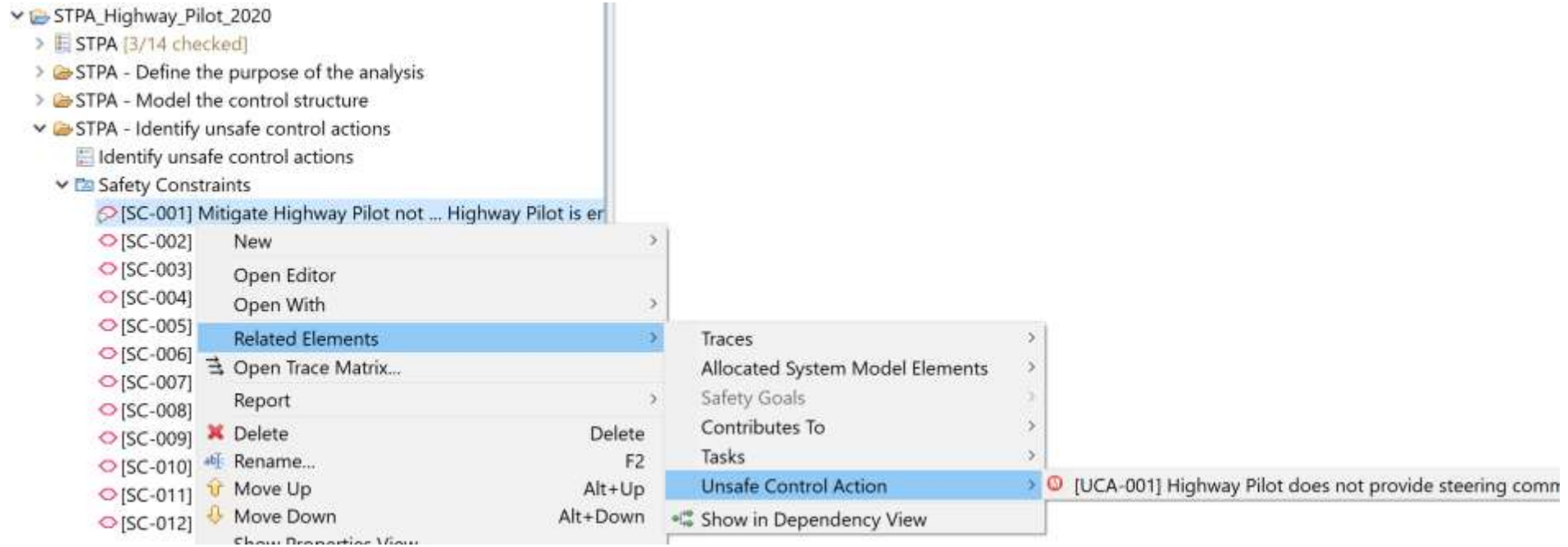
ID	Loss Scenario	Failure Modes
LS-071	Steering Servo Motor fails to change angle of wheels due to the failure of power source leading to UCA-5	[Power: 12V] No power provided [Steering Servo Motor] Failure of Steering Servo Motor

- STPA's loss scenarios include but are not limited to paths in cause/effect nets

- This information can be the starting point for and link to further analysis like FMEDA and quantitative FTA to fullfill the required metrics

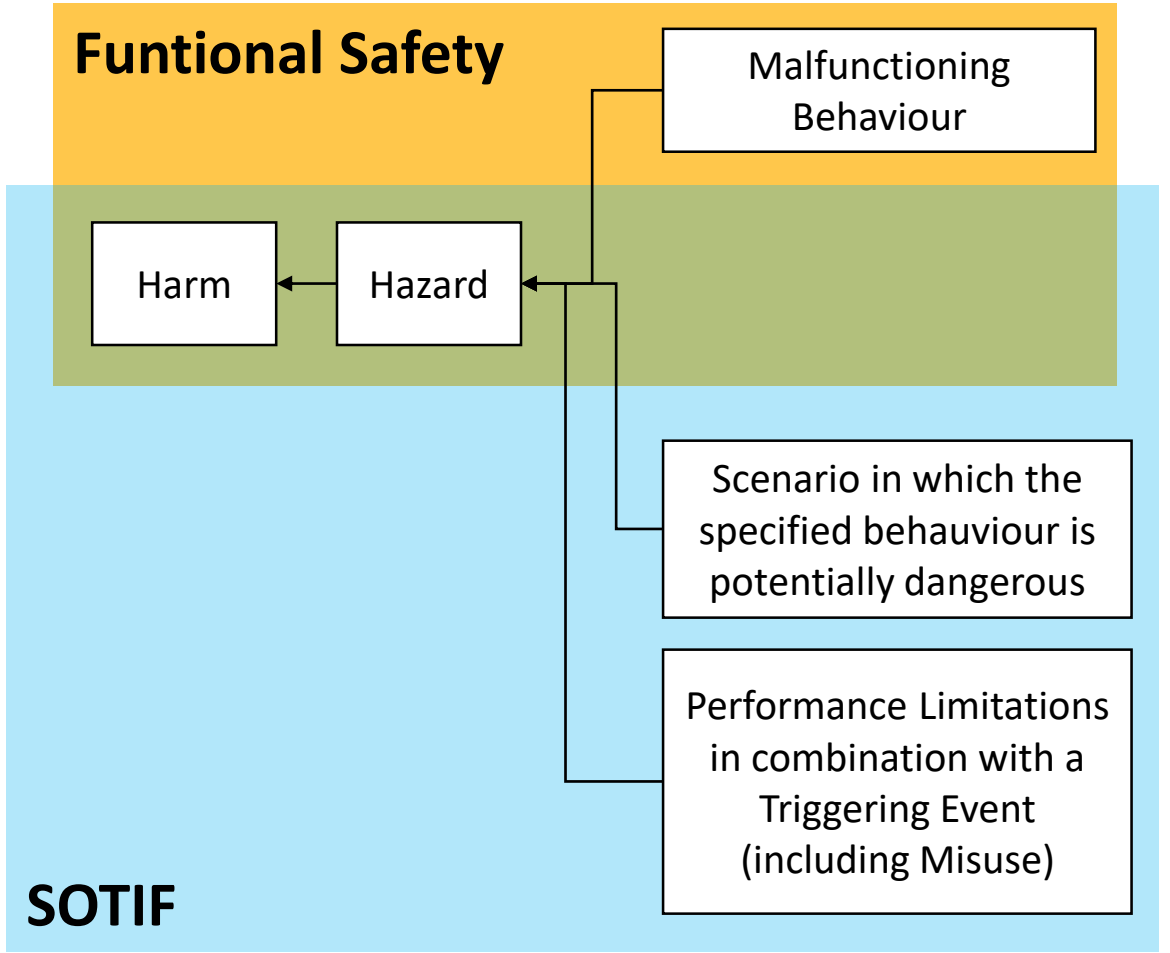


- Create a relation between STPA and your development by establishing a connection between STAMP and SysML through allocation
- Derive more detailed requirements from the Safety Constraints and allocate them to elements of the system architecture to drive the development and define responsibility
- Derive test requirements/scenarios especially for SOTIF verification and validation
- Use Task Management to organize teamwork



Conclusion: Joined analysis for FuSa and SOTIF with STPA

- STAMP is complementary to the physical/architectural models and enables to focus on the right information at a higher level of detail
- STPA steps are overlapping for FuSa and SOTIF activities which indicates an enormous possibility to save time if carried out in conjunction
- STPA's step 4 analyzes the system for malfunctions as well as limitations and triggering events



State of STPA in medini

Selected customers were provided a tech preview of STPA in medini and their feedback is used to evaluate the applicability of the features, those customers …

- Use domain specific templates for Automotive, Aerospace, and Industry
- Analyze multiple disciplines in a joined approach
  e.g. Functional Safety, SOTIF, Cyber Security, QM
- Benefit of medini's model-based approach leading to consistency and traceability
- Import and export data with medini's 3rd party tool integration capabilities
  e.g. requirements management, task management, system modelling
- Combine benefits of STAMP, pros of STPA, and other analysis methods
  e.g. STPA, HARA/PHA, FMEA, FMEDA, FTA
- Plan their activities in medini and develop technical solutions for their projects

WMG, THE UNIVERSITY OF WARWICK

21-22 OCTOBER 2020

THE USE OF STAMP FOR DEVELOPING A PROACTIVE SAFETY ENGINEERING OF THE MARITIME INDUSTRY

Osiris Valdez Banda,
Assistant Professor of Marine Technology (Research Group on Safe and Efficient Marine Systems and Experience),
Aalto University, Finland

Aalto University
School of Engineering

The use of STAMP for developing a proactive safety engineering of the maritime industry

Osiris A. Valdez Banda
Assistant Professor
Research group on Safe and Efficient Marine Systems and Experience, Aalto Marine and Arctic Technology, Finland

European STAMP Workshop and Conference (ESWC) 2020
Virtual Event organized by The University of Warwick

Overview

This presentation covers a review of five year of STAMP-based applications in the Finnish maritime cluster:

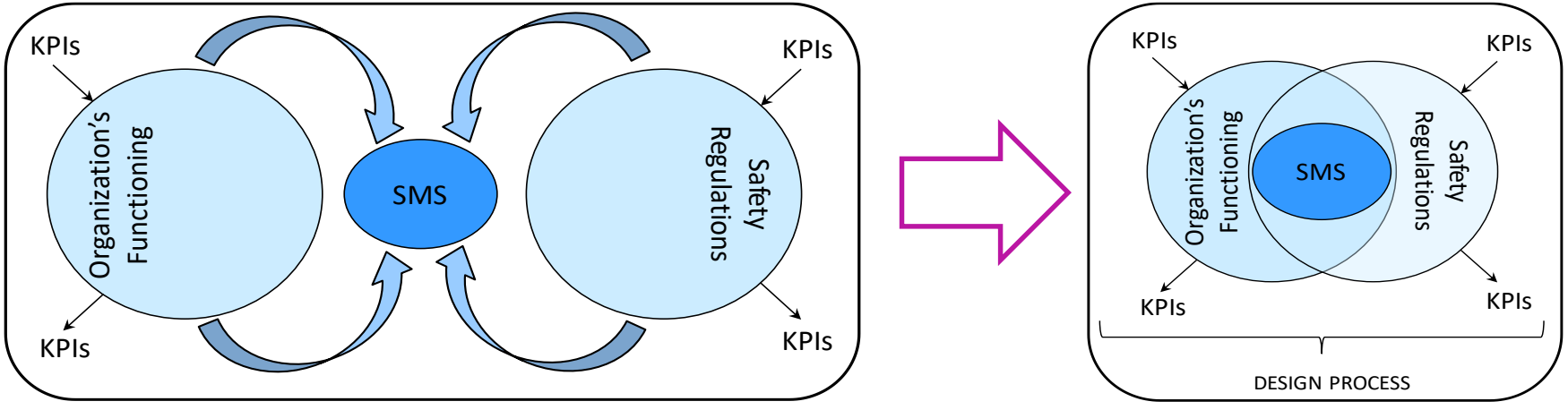
- STAMP-based approach for designing maritime safety management systems (STAMP Safety Intent Specification)
- Measuring the validity of the STAMP-based solutions (VTS case study)
- STPA for guiding the design of an autonomous vessel
- STPA against traditional modelling techniques for hazard analysis

STAMP-based approach for designing maritime safety management systems

Valdez Banda, O. A., & Goerlandt, F. (2018). A STAMP-based approach for designing maritime safety management systems. *Safety Science*, *109*, 109-129.

Aalto University
School of Engineering

Safety management perspective



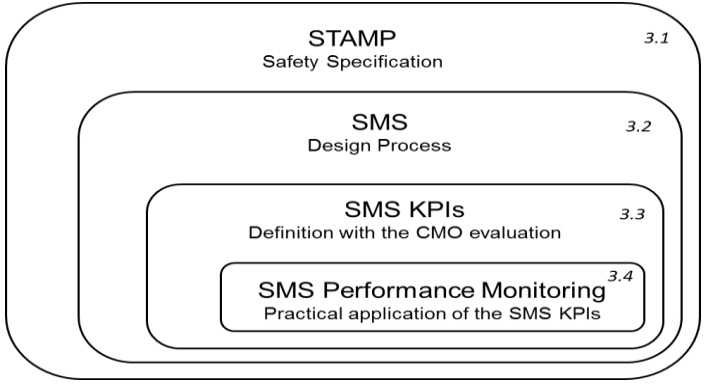
Elements influencing and interacting in the function of SMS

Aim

Elaboration of a system and safety engineering process for designing SMS. A process which can give answer to the following questions:

- How maritime organizations can systematically design SMS which can represent and constantly improve the management of safety?
- How to define safety requirements and controls which are capable of ensuring the functioning of a SMS at all levels?
- What mechanisms can be implemented to efficiently monitor, review and guide the functioning of SMS?

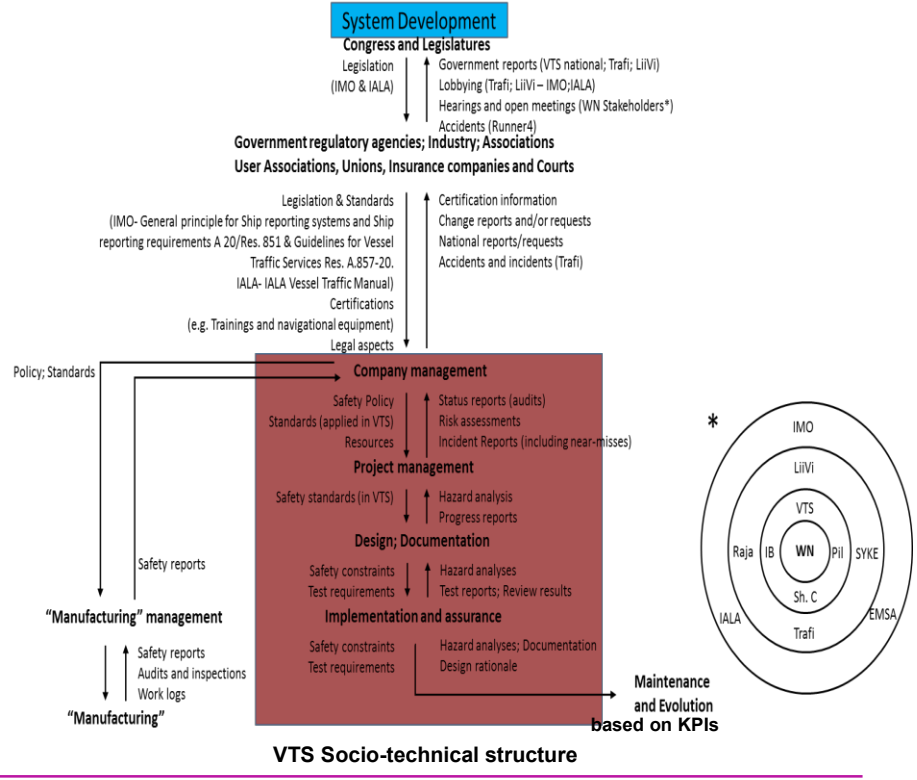
Methodology



	Environment	Operator	System and components	Verification and validation
Level 0: Program management	Management plans, safety plan, safety management procedures and safety plans			
Level 1: System purpose	Assumptions and constraints	Responsibilities Requirements	Goals, requirements, design, constraints and limitations	Preliminary Hazard analysis
Level 2: System principles	External interfaces	Task analysis and allocation, Controls and Displays	Logic principles, functional decomposition and allocation	Validation plan and System Hazard analysis
Level 3: System architecture	Environment models	Operator Task models and HCI models	Blackbox functional models and Interface specifications	Analysis plans and results, Subsystem Hazard analysis
Level 4: Design representation		Human – Computer Interface Design	Software and hardware design aspects	Test plans and results
Level 5: Physical representation		Guided User Interface design, physical control design	Software code, hardware assembly instructions	Test plans and results
Level 6: System operations	Audit procedures	Operator manuals, Maintenance and training materials	Error reports, and change request.	**Performance monitoring (KPIS)**

Safety Intent Specification

CASE STUDY:
VTS Finland



VTS Socio-technical structure

Proposed process for designing SMS

Level	Task
0	Review of the current practices for managing the function of the organization
1	Define system goals and constraints • Define accidents • Hazard identification • Preliminary hazard analysis • Environmental assumptions • Initial restrictions of the SMS • SMS requirements • Link between the requirements and detected hazards • High-level safety constraints of the SMS
2	Integrated principles for the function of the SMS under design • Interface • Hazard analysis and validation of the requirements (STPA application)
3 – 5*	Architectural design and functional allocation • Mapping of the elements in the SMS System design and physical representation. • Assessing of the SMS design and physical representation
6	Review of the actual performance of the designed SMS • Elaboration of auditing procedure • Review of personnel skills (training provision) and safety management (internal audit) • Definition of the KPIs for the SMS • Monitoring the performance of the SMS

Case study: VTS Finland

VTS Finland provides services for information, navigational assistance and traffic organization in Finnish sea areas

VTS areas:

- Bothnia VTS
- West Coast VTS
- Archipelago VTS
- Hanko VTS
- Helsinki VTS
- Kotka VTS
- Saima VTS

VTS centres:

- Gulf of Finland VTS
- Western Finland VTS
- Saima VTS

Results (1)

18 main accidents

Accident type	Accident	Navigational season
Internal	1. Fire on the VTS centre	Both seasons
	2. Blackout in the VTS centre	Both seasons
External	3. Collision ship-to-ship 3.1 In meeting 3.2 Passing 3.3 Crossing 3.4 In pilot assistance.	Both seasons
	4. Collision with a fixed object	Both seasons

26 identified hazards

Hazard	Accident
A.1 Electrical equipment without proper maintenance A.2 Flammable material no properly controlled A.3 Lighting during storm affecting electrical equipment A.4 Fire in neighbouring building and/or office	1
B.1 Power grid failure B.2 Electrical equipment without proper maintenance	2
C.1 Radar equipment without proper maintenance C.2 Image system (AIS) outdated and/or without proper maintenance C.3 Communication equipment (radio, telephone, and IT) without proper maintenance C.4 Weather causing failures (lighting storms, winter storms, heavy rain, strong winds..)	3

Preliminary Hazard analysis

Hazard	Severity				Likelihood
	H	T	E	P	
A.1	3	1	2	4	Low
A.2	3	1	2	4	Low
A.3	2	1	2	3	Low
A.4	3	1	2	3	Low
B.1	1	1	1	2	Medium
B.2	2	1	1	2	Low
C.1	1	3	1	2	Low
C.2	1	3	1	1	Low
C.3	1	2	1	1	Low
C.4	1	2	1	2	Medium

Severity Level	H Human	T Traffic operations	E Environment	P Property
4	Loos of life	Traffic operations discontinued	Catastrophic affectations to the environment	VTS centre/ ship loss
3	Severe injury or illness	Major affectations to the operations	Major affectations to the environment	VTS centre/ ship major damage
2	Minor injury or illness	Minor affectations to the operations	Minor affectations to the environment	VTS centre/ ship minor damage
1	Insignificant injury or illness	Insignificant affectations to the operations	Insignificant affectations to the environment	VTS centre/ ship insignificant damage

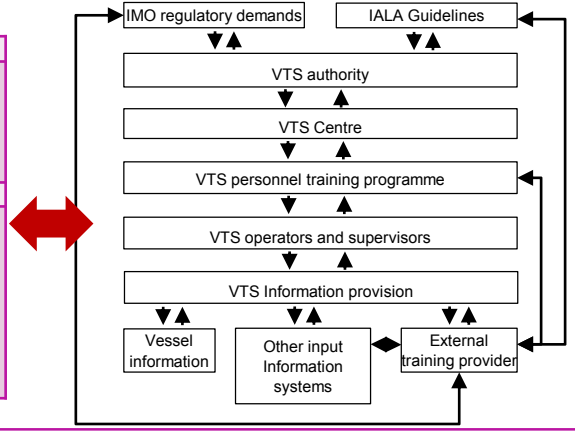
Results (2)

Definition of the practical functioning of the requirements

Req./G2/2. A vessel approaching to a point of contingency must be informed about the situation and recommendations (guidance) should be provided.	
Interface	Radio is the most common mean used to inform about contingencies in the planned route. In case communication by radio is not possible, other alternatives must be used. The requirement could have connection with other organization such as: pilots, icebreakers, SAR services, shipping company and any organisation affected by the vessel logistics chain.
Controls	Contingencies are reported by radio to VTS centres. This enables the marking and displaying of the areas of contingency within VTS monitoring system.
Logic principles	Once contingencies are reported, marked and displayed in the VTS monitoring system, VTS operators inform the potential risk to other vessels approaching the area and provide recommendations about how to proceed.

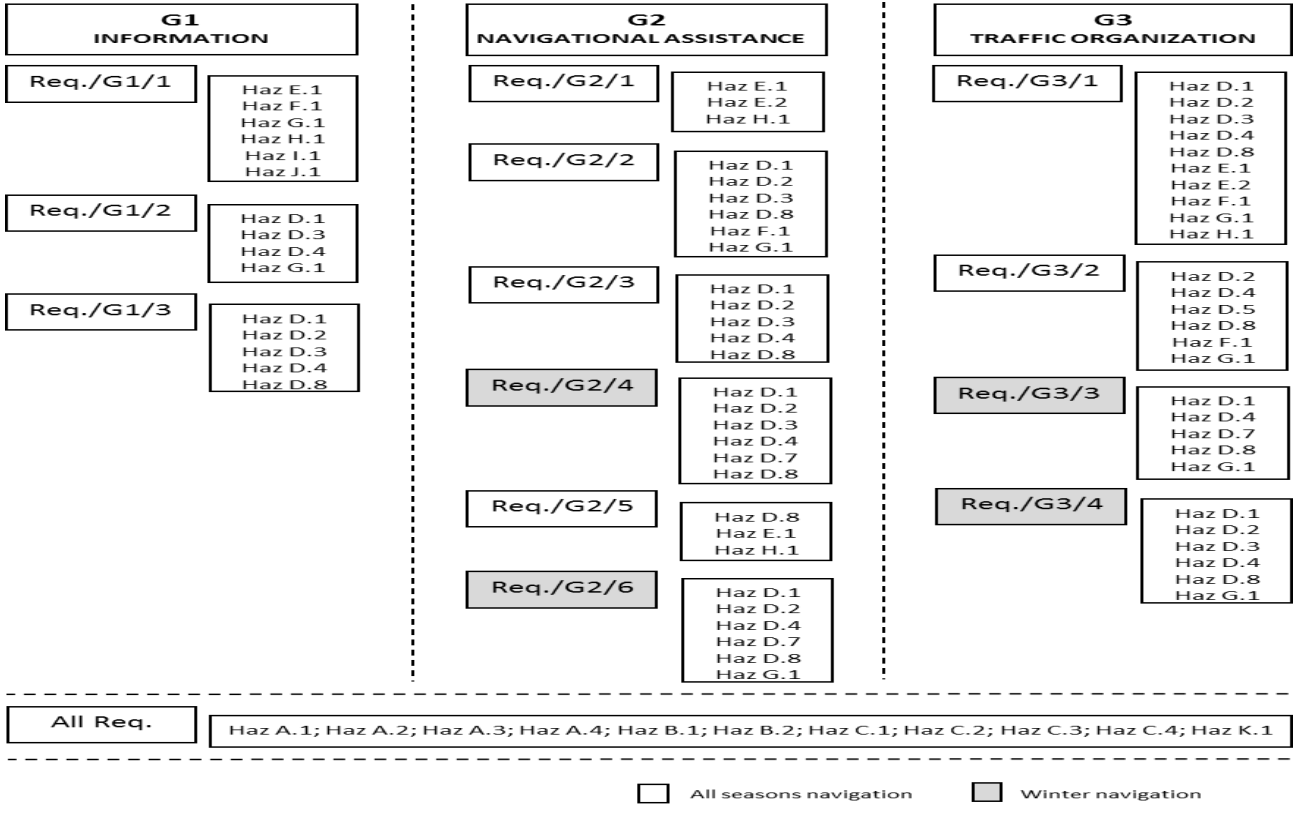
Re-defining the requirements

Detecting potentially Unsafe Controlled Actions (UCAs)
UCA 1. The training provided for VTS personnel does not consider the demands and guidelines of the existing normative. UCA 2. The training provided does not match the needs and common characteristics of an actual service provision. UCA 3. The training does not efficiently consider the actual scope and limitations on the provision of navigational assistance. UCA 4. The training does not efficiently consider the common input from relevant information systems such as pilots, icebreakers, SAR services
Redefine of the requirements (safety controls)
SC. The operators are trained to be efficient when navigational assistance. Demanded basic training by IALA is provided for operators and supervisors. The training is strengthened by having exercises in simulated environments which are evaluated by training experts. This includes: - Demanded basic training in IMO regulations (e.g. SCTW) and IALA guidelines are included in the training offered. - The training programme efficiently covers the specifications of the actual scope and limitation in the provision of navigational assistance by VTS Finland. - Trainers incorporate the actual characteristics on the exchange of information between VTS centres and vessels, including the understanding about the common conflicts during communication.



Results (3)

Requirements of the SMS



Conclusions

- The process is proficient for adopting the safety practices of the organization and transferring these into the functioning of the SMS. This enables good **cooperation and communication with the SMS stakeholders and harmonizing safety management practices**.

- The process is supported with **tools to review the safety performance of the SMS** and to revise the objectives and general functioning of the SMS.

- The designed SMS can be utilized and maintained in a smoothly and systemically manner. **This prevents making unpredicted and expensive modifications and adaptations afterwards.**

- Process downsides: time and resources consuming. Particularly, for an industry heavily educated to analyse safety and risks with traditional approaches (e.g. sequential models and tools and PRA) are promoted in official guidelines.

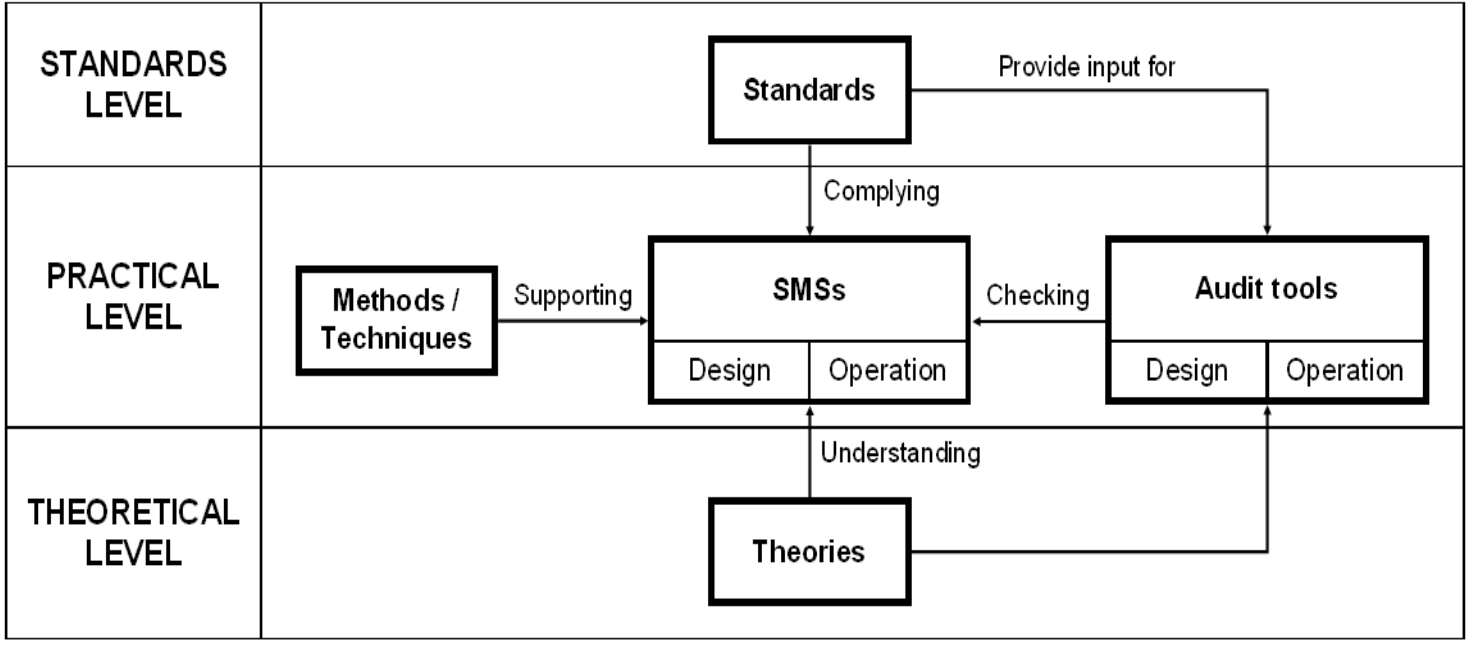
Measuring the validity of the STAMP-based solutions (VTS case study)

Valdez Banda, O. A., Goerlandt, F., Salokannel, J., & van Gelder, P. (2019). An initial evaluation framework for the design and operational use of maritime STAMP-based safety management systems. WMU Journal of Maritime Affairs, 18(3), 451-476.

Aalto University
School of Engineering

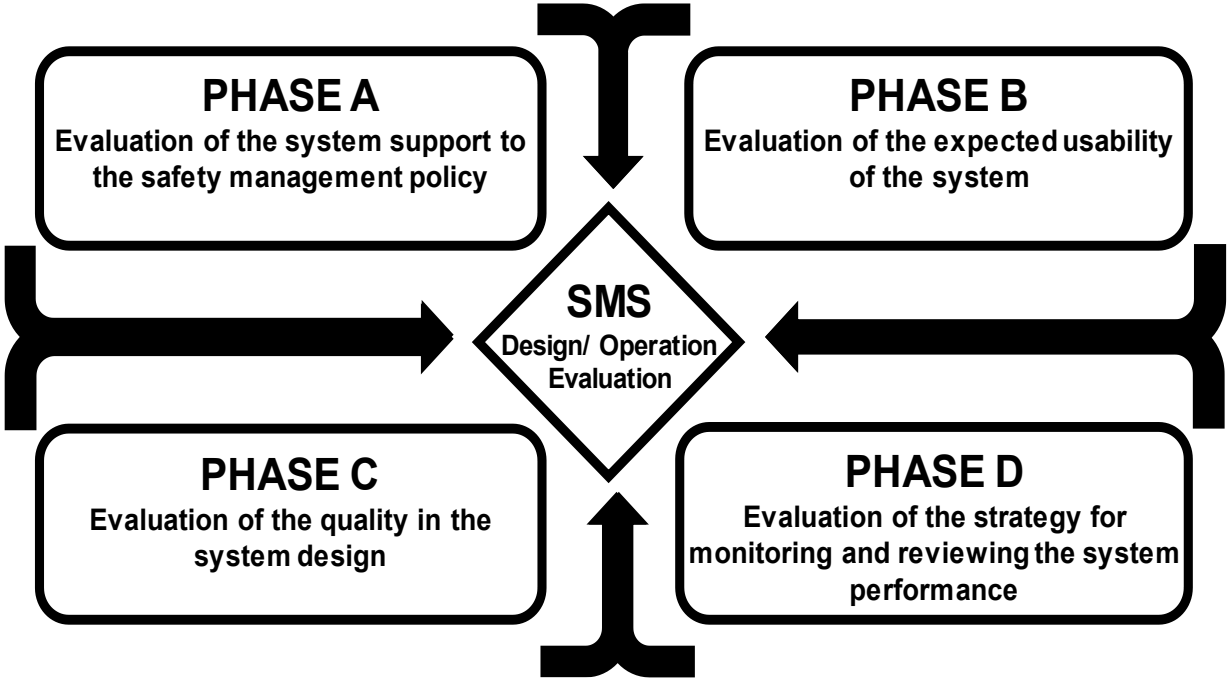
Safety Management Systems

The adopted generic model



Li and Guldenmund (2018)

Evaluation framework



Valdez Banda et al. 2019

Phase A

Evaluation of the system support to the safety management policy

Code	Capability	Queries	SMS design	SMS operation
Phase A				
A.1	Analytical	Is the SMS a good reflection of the real system?	?	?
A.2	Advisory	Is the SMS a good guide for policy application?	?	?
A.3	Strategic	Is the SMS supportive for leading the policy?		
A.4	Mediation	Is the SMS a good mediator among different stakeholders?	?	?
A.5	Participatory	Is the SMS a good promoter of personnel participation?	?	?
A.6	Argumentation	Is the scope of the SMS clear?		
		Is the SMS handling relevant information?	?	?
		Is the SMS linked to the policy practices?	?	?
		Is the SMS good for knowledge creation?		

Framework application

A workshop with ten workers of VTS Centres in Finland

One manager, two supervisors and seven officers of VTS

The workshop was organized in five sessions:

1) Introduce and explain the foundations and the general structure of the process for designing the SMS for VTS Finland.
2) Introduce the purpose, scope, and objectives of the SMS.
3) Presentation of the actual SMS.
4) The description of the KPIs and the tool designed to monitor and review the performance of the SMS.
5) Application of the framework, questionnaire and discussion

Results (1)

Phase A (Support to the safety management policy)

- 80 % of the experts found that the system design and structure accurately represent the actual safety management at VTS and the specification on regulatory demands.
- 80% agree that the designed SMS can promote and improve personnel involvement.
- 70% evaluated that the SMS features a good design to detect and anticipate potential hazards affecting the functioning of VTS.
- The survey feedback indicates that the foundations of the proposed SMS are difficult to understand in just five sessions. The experts mentioned that specialized training and practical exercises need to be organize for that purpose.

Results (2)

Phase B (Usability of the SMS)

- 70% of the experts agree the SMS is properly adapted to the safety management strategy of VTS Finland.
- 50% of the experts expect that, with the current design, the system can support the development of the safety management strategy.

Phase C (Quality of the system design)

- 80% agree that the SMS is accurate and suitable for the management of safety at VTS.
- 40% agree that the SMS should be easy to maintain
- 40% disagree that the SMS is easy to understand at glance

Phase D (SMS performance monitoring)

- Experts have a positive perspective towards the SMS capability to process to plan KPIs, collect the information, report KPI and commit to safety

Conclusions

- The application of the framework showed that the designed SMS received an overall positive evaluation in terms of how **accurately it represents safety management** at VTS.
- VTS personnel evaluated that the SMS **has potential to improve** the safety management of the organization.
- **Complete and relevant** information is covered in the SMS for matching regulatory demands and the function of the organization.
- The evaluation suggests that the **main weakness** in the designed SMS concerns **the description of the complexity of the system**.
- The evaluation indicated that the **SMS is not** yet ready/mature enough to be implemented (without appropriate training) but it shows high potential.

STPA for guiding the design of an autonomous vessel

Valdez Banda, O. A., Kannos, S., Goerlandt, F., van Gelder, P. H., Bergström, M., & Kujala, P. (2019). A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. Reliability Engineering & System Safety, 191, 106584.

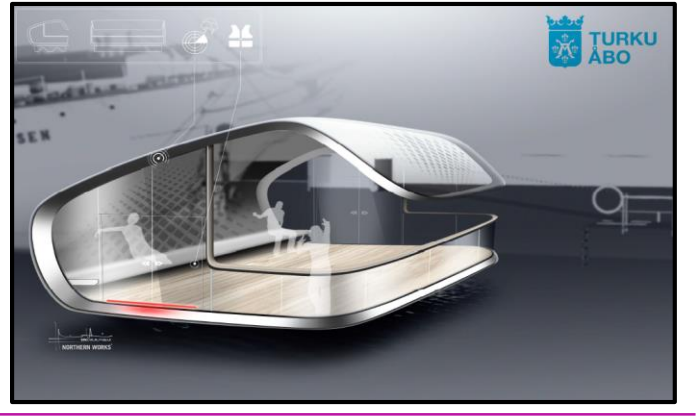
Aalto University
School of Engineering

Process foundations and application

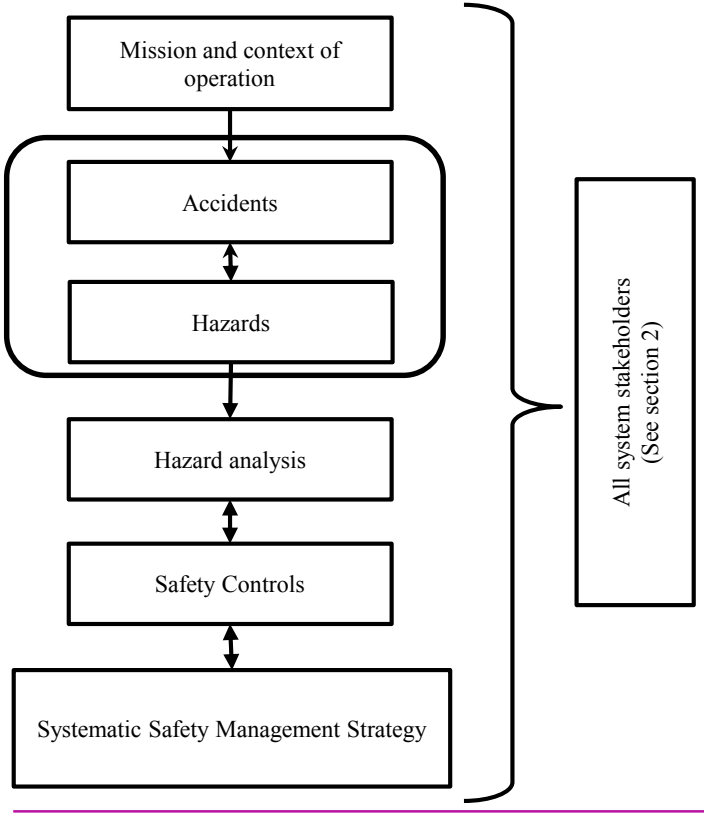
STPA is utilized as the basis for an analysis process that can be used in **the earliest design phase**, providing initial information to guide the subsequent design stages.

The aim is to support the subsequent **design stages** with the provision of valuable information to ensure efficiency and safety.

This process is applied to **analyse the safety hazards** in the foreseen functioning of two concepts of autonomous ferries operating in urban waterways.



The process



Step	Task
1	Definition of accidents and identification of hazards
2	Detailed hazard description and definition of mitigation actions
3	Definition of the safety controls
4	Unsafe control actions (UCAs) and redefinition of safety controls
5	Representation of the initial safety management strategy

Data

The process uses information produced in:

- Previous maritime risk analysis and,
- **The analysis of the new operational context of these autonomous vessels (expert consultation):**

Lloyd's Register, Suomenlinnan Liikenne Oy, VG-Shipping Oy, Fleetrange Oy, Trafi, ABB Marine, Varsinais-Suomen Pelastuslaitos, Rajavartiolaitos, Uudenkaupungin Työvene Oy, Besase Oy, Arctia Shipping Oy, Yrkeshögskolan Novia, Aalto University, Metropolia Ammattikorkeakoulu, SSF Oy, Paikkatietokeskus FGI, Rosita Oy, Meriturva, City of Turku.

Process: step one

Definition of accidents and identification of hazards

- 10 accidents covered
- 15 Hazards identified and analyzed
- Clear interconnection among accidents and hazards
- Combinatorial analysis of current accidents and expected accidents for autonomous vessels

Accident	Hazards
1. Allision with a pier	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical failure) H4. Heavy weather/sea conditions H5. Strong currents H6. Position reference equipment failure
2. Collision with a moving object	
2.1 Collision with another vessel	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical fault)
2.2 Collision with a small moving target (e.g. canoe, SUP-board, etc.)	H1. Object detection sensor error H2. AI software failure H3. Technical failure (e.g. mechanical failure)
3. Collision with a fixed object (e.g. buoys, beacons, etc.)	H1. Object detection sensor error H2. AI software failure H3. Technical fault (e.g. mechanical failure) H4. Heavy weather/sea conditions H5. Strong currents H6. Position reference equipment failure
4. Grounding	H2. AI software failure H3. Technical failure (e.g. mechanical failure) H6. Position reference equipment failure H4. Heavy weather/sea conditions H5. Strong currents
5. Bottom touch	H2. AI software failure H3. Technical failure (e.g. mechanical failure) H6. Position reference equipment failure H4. Heavy weather/sea conditions H5. Strong currents
6. Capsizing/ Sinking	H7. Overloading of the vessel H8. Shifting of weights H9. Flooding
7. Fire on board	H10. Ignition of electrical equipment or wiring H11. Passenger starting a fire
8. Man over board	H12. Unintended falling overboard H13. Intended jumping overboard
9. Medical emergency on board	H14. Person(s) getting injured H15. Person(s) medical condition
10. Medical emergency on pier	H14. Person(s) getting injured H15. Person(s) medical condition

Process: step two

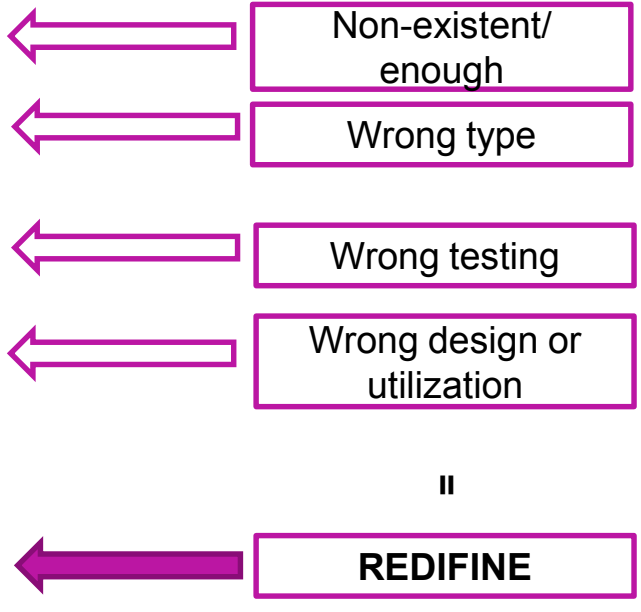
Detailed hazard description and definition of mitigation actions

Hazard	H1. Object detection sensor error		
Hazard effect/ description	What exactly? How severe?		
Causal factors	Potential causes?		
Mitigation actions	What can we do? How to mitigate/control it?	Cost/Difficulty High Low Medium Medium Low Low Low	Approach (1-4) * 4 3 3 4/3 3 3 2
*Mitigation approach	Level 4 3 2 1	Detailed description Attempt to completely eliminate the hazard Attempt to reduce the likelihood that the hazard will occur Attempt to reduce the likelihood that the hazard results in an accident Attempt to reduce the damage if the accident occurs	

Process: step three and four

Unsafe control actions (UCAs) and redefinition of safety controls: how the safety control can fail and why?

Safety controls (mitigation approach)
SC 1 Sensor system redundancy and diversity
Detecting potentially Unsafe Controlled Actions (UCAs) and redefining the safety control
UCA 1. Sensor does not function properly and there is no other sensor available
Potential causes
- Lack of economic resources
UCA 2. Equipment chosen to provide the redundancy are not suitable
Potential causes
- Lack of economic resources
- Lack of knowledge of sensors characteristics when planning the equipment set needed
UCA 3. Sensor failure is not detected
Potential causes
- Not enough coverage with the diagnosis
UCA 4. External or common cause failures takes several equipment down at the same time
Potential causes
- Inappropriate system design
- Incorrect installation
- Incorrect usage
- Environmental conditions
Redefining of the safety control
- If one sensor fails the redundancy ensures there is going to be another sensor functioning
- Equipment chosen to provide the redundancy have to be the correct ones in order to provide the user with the required information at all times



Process: step five

Representation of the initial safety management strategy

Safety Control (SC)	Accident 1	2,1	2,2	3	4	5	6	7	8	9	10
1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1 H1 H1	H1	H1		H10			
2	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H10			
3	H2 H1 H4	H2 H1	H2 H1	H2 H1 H4	H2 H4	H2 H4		H11			
4	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
5	H3 H1 H4	H3 H1	H3 H1	H3 H1 H4	H3 H4	H3 H4			H12	H12	H12
6	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H8		H12		
7	H4 H2 H4	H2	H2	H4 H2 H4	H4 H2 H4	H4 H2 H4	H9		H12		
8	H4 H2	H2	H2	H4 H2	H4 H2	H4 H2	H7 H9		H12		
9	H3	H3	H3	H3	H3	H3	H7	H11	H12		
10	H3	H3	H3	H3	H3	H3	H7	H11		H14	H14
11	H4			H4	H4	H4	H7	H11		H14	H14
12	H4			H4	H4	H4	H8			H14	H14
13	H6			H6	H6	H6	H8			H14	H14
14	H6			H6	H6	H6	H9				
15	H6			H6	H6	H6	H9				
16	H6			H6	H6	H6	H8	H10			
17							H8		H12		
18							H9		H12		
19							H9			H14	H14
20								H10			
21								H10			
22								H10			
23								H11			
24								H11			
25									H12	H12	H12
26									H12		
27										H14	H14
Total SC	31	16	16	31	25	25	15	12	10	9	9

SC control strategy:

- Attempt to eliminate the hazard
- Reduce the likelihood that the hazard will occur
- Reduce the likelihood that the hazard results in an accident
- Reduce the damage if the accident occur

Conclusions

The process produces itemized information **to guide (with information of safety demands) the initial design** of the autonomous ferry and the components of its operational system.

The logic principle of the safety controls provides the **foundations for developing a safety management strategy** at the earliest design phase.

The study results support the elaboration of **plans, conceptual designs, ship arrangements, and the setting** of other crucial elements for designing and building the autonomous ferry.

Comparison of the modeling approaches and risk analysis methods for complex ship systems

Valdez Banda, O., Kujala, P., Hirdaris, S., & Basnet, S. (2020). Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC) 2019.

Aalto University
School of Engineering

Aim and motivation

Autonomous projects – unavailability of data for probabilistic methods.

Development of advanced technologies – need to focus on new types of risks. i.e. software errors, design errors and risks due to unsafe interactions.

Dominant risk analysis methods:

Failure Mode and Effects Analysis (1949)

Fault Tree Analysis (1962)

Case study (FTA vs STPA)

Case:	Implementation of methods in some parts of Azimuth thruster.
Location:	Rolls-Royce research and development center, Turku, Finland
Aim:	Test and evaluation of the methods with experts in R-R.
Test:	The methods were implemented to model and identify risks in a part of the azimuth thruster. Experts of Rolls-Royce (with diverse backgrounds) and familiar to the functionality of the azimuth thruster implemented the methods.
Tools:	Edraw Max (Tree structure method and Fault Trees Analysis) RMStudio (STPA)

Evaluation

Fault Trees Analysis					
Criteria's	**Expert 1**	**Expert 2**	**Expert 3**	**Expert 4**	**Average rating**
Method complexity	4	4	4	5	**4.3**
Analysis time	4	3	5	5	**4.3**
Risk Identification	2	3	5	3	**3.3**
Risk Mitigation	1	3	1	3	**2.0**
Structure of the model	3	4	4	5	**4.0**

Systems-Theoretical Process Analysis					
Criteria's	**Expert1**	**Expert 2**	**Expert 3**	**Expert 4**	**Average rating**
Method complexity	3	2	2	3	**2.5**
Analysis time	3	3	2	3	**2.8**
Risk Identification	4	3	3	4	**3.5**
Risk Mitigation	4	3	3	3	**3.3**
Structure of the model	4	2	4	3	**3.5**

0 – 1.0	Poor
1.1 – 2.0	Satisfactory
2.1 – 3.0	Average
3.1 – 4.0	Good
4.1 – 5.0	Excellent

- **FTA is simpler and faster** to implement than STPA (parituclalry is you are familiarized with it.
- However, STPA **is better at identifying and mitigating risks** related to component interactions and human errors than FTA.
- **STPA has a greater capability** to support the further development and application of the systems

Conclusions

Conclusions (1)

- **In Finland,** the maritime cluster is eager to find and test alternatives for safety proactive methods that ensure and enhance maritime shipping.

- **STAMP** as system-theoretic model of accidents offers a systemic and proactive approach for dealing with the risk of the complex socio-technical system integrated in advance maritime shipping concepts.

- **STPA** has been utilized and tested against traditional methods, attracting the interest of several stakeholders who are leading the work for advance maritime shipping concepts (e.g. Smart/ autonomous/ resilience ships).

Conclusions (2)

- Maritime safety researchers we still face **some resistance** in the introduction of advance methods (e.g. STPA) particularly in the link to methods recommended by regulations. However, new issues represented in current research case studies are creating the need for inclusion and utilization of new methods.

- The application of STAMP and its family tools continues in the concept of smart shipping (Autonomous shipping and remote piloting operations). Some references below:
  - *Chaal, M., Valdez Banda, O. A., Glomsrud, J. A., Basnet, S., Hirdaris, S., & Kujala, P. (2020). A framework to model the STPA hierarchical control structure of an autonomous ship. Safety Science, 132, 104939.*
  - *Basnet, S., Valdez Banda, O. A., Chaal, M., Hirdaris, S., & Kujala, P. (2020). Comparison of system modelling techniques for autonomous ship systems. In Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) 2019 (pp. 125-139). Sciendo.*

Thank you

Osiris A. Valdez Banda
Assistant Professor
Research group on Safe and Efficient Marine Systems and Experience,
Aalto Marine and Arctic Technology, Finland

osiris.valdez.banda@aalto.fi