ρTechnology

experience & innovation

CO-CPS: A sample XSTAMPP usage in V2I traffic management scenario based on STAMP model

5° Scandinavian Conference on

SYSTEM & SOFTWARE SAFETY

Stockholm, May 22-23, 2017

ρTechnology

experience & innovation

Agenda

- RoTechnology R&D Area
- V2I Traffic Management scenario
- The STAMP model
- Applying EWaSAP to System-of-Systems
- The XSTAMPP tool
- Wrap-up

R&D Area

Participating in research projects fosters our technical capacities and nurtures our staff. Our main objective is the participation to the European programs in association with reference companies and universities.

MegaM@Rt2 An scalable model-based framework for continuous development and runtime validation of complex systems
Coordinator: SOFTEAM, France

Teinvein Vehicle Interfacing System to the environment and other vehicles for sustainable mobility.
Coordinator: STMicroelectronics

SafeCOP Safety of cyber-physical systems, with wireless communication, multiple stakeholders in unpredictable environments.
Coordinator: Alten Sverige AB

Seamless A Geo-referenced system for data acquisition over a secure, encrypted and energy-efficient WSN
Coordinator: Ro Technology

Unione Europea Fondo Europeo di Sviluppo Regionale fesr Regione Lombardia

MINISTERO DELLA DIFESA

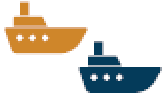
ECSEL Joint Undertaking Electronic Components and Systems for European Leadership

SafeCOP

- V2I traffic management scenario in Safe Cooperating Cyber-Physical Systems using Wireless Communications (SafeCOP)

V2I in SafeCOP

- Aims to provide an approach to the safety assurance of the Cooperative Open Cyber-Physical Systems (CO-CPS) for multiple stakeholders and variable operating environments
- Main objectives:
  - Security of communications
  - Security framework for runtime mechanisms
  - Traffic management application

UC1. Cooperative moving of empty hospital beds	UC2. Cooperative bathymetry w/ boat platoons	UC3. Vehicle control loss warning	UC4. Vehicles and roadside units interaction	UC5. V2I cooperation for traffic management
				

V2I in SafeCOP

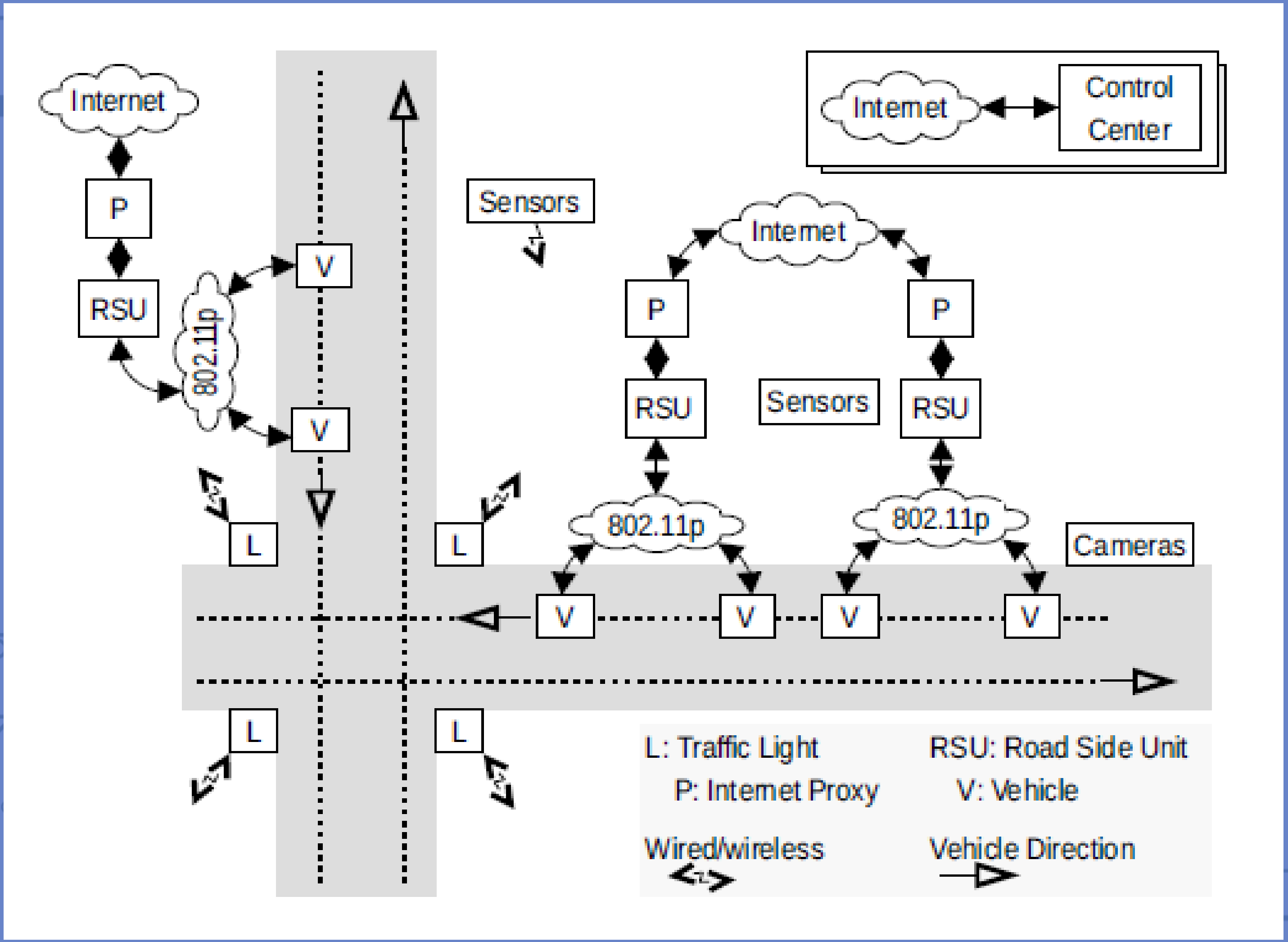
Cooperative Awareness Messages (CAM)

Traffic Management Application

Green Light Optimal Speed Advisory (GLOSA)

Adaptive Traffic Light System (A-TLS)

V2I in SafeCOP



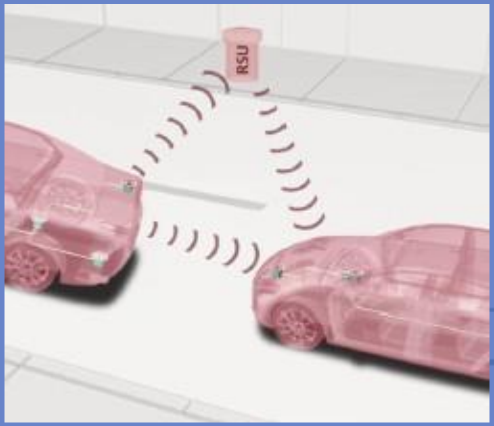
V2I industrial scenario Block Diagram

V2I in SafeCOP

- On Board Units (OBU) collect individual vehicle data:
  - Dynamic data (e.g. accelerations, angular speeds, magnetic field)
  - Position data (e.g. latitude/longitude, speed, heading)
  - Vehicle data (e.g. brake, engine rpm, gear)
- Main components:
  - 9-DOF inertial measurement unit
  - High-precision GPS receiver
  - CAN bus interface connected to the OBD
  - V2I connectivity module (e.g. 3G/4G, wireless 802.11.p)

V2I in SafeCOP

- Road Side Units (RSU) receive CAM from OBUs and is equipped with legacy sensors that detect passing vehicles.
- Main components:
  - Camera (provides video feed to the Control Center)
  - V2I connectivity module (e.g. 3G/4G, wireless 802.11.p, Wired)



V2I in SafeCOP

- Traffic Management Application **basic functions:**
  - Collect data, perform data fusion and determine vehicle types and their kinematics
  - Optimize and actuate the traffic light signaling plan in a coordinated manner
  - Compute and distribute to vehicles their optimal speeds

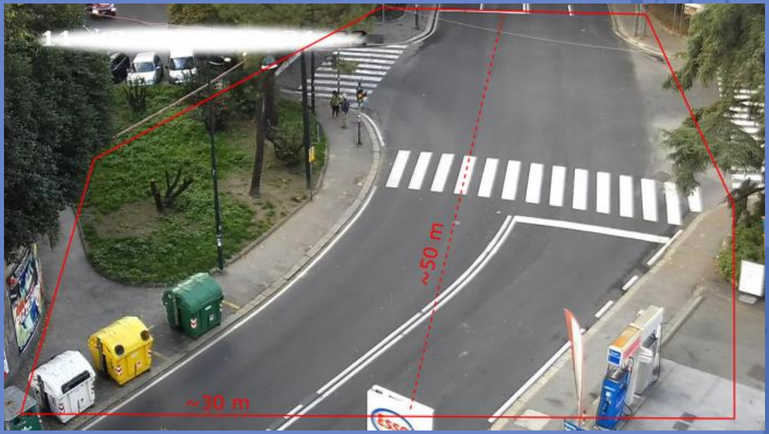
V2I in SafeCOP

- Traffic Management Application **hazards functions:**
  - Check for malicious attack to the wireless network
  - Monitor communication congestion/interruption
  - Detect dangerous traffic conditions
- Switching Neural Network (SNN) creates intelligible rules that requires a very small amount of computational resources allowing an efficient implementation on simple hardware devices (e.g. FPGA, 8-bit microcontroller)

```
if
   (level of congestion > threshold_1)
  and
   (frequency of specific flags in the
     packet headers > threshold_2)
  and
   (number of open sockets > threshold_3)
then
   (risk alert is above the acceptable
    threshold)
```

V2I in SafeCOP

- Video Content Analysis (VCA) platform running on the Control center is capable to extract information about potentially dangerous situations:
  - Presence of objects moving inside the reference area
  - Presence of motionless objects in the reference area for longer than a minimum time threshold
  - Detection of vehicles slowing down inside the scene
  - Vehicles moving in forbidden directions
  - Presence of people inside sensitive areas
  - Detection of dangerous environmental conditions (e.g. smoke, fog, fire) in sensitive areas



- **Systems-Theoretic Accident Model and Process (STAMP)**

ρTechnology

experience & innovation

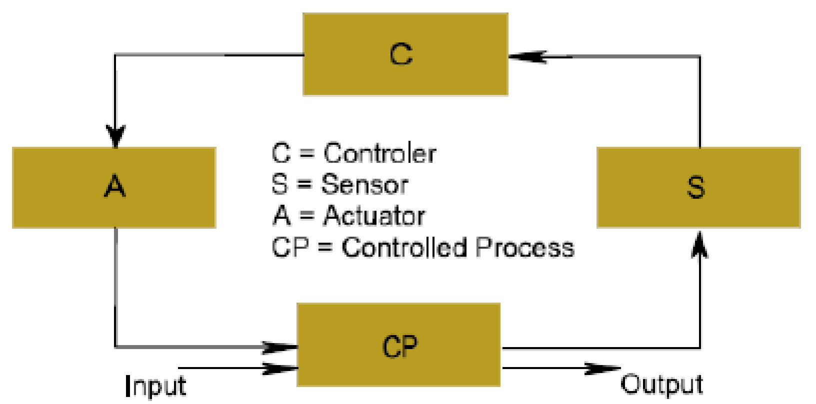
STAMP

- Accident = undesiderable or unplanned event that leads to a loss.

- Hazard = a system state or set of conditions that combined with the worst-case environmental conditions will lead to an accident.

STAMP

- Accidents are treated as a control problem.
- Safety Constraints are enforced on component behaviour and interactions.



STAMP basic control loop

STAMP

- System Theoretic Process Analysis (**STPA**) = developed to include the causal factors identified by STAMP methodology
- STPA for Security (**STPA–SEC**) = identify security vulnerability and requirements in addition to traditional STPA.
- Causal Analysis based on STAMP (**CAST**) = used to identify questions to fully understand why accidents occours.
- Early Warning Sign Analysis based on the STPA (**EWaSAP**) = Aims to identify perceivable signs which indicate flaws in process control loops of the system

- Early Warning Sign Analysis based on the STPA (**EWaSAP**)

STPA

- Top-Down approach
- Defines three steps :
  0) **Identify hazards and accidents, initial control structure**
  1) **Define unsafe control actions**

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order causes hazard	Stopping too soon/applying too long causes hazard

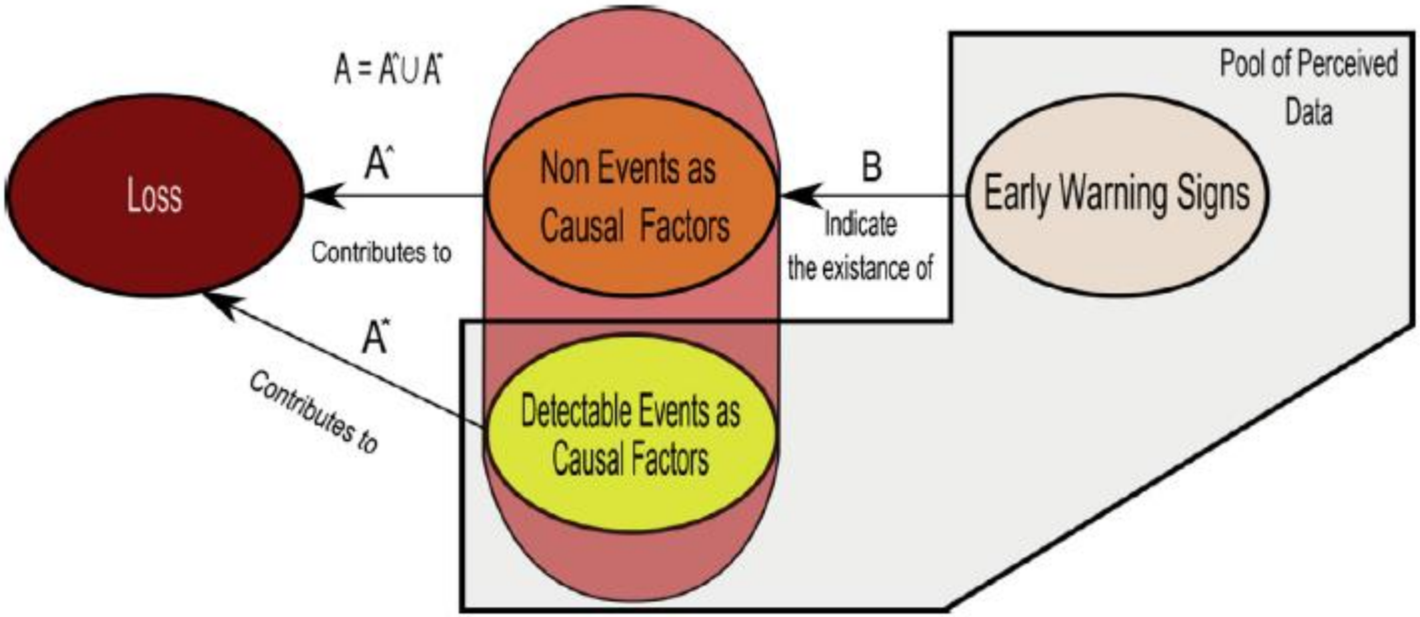
  2) **Define causal scenarios:**
    - For each unsafe control action investigate the control loop to identify possible scenarios of how it could be triggered
    - For each control action, identify what can cause its inappropriate execution
- Output = Safety Requirements

EWaSAP

- An extension of STPA analysis that adds awareness actions, enabling controllers to transmit warnings and alerts that justify the presence of flaws and vulnerabilities in their controlled process based on the process models they posses.
- Find factors that are out of the pool of the possible perceived data that traditional hazard analyses are unable to detect due to limitations of the inner nature of sequential accident models:
  - Managerial deficiencies
  - Safety culture flaws
  - Undesirable behaviours and ineractions of system components
  - Software flaws
  - System changes due to evolution and adaptation that affect safety

EWaSAP

I.M. Dokas et al. / Safety Science 58 (2013) 11–26



EWaSAP justification model

- Step 1: find anyone/anything outside the system who need to be informed about perceived progress status (e.g. emergencies operators)
- Step 2: identify useful tools (e.g. sensory devices) belong to systems outside the one in focus and establish synergy
- Step 3: Enforce Internal Awareness Actions

EWaSAP

- Typical classification of awareness actions refers to the transmission of:
  - **“all clear” signals** (controlled process is in a safe state)
  - **Warnings** (perceived data signals the presence of flaws in the controlled process)
  - **Alerts** (hazard occurred in the controlled process)
  - **Algedonic signals** (special alarms and rewards that are sent directly to the controllers at the highest levels of the hierarchy when a serious condition is detected)

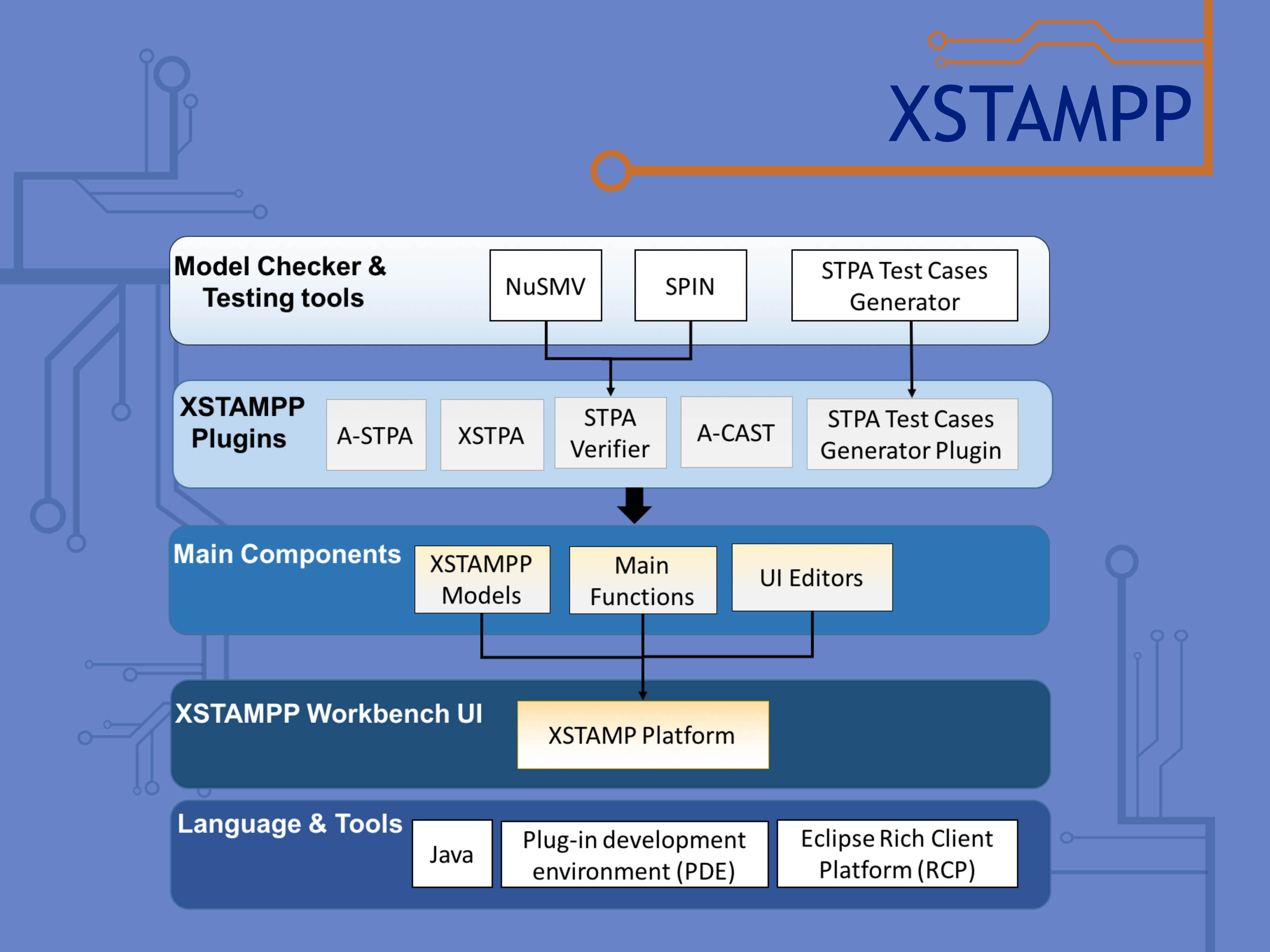
EWaSAP

- Safety challenge: design the perceived signs and the transmitted warning signals in a way that will not contribute to system hazards:
  - Not transmitted
  - Not perceived or hard to be perceived
  - Incomprehensible
  - false

- XSTAMPP- a tool for Safety Engineering of Software Intensive Systems

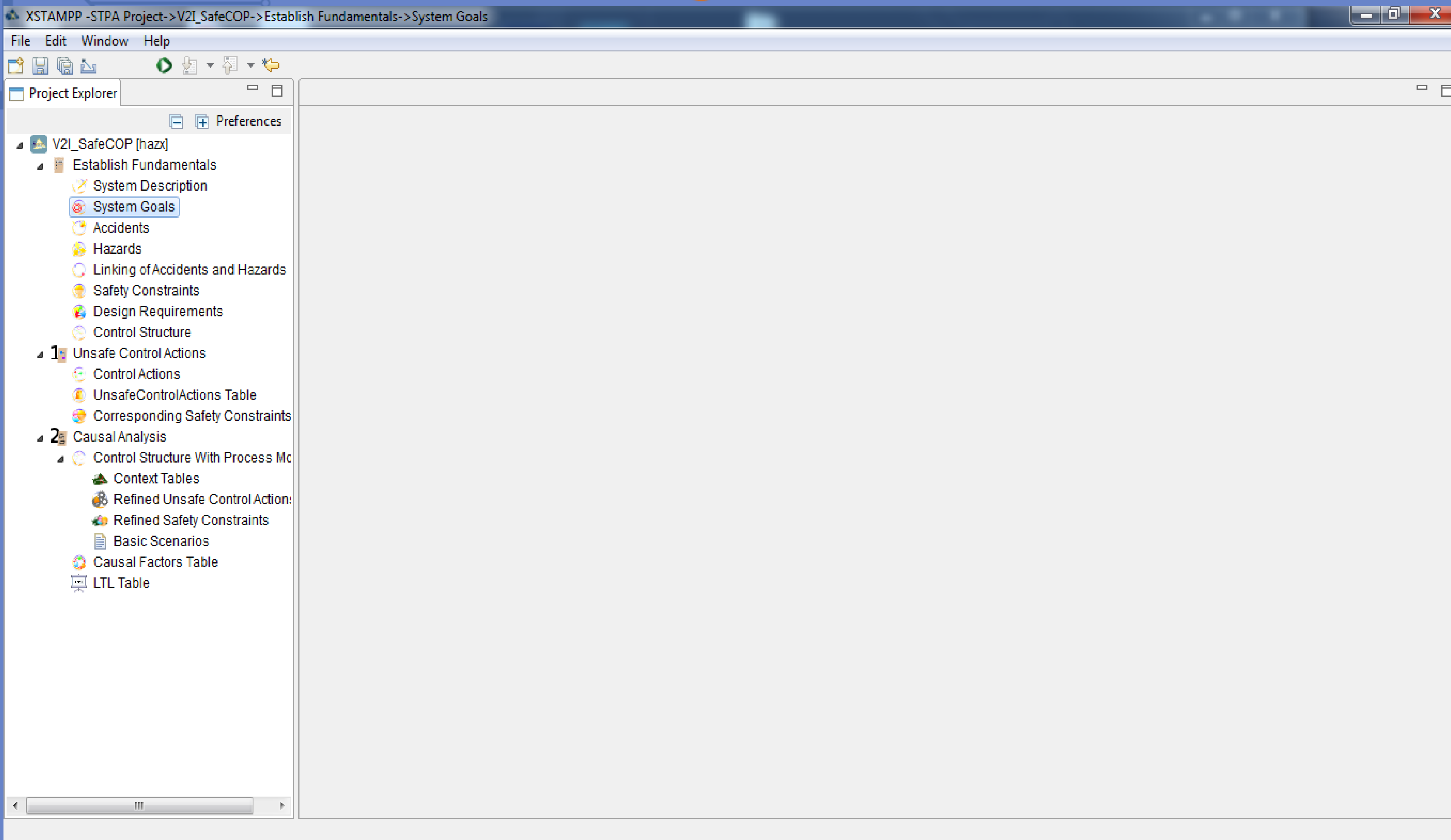
XSTAMPP

- Developed by Institute of Software Technology, University of Stuttgart, Germany
- Support platform designed to serve the widespread adoption of STPA and to guide the users through the design process of the system
- http://www.xstampp.de/



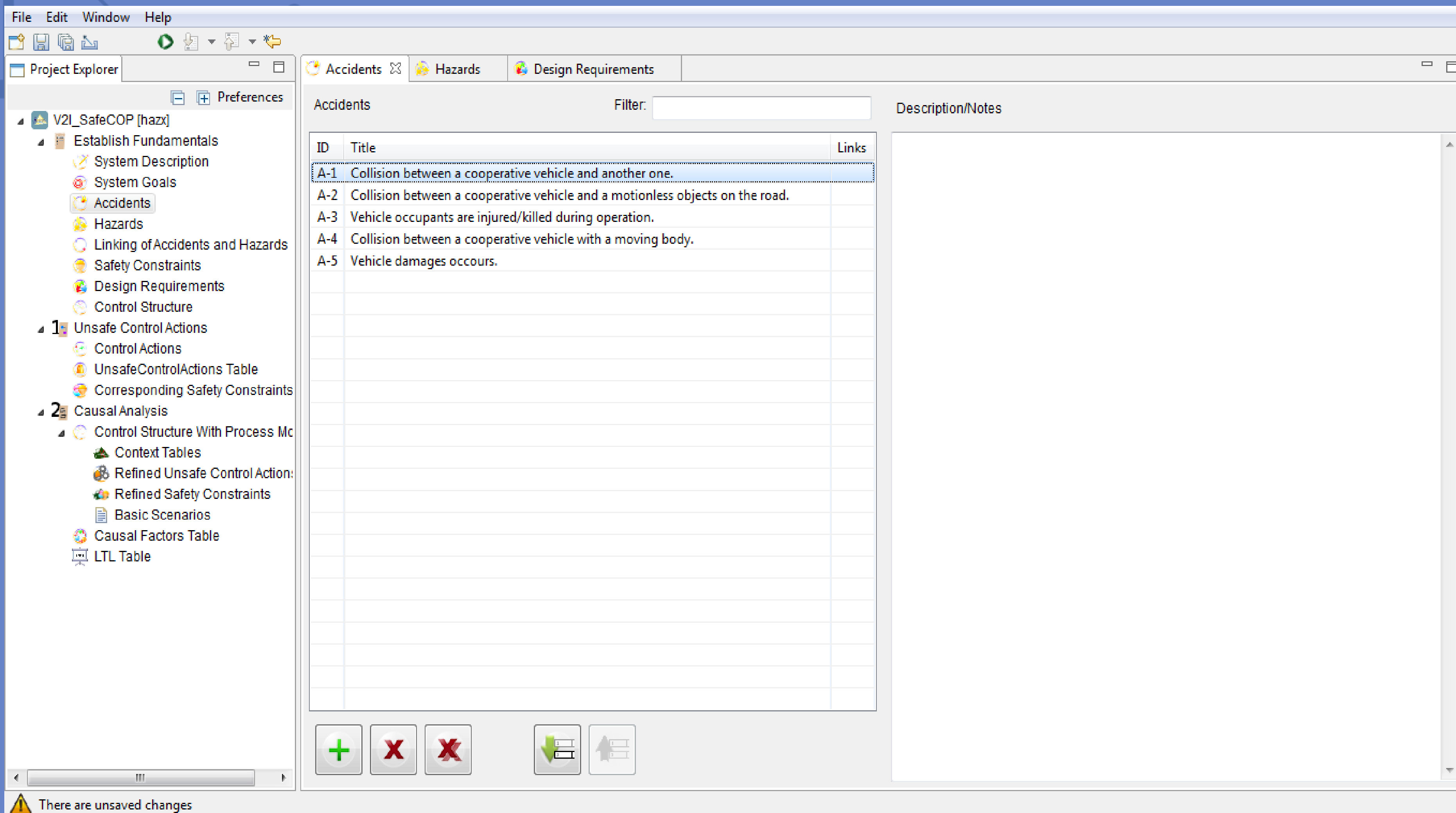
XSTAMPP
Model Checker & Testing tools
NuSMV
SPIN
STPA Test Cases Generator
XSTAMPP Plugins
A-STPA
XSTPA
STPA Verifier
A-CAST
STPA Test Cases Generator Plugin
Main Components
XSTAMPP Models
Main Functions
UI Editors
XSTAMPP Workbench UI
XSTAMP Platform
Language & Tools
Java
Plug-in development environment (PDE)
Eclipse Rich Client Platform (RCP)

XSTAMPP

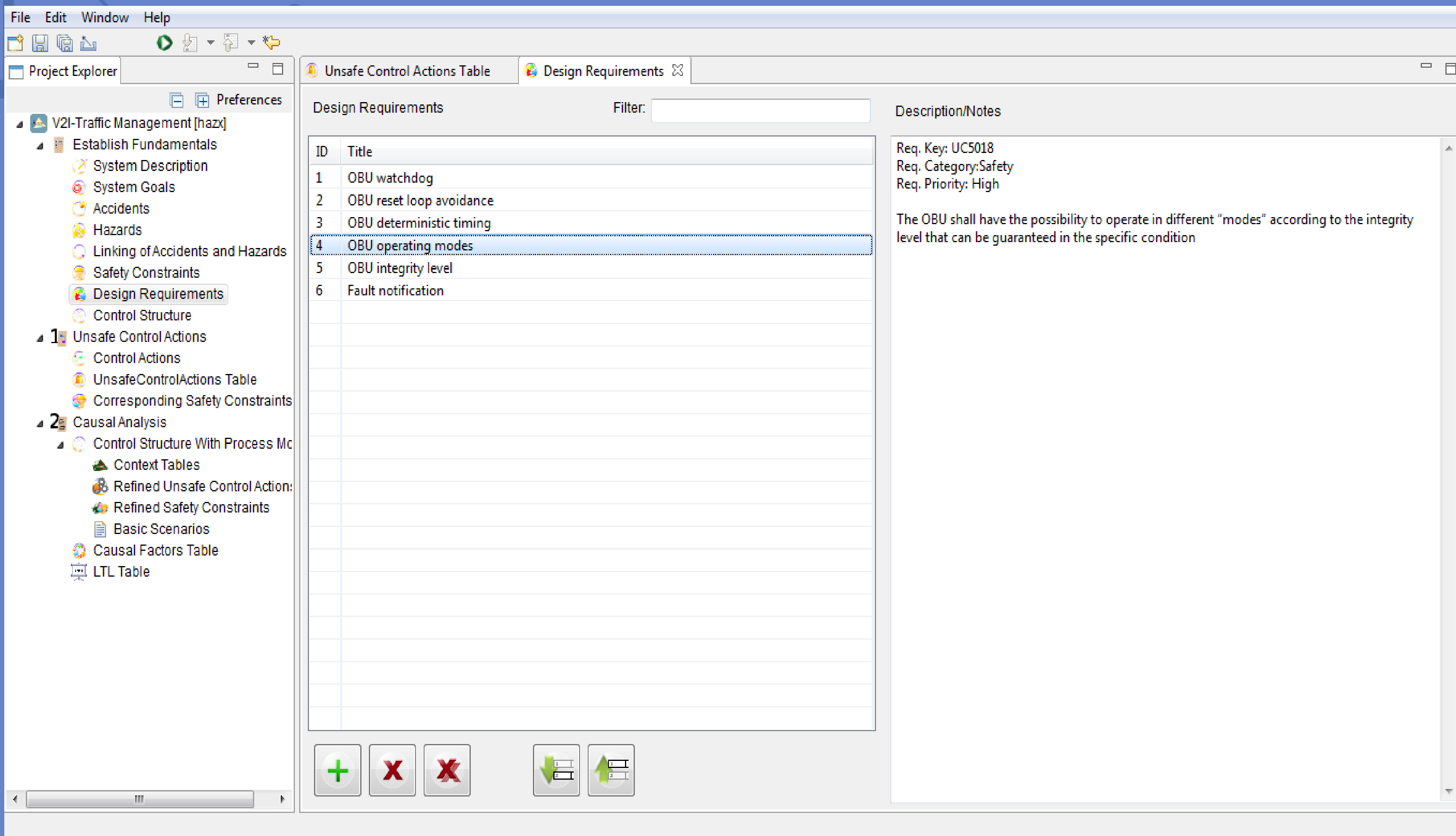


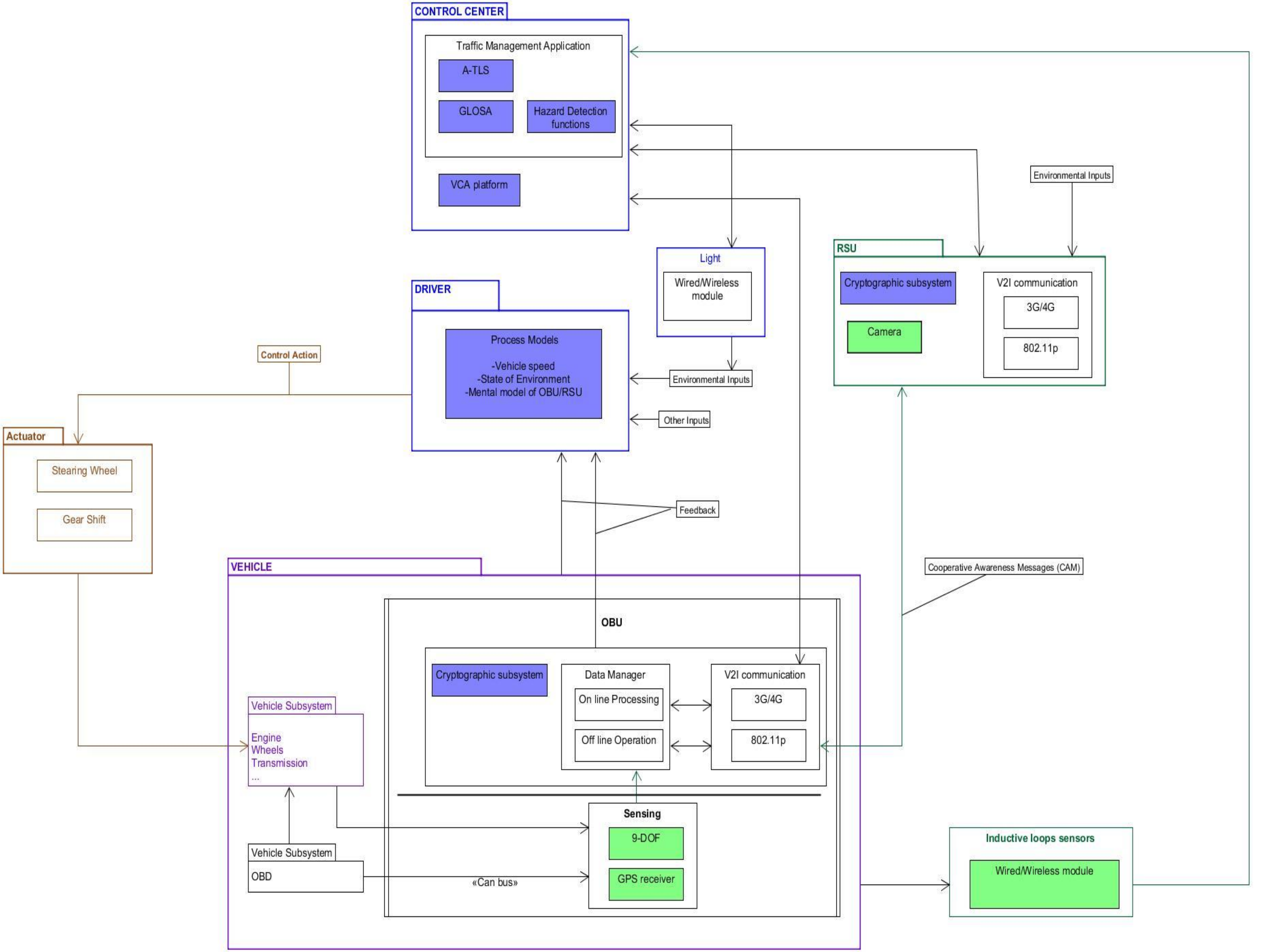
XSTAMPP -STPA Project->V2I_SafeCOP->Establish Fundamentals->System Goals
File Edit Window Help
Project Explorer
Preferences
V2I_SafeCOP [hazx]
Establish Fundamentals
System Description
System Goals
Accidents
Hazards
Linking of Accidents and Hazards
Safety Constraints
Design Requirements
Control Structure
1 Unsafe Control Actions
Control Actions
UnsafeControlActions Table
Corresponding Safety Constraints
2 Causal Analysis
Control Structure With Process Mc
Context Tables
Refined Unsafe Control Action:
Refined Safety Constraints
Basic Scenarios
Causal Factors Table
LTL Table

XSTAMPP

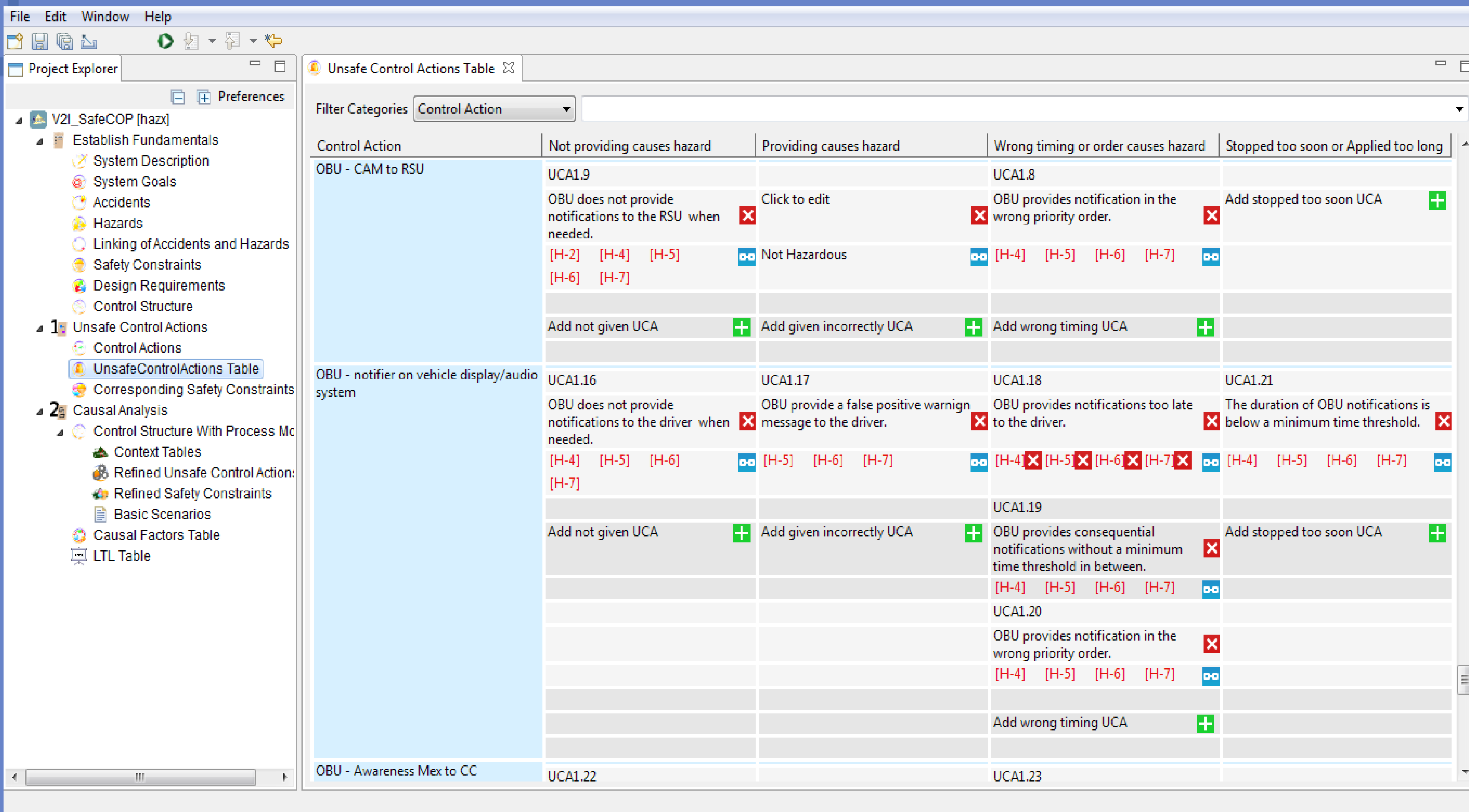

File Edit Window Help
Project Explorer
Preferences
V2I_SafeCOP [hazx]
Establish Fundamentals
System Description
System Goals
Accidents
Hazards
Linking of Accidents and Hazards
Safety Constraints
Design Requirements
Control Structure
1 Unsafe Control Actions
Control Actions
UnsafeControlActions Table
Corresponding Safety Constraints
2 Causal Analysis
Control Structure With Process Mc
Context Tables
Refined Unsafe Control Action:
Refined Safety Constraints
Basic Scenarios
Causal Factors Table
LTL Table
Accidents
Hazards
Design Requirements
Accidents
Filter:
Description/Notes
ID
Title
Links
A-1 Collision between a cooperative vehicle and another one.
A-2 Collision between a cooperative vehicle and a motionless objects on the road.
A-3 Vehicle occupants are injured/killed during operation.
A-4 Collision between a cooperative vehicle with a moving body.
A-5 Vehicle damages occours.
There are unsaved changes

XSTAMPP


File Edit Window Help
Project Explorer
Preferences
V2I-Traffic Management [hazx]
Establish Fundamentals
System Description
System Goals
Accidents
Hazards
Linking of Accidents and Hazards
Safety Constraints
Design Requirements
Control Structure
Unsafe Control Actions
Control Actions
UnsafeControlActions Table
Corresponding Safety Constraints
Causal Analysis
Control Structure With Process Mc
Context Tables
Refined Unsafe Control Action:
Refined Safety Constraints
Basic Scenarios
Causal Factors Table
LTL Table
Unsafe Control Actions Table
Design Requirements
Design Requirements
Filter:
ID
Title
1 OBU watchdog
2 OBU reset loop avoidance
3 OBU deterministic timing
4 OBU operating modes
5 OBU integrity level
6 Fault notification
Description/Notes
Req. Key: UC5018
Req. Category:Safety
Req. Priority: High
The OBU shall have the possibility to operate in different "modes" according to the integrity level that can be guaranteed in the specific condition

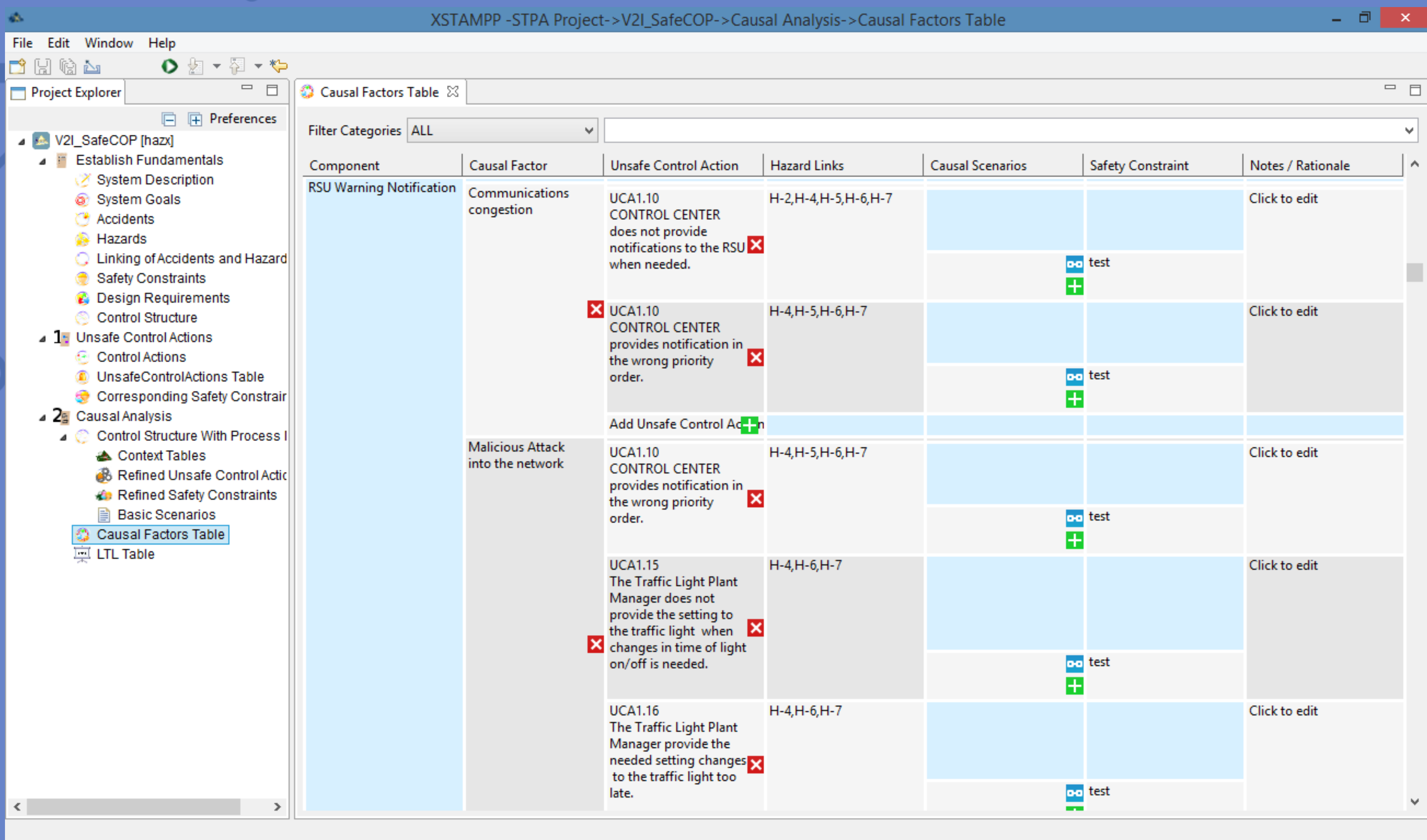

CONTROL CENTER
Traffic Management Application
A-TLS
GLOSA
Hazard Detection functions
VCA platform
Environmental Inputs
Light
Wired/Wireless module
RSU
Cryptographic subsystem
V2I communication
3G/4G
802.11p
Camera
DRIVER
Process Models
-Vehicle speed
-State of Environment
-Mental model of OBU/RSU
Control Action
Environmental Inputs
Other Inputs
Actuator
Stearing Wheel
Gear Shift
Feedback
Cooperative Awareness Messages (CAM)
VEHICLE
OBU
Cryptographic subsystem
Data Manager
On line Processing
Off line Operation
V2I communication
3G/4G
802.11p
Vehicle Subsystem
Engine
Wheels
Transmission
...
Sensing
9-DOF
GPS receiver
Vehicle Subsystem
OBD
«Can bus»
Inductive loops sensors
Wired/Wireless module

XSTAMPP



File
Edit
Window
Help
Project Explorer
Preferences
V2I_SafeCOP [hazx]
Establish Fundamentals
System Description
System Goals
Accidents
Hazards
Linking of Accidents and Hazards
Safety Constraints
Design Requirements
Control Structure
1 Unsafe Control Actions
Control Actions
UnsafeControlActions Table
Corresponding Safety Constraints
2 Causal Analysis
Control Structure With Process Mc
Context Tables
Refined Unsafe Control Action:
Refined Safety Constraints
Basic Scenarios
Causal Factors Table
LTL Table
Unsafe Control Actions Table
Filter Categories
Control Action
Control Action
Not providing causes hazard
Providing causes hazard
Wrong timing or order causes hazard
Stopped too soon or Applied too long
OBU - CAM to RSU
UCA1.9
OBU does not provide notifications to the RSU when needed.
[H-2] [H-4] [H-5] [H-6] [H-7]
Add not given UCA
Click to edit
Not Hazardous
Add given incorrectly UCA
UCA1.8
OBU provides notification in the wrong priority order.
[H-4] [H-5] [H-6] [H-7]
Add wrong timing UCA
Add stopped too soon UCA
OBU - notifier on vehicle display/audio system
UCA1.16
OBU does not provide notifications to the driver when needed.
[H-4] [H-5] [H-6] [H-7]
Add not given UCA
UCA1.17
OBU provide a false positive warnign message to the driver.
[H-5] [H-6] [H-7]
Add given incorrectly UCA
UCA1.18
OBU provides notifications too late to the driver.
[H-4] [H-5] [H-6] [H-7]
UCA1.19
OBU provides consequential notifications without a minimum time threshold in between.
[H-4] [H-5] [H-6] [H-7]
UCA1.20
OBU provides notification in the wrong priority order.
[H-4] [H-5] [H-6] [H-7]
Add wrong timing UCA
UCA1.21
The duration of OBU notifications is below a minimum time threshold.
[H-4] [H-5] [H-6] [H-7]
Add stopped too soon UCA
OBU - Awareness Mex to CC
UCA1.22
UCA1.23

XSTAMPP


XSTAMPP -STPA Project->V2I_SafeCOP->Causal Analysis->Causal Factors Table
File Edit Window Help
Project Explorer
Preferences
V2I_SafeCOP [hazx]
Establish Fundamentals
System Description
System Goals
Accidents
Hazards
Linking of Accidents and Hazard
Safety Constraints
Design Requirements
Control Structure
1 Unsafe Control Actions
Control Actions
UnsafeControlActions Table
Corresponding Safety Constrair
2 Causal Analysis
Control Structure With Process I
Context Tables
Refined Unsafe Control Actic
Refined Safety Constraints
Basic Scenarios
Causal Factors Table
LTL Table
Causal Factors Table
Filter Categories ALL
Component
Causal Factor
Unsafe Control Action
Hazard Links
Causal Scenarios
Safety Constraint
Notes / Rationale
RSU Warning Notification
Communications congestion
UCA1.10 CONTROL CENTER does not provide notifications to the RSU when needed.
H-2,H-4,H-5,H-6,H-7
Click to edit
test
UCA1.10 CONTROL CENTER provides notification in the wrong priority order.
H-4,H-5,H-6,H-7
Click to edit
test
Add Unsafe Control Action
Malicious Attack into the network
UCA1.10 CONTROL CENTER provides notification in the wrong priority order.
H-4,H-5,H-6,H-7
Click to edit
test
UCA1.15 The Traffic Light Plant Manager does not provide the setting to the traffic light when changes in time of light on/off is needed.
H-4,H-6,H-7
Click to edit
test
UCA1.16 The Traffic Light Plant Manager provide the needed setting changes to the traffic light too late.
H-4,H-6,H-7
Click to edit
test

Conclusions

Conclusions

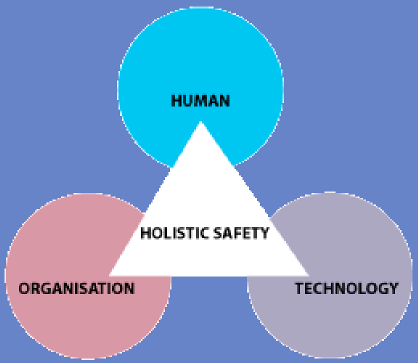
- The usage of XSTAMPP tool encourages the natural work flow of STPA analysis
- The tool guides also the non-expert user through the process of linking together accidents and hazard and facilitates the connection between unsafe actions and system constraints
- The Possibility to export the project in PDF and CSV extensions grants modularity with external third parts

Conclusions

- In the STPA project type of the tool is not yet possible to build hierarchical and detailed diagrams at different levels when designing complex control structure systems
- Is not yet possible to draw sub-blocks in the control structure diagram
- It is hard to edit multiple unsafe control actions in the proper table
- Some functionalities (e.g. safety constraints under causal scenarios tab) and plugins (e.g. EWaSAP) are still currently under development

Conclusions

- Over the past years, an increasing number of sociotechnical changes are emerged making systems more complex:
  - Fastest rate of change of technologies
  - Time To Market (TTM) is getting shorter every year compared to the past decade, making harder for industries, research institutes and universities to fill the security gaps
  - The human role within the sociotechnical systems have changed
- A more holistic approach and the use of new systemic models (e.g. STAMP) should help the safety community to include new variables during the design phase of complex systems, making them safer



Conclusions

- Whilst on the one hand the V2I traffic management scenario open the doors to new applications of CO-CPS toward V2X autonomous systems, on the other it leaves room for new safety challenges that go beyond the scientific and technical focus, embracing new social, economical and political aspects.

Thank You!

ρTechnology

experience & innovation

Via dei Mille 41/A - Rome, Italy
http://www.rotechnology.it
fb: Ro-Technology
info@rotechnology.it
Phone: +39 0621128876