L3HARRIS
FAST. FORWARD.

RAAML COMPLIANT BASED STPA TOOL INTEGRATION AT L3HARRIS TECHNOLOGIES

REID ARCHIBALD | Manager, Systems Engineering – Systems Safety
MARK RELOVA | Scientist, System Engineering
LUCAS RENATO JOSE da SILVA GUSMAN | Specialist, Systems Engineering

May 18, 2023

Brief Overview

L3HARRIS

- L3H SAS is undergoing a “Digital Thread” initiative to provide interconnection between pre-production and production artifacts
- L3H SAS is increasingly utilizing MBSE techniques to design system architectures
- STPA has been adopted within L3H SAS as a safety analysis method because it supports the Digital Thread initiative and can be incorporated into a MBSE environment

- OMG recently released (2021) a new standard, Risk Analysis and Assessment Modeling Language, which includes modeling constructs for creating STPA elements within a SysML model.

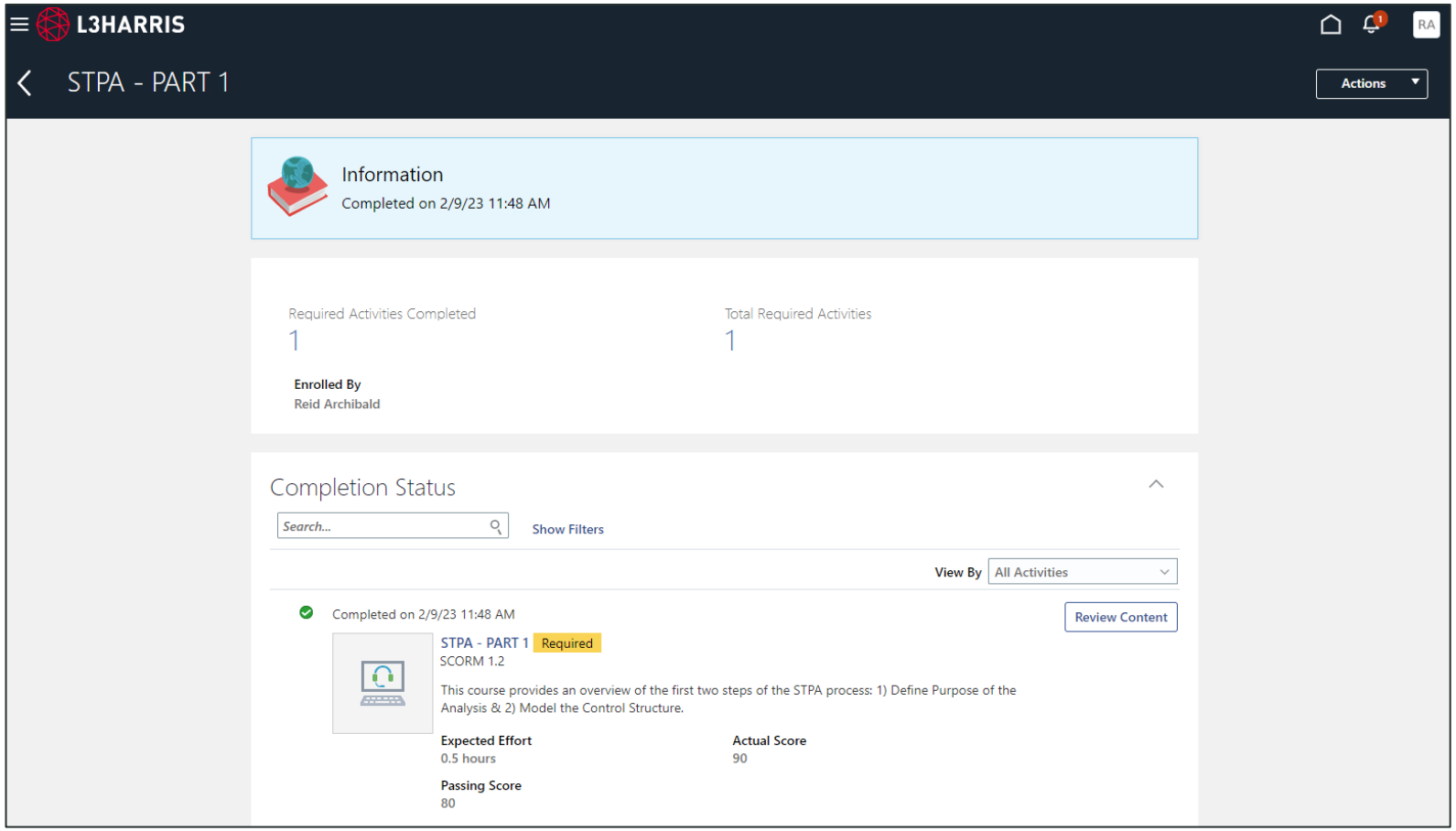
RAAML

OMG RISK ANALYSIS AND ASSESSMENT MODELING LANGUAGE

Initial Problems with Adopting STPA @ L3H SAS

How do we go from knowing nothing about STPA to knowing something?

A. In-house training module development for general STPA knowledge needs



STPA is a relatively new technique, How do we include it within company command media?

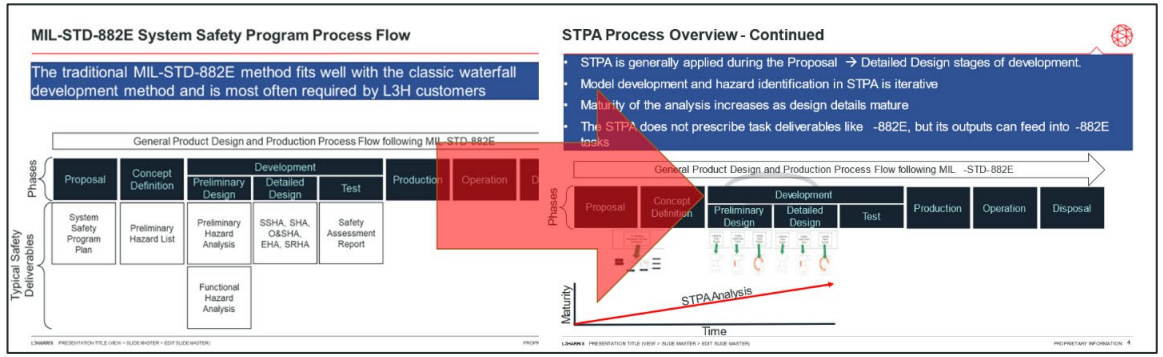
A. In-house training module development for general STPA knowledge needs

B. STPA overview presentations for key leadership and business areas

STPA vs. Traditional Methods

	Traditional Method (FTA, FMEA, ETA, HAZOP)	Systems Theory Method (STPA)
Hazards	• Component Failures→ Hazards • ⇓ Component Failure Rates→ ⇑Safety	• Unconstrained Behaviors→ Hazards • Constrained Behaviors→ ⇑Safety
Behaviors	• Restricted to behaviors of HW • Behaviors are separate sequential events E1 → E2 → E3	• Behaviors may be of HW, SW and Human • Sequence of behaviors may vary E1 ↔ E2, E1 → E3, E2 → E3
Usability	• Traceable to model elements • MBSE add-ons are available	• Traceable to model elements • STPA is MBSE (Control/Feedback Loops) Controller ControlAction ↓ ↑ Feedback Process
Development Lifecycle	• Performed during PDR/CDR • Findings can be expensive	• Basic models can be developed during concept phase • Findings are relatively cheap

L3HARRIS PRESENTATION TITLE (VIEW > SLIDE MASTER > EDIT SLIDE MASTER) PROPRIETARY INFORMATION 3



What tools are we going to use to perform STPA analyses?

A. In-house training module development for general STPA knowledge needs

B. STPA overview presentations for key leadership and business areas

C. **Exploration of tooling options to help standardize STPA process approach (this was back in 2019)**

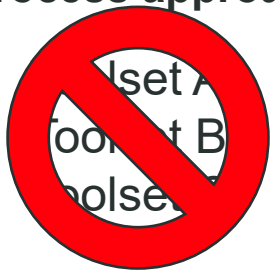
- Toolset A
- Toolset B
- Toolset C

What tools is L3H SAS going to use to perform STPA analyses?

A. In-house training module development for general STPA knowledge needs

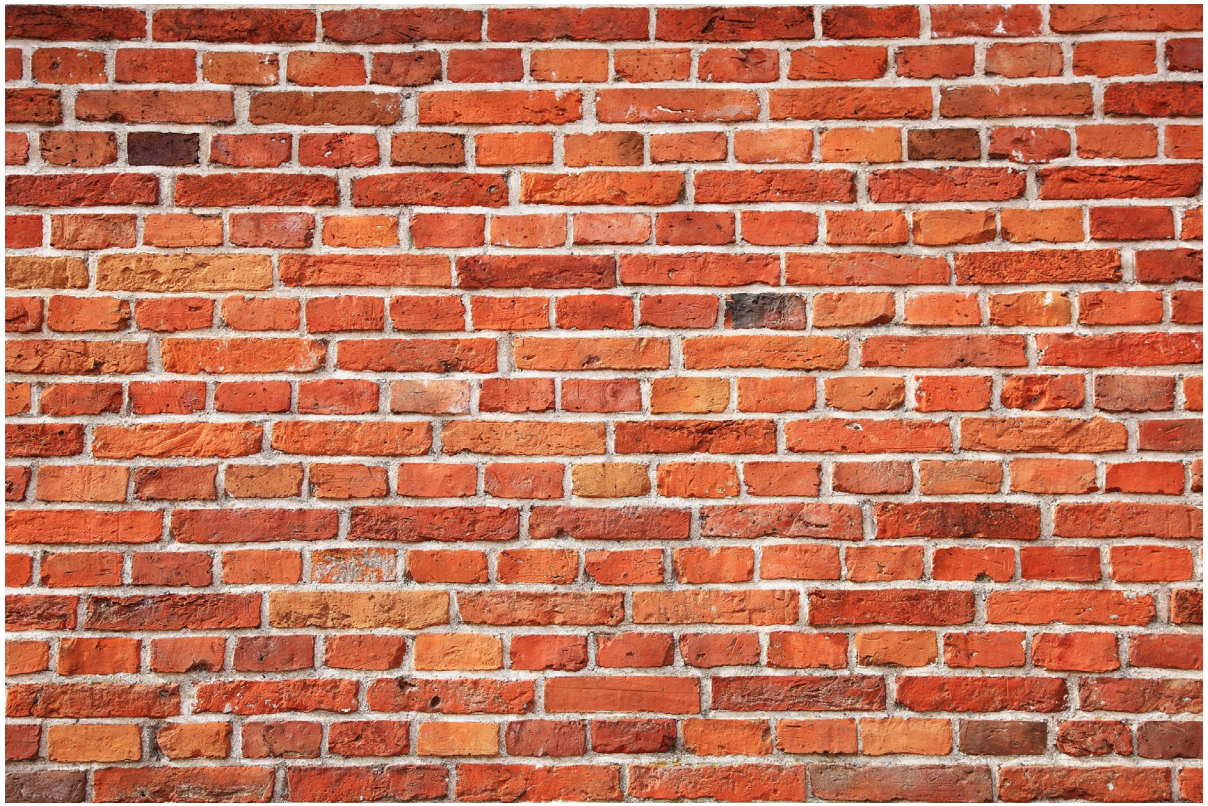
B. STPA overview presentations for key leadership and business areas

C. **Exploration of tooling options to help standardize STPA process approach (this was back in 2019)**



- lset A
- oolset B
- oolset

Each option led to a "brick wall"



Development of the RAAML Compliant STPA Toolset @ L3H SAS

Development of the RAAML Compliant STPA Toolset @ L3H SAS – Discovery Phase

Q1 2020, a customer wanted a Sys Arch model that included a Safety Model

→

Q2 2020, first L3H SAS SSE receives MBSE training

→

Q2 2020, STPA is identified as a viable method for creating a Safety Model

STPA is MBSE

Where the S stands for Safety

Discovery | Implementation | Update

Development of the RAAML Compliant STPA Toolset @ L3H SAS - Implementation

Q1 2020, a customer wanted a Sys Arch model that included a Safety Model

Q2 2020, first L3H SAS SSE receives MBSE training

Q2 2020, STPA is identified as a viable method for creating a Safety Model

Q3 2020, a working STPA profile was created

12 months of “tweaking” of the profile tool and development of the safety model

Q3 2021, a general training module for STPA in MBSE was released

Q1 2022, first STPA in MBSE training provided

Incorporation of the Safety model with the Sys Arch model led to further benefit discoveries

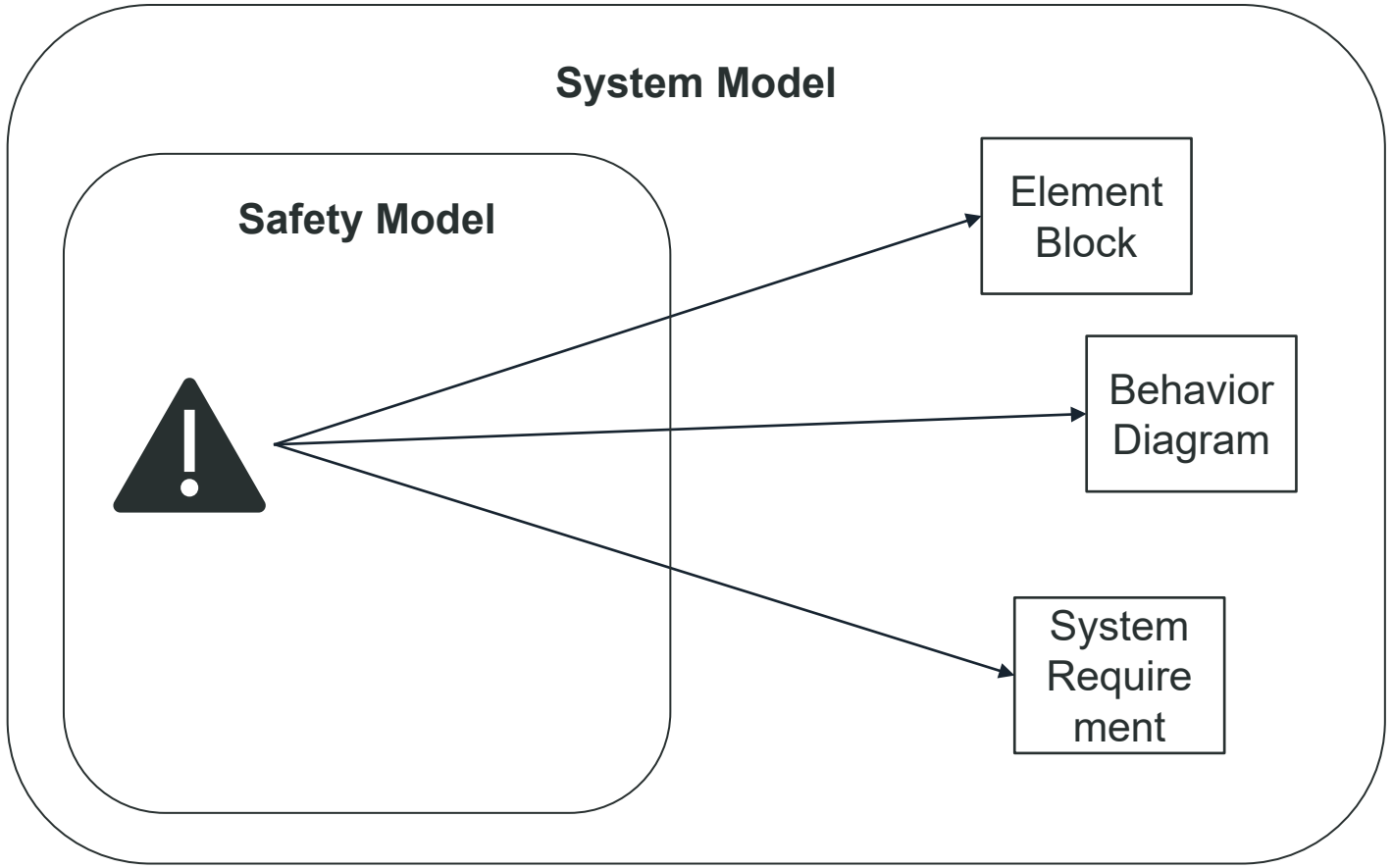
Discovery

Implementation

Update

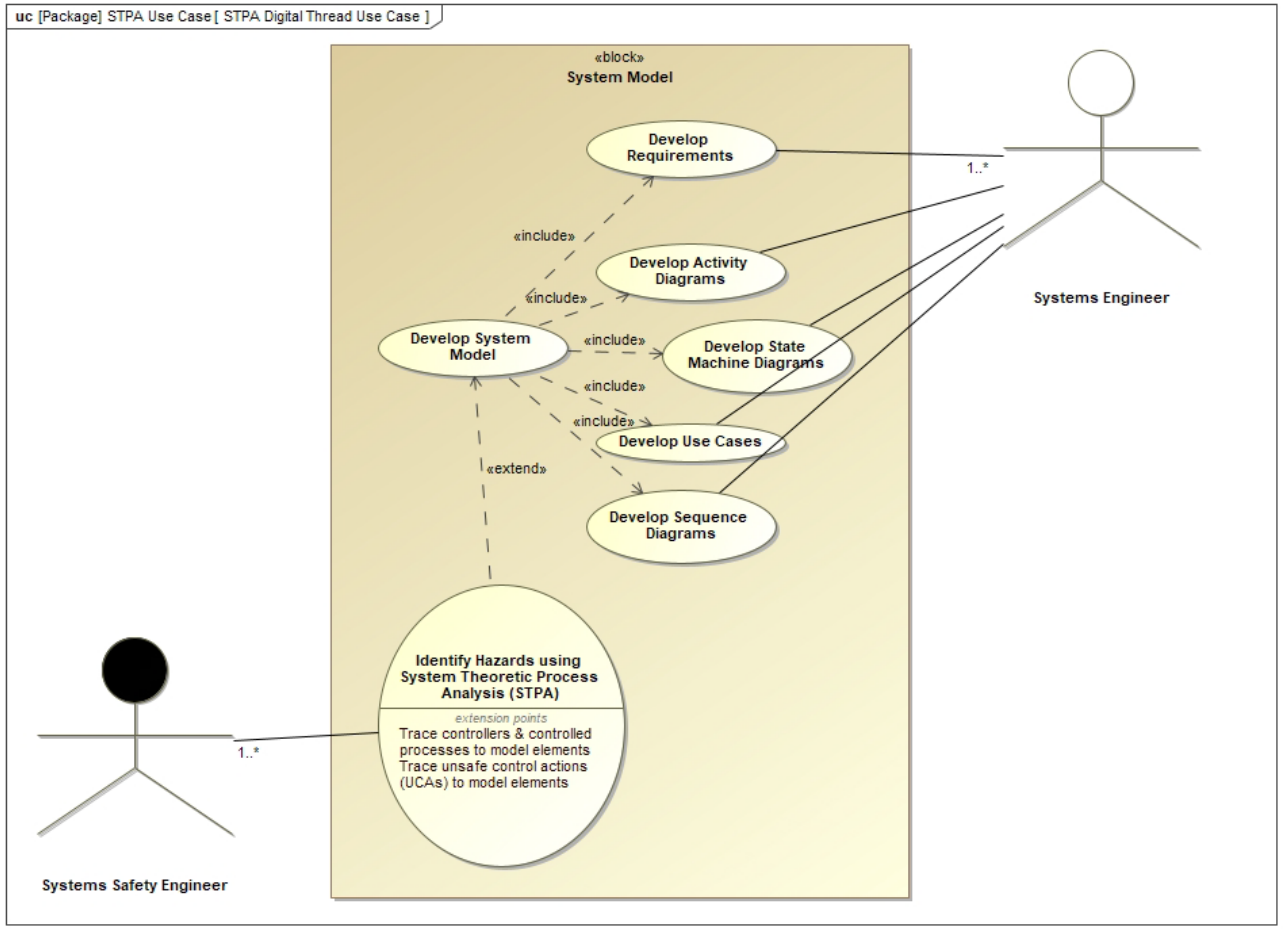
Benefits doing STPA in a SysML Capable Modeling Tool

Increased traceability and single location of safety analysis documentation



Benefits doing STPA in a SysML Capable Modeling Tool

Enhanced collaboration between Systems Safety and Systems Engineering resulting in improved efficiency and reduced costs



Development of the RAAML Compliant STPA Toolset @ L3H SAS - Update

Q1 2020 a customer wanted a Sys Arch model that included a Safety Model

Q2 2020, first L3H SAS SSE receives MBSE training

Q2 2020 STPA is identified as a viable method for creating a Safety Model

Q3 2020, a working STPA profile was created

Currently, L3H SAS is working to complete a RAAML compliant STPA Profile for use on future programs

Q3 2021, a general training module for STPA in MBSE was released

Q1 2022, first STPA in MBSE training provided

Q1 2023, transition of STPA Profile 1.0 to RAAML compliance begun

Q2 2023, estimated completion of STPA Profile 2.0 (RAAML Compliant)

Discovery

Implementation

Update

Benefits of using a RAAML Compliant STPA Tool Integration

RAAML Compliance Facilitates: Shareability among Contractors, Customers and different MBSE toolsets

Benefits of using a RAAML Compliant STPA Tool Integration

RAAML Compliance Facilitates: Improved Error Detection

Key Differences Between the STPA Profile 1.0 vs STPA Profile 2.0

Key Differences Between STPA Profile 1.0 vs STPA Profile 2.0

STPA Profile 1.0	STPA Profile 2.0
UCA and Loss Scenarios were grouped together as attributes of a single UCA ()	UCAs and Loss Scenarios are separate model elements

#	Name	UCA Type	UCA	Effect(s)	Causal Scenarios	Traced To	Traced From
1	BAUCA1.a.1	a. "is not provided when..."	The Driver does not press the brake pedal when an obstacle is in oncoming path of the vehicle.	The vehicle will continue to move in its current direction. The speed of th evehicle and size/mobility of the object will determine the severity of the impact. Worst case scenario could result in driver, passenger or obstacle (pedestrian or other vehicle driver) death/serious injury.	The driver is unaware there is an obstacle in the pathway of the vehicle.	Item Flow:flow for Press Brake Pedal[Driver -> Brake Control Module] H-1 H-2	BASR.001 BASR.002

UCA - Profile 1.0

Loss Scenario - Profile 1.0

UCA - Profile 2.0

#	Name	Documentation	Base Classifier	ControlAction
1	UCA-1	The driver does not press the brake pedal when an obstacle is in oncoming path of the vehicle.	*NotProvided*	Press Brake Pedal

Loss Scenario - Profile 2.0

#	Name	Documentation	Associated UCAs	ProcessModels	Factors	Mitigation	Situation Type
1	LS-1	Test Loss Scenario	UCA-1	Driver does not see obstacle	Radar does not detect object No headlights to iluminate object Weather conditions obstruct driver's view of object	8 Test Requirement STPA1	*LossScenario*

Allows for querying the model for specific UCAs and their associated loss scenarios

Key Differences Between STPA Profile 1.0 vs STPA Profile 2.0

STPA Profile 1.0	STPA Profile 2.0
No use of Process Model elements in the model	Inclusion of distinct Process Model elements

Process Model - New for Profile 2.0

#	Name	Documentation	Base Classifier	Associated LossScenario
1	Driver does not see obstacle	The driver is unaware of obstacle in pathway of the vehicle	*InadequateFeedbackAndInputs*	LS-1

Similar Process Model and their effects can be queried to help identify trends that contribute to inadequate processes

Key Differences Between STPA Profile 1.0 vs STPA Profile 2.0

STPA Profile 1.0	STPA Profile 2.0
Operational Situations were included within the UCA description attribute	Operation Situations are a standalone element.

#	Name	UCA Type	UCA	Effect(s)	Causal Scenarios	Traced To	Traced From
1	BAUCA1.a.1	a. "is not provided when..."	The Driver does not press the brake pedal when an obstacle is in oncoming path of the vehicle.	The vehicle will continue to move in its current direction. The speed of th evehicle and size/mobility of the object will determine the severity of the impact. Worst case scenario could result in driver, passenger or obstacle (pedestrian or other vehicle driver) de	The driver is unaware there is an obstacle in the pathway of the vehicle.	Item Flow:flow for Press Brake Pedal[Driver -> Brake Control Module] H-1 H-2	BASR.001 BASR.002

Operational Situation Profile 1.0

Specific Operational Scenarios can be associated with multiple UCAs and Loss Scenarios, thus safety analysis can be targeted at specific phases of system operation.

Operational Situation Profile 2.0

#	Name	Documentation	Base Classifier	Situation Type
1	Driving at speed under optimal weather conditions		AbstractOperationalSituation	AbstractOperationalSitu
2	Stopping for stop light/stop sign		AbstractOperationalSituation	AbstractOperationalSitu
3	Parking on flat ground		AbstractOperationalSituation	AbstractOperationalSitu
4	Parking on incline		AbstractOperationalSituation	AbstractOperationalSitu
5	Lane Change		AbstractOperationalSituation	AbstractOperationalSitu

Key Differences Between STPA Profile 1.0 vs STPA Profile 2.0

STPA Profile 1.0	STPA Profile 2.0
Factors that lead to a loss were included within the Loss Scenario statement	Factors that lead to a Loss Scenario are separate model elements

#	Name	UCA Type	UCA	Effect(s)	Causal Scenarios	Traced To	Traced From
1	BAUCA1.a.1	a. "is not provided when..."	The Driver does not press the brake pedal when an obstacle is in oncoming path of the vehicle.	The vehicle will continue to move in its current direction. The speed of th evehicle and size/mobility of the object will determine the severity of the impact. Worst case scenario could result in driver, passenger or obstacle (pedestrian or other vehicle driver) death/serious injury.	The driver is unaware there is an obstacle in the pathway of the vehicle.	Item Flow:flow for Press Brake Pedal[Driver -> Brake Control Module] H-1 H-2	BASR.001 BASR.002

Factors Profile 1.0

Specific Factors can be reused across multiple Loss Scenarios

Factors Profile 2.0

#	Name	Documentation	Situation Type	Associated LossScenario
1	No headlights to iluminate object	Headlights will help the driver see objects in low light settings.	Factor	LS-1
2	Weather conditions obstruct driver's view of object	Accumulation of precipitation on the windshield of the vehicle may cause the driver to not be able to see objects in the pathway of the vehicle	Factor	LS-1
3	Radar does not detect object	If the vehicle is equipped with a radar, failure or delay of the radar to detect an object may result in the driver not receiving a warning of an object in the pathway of the vehicle	Factor	LS-1

Conclusion

Summary of key points

- Organization adoption of STPA is slow, but Training and Tooling help sell STPA to the C-Suite
- STPA is MBSE
- Standardizing the use of STPA within a SysML environment will help further STPA adoption across industries

Future plans for L3H SAS's RAAML compliant STPA tool

- L3H SAS will continue to develop its RAAML compliant STPA tool set to ensure complete compliance and usability
- Continue to find practitioners outside of the traditional System Safety role to further its use outside of safety critical systems (cyber security, mission success and organization process improvement)

Big Thanks!

Mark Relova, (Scientist, Systems Engineering – L3H SAS) and Lucas Gusman (Specialist, Systems Engineering) – L3H SAS who did the heavy lifting to transition STPA Profile 1.0 to STPA Profile 2.0!

OMG for the release of the RAAML Specification - https://www.omg.org/spec/RAAML

Comments/Questions

Contact: Reid Archibald – Reid.Archibald@L3Harris.com