2023 Annual INCOSE international workshop

HYBRID EVENT

Torrance, CA, USA

January 28 - 31, 2023

Auto Working Group

INCOSE WG Round Robin

www.incose.org/IW2023

Cyber/Safety Stream

Starting Assumption

It may be impossible to build secure, safe systems of the complexity of a modern connected automobile without an advance in SE capability

40% or more of a vehicle's development budget can be attributed to ADAS integration, V&V

Proff & Wolf 2020

91% of software developers say it is difficult to impossible to know when a code change in one electronic control unit (ECU) affects another

Strategy Analytics & Aurora Labs 2020

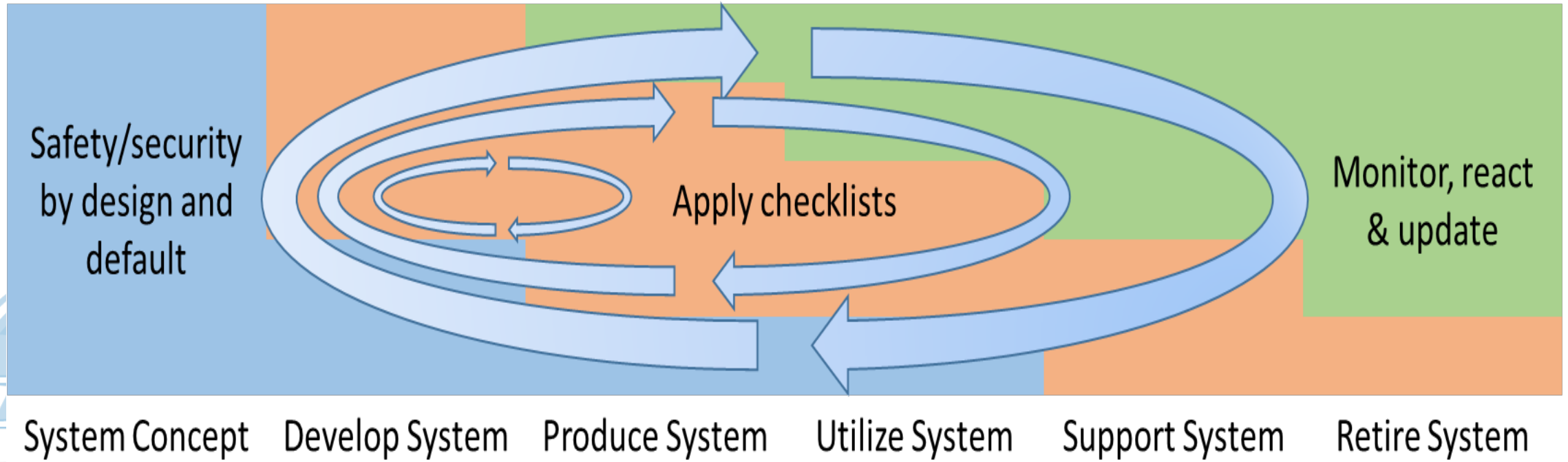
Variant management is now so difficult that cars are rolling off the production line with untested software configurations

Charrette 2020

The automotive industry's safety-based engineering tradition will not scale to meet the demands of cybersecurity… new [regulatory] obligations require a step-change in systems and processes to manage ongoing assurance activity

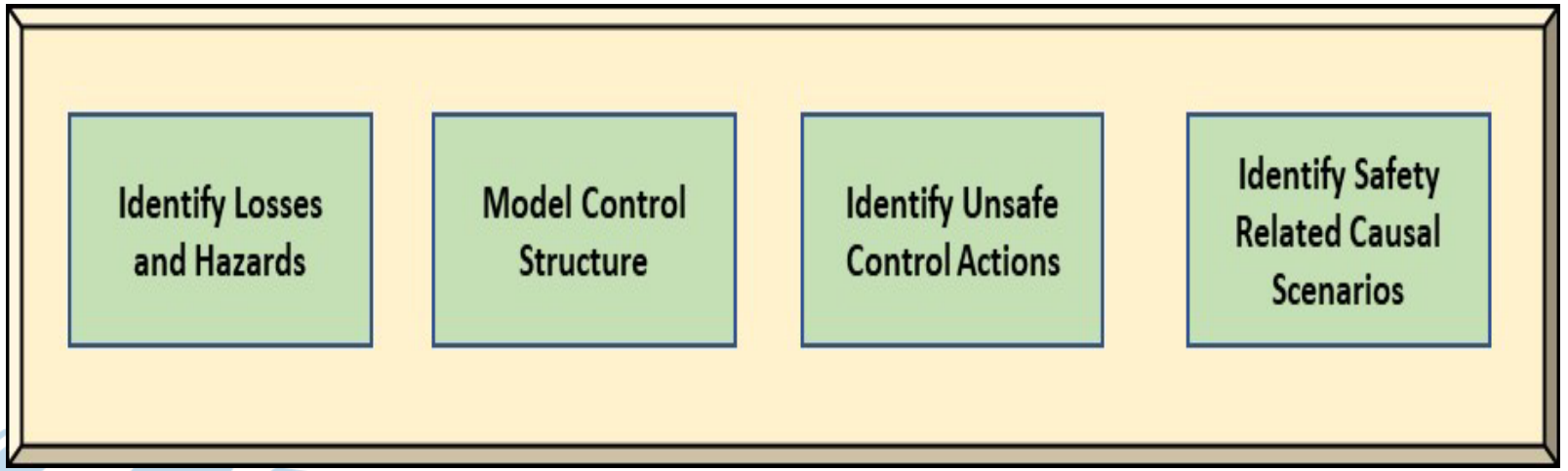
Ruddle 2021

Full Lifecycle Problem



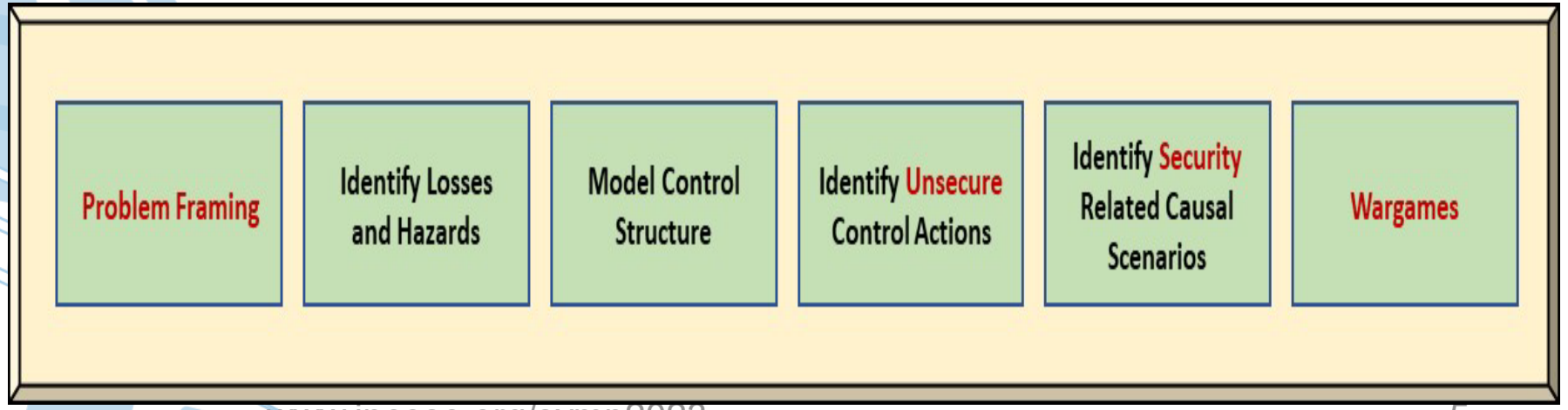
Engineering Styles Mapped to ISO/IEC/IEEE 15288 and 24748 Lifecycle Phases

STPA is not optional, but neither is it enough!



STPA core

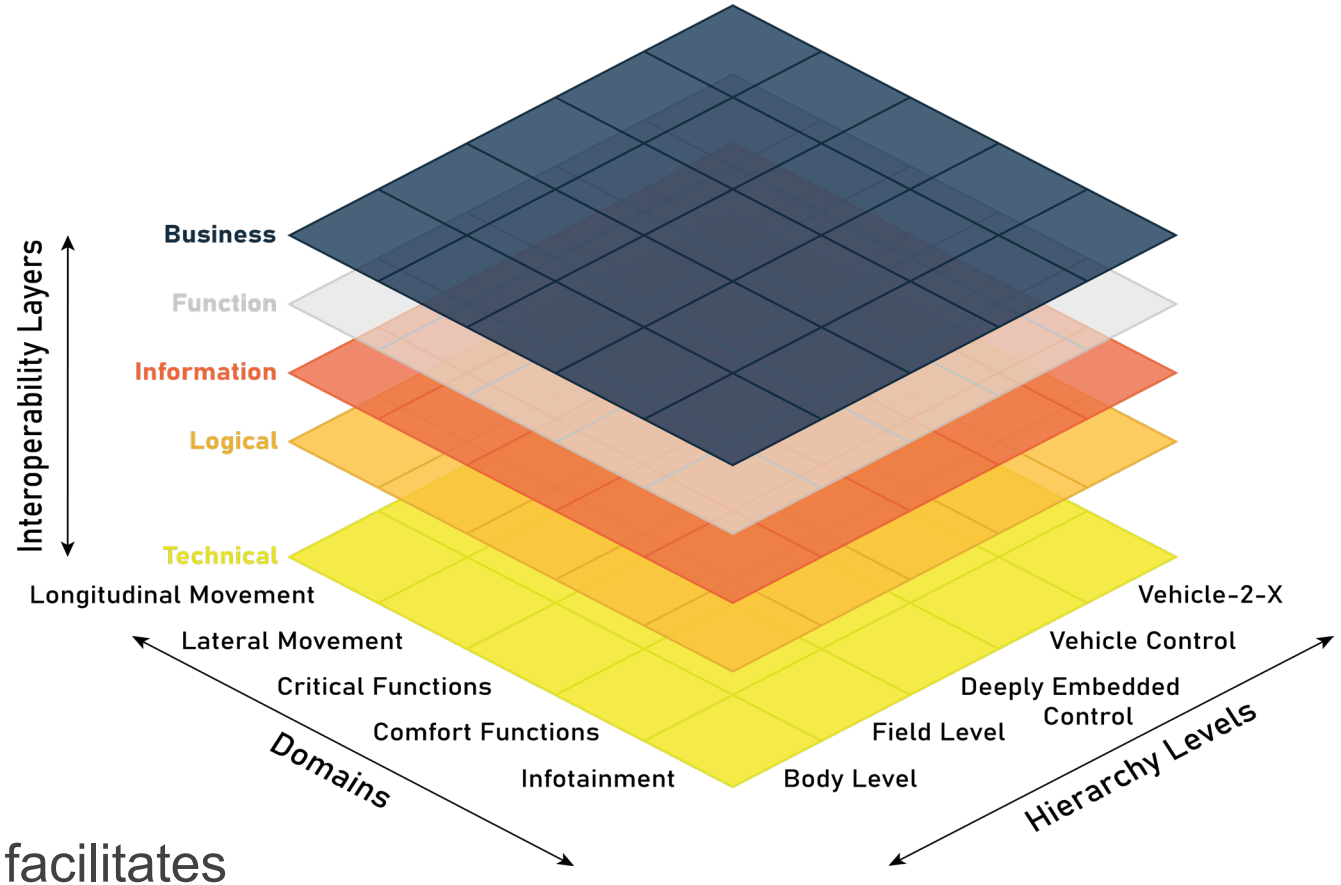
STP-Sec



Frameworks

Automotive Reference Architecture Model (ARAM)

3D Modeling Framework



- Domain Specific-Language (DSL) facilitates communication between stakeholders across automotive domain disciplines
- Provides guidelines for a structured first draft of the system under development
- Adaptable to development of massive, structurally complex systems (whole vehicle) & simpler subsystems (within the vehicle)
- Underlying common architectural model provides internal traceability & interoperability with other domains e.g. smart grid

Key good practice recommendations

Full Lifecycle Engineering

- Evolve and assure business models for long lifecycles.
- Invest in organizational infrastructure for through-life monitoring of vehicles

Holistic Hazard and Threat Analysis

- Move beyond fault- and failure-centric approaches restricted to vehicle scope
- Examine entire system context (vehicle, infrastructure, enterprise) for risks due to technology, humans, environment, system design, feedback loops, emergent risks

Loss-Driven Systems Engineering

- Adopt methods to support an LDSE approach to resilience by design and default

Common Frameworks

- To keep costs of safety and cybersecurity engineering under control, move to some set of common MBSE frameworks.
- Seek value-adding unification where possible, but ensure integration if this is not achievable.

Planned Future Work

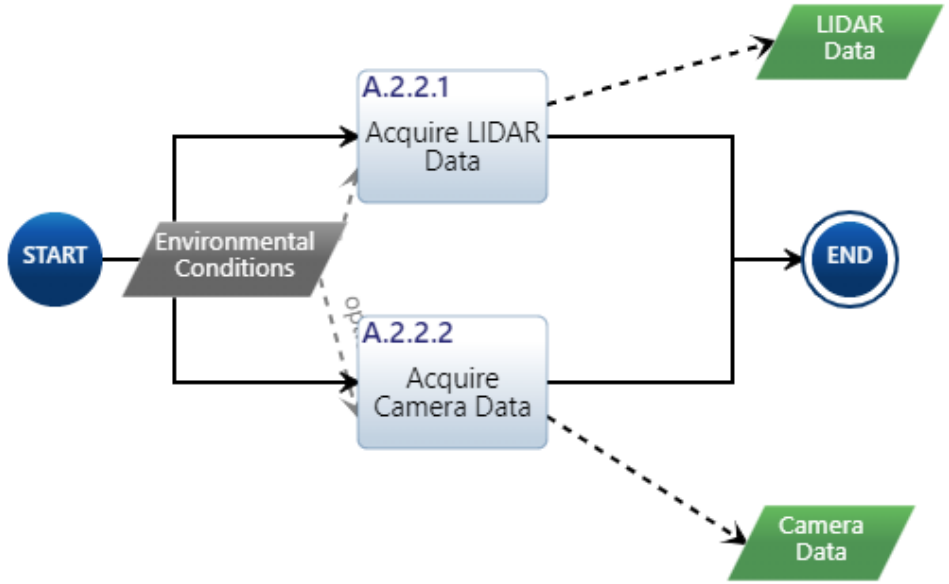
Evaluation of ARAM	Feedback from industry and case studies for V&V of the framework.
RAAML	Integration into AFs and development of a security library
STPA & Control Loop Dynamics	Investigate how classical control engineering concepts can be brought to bear on STPA to enrich the types of loss scenarios that can be identified.
DevSecOps and MBSE	Explore how Domain Driven Design can be improved to deliver the stakeholder transparency, traceability, and accountability needed for safety-critical applications.
Collaboration	Strengthen ties with other INCOSE WGs engaged in FuSE activities, such as the Systems Security Engineering WG Build links with related projects in industry and academia e.g. RAAML, CMI SEI DevSecOps PIM Further work with ISO to map additional standards and process models

Capstone Stream

Capstone Overview

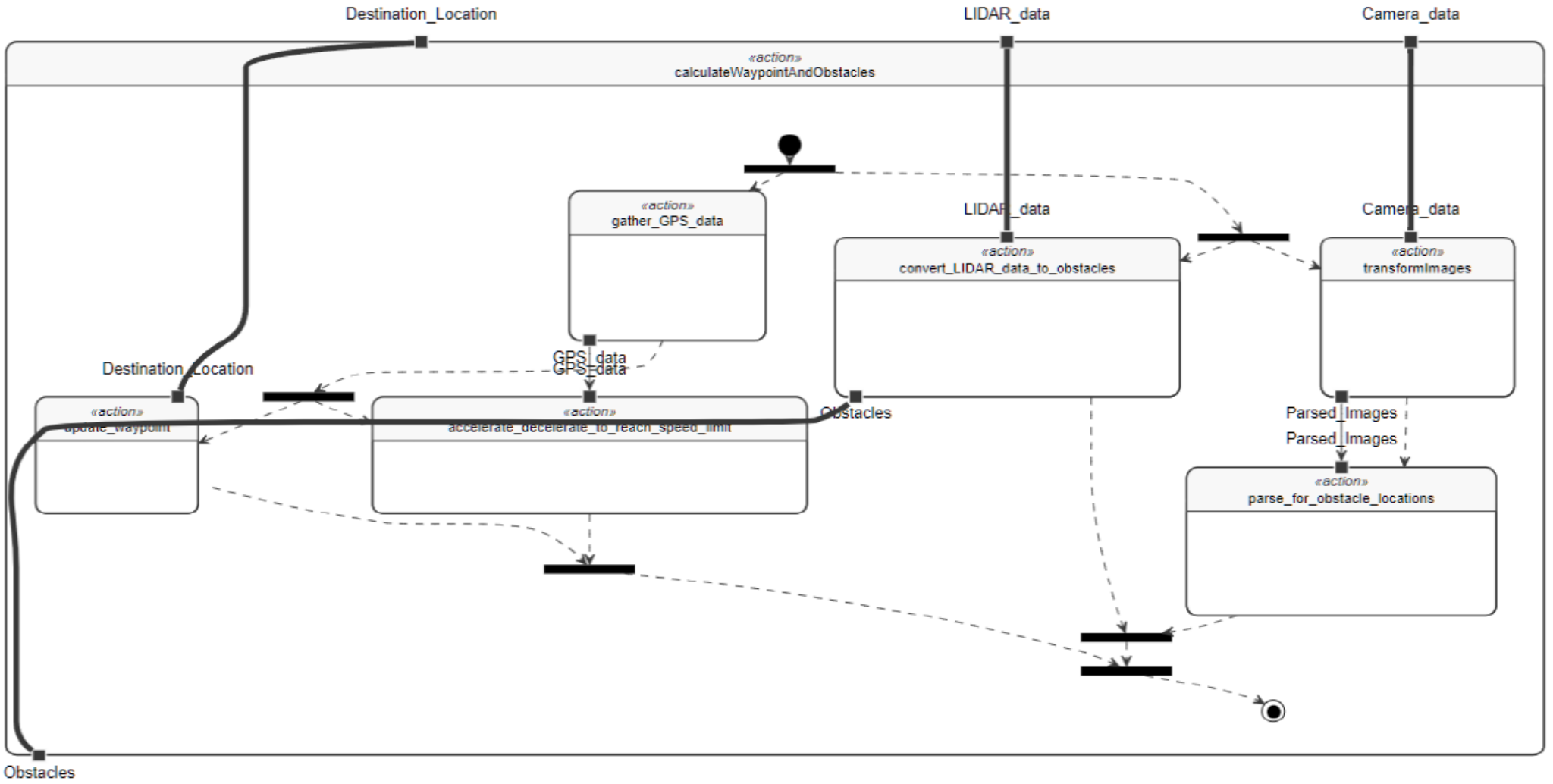
- Sponsored by INCOSE Auto WG
- Teams from George Mason University Master's Capstone Class
- Spring 2021, Fall 2021, Spring 2022
- Not enough students in Fall 2022 and Spring 2023
- Focused on migration to SysML V2

LML to SysML V2




```
action def Drive_Vehicle (in
Destination_Location : data, in
Initial_Location : data);
action def Monitor_Environment (in
Environmental_conditions : data, out
Lidar_data : data);
action def
  Calculate_Waypoint_and_Obstacles
  (in LIDAR_data : data, in
  Camera_data : data, in
  Destination_Location : data, out
  Obstacles : data);
action def Navigate_Vehicle;
```

Jupyter-lab pilot and Graphviz



Next Steps

- IW 2023 Automotive Working Group discussion
  - Demand for the program?
  - Revisit goals
  - Consider options

2023 Annual INCOSE international workshop

HYBRID EVENT

Torrance, CA, USA

January 28 - 31, 2023

www.incose.org/IW2023