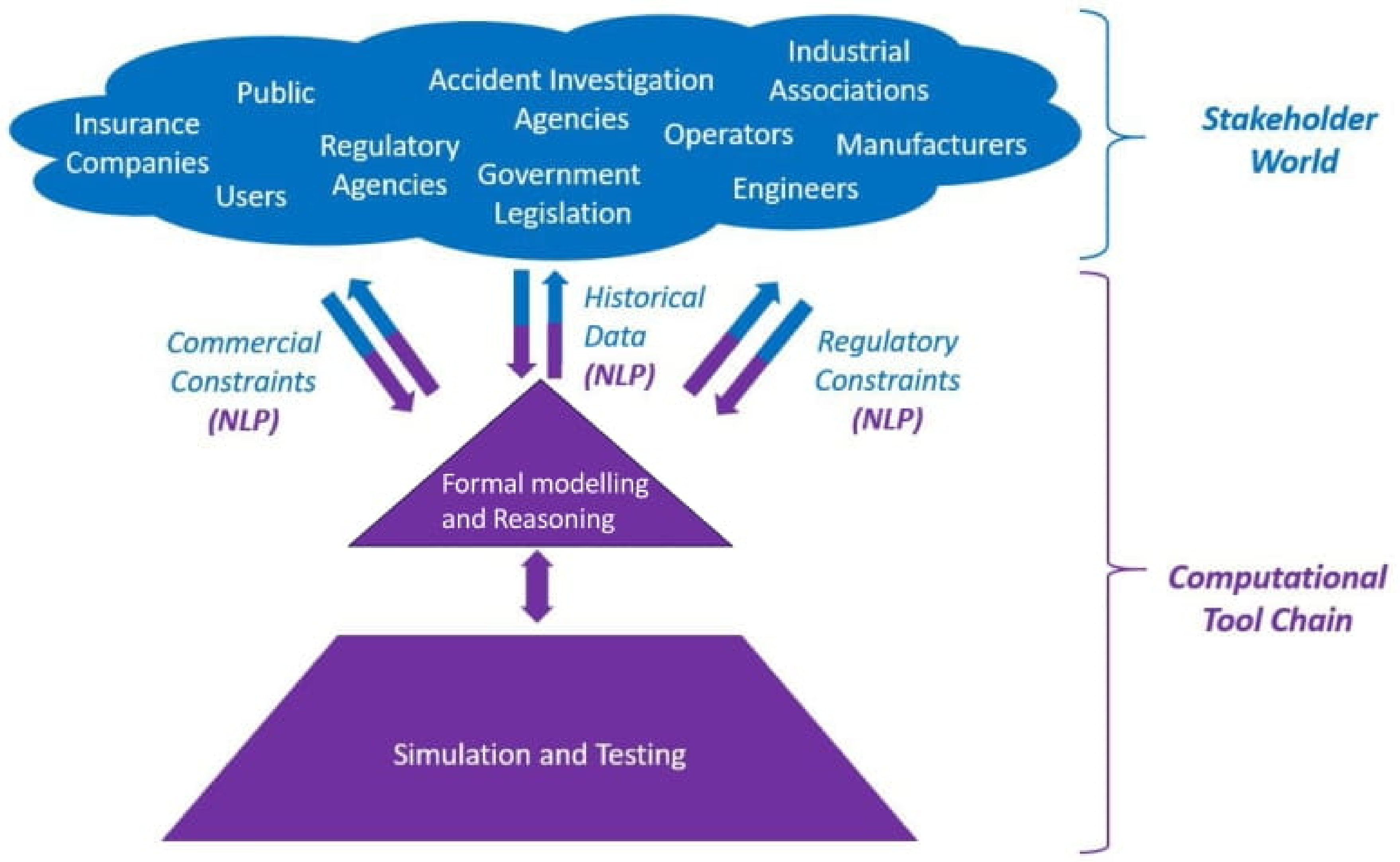
Computational Tools to Ensure Trustworthiness

Heriot-Watt University , University of Edinburgh, University of Glasgow

Yuhui Lin, Research Associate, Heriot-Watt University
Y.Lin@hw.ac.uk
Mattias Appelgren, Research Associate, University of Edinburgh
mattias.appelgren@ed.ac.uk

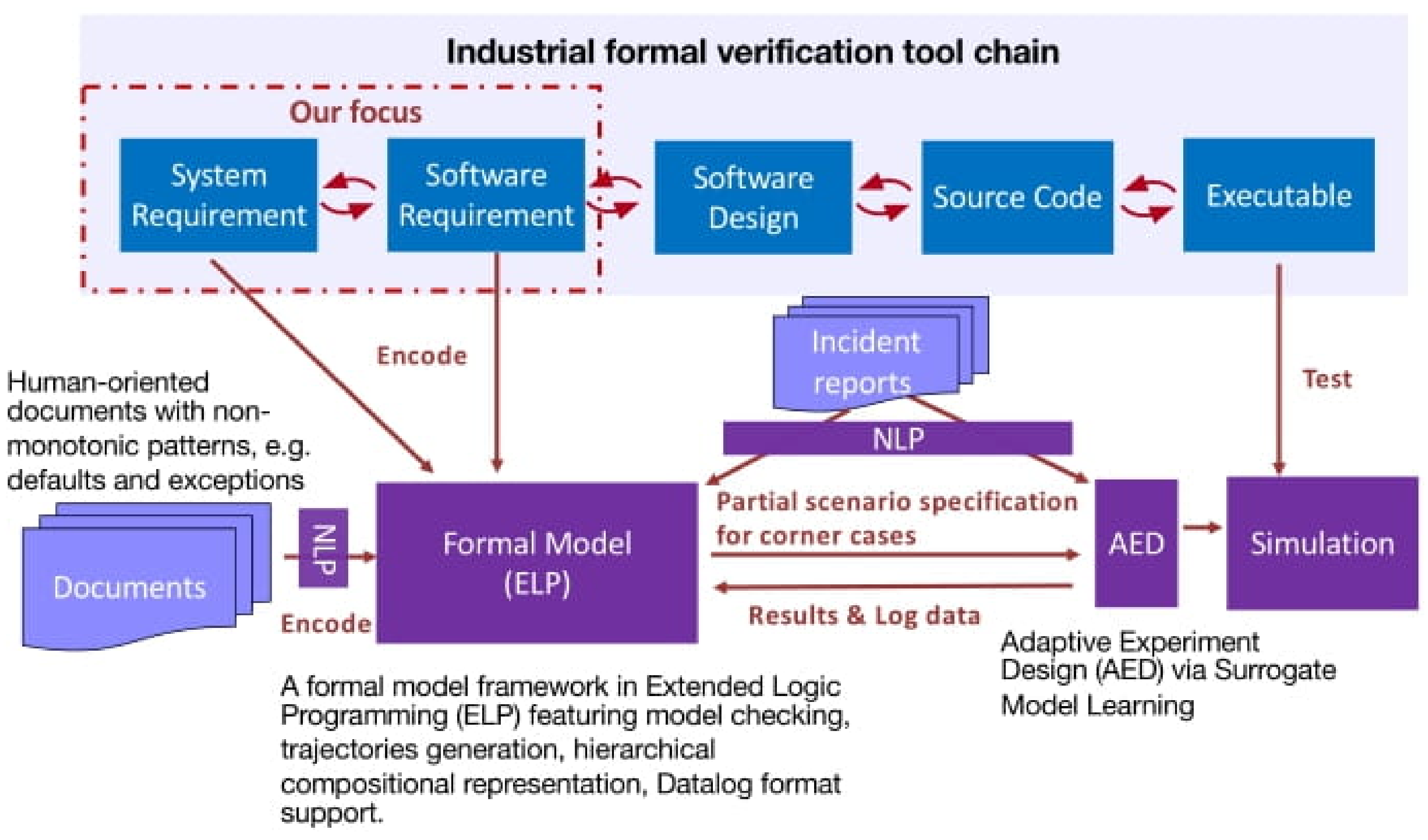
Scope and Overview



Responsible Research & Innovation – Anticipate, Reflect, Engage, Act (AREA)

Our aim is to promote openness where governance and regulation interfaces with the engineering of autonomous systems. Specifically, we seek to calibrate stakeholder expectations with regards to the benefits and limitations of autonomous systems. Engagement with stakeholders will therefore play a vital role in shaping the ongoing research of the TAS Node for Governance and Regulation.

Computational Tool Chain


Industrial formal verification tool chain
Our focus
System Requirement
Software Requirement
Software Design
Source Code
Executable
Encode
Test
Incident reports
NLP
Human-oriented documents with non-monotonic patterns, e.g. defaults and exceptions
Documents
NLP
Encode
Formal Model (ELP)
Partial scenario specification for corner cases
Results & Log data
AED
Simulation
A formal model framework in Extended Logic Programming (ELP) featuring model checking, trajectories generation, hierarchical compositional representation, Datalog format support.
Adaptive Experiment Design (AED) via Surrogate Model Learning

- We aim to develop a formal system requirements framework that is capable of encoding high-level system requirements and related domain properties, e.g. physical components, regulations and user manuals.
- Investigating the use of Extended Logic Programming (ELP) for verifying the compliance of autonomous vehicles (simulated or data logs) to road traffic regulations.
- ELP provides a natural formalism for representing and reasoning about default style regulations as well as data logs.
- Plan to further use ELP to investigate how safety properties might be violated, e.g. interaction failures or invalid design assumptions, and therefore anticipate corner cases that could lead to accidents.
- The expectation is that ELP will facilitate a link with legal reasoning.

Mechanizing Regulations and Requirements

Non-monotonic patterns in human oriented documents

Human oriented documents, e.g. regulations, system requirements and user manuals, are typically structured in a non-monotonic style with default, exception and general overriding rules.

```
                Dutch traffic regulation
(Default)
RVV.3: Drivers are required to keep as far over to
the right as possible.

(Exception)
RVV.13: When traffic is queuing, and where the
carriageway is divided into several lanes heading in
the same direction, it is not necessary to keep to
the right-hand lane.

(General overriding)
RVV.82: Road users are required to follow
instructions given verbally or by means of gestures
by authorised officers
```

```
System requirement – Landing gears

(Default)
When a leg is Up and Locked, the
leg indicator shall be lit green.

(Exception)
When the (Weight On Wheels) leg
indication is Airborne, and each
leg has been in the Up and Locked
state for ten seconds, then the
green light shall extinguish.
```

A logic programming approach for formalization

We are investigating the use of a logic programming technique called *Extended Logic Programming* (ELP) which extends traditional logic programming, e.g. *Prolog*, with explicit negation (`-P`) while also supporting the default negation-by-failure (`not P`), e.g.

```
                         A level crossing example
cross :- not train.     %% Cross it when you don't see trains.
cross :- -train.        %% Cross it when there is evidence of no incoming train.
```

- ELP provides a natural formalism for the representation and reasoning about default style regulations.
- The logic programming formalism can also work naturally with log data from a declarative database, e.g. *Datalog* which is a subset of *Prolog*.

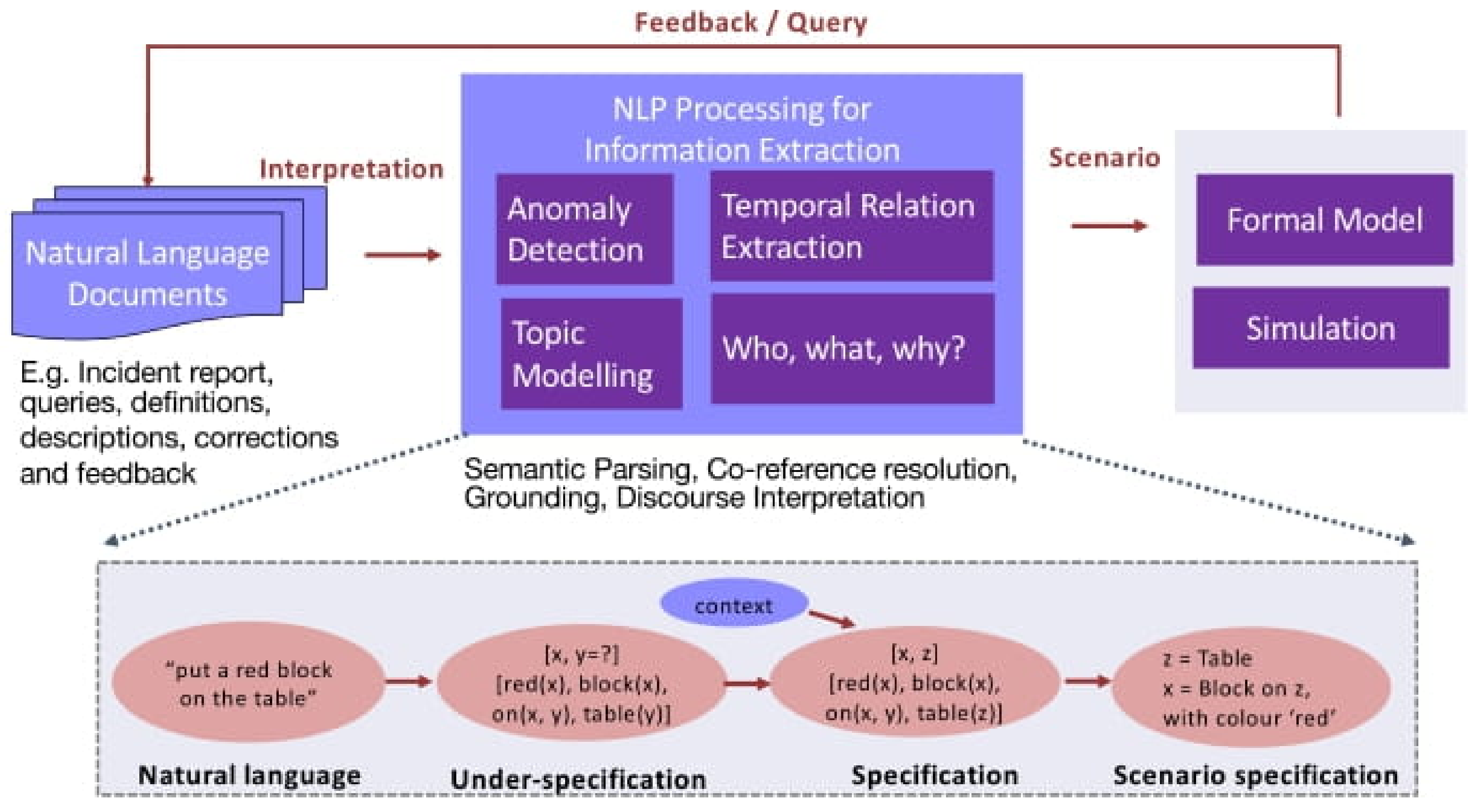
```
                         Encodings in ELP
(Default)
applies(default, …) :- …, not -applies(default, …), not inexp_ab(default, …).

(Exception)
applies(exception …) :- …, not -applies(exception, …), not inexp_ab(exception, …).
-applies(default, …) :- applies(exception …).
```

Hierarchical compositional system representation

- A framework in ELP to encode a system model, domain properties and system requirements.
- System models are compositional and hierarchical.
- Hierarchical representations provides a *zoom in* and *zoom out* capability.

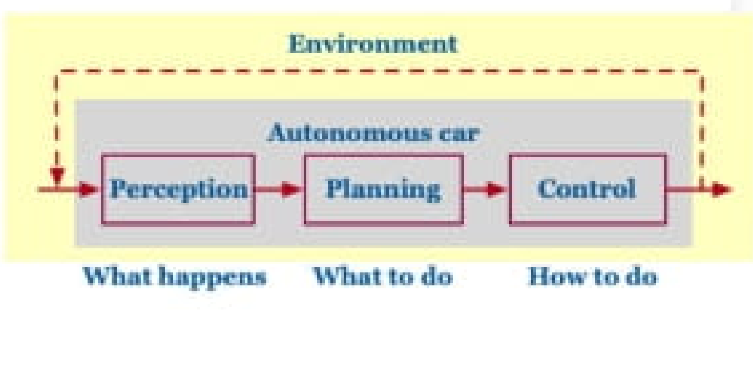
Natural Language Processing

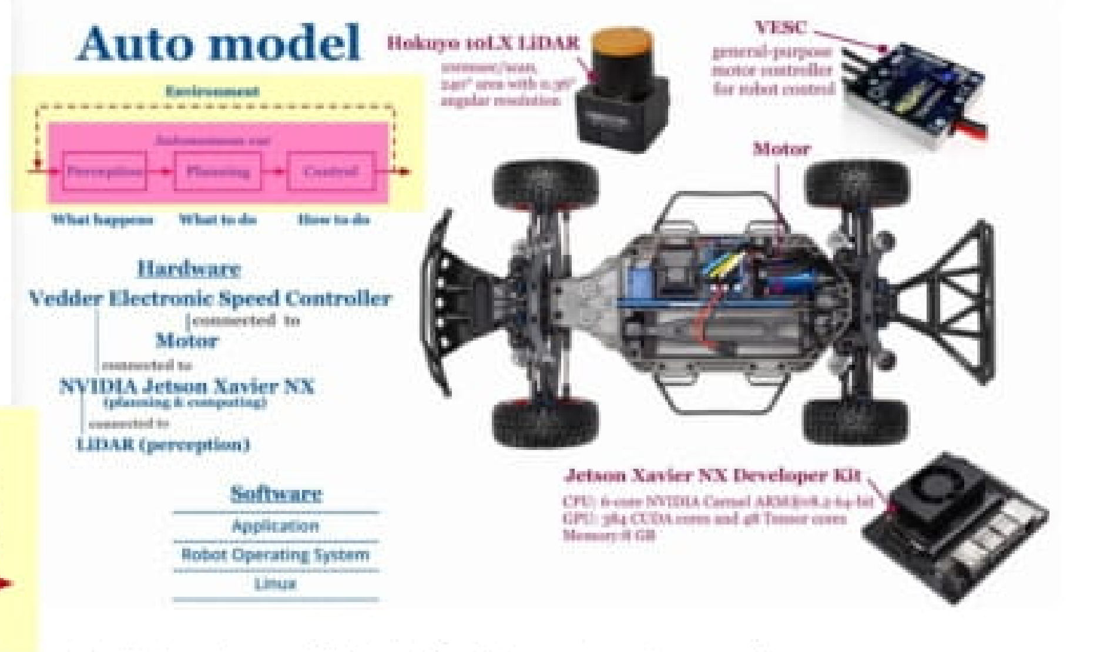
- Goal is to support the iterative creation of a simulation environment through a NL dialogue.
- Generating executive summaries of incident reports based upon a range of stakeholder narratives – useful to stakeholders working in governance and regulation.
- Extracting information from incident reports, e.g. identifying agents and events, and extract temporal relationships between events – provides a mechanism for categorizing incidents and checking conformance (e.g. w.r.t. regulations) and identifying anomalies.
- Natural Language Processing (NLP) frontend for Adaptive Experiment Design – a probabilistic programming language for specifying simulation environments.
- The approach could potentially be extended for formal modelling.


Feedback / Query
Interpretation
Natural Language Documents
E.g. Incident report, queries, definitions, descriptions, corrections and feedback
NLP Processing for Information Extraction
Anomaly Detection
Temporal Relation Extraction
Topic Modelling
Who, what, why?
Semantic Parsing, Co-reference resolution, Grounding, Discourse Interpretation
Scenario
Formal Model
Simulation
context
"put a red block on the table"
[x, y=?] [red(x), block(x), on(x, y), table(y)]
[x, z] [red(x), block(x), on(x, y), table(z)]
z = Table x = Block on z, with colour 'red'
Natural language
Under-specification
Specification
Scenario specification

Public Engagement

We demonstrated an autonomous toy car with 1/10th size ratio in *Edinburgh Science Festival 2022*. We explained the main setup differences from a traditional car to an autonomous model.





* Collaboration with *AISEC* for the car development
* Credits to *F1Tenth.org* for car building information