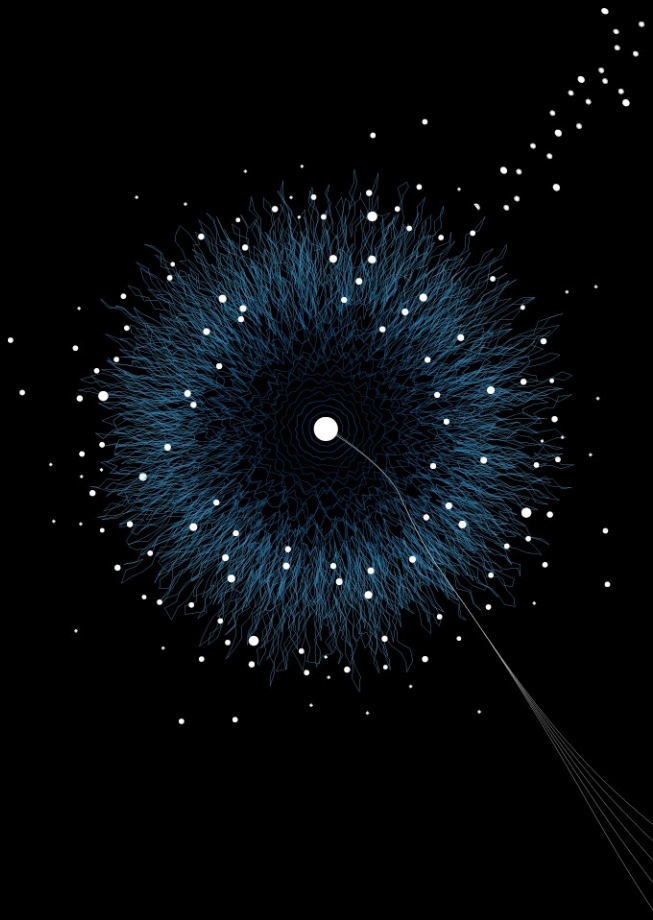
RAMS-Europe 2025
06.08.2025

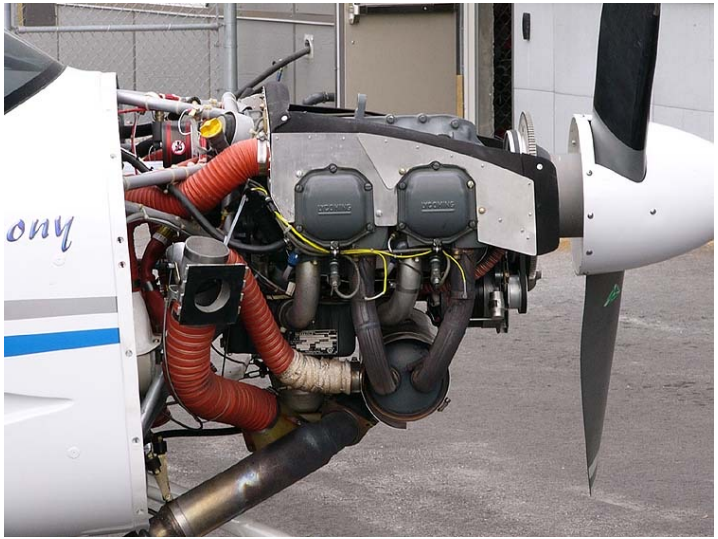
FAULT TREE SYNTHESIS FROM KNOWLEDGE GRAPHS

AIMÉ NTAGENGERWA, GEORGIANA CALTAIS,
MARIËLLE STOELINGA

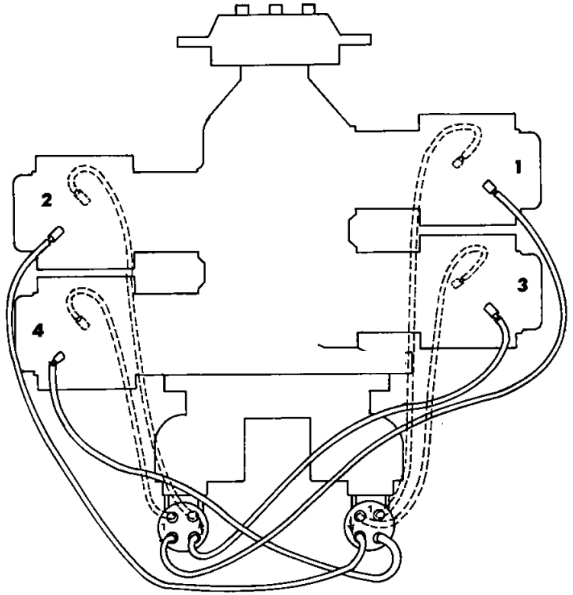


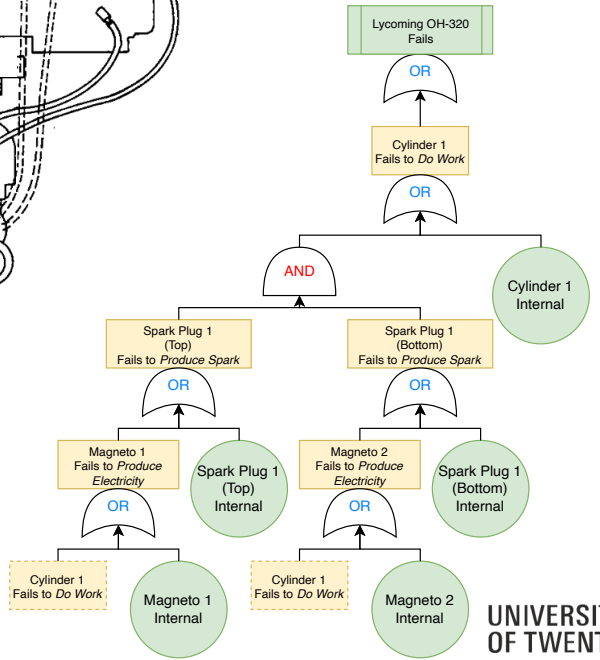
UNIVERSITY
OF TWENTE.

THE GOAL



A Lycoming O-320-D2A installed in a Symphony SA-160
By *Ahunt* at English Wikipedia, Public Domain
https://commons.wikimedia.org/w/index.php?curid=8015248





UNIVERSITY OF TWENTE.

MOTIVATION

- Incompatible modeling languages across engineering teams
- Limited system knowledge is early design stages
- Risk analysis is costly

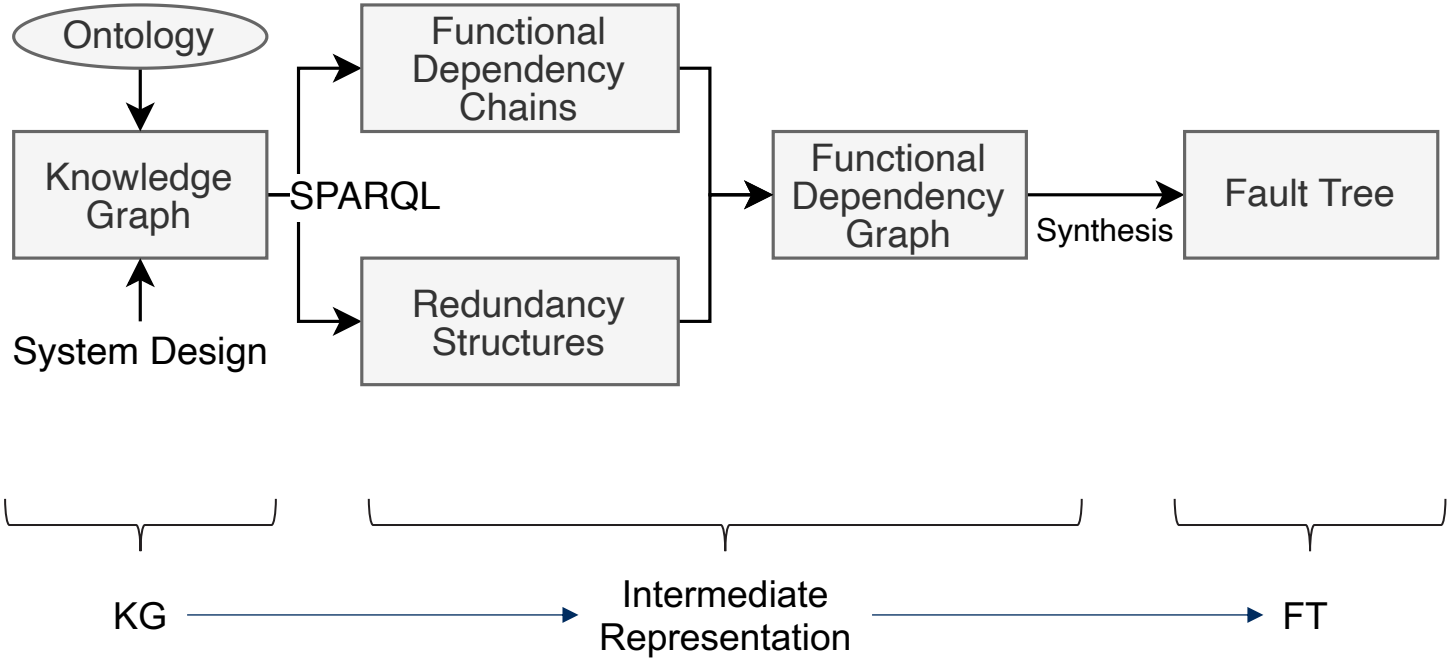
Hence...

- Central conceptual model of CPS design (ontology)
- Minimal knowledge assumptions
- Automatic synthesis of risk models (Fault Trees)

OVERVIEW

- **Methodology Overview**
- Background
- From Knowledge Graphs to Fault Trees
  - Running Example
- Limitations and Future Work

METHODOLOGY

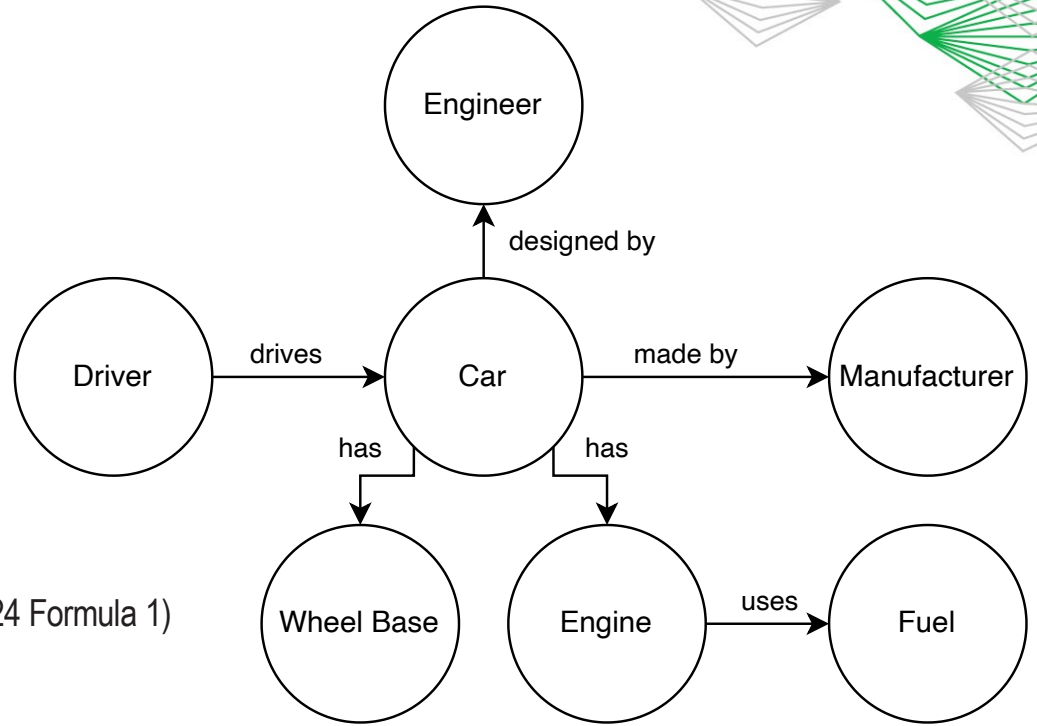


OVERVIEW

- Methodology Overview
- **Background**
- From Knowledge Graphs to Fault Trees
  - Running Example
- Limitations and Future Work

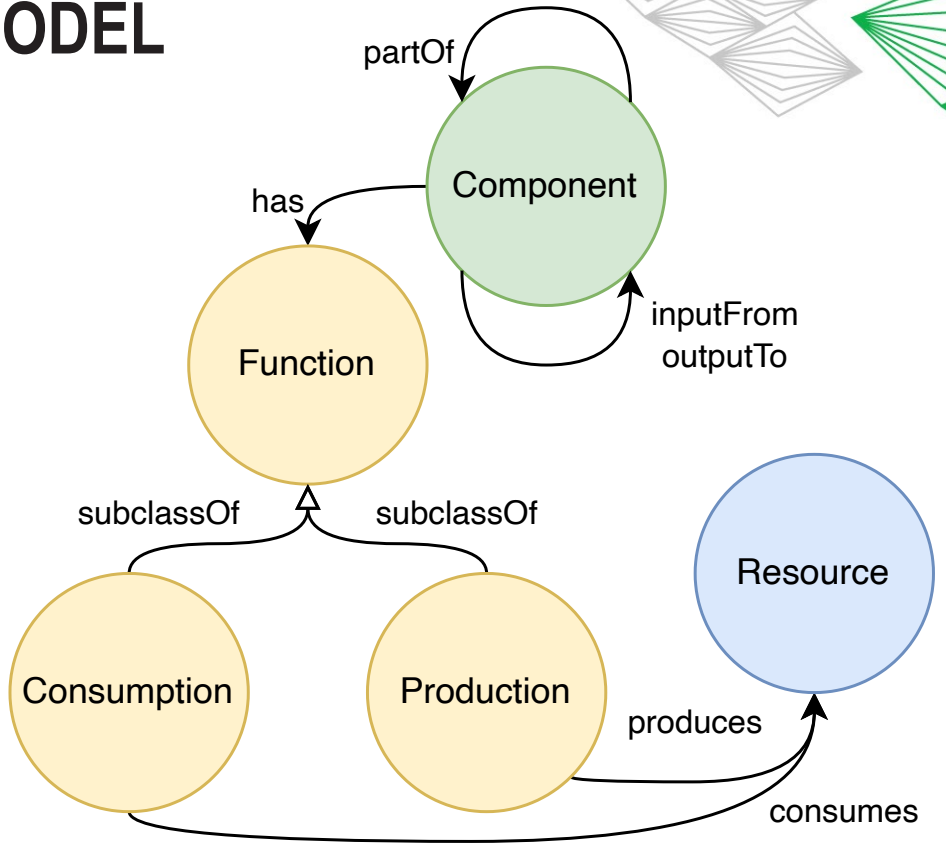
KNOWLEDGE GRAPHS

- Knowledge base with a graph structure
- Supports fact inference
  - I.e. (Driver, drives, Car) implies (Driver, has, License)
- Structured by an *ontology* (a conceptual model)
- It's all about the *instances*
  - I.e. (Charles Leclerc, drives, Ferrari SF-24 Formula 1)



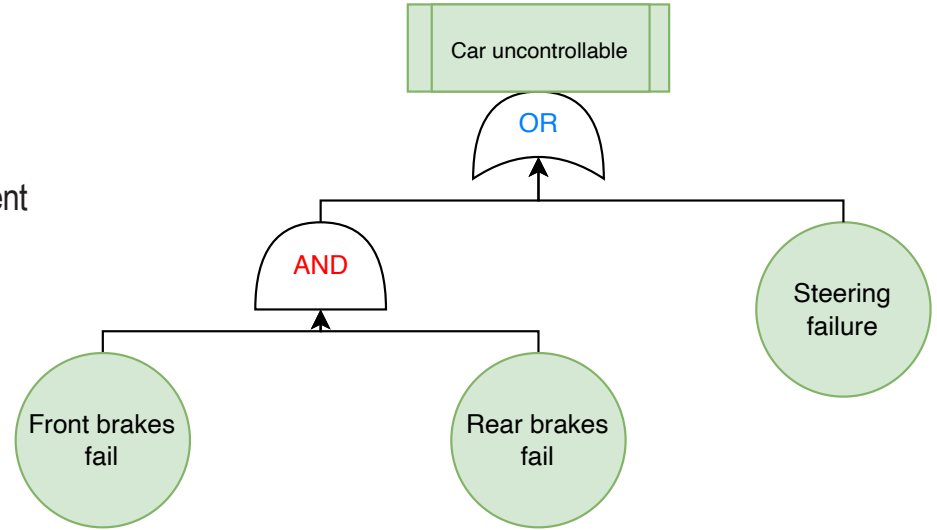
OUR CONCEPTUAL MODEL

- Describes the *domain* of CPS design
- **Minimal knowledge** assumptions
  - Compositionality
  - Functionality



FAULT TREES

- Visual causal model
- Basic Events, Gates and a Top-level Event
- Risk analysis
  - Minimal cut sets (MCS)



MCS: { *Front brakes fail*, *Rear brakes fail* }, { *Steering failure* }

OVERVIEW

- Methodology Overview
- Background
- **From Knowledge Graphs to Fault Trees**
  - **Running Example**
- Limitations and Future Work

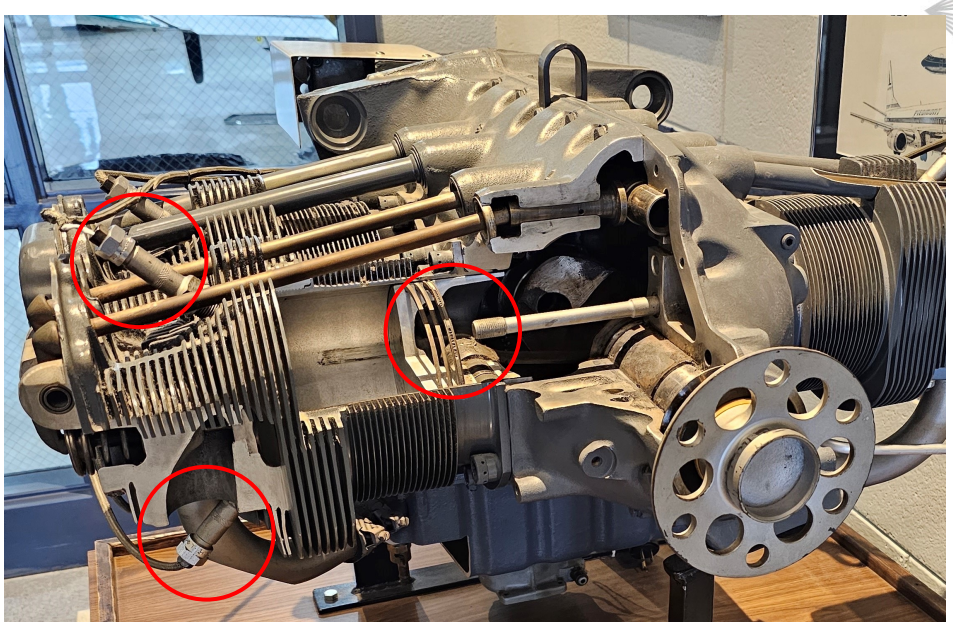
RUNNING EXAMPLE

- Lycoming O-320 aircraft engine
- Designed for reliability

A Lycoming O-320-D2A installed in a Symphony SA-160
By *Ahunt* at English Wikipedia, Public Domain
https://commons.wikimedia.org/w/index.php?curid=8015248

... A BETTER LOOK

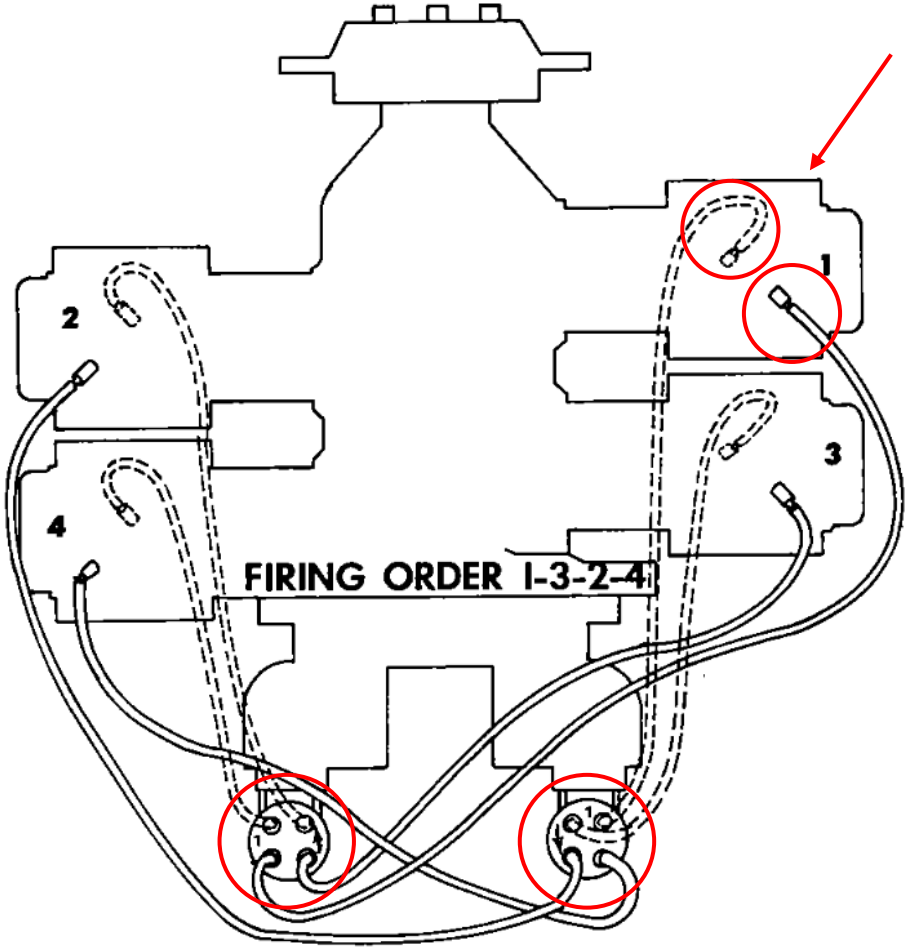
- We see that an engine consists of many components, i.e.:
  - Cylinders and pistons
  - Ignition system
  - Lubrication system
  - etc.



A Lycoming OH-320-D2A cutaway
By *KOMRADE DIMITRI,* Own work, CC BY-SA 4.0
https://commons.wikimedia.org/w/index.php?curid=133450956

THE IGNITION SYSTEM

- The simplified diagram shows:
  - Cylinders
  - Spark plugs
  - Magnetos[1]
- And interestingly
  - Two magnetos
  - Two spark plugs per cylinder

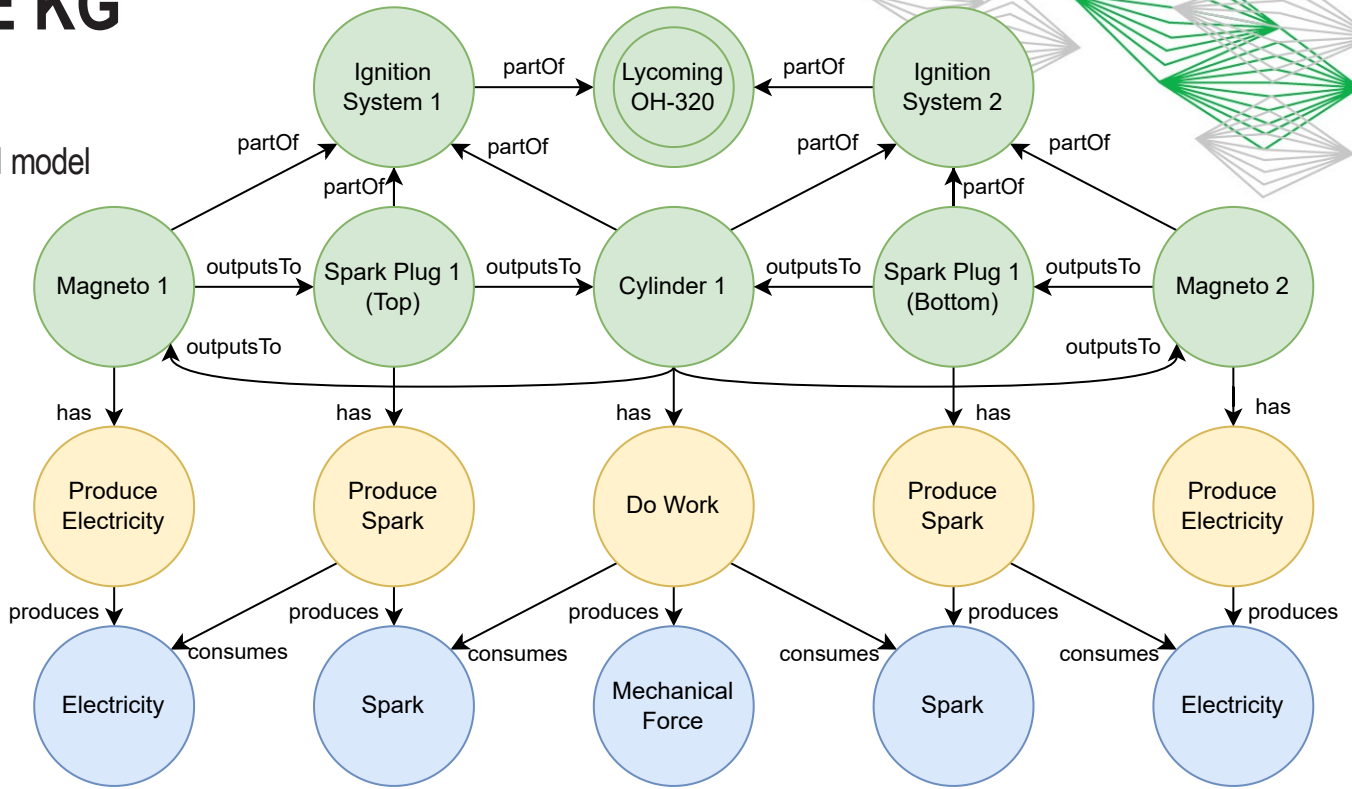


Ignition Wiring Diagram
By *Textron Lycoming, Overhaul Manual Direct Drive Engine (Part No. 60294-7)*

[1] Magnetos convert mechanical energy into high-voltage electricity.

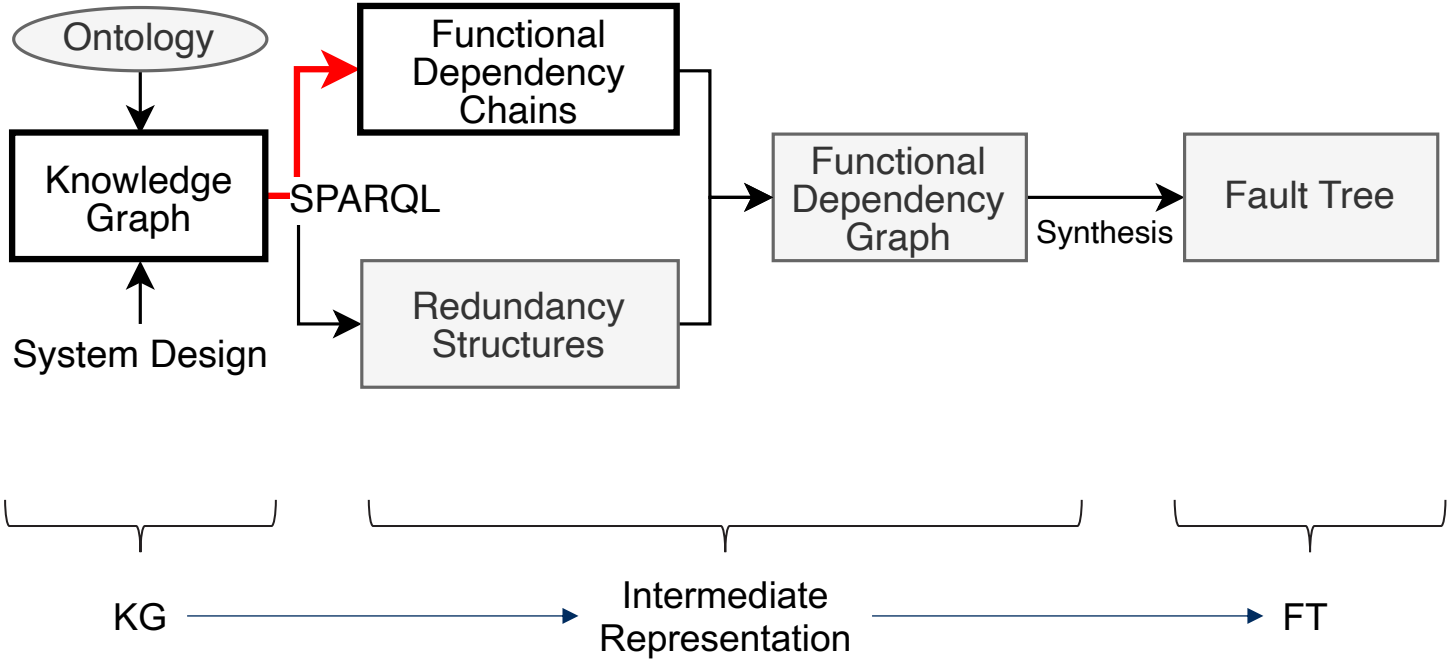
THE EXAMPLE KG

- Instantiates the conceptual model with the system design
- *... Unreadable*

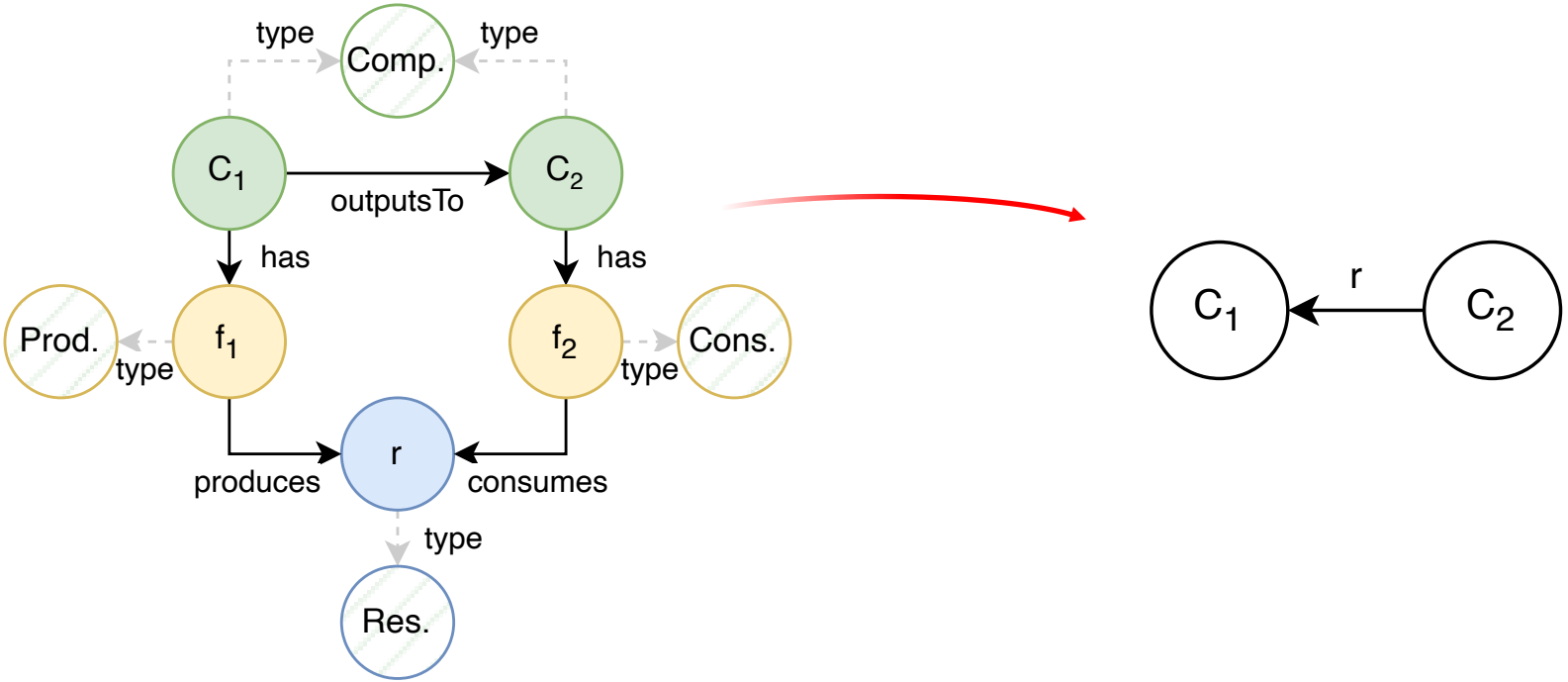


UNIVERSITY OF TWENTE.

FDEP GRAPH CONSTRUCTION

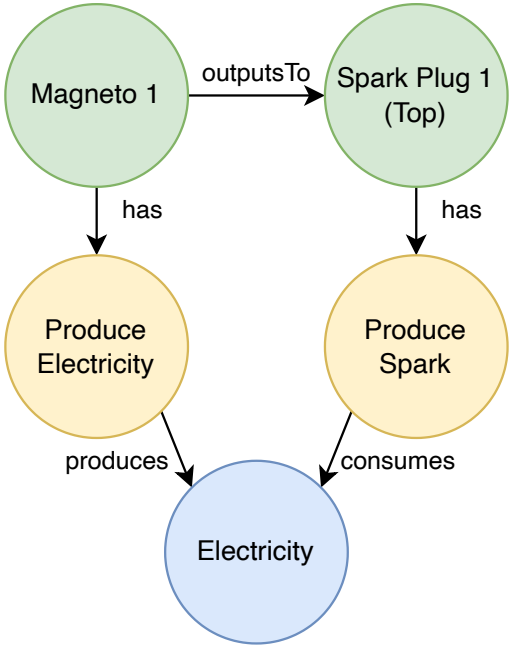


CHAINS OF FUNCTIONAL DEPENDENCY

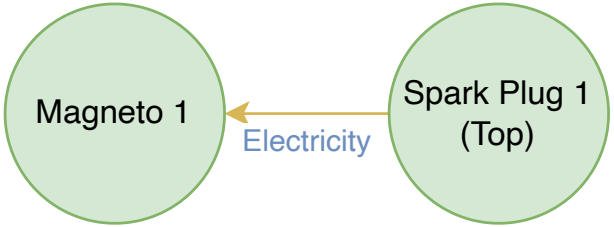


UNIVERSITY OF TWENTE.

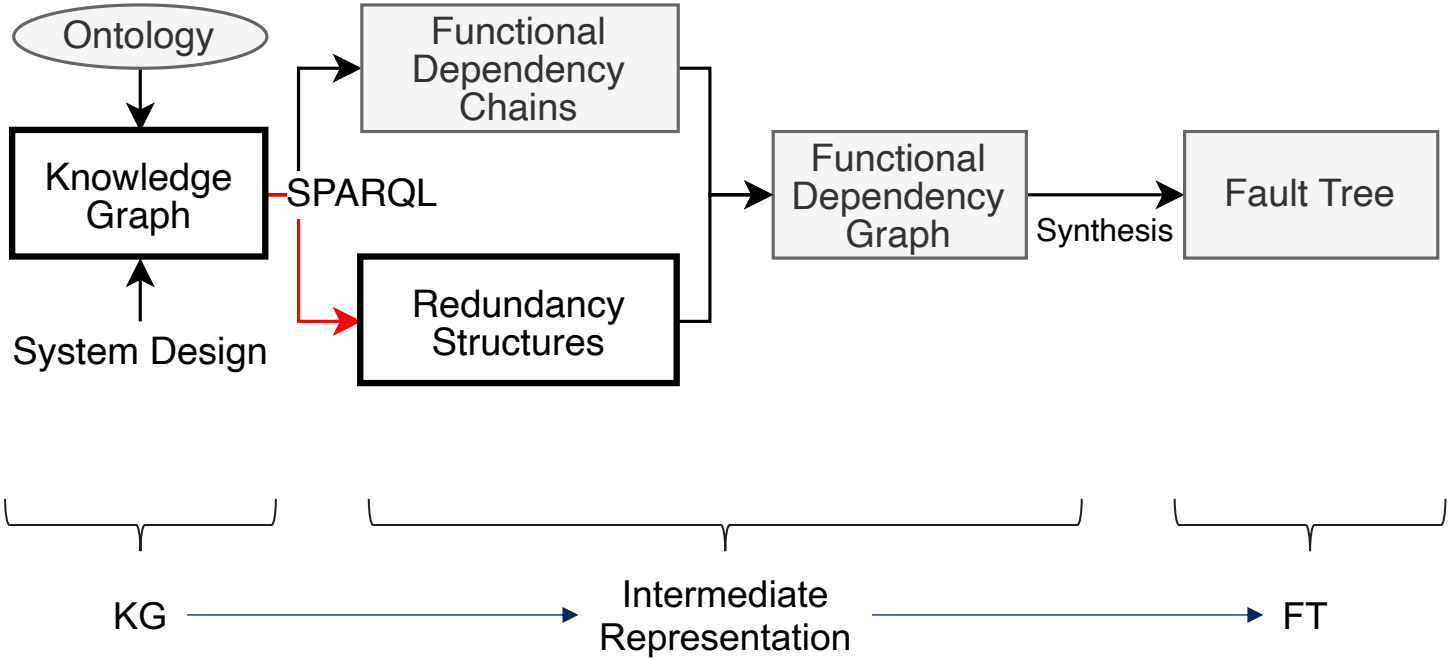
EXAMPLE



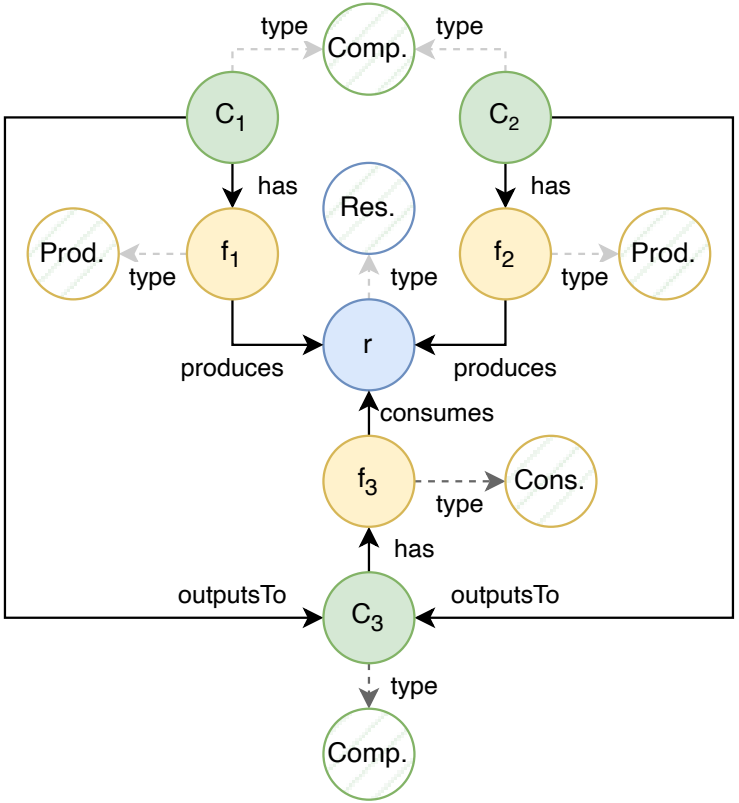
SPARQL

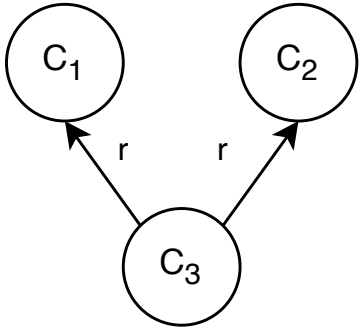


FDEP GRAPH CONSTRUCTION



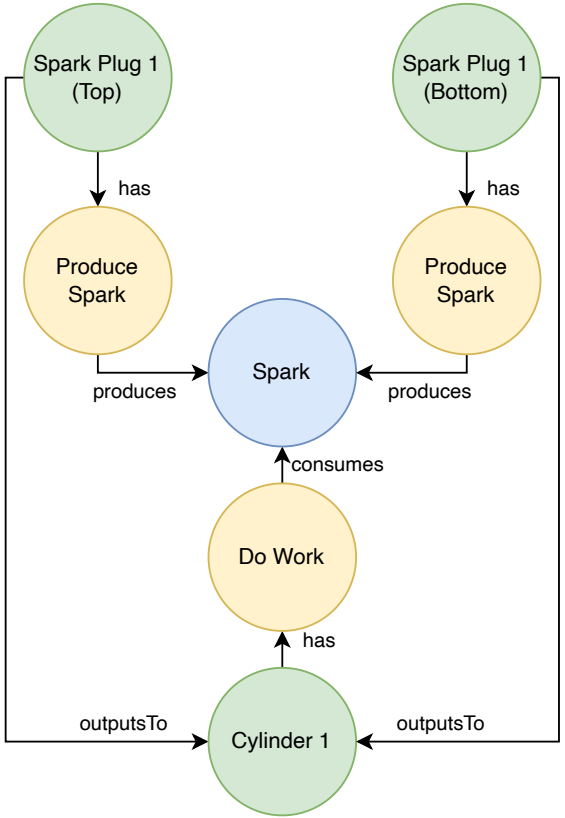
REDUNDANCY STRUCTURES



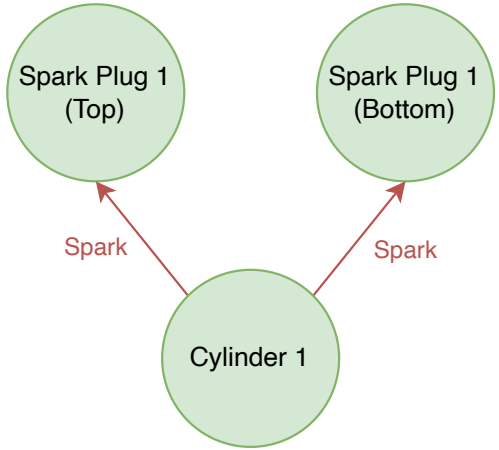


UNIVERSITY OF TWENTE.

EXAMPLE

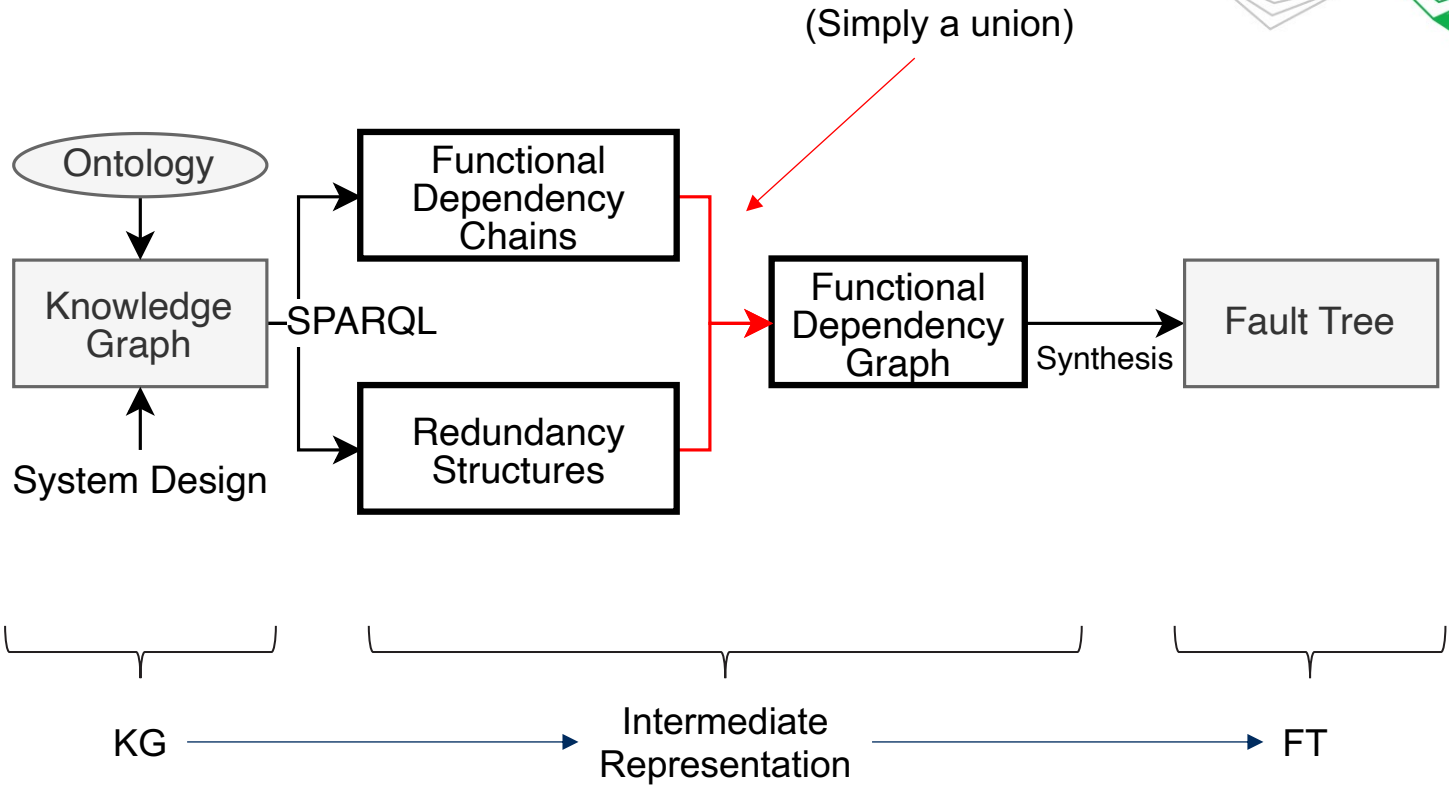


SPARQL

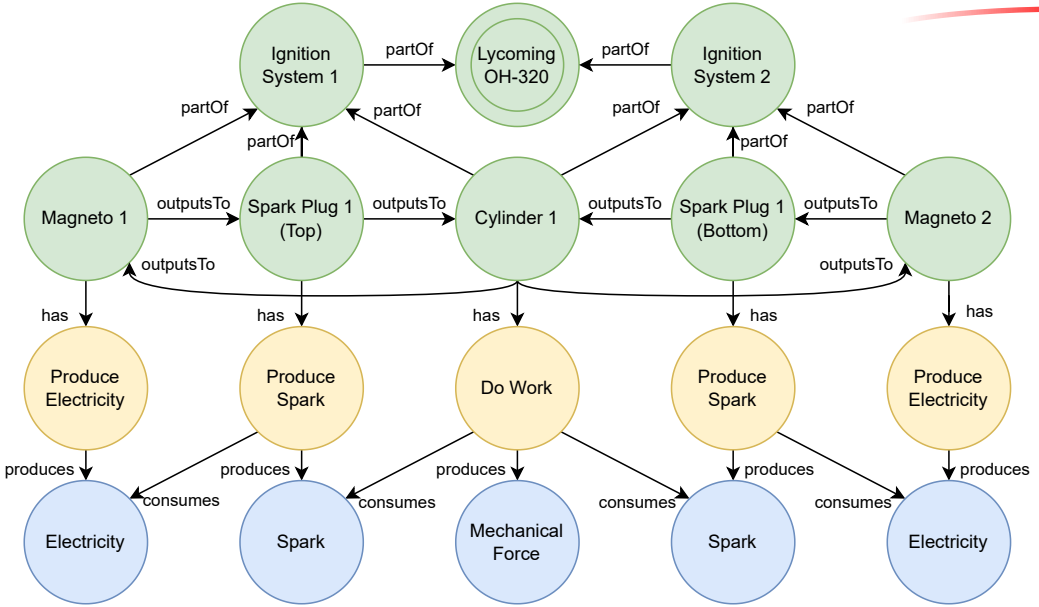


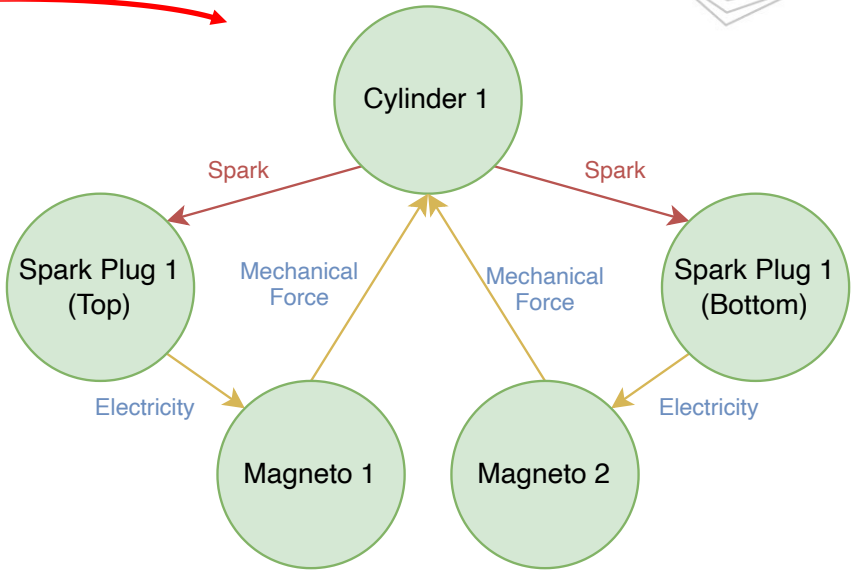
UNIVERSITY OF TWENTE.

FDEP GRAPH CONSTRUCTION



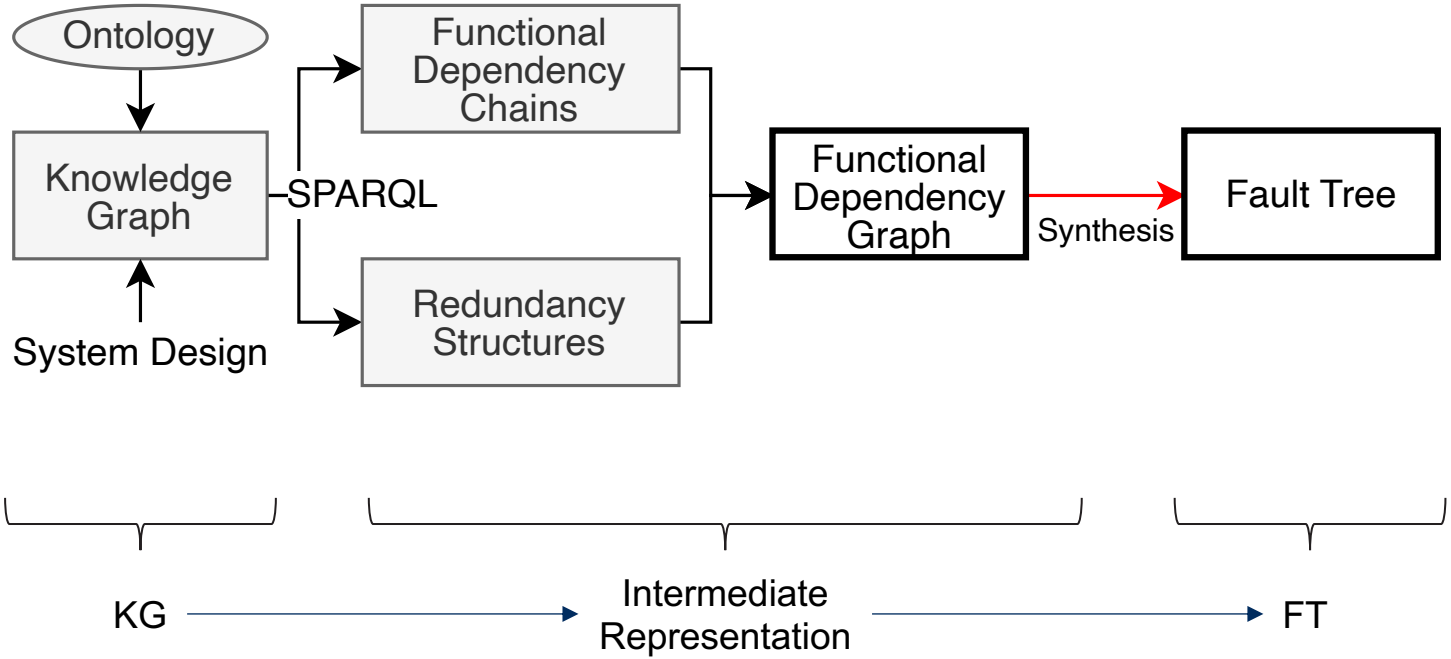
EXAMPLE



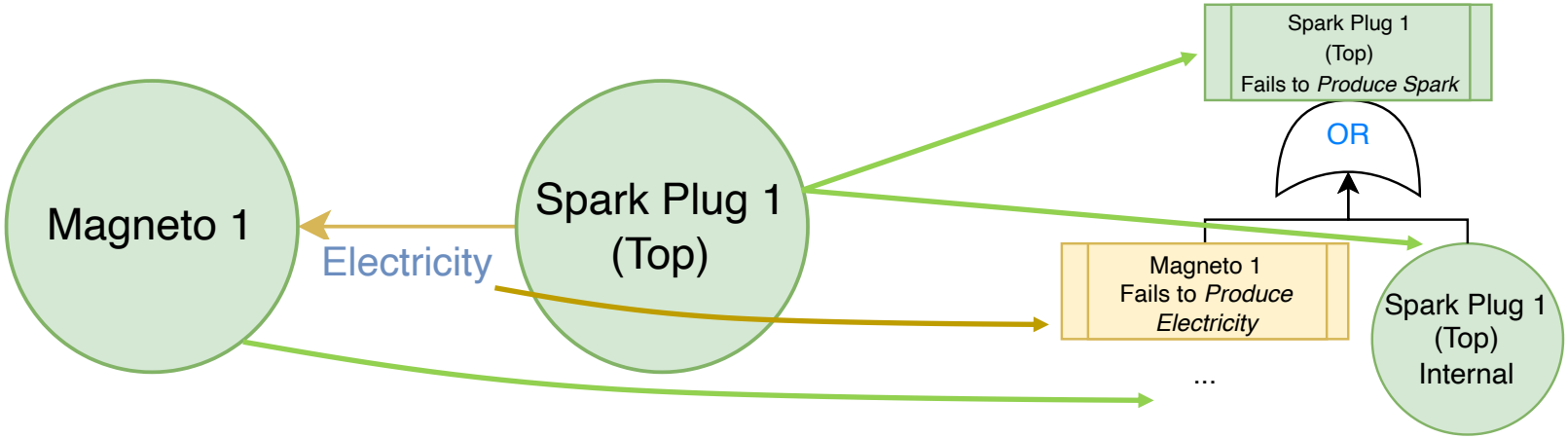


UNIVERSITY OF TWENTE.

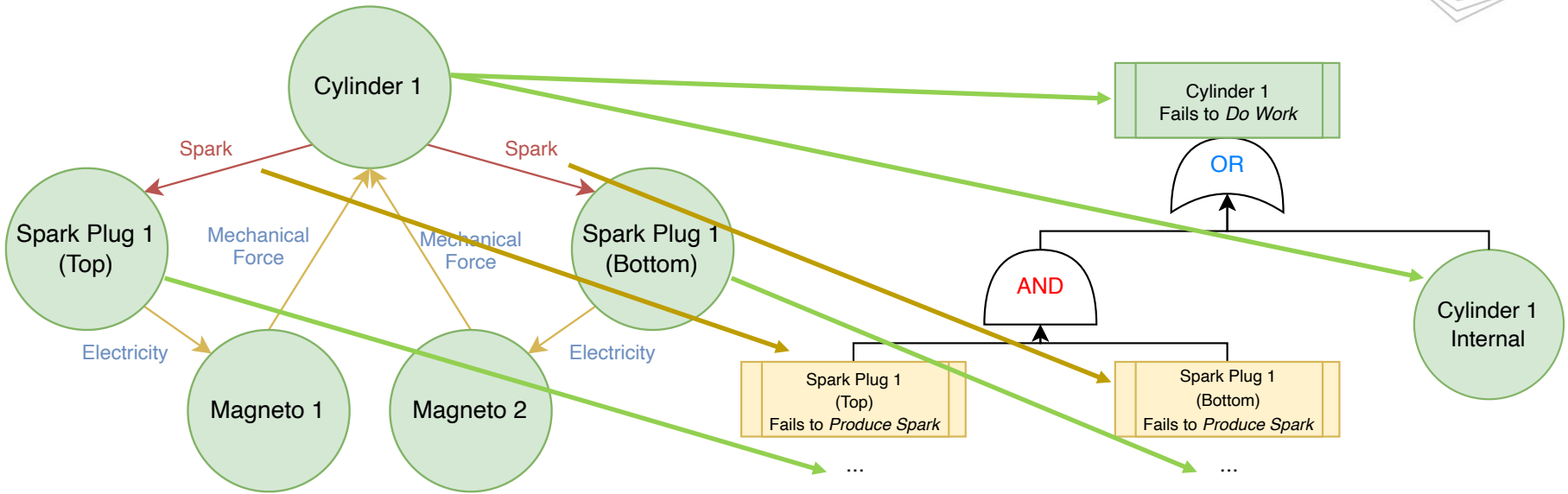
FAULT TREE SYNTHESIS



FAULT TREE SYNTHESIS

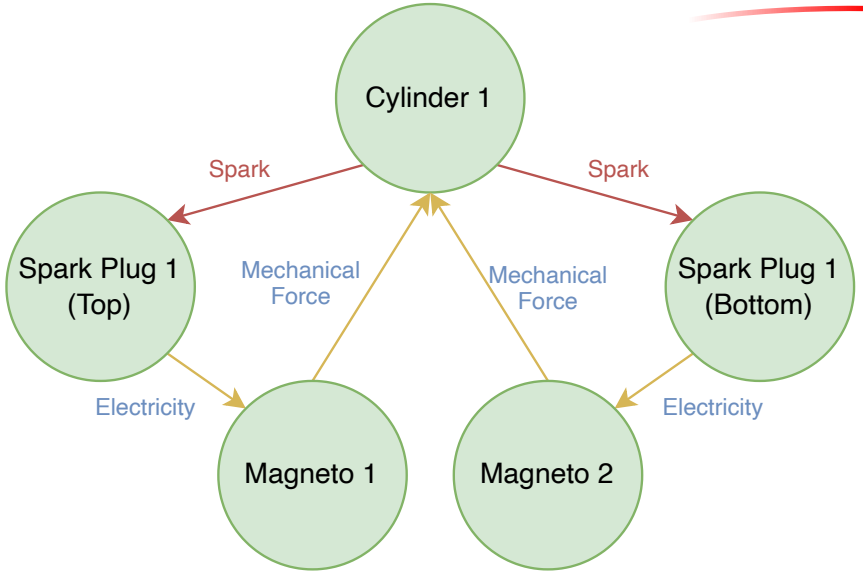


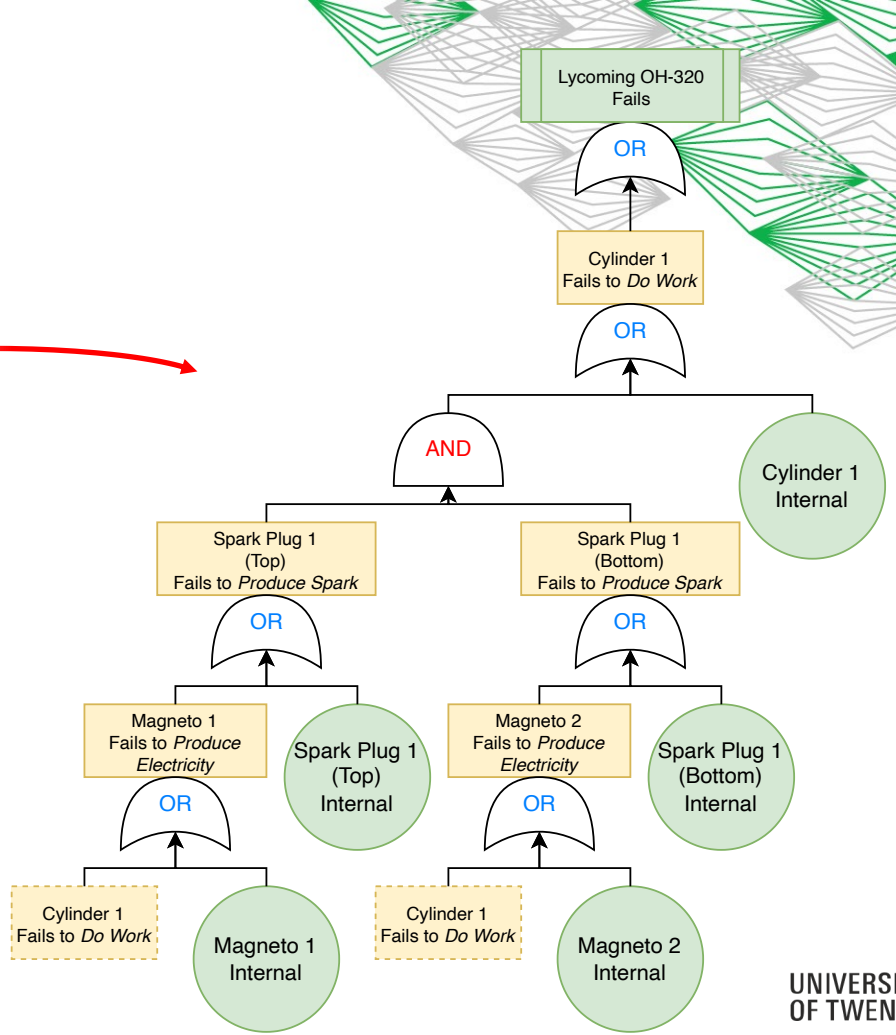
FAULT TREE SYNTHESIS



UNIVERSITY
OF TWENTE.

EXAMPLE





UNIVERSITY OF TWENTE.

RISK ANALYSIS

A Lycoming O-320-D2A installed in a Symphony SA-160
By *Ahunt* at English Wikipedia, Public Domain
https://commons.wikimedia.org/w/index.php?curid=8015248

Our engine fails if:

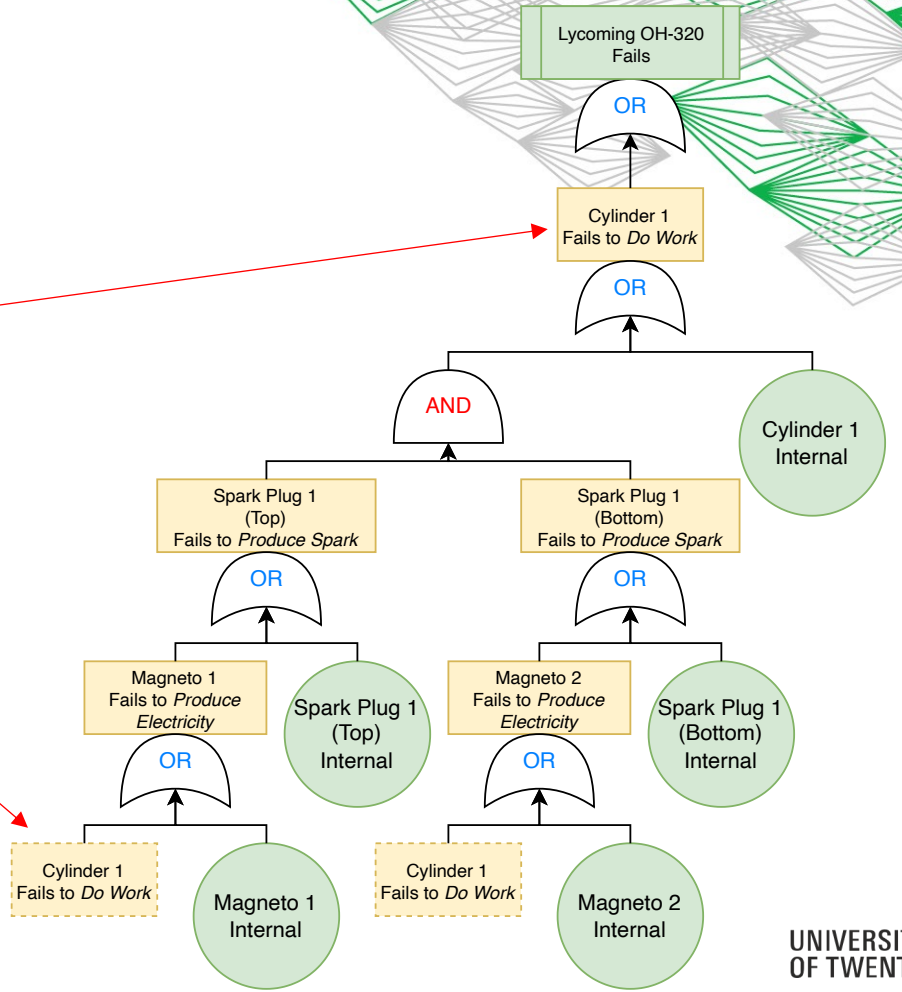
- **Just** *Cylinder 1* fails
- **Both** *spark plugs* fail
- **Both** *magnetos* fail
- The *top spark plug* **and** *magneto 2* fail
- The *bottom spark plug* **and** *magneto 1* fail

OVERVIEW

- Methodology Overview
- Background
- From Knowledge Graphs to Fault Trees
  - Running Example
- **Limitations and Future Work**

LIMITATIONS

- Cycles are hard!
- No dynamic behavior
- No quantity specifications
  - Flow rates, units, multiplicity
  - Failure probability



UNIVERSITY OF TWENTE.

FUTURE WORK

- A stronger ontology:
  - Grounded in a Foundational Ontology (UFO)
  - Quantified, explicit requirements
  - Dynamic system model
  - Failure probabilities of components
- How do we get the system design into the knowledge graph?
- More models!