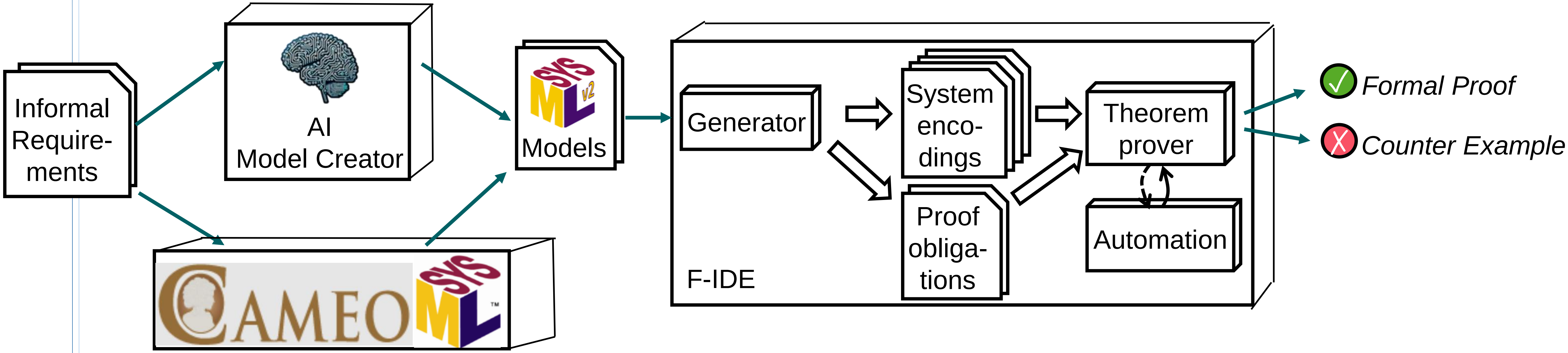
A SysML-based Framework for Analyzing Security and Safety Properties Applied on an Aerospace Data Link Uplink Feed System

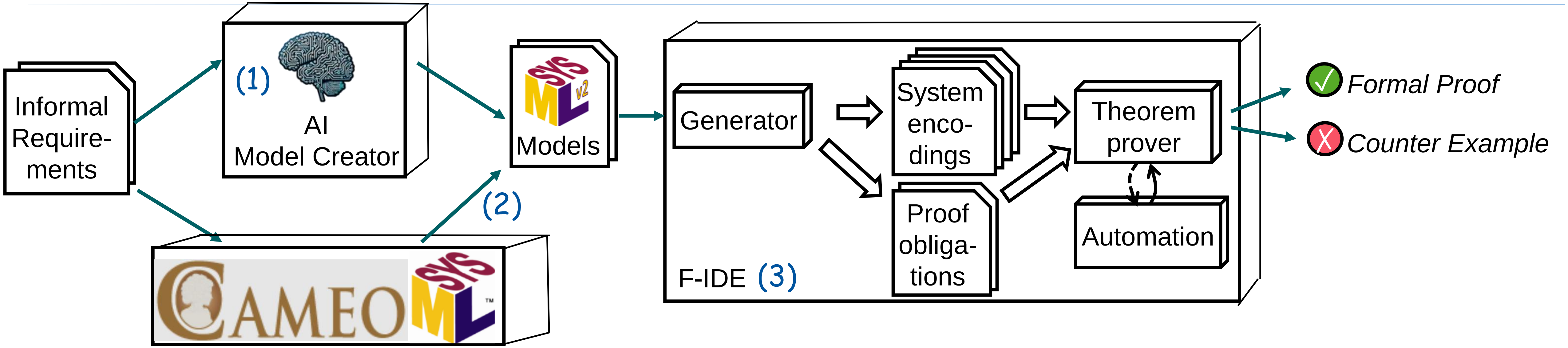


SE Software Engineering | RWTH AACHEN UNIVERSITY

Context

- Background
- MBSE in Aerospace Projects

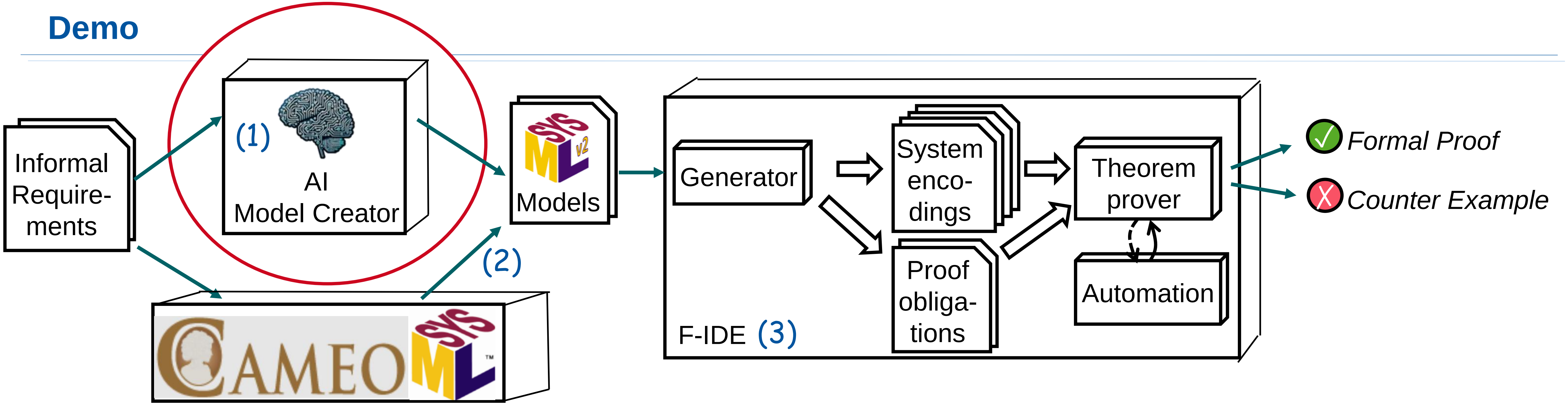
In this talk



- In this talk:

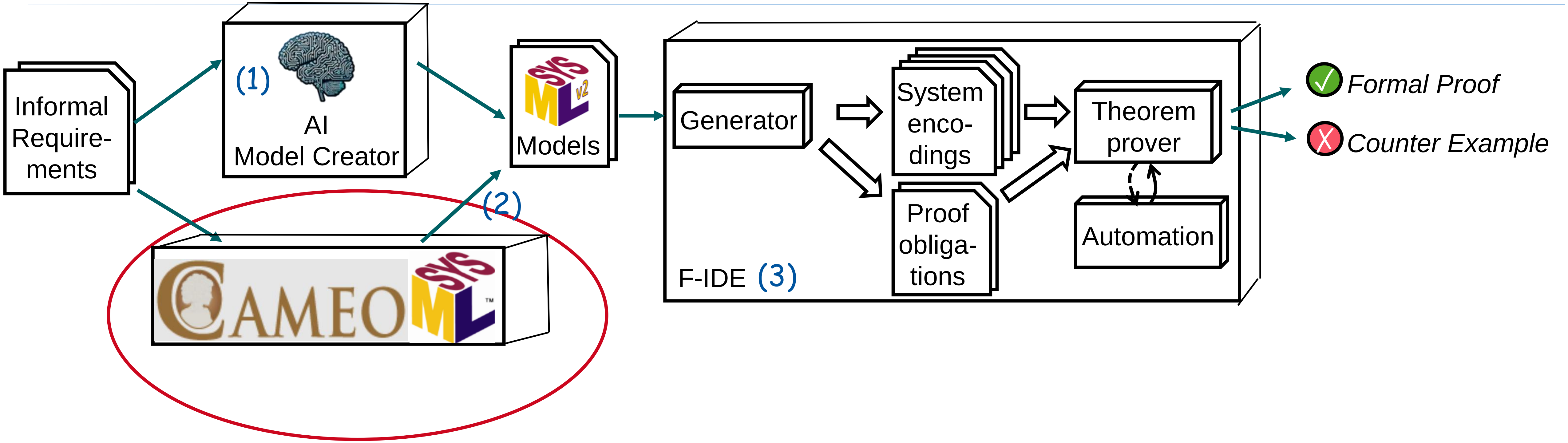
  1. AI-LLM-Tool to create SysML v2 models
  2. Cameo PlugIn exporting SysML v1 graphical as SysML v2 textual (MontiBelleML)
  3. (Web-based) Formal Integrated Verification Environment

Demo



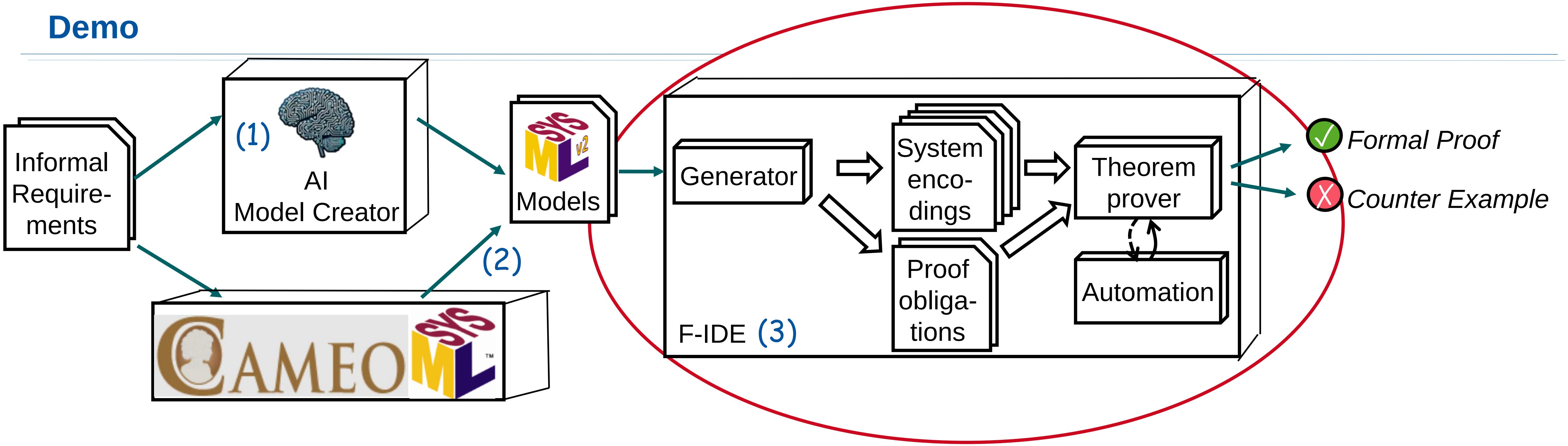
With support from collegues:

Demo



With support from collegues:

Demo



With support from collegues:

An MBSE Solution

- An MBSE Solution = Modeling Language x Methodology x Toolbox

  - ESA MBSE Solution = (ESA SysML Profile, ESA Methodology, ESA SysML Toolbox)

    SysML v1, SysML v2

    Cameo, Capella, SysIDE

  - Thales (Arcadia) MBSE Solution = (DSML, Arcadia, Capella)

  - Dassault MBSE Solution = (SysML v1, Magic Grid, CATIA Magic)

  - MontiBelle MBSE Solution = (MontiBelleML, MontiBelle, MontiBelle Toolbox)

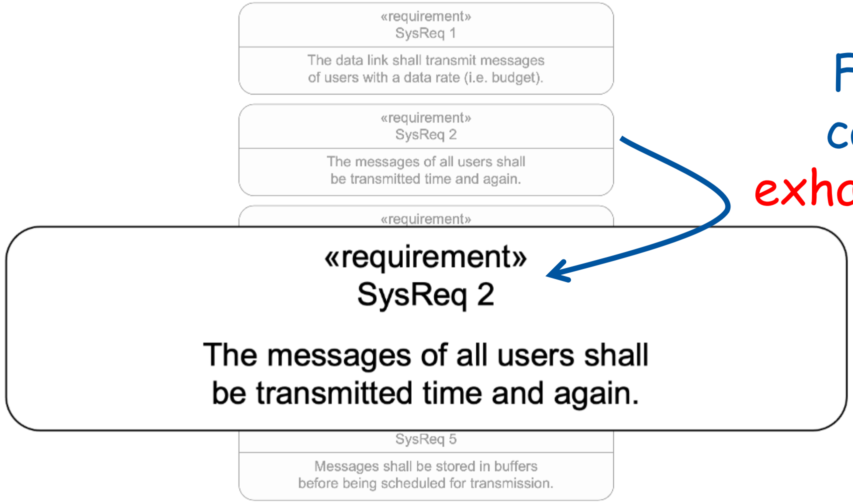
    SysML v1, SysML v2 profile

    (Web-based) Formal Integrated Development Environment, Cameo, LLM-Synthetiser

    Based on *SPES Methodology* (based on *FOCUS' USP*)

Case Study: Prioritized Data-Link Upload-Feed

- Satellite sends messages to base station over bandwidth-restricted link
- Messages are thus prioritized to ensure critical data takes precedence
- Flooding with lower-priority messages from attackers could cause a Security->Avaliability->Denial-Of-Service issue
- No priority level should starve!



«requirement»
SysReq 1
The data link shall transmit messages of users with a data rate (i.e. budget).

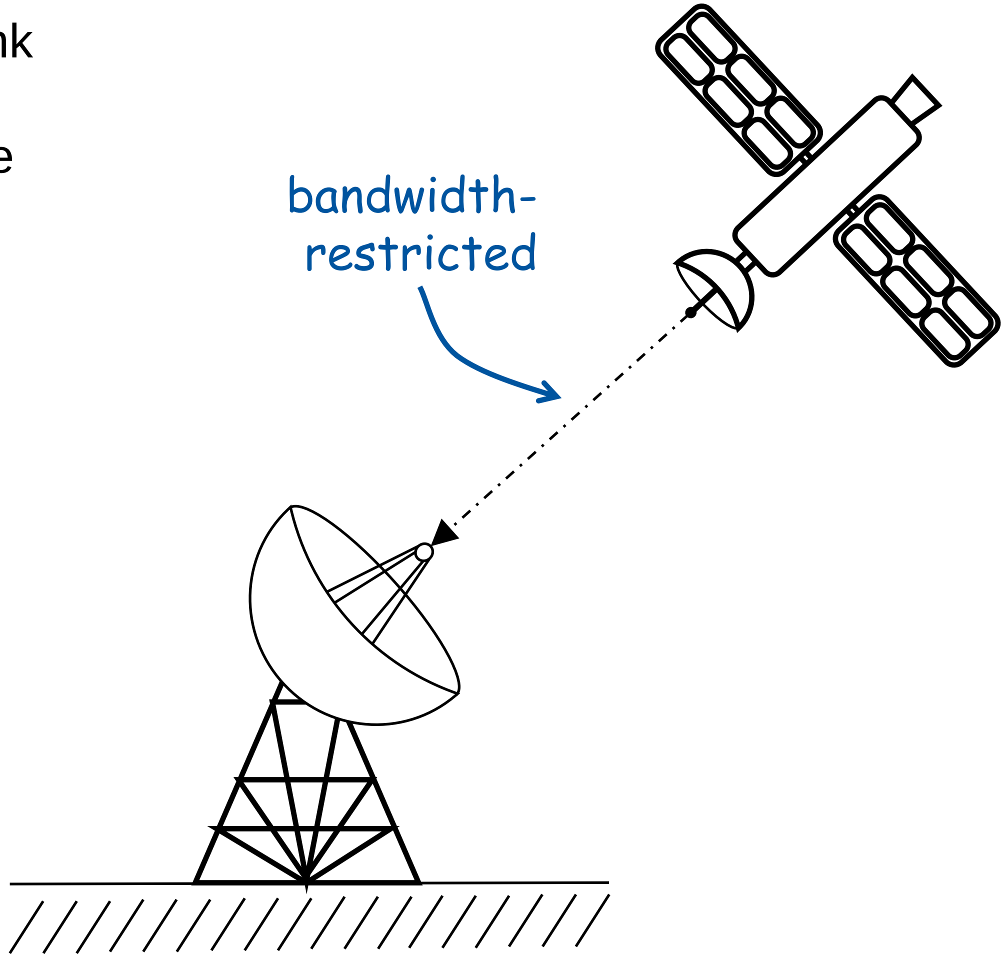
«requirement»
SysReq 2
The messages of all users shall be transmitted time and again.

«requirement»

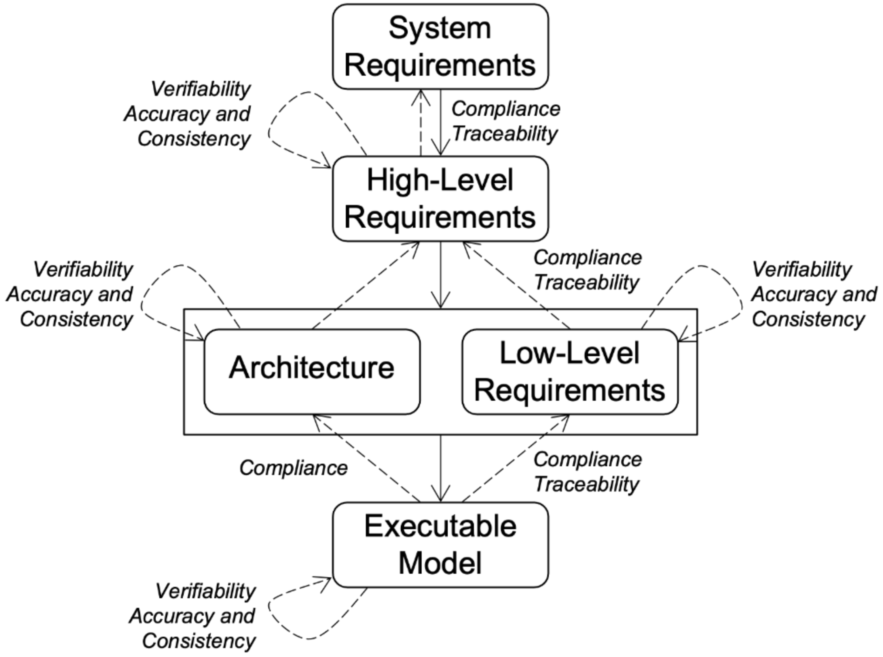
«requirement»
SysReq 2
The messages of all users shall be transmitted time and again.

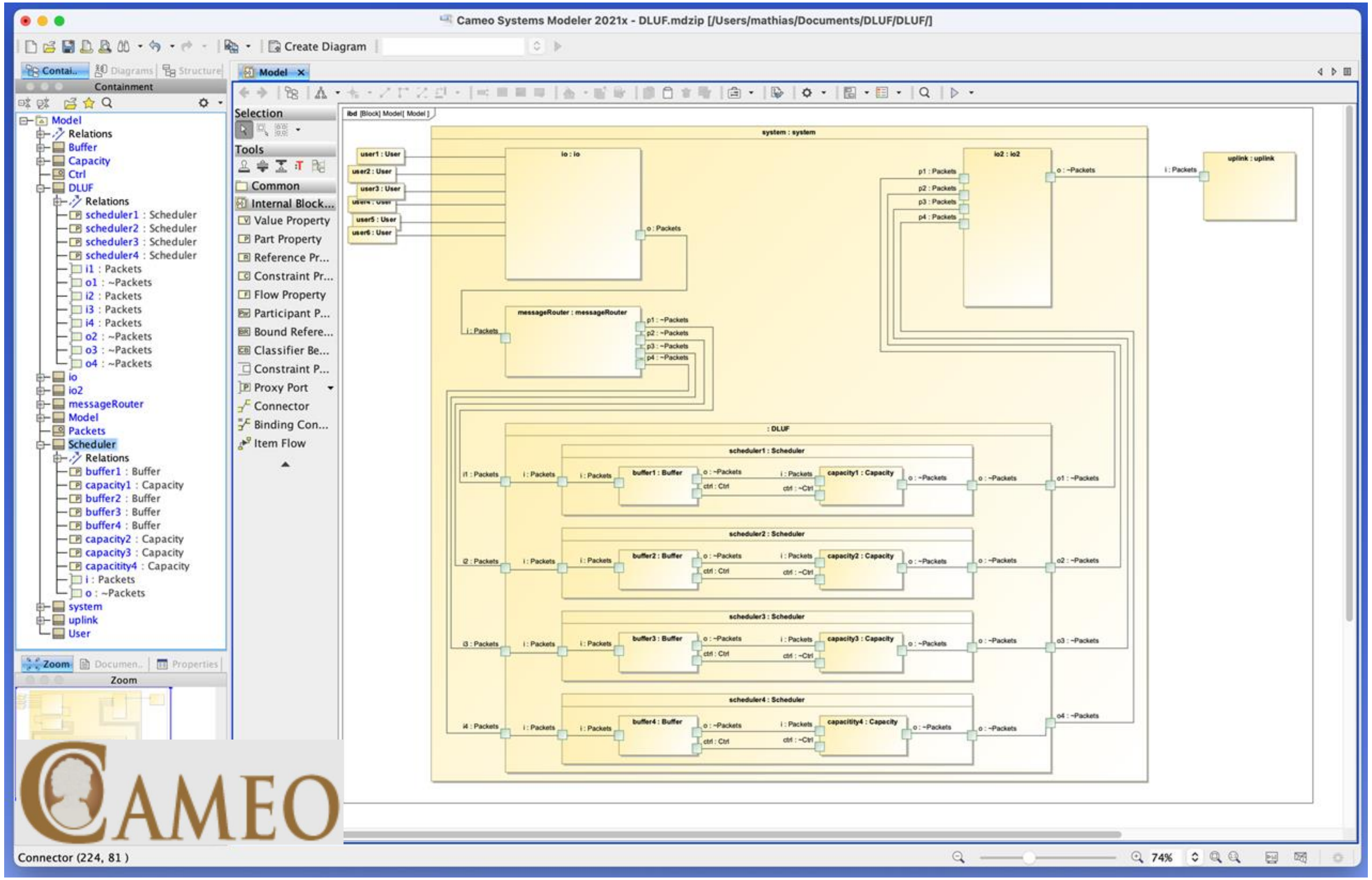
SysReq 5
Messages shall be stored in buffers before being scheduled for transmission.

Fairness/Liveness cannot be covered exhaustively by tests



V-Modell

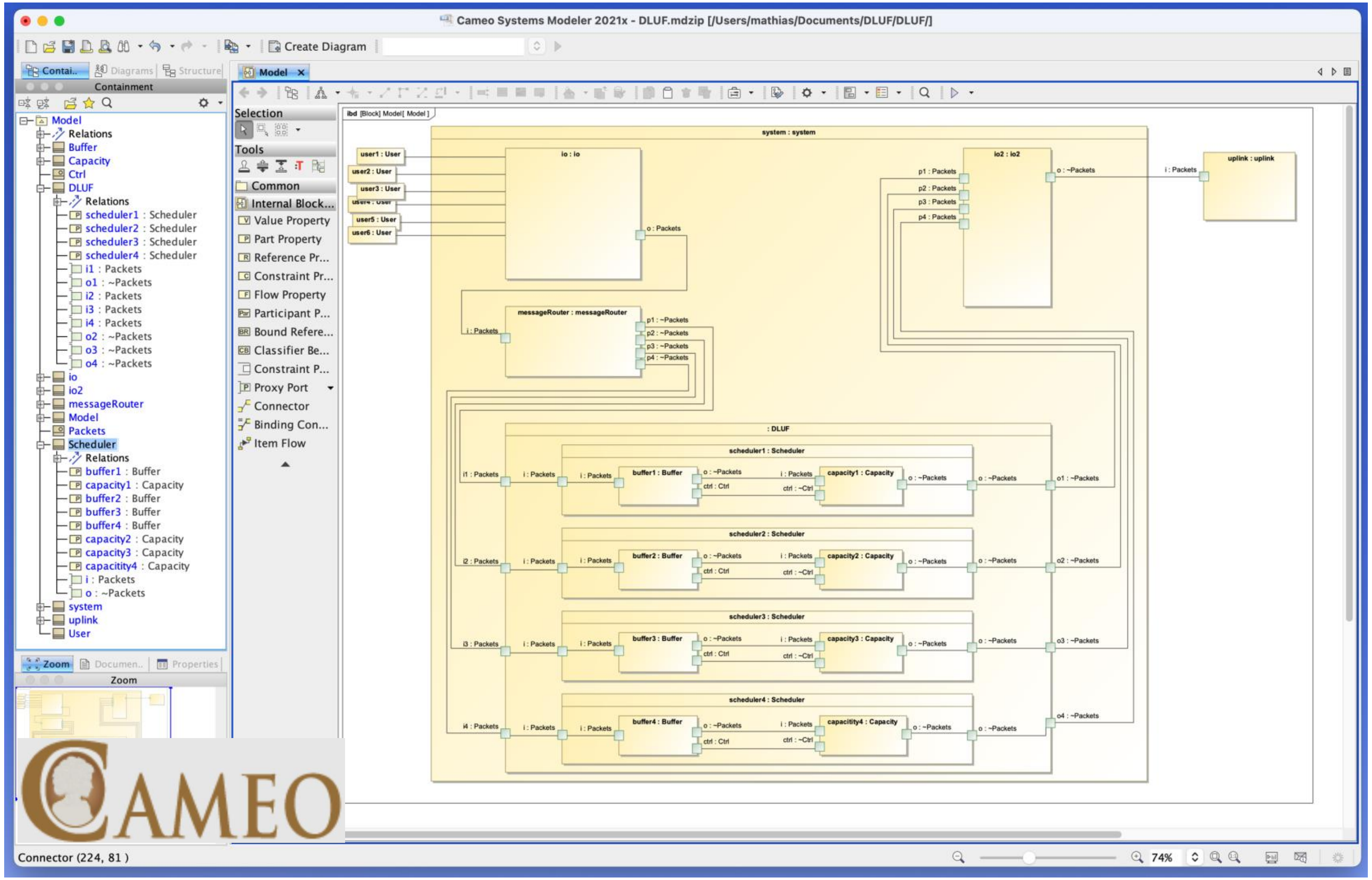

System Requirements
Verifiability Accuracy and Consistency
Compliance Traceability
High-Level Requirements
Verifiability Accuracy and Consistency
Compliance Traceability
Verifiability Accuracy and Consistency
Architecture
Low-Level Requirements
Compliance
Compliance Traceability
Executable Model
Verifiability Accuracy and Consistency


Cameo Systems Modeler 2021x - DLUF.mdzip [/Users/mathias/Documents/DLUF/DLUF/]
Create Diagram
Contai... Diagrams Structure
Containment
Model
Relations
Buffer
Capacity
Ctrl
DLUF
Relations
scheduler1 : Scheduler
scheduler2 : Scheduler
scheduler3 : Scheduler
scheduler4 : Scheduler
i1 : Packets
o1 : ~Packets
i2 : Packets
i3 : Packets
i4 : Packets
o2 : ~Packets
o3 : ~Packets
o4 : ~Packets
io
io2
messageRouter
Model
Packets
Scheduler
Relations
buffer1 : Buffer
capacity1 : Capacity
buffer2 : Buffer
buffer3 : Buffer
buffer4 : Buffer
capacity2 : Capacity
capacity3 : Capacity
capacitity4 : Capacity
i : Packets
o : ~Packets
system
uplink
User
Zoom Documen... Properties
Zoom
Model
Selection
Tools
Common
Internal Block...
Value Property
Part Property
Reference Pr...
Constraint Pr...
Flow Property
Participant P...
Bound Refere...
Classifier Be...
Constraint P...
Proxy Port
Connector
Binding Con...
Item Flow
ibd [Block] Model[Model]
system : system
user1 : User
user2 : User
user3 : User
user4 : User
user5 : User
user6 : User
io : io
o : Packets
io2 : io2
p1 : Packets
p2 : Packets
p3 : Packets
p4 : Packets
o : ~Packets
i : Packets
uplink : uplink
messageRouter : messageRouter
i : Packets
p1 : ~Packets
p2 : ~Packets
p3 : ~Packets
p4 : ~Packets
: DLUF
scheduler1 : Scheduler
scheduler2 : Scheduler
scheduler3 : Scheduler
scheduler4 : Scheduler
buffer1 : Buffer
buffer2 : Buffer
buffer3 : Buffer
buffer4 : Buffer
capacity1 : Capacity
capacity2 : Capacity
capacity3 : Capacity
capacitity4 : Capacity
ctrl : Ctrl
ctrl : ~Ctrl
o1 : ~Packets
o2 : ~Packets
o3 : ~Packets
o4 : ~Packets
CAMEO
Connector (224, 81)
74%

Statistics

Statistics

- 38 SysML Specifications
- 38 generated equivalent theorem prover specifications
- 26 generated formal certificates discharging certification subgoals (~1400 A4-pages of machine proofs)



Future Work for Space Missions

1. Verification of „ESA SysML v2 Profile“ - models
   - Verification PlugIn for SysIDE - enriching verification capabilities by generative theorem proving

2. Cameo PlugIn exporting SysML v1 graphical as „ESA SysML v2 Profile“ textual in SysIDE

3. LLM-based tool for creating „ESA SysML v2 Profile“ textual models from informal requirements

4. Theorem-Prover PlugIn for TASTE
   - Encoding SDL state-machine-based property specification techniques of TASTE in Isabelle
   - Developing a Code Generator from SDL to Isabelle
     - Agents/components as Main structural entities
     - Blocks (internal roots) as containers of agents, used to break down complexity and size of systems
     - Processes (atomic agents, leaves) as bottom-level agents
     - Behavior of processes defined using state machines

Thank You!