Improving Responsiveness of MBSE of CPS
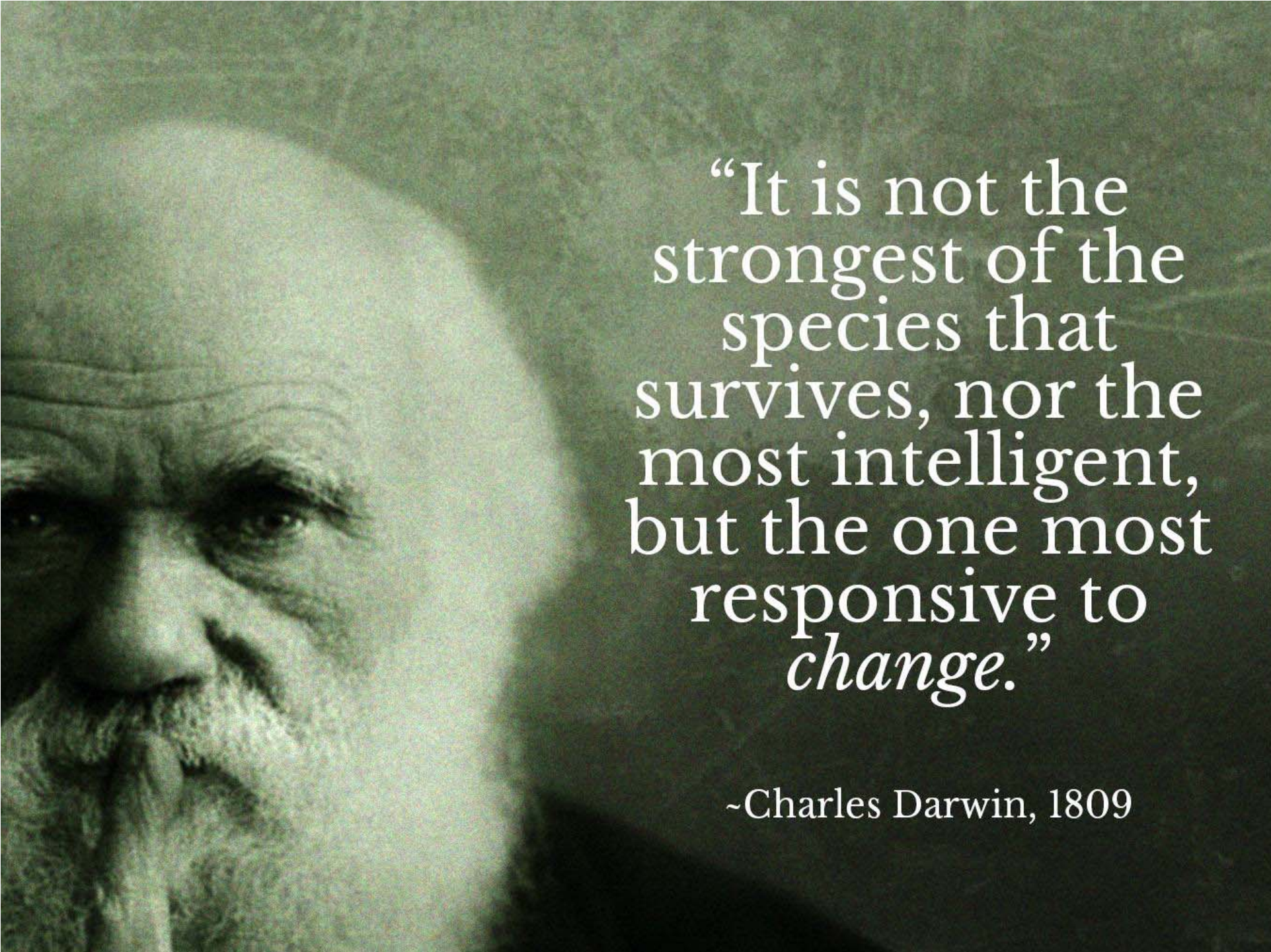
I WANT IT:

LATER ○

NOW ○

Hans Vangheluwe
Joachim Denil

Universiteit Antwerpen

McGill

"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to *change.*"

~Charles Darwin, 1809

- **Problem**:
project risk high
- **Cause**: changing requirements during project
  - E.g., SCNF: train too wide for platforms
- **Solution**: *early* and *repeated* *system-level* evaluation

→ general approach:
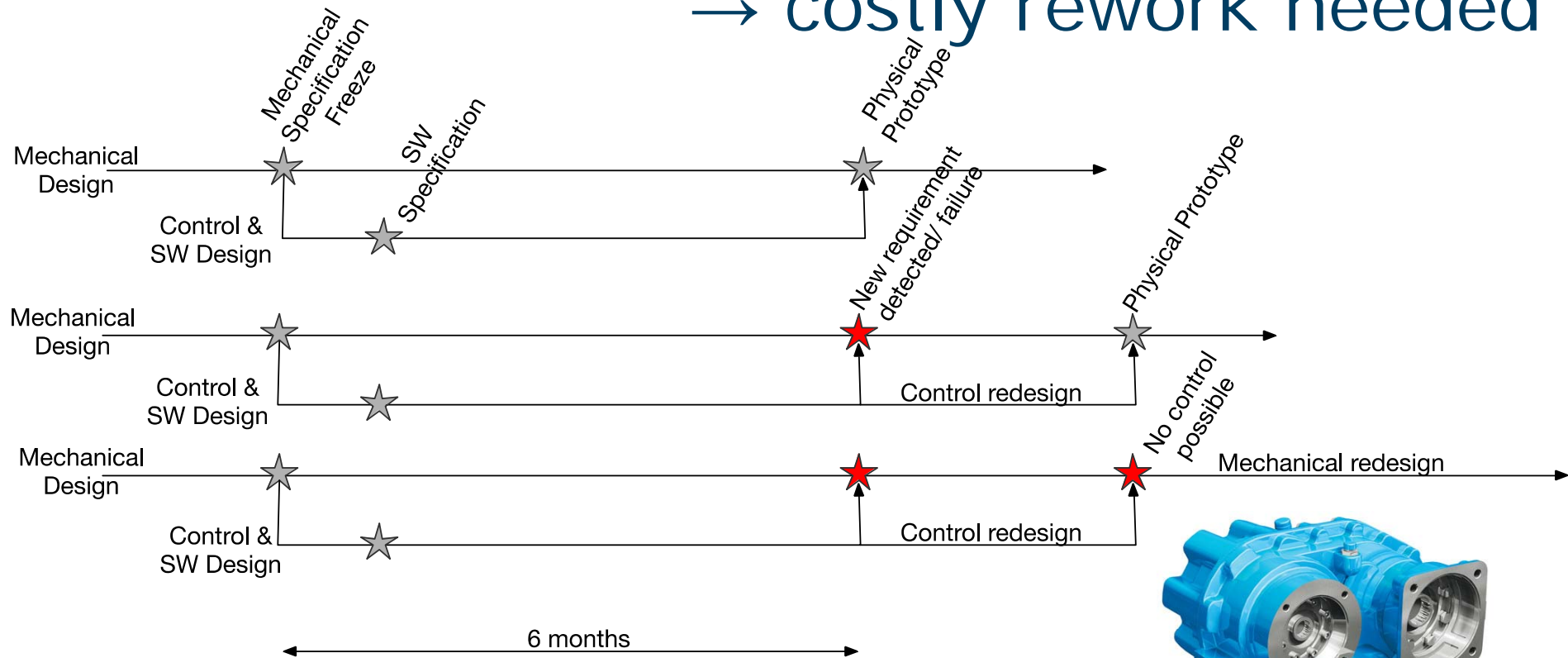**adapt** successful approaches from software engineering to MBSE!

early industrial successes in
- TETRA pack
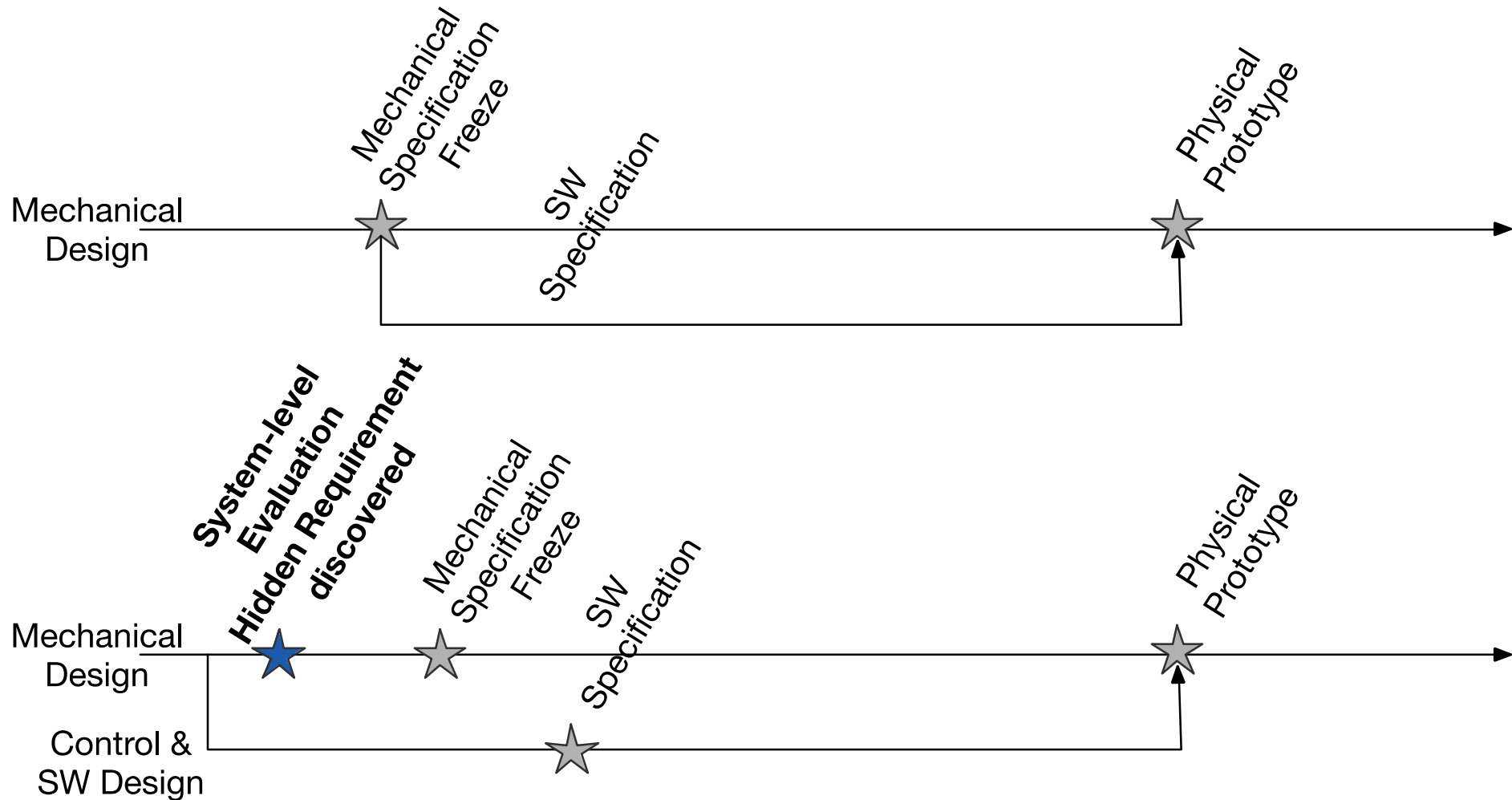- Marel
- SAAB EDS
- Andritz Hydro

Universiteit Antwerpen

McGill

problem:
undetected missing requirements
→ costly rework needed

Mechanical Specification Freeze

SW Specification

Physical Prototype

Mechanical Design

Control & SW Design

New requirement detected/ failure

Physical Prototype

Mechanical Design

Control & SW Design

Control redesign

No control possible

Mechanical Design

Control & SW Design

Control redesign

Mechanical redesign

6 months

Universiteit Antwerpen

solution: front-loading full-system evalation

Mechanical Design

Mechanical Specification Freeze

SW Specification

Physical Prototype

System-level Evaluation Hidden Requirement discovered

Control & SW Design

Universiteit Antwerpen

McGill

"agile" for MBSE of CPS

Inputs:

Functional Requirements (From customer)

Historical Dat

Team capabilities

Select Requirements

Project focus:
Methods, Techniques and
Tool support for
"agile" MBSE

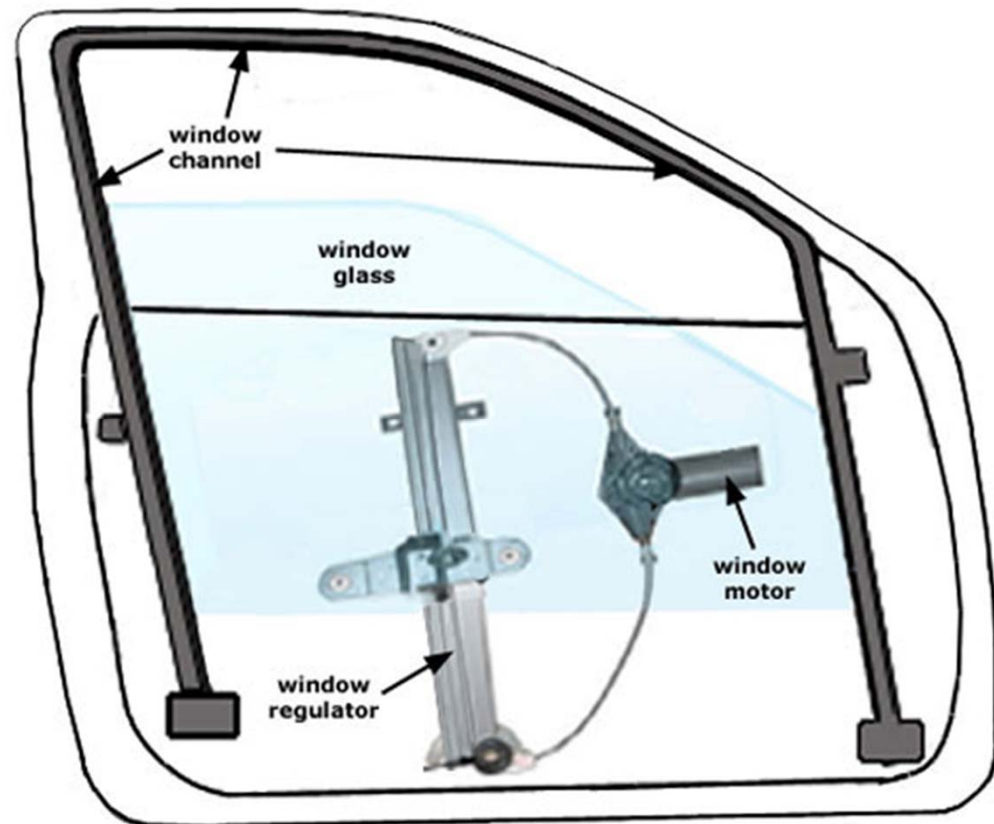Output: Consistent set of Models satisfying selected requirements

Universiteit Antwerpen

McGill

small, but representative:

- Multi-view
- Multi-abstraction
- Multi-formalism
- Multi-domain
- Multi-developer
- Functional requirements
- Safety requirements
- Product family
- Design-space exploration
- Deployment-space exploration
- …

window channel

window glass

window motor

window regulator

agcoauto.com

Universiteit Antwerpen

McGill

Agile Model-Based Systems Engineering for CPS:
Challenges and Solutions

Joachim Denil
University of Antwerp/Flanders Make

Rick Salay
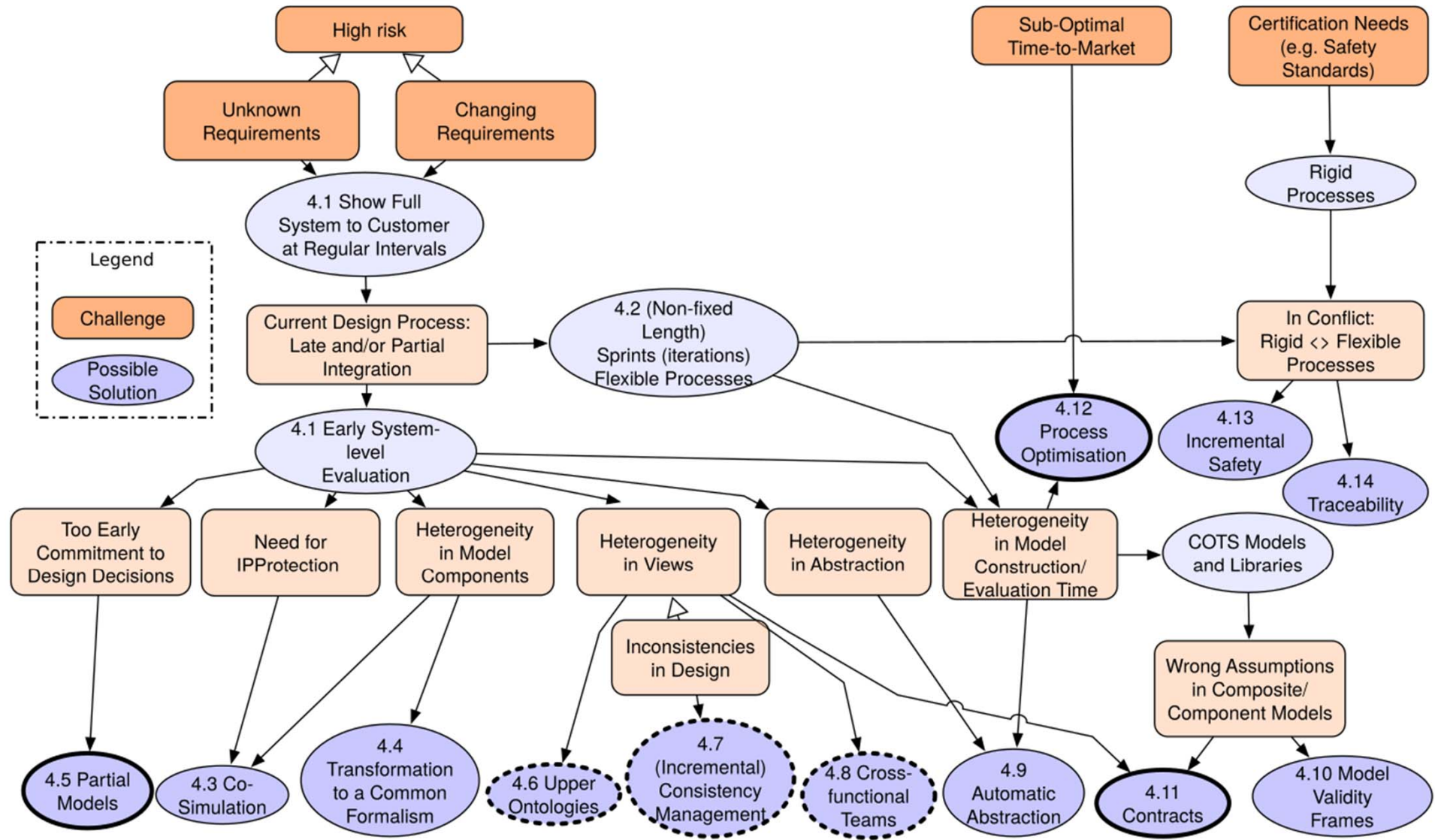University of Toronto & University of Waterloo

Chris Paredis
Georgia Tech

Hans Vangheluwe
University of Antwerp/Flanders Make & McGill University
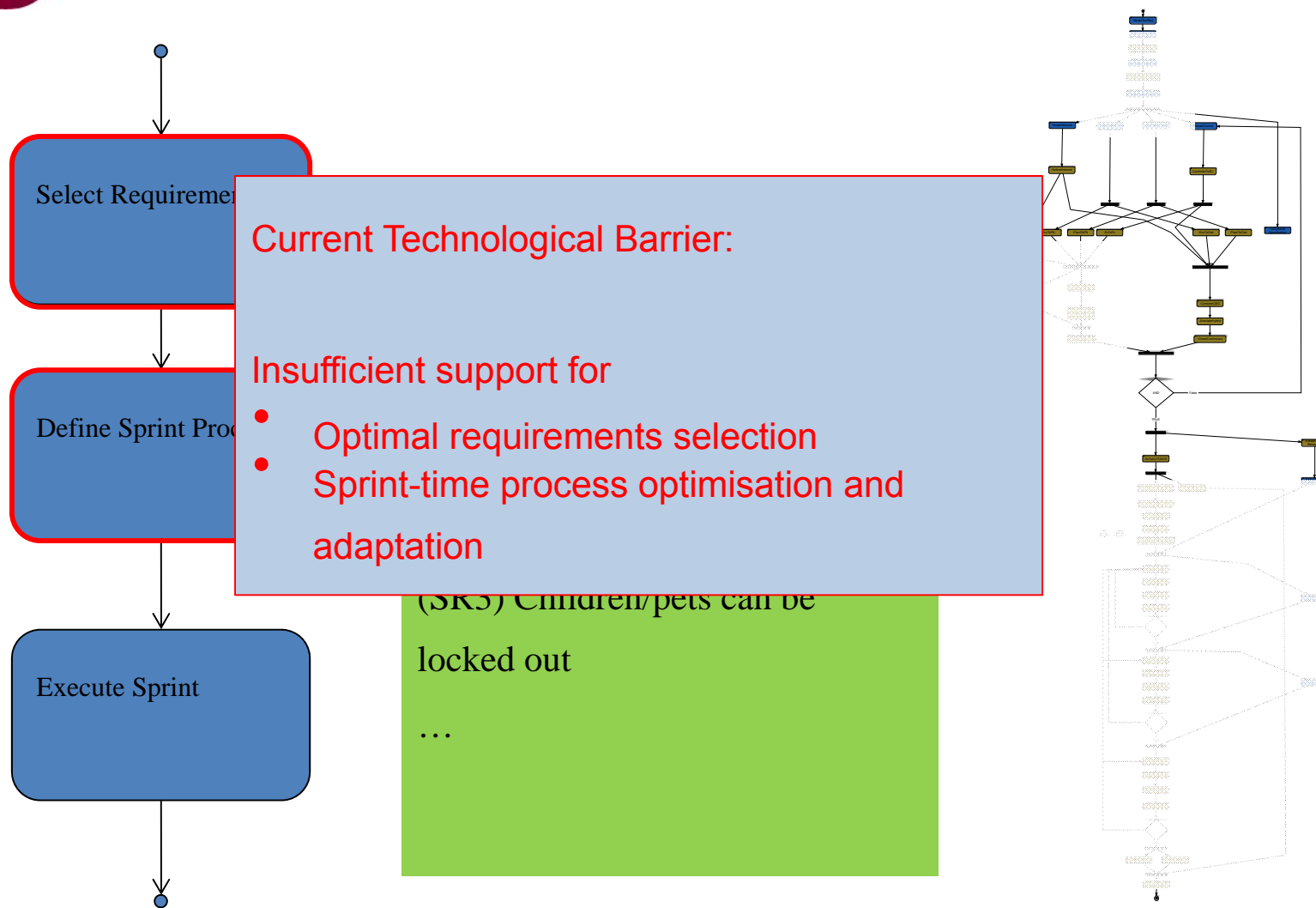
ABSTRACT

Engineering organisations following a traditional development process often suffer from under-specified requirements and from poor responsiveness to changes in those requirements during the course of a project. Furthermore, these organizations need to deliver highly dependable products and decrease time-to-market. In the software engineering community, Agile methods have proposed to address similar issues. Pilot projects that apply agile approaches in Cyber-Physical Systems (CPS) engineering have reported some success. This position paper studies the challenges faced when adopting an agile process to design CPS. These challenges are broken down into their essential components and solutions are proposed, both pertaining to model/simulation management and to processes.

McGill

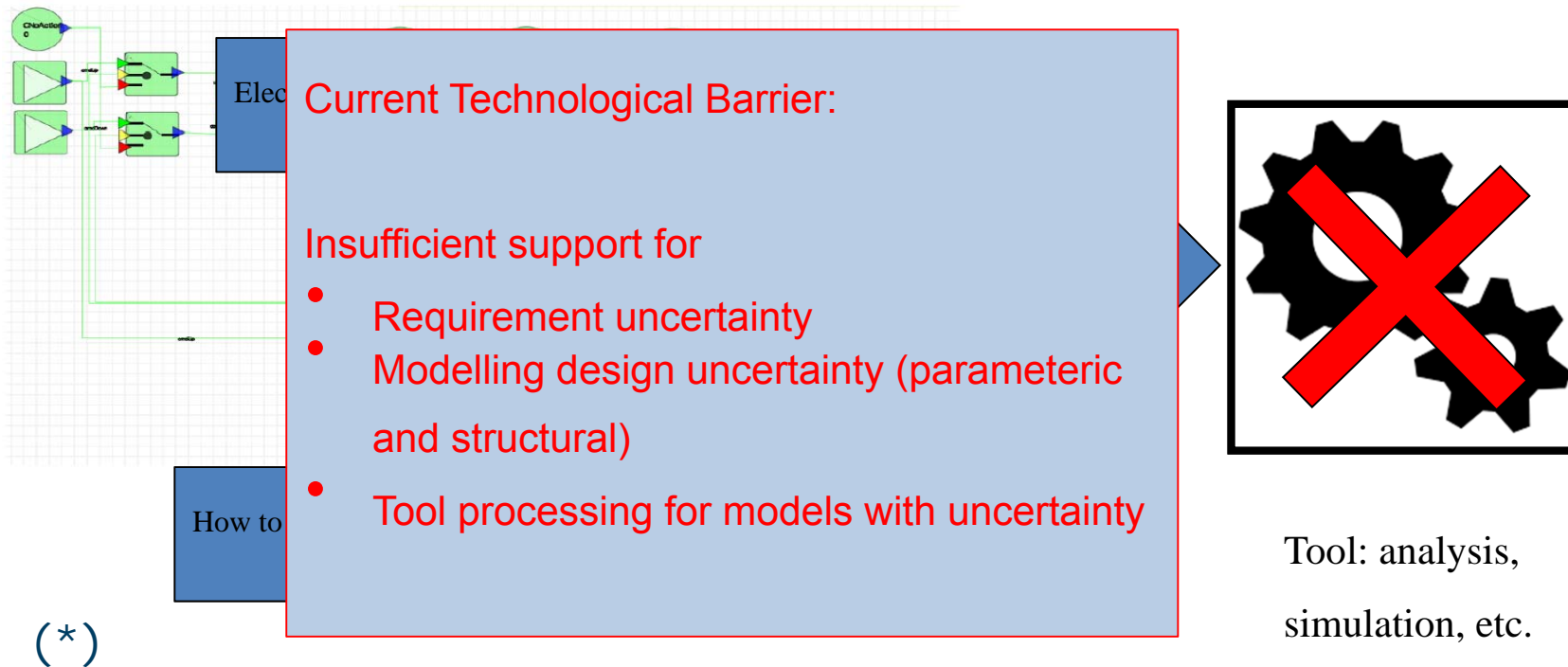# exploring the mapping between industry challenges and technical solutions

Select Requiremen

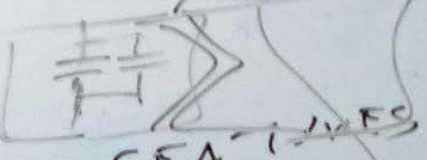Define Sprint Proc

Execute Sprint

Current Technological Barrier:

Insufficient support for
- Optimal requirements selection
- Sprint-time process optimisation and adaptation

(SR3) Children/pets can be locked out

…

Universiteit Antwerpen

McGill

4.5 Modelling Design Uncertainty[(*)]:
partial models
(aka "models with holes")

Elec...

Current Technological Barrier:

Insufficient support for

- **Requirement uncertainty**
- **Modelling design uncertainty (parameteric and structural)**
- **Tool processing for models with uncertainty**

How to...

Tool: analysis, simulation, etc.

[(*)]

deferring decisions, leaving (discrete/continuous) set of options open

Universiteit Antwerpen

McGill

1 SET OF FEATURES
+
PRODUCT FAMILY

CREE

"SAMPLING"
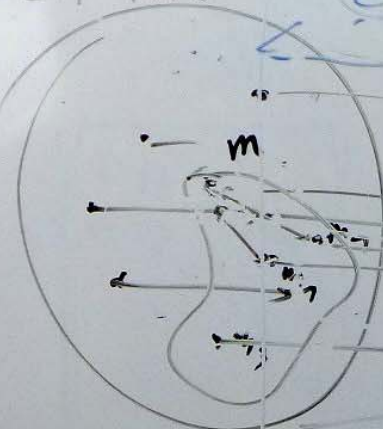
DESIGN ALTERNATIVES

A. DISCRETE.

B. CONT. $\frac{d\vec{x}}{dt} = \frac{f}{p}(\vec{x}, t)$

PDE
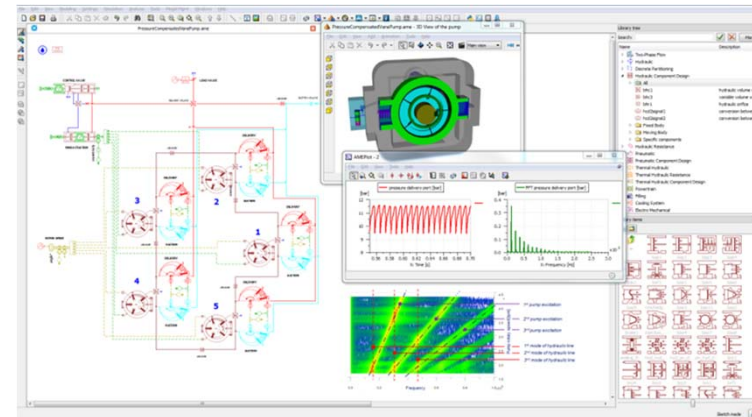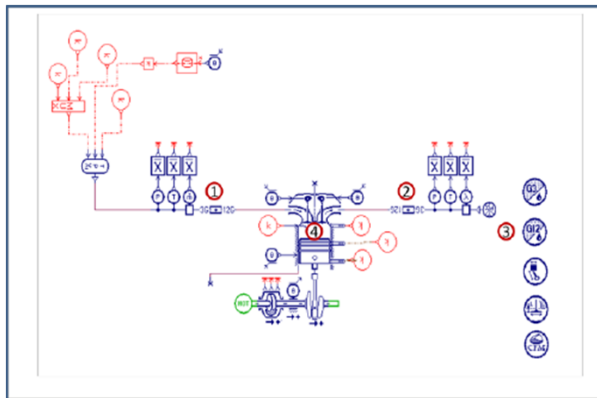
TRSE

MONTE CARLO

PDF

Engine

Engine Control

Trans

Functiona
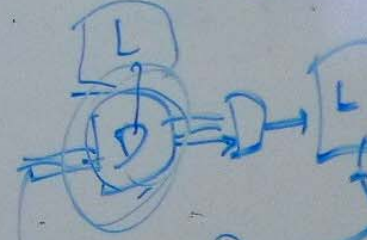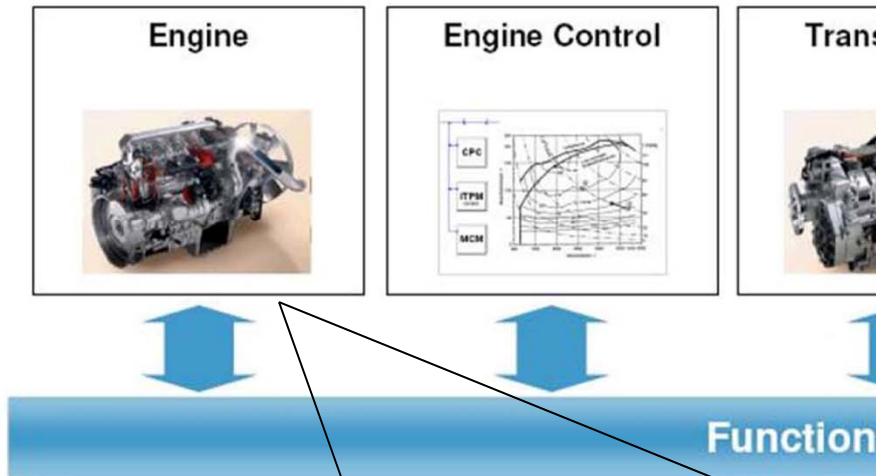
Current Technological Barrier:

Insufficient support for
- Co-sim of heterogeneous models
- Levels of Abstraction
- Correctness

Universiteit Antwerpen

McGill

4.6 ... 4.8 Consistency Management
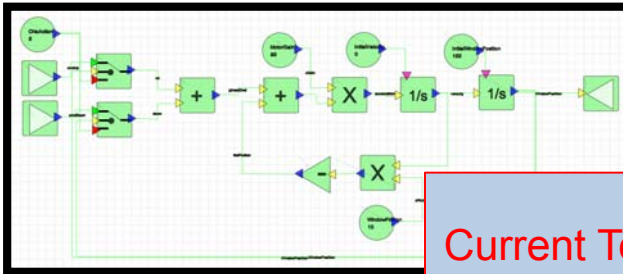
Current Technological Barrier:

Insufficient support for
- Cross-disciplinary teams
- Incremental dependency modelling
- Automated inconsistency detection
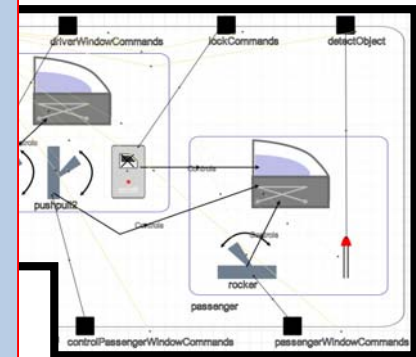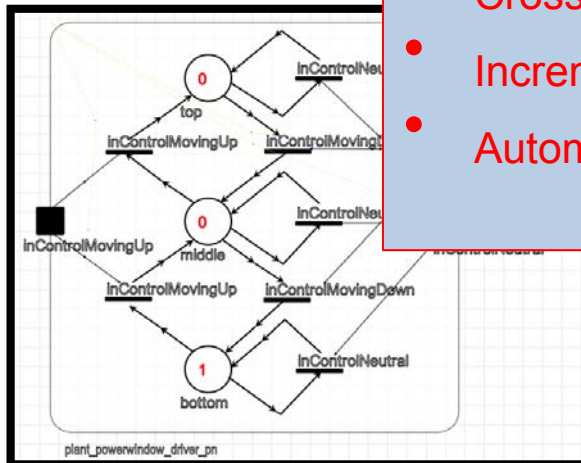
Current Technological Barrier:

Insufficient support for
- Lightweight approach to contracts for agility

is refined by the OEM

is delegated for implementation by a supplier

Universiteit Antwerpen

McGill

Example

Universiteit Antwerpen

McGill
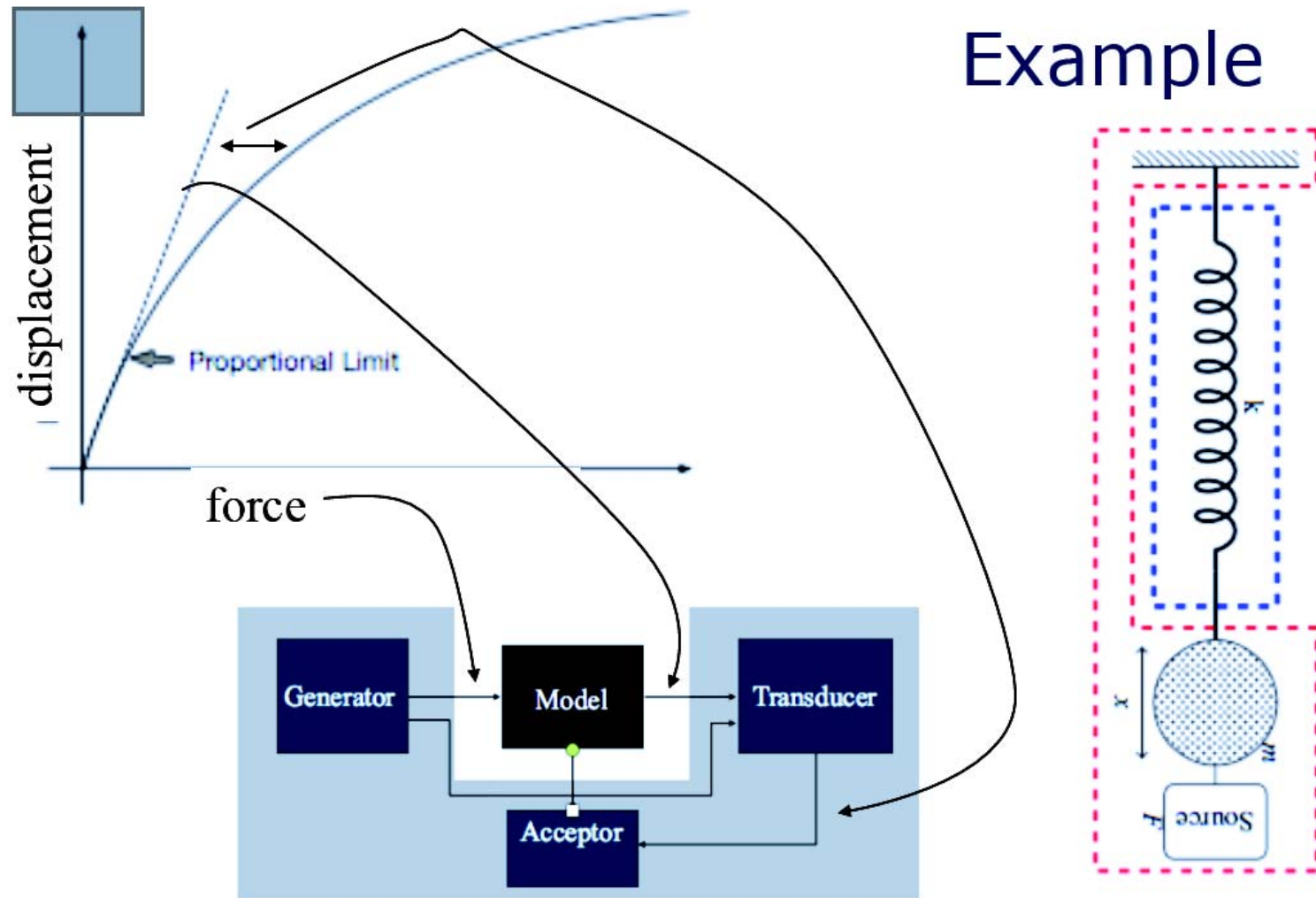
Example Safety

Case

Goal:

...afe

current sprint

Goal SR1
pinch pas...

Can lock
...n/pets

...

Current Technological Barrier:

Insufficient support for
- **Determining change impact on safety case**
- **Evidence management**

Simulation results

Model checking discrete controller

Test results from submerging prototype

Also need evidence that previous evidence is still valid

Universiteit Antwerpen

McGill
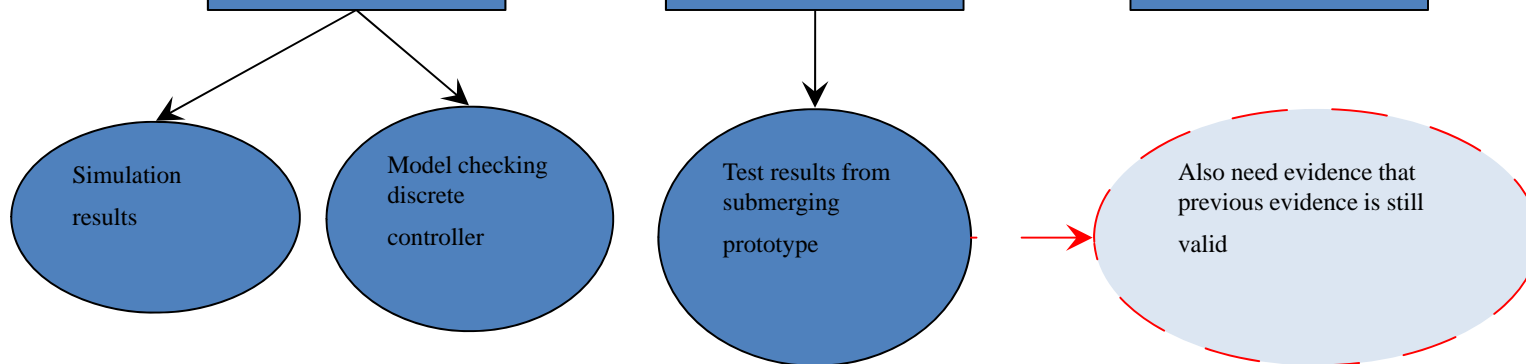
4.13 Incremental Safety
(caring about scale-ability)

Select Requirements

Functional Reqs (via Bus.analysis)

Safety Reqs (via Hazard analysis)

Define Sprint Process

Incrementally updated

Execute Sprint

System artifacts (e.g. models)

Safety Case

Universiteit Antwerpen

McGill

Legend
- Challenge
- Possible Solution

High risk

Unknown Requirements → Changing Requirements → High risk

Sub-Optimal Time-to-Market

Certification Needs (e.g. Safety Standards)

4.1 Show Full System to Customer at Regular Intervals

Rigid Processes

Current Design Process: Late and/or Partial Integration

4.2 (Non-fixed Length) Sprints (iterations) Flexible Processes

In Conflict: Rigid <> Flexible Processes

4.12 Process Optimisation

4.13 Incremental Safety

4.1 Early System-level Evaluation

4.14 Traceability

Too Early Commitment to Design Decisions

Need for IPProtection

Heterogeneity in Model Components

Heterogeneity in Views

Heterogeneity in Abstraction

Heterogeneity in Model Construction/ Evaluation Time

COTS Models and Libraries

Inconsistencies in Design

Wrong Assumptions in Composite/ Component Models

4.5 Partial Models

4.3 Co-Simulation

4.4 Transformation to a Common Formalism

4.6 Upper Ontologies

4.7 (Incremental) Consistency Management

4.8 Cross-functional Teams

4.9 Automatic Abstraction

4.11 Contracts

4.10 Model Validity Frames

McGill