Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors

Friederike Bruns[1], Francesco Tosoni[2],
Sven Mehlhop[3], **Andreas Rauh**[1],
Franco Fummi[2], Frank Oppenheimer[3]

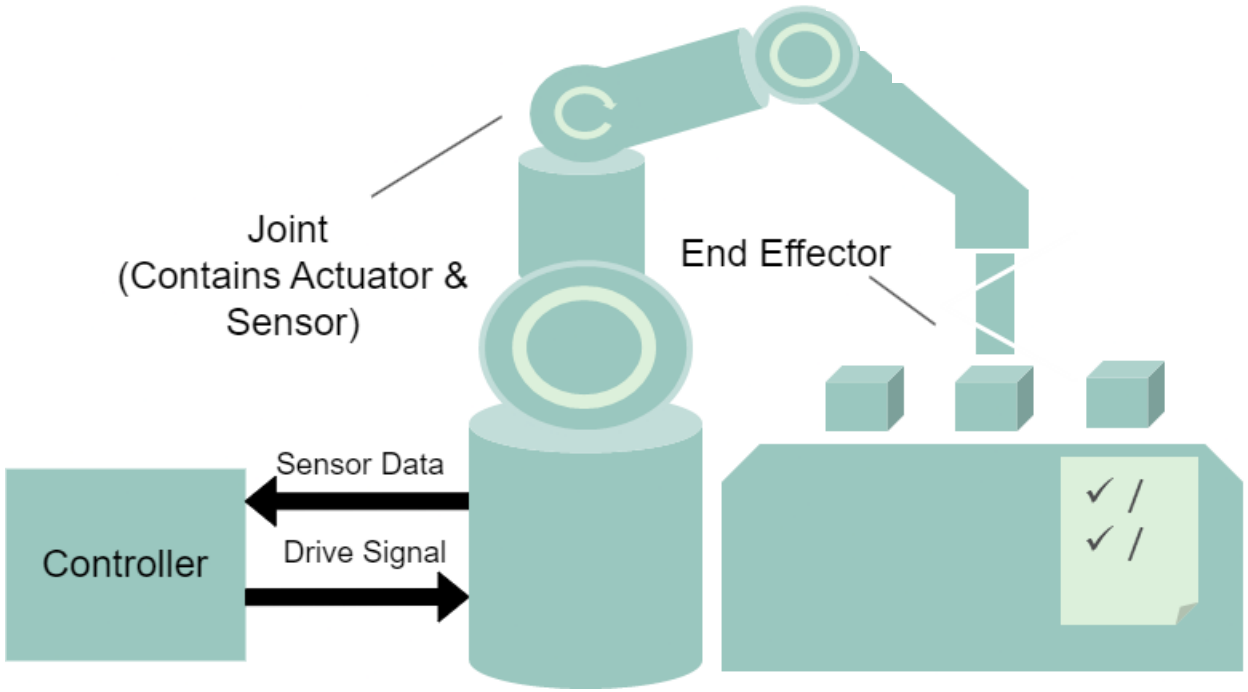
[1]DCIS University of Oldenburg, [2]DIMI University of Verona, [3]Manufacturing OFFIS e.V.

ROBEX Seminar at ENSTA Bretagne, Brest, France, Oct. 30, 2024

originally presented at the IEEE Intl. Conference on Emerging Technologies and Factory Automation (ETFA), Padova, Italy, 2024

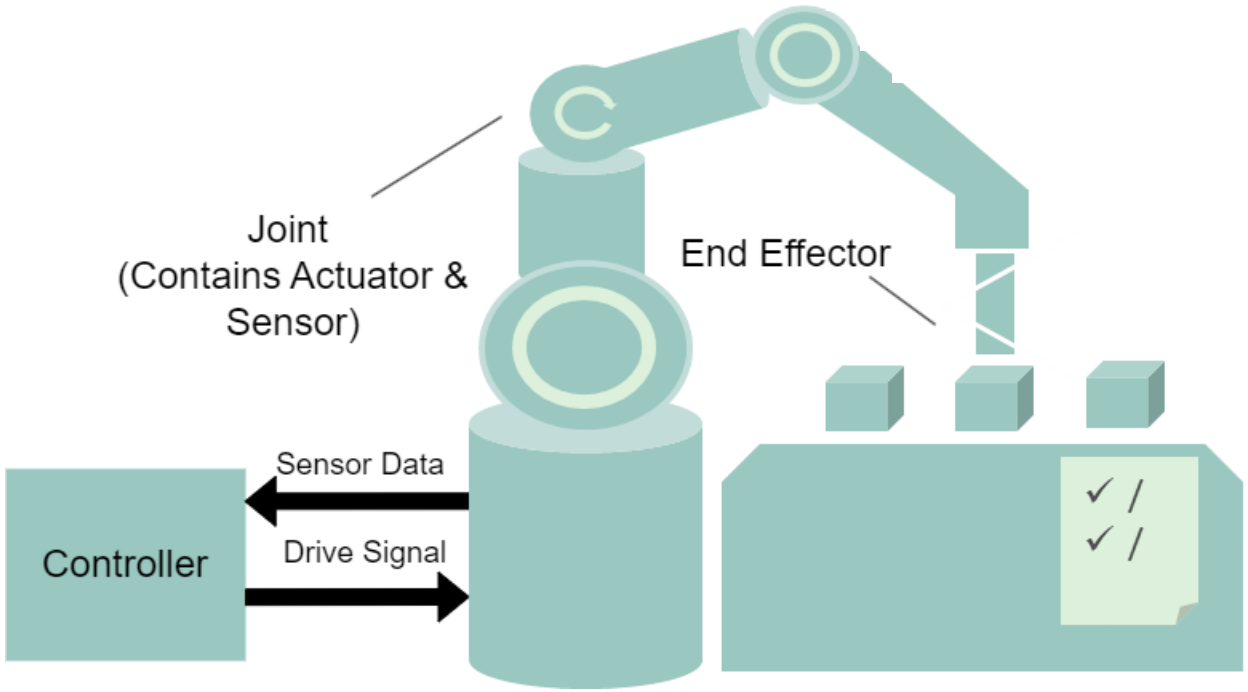
Carl von Ossietzky Universität Oldenburg

Motivation



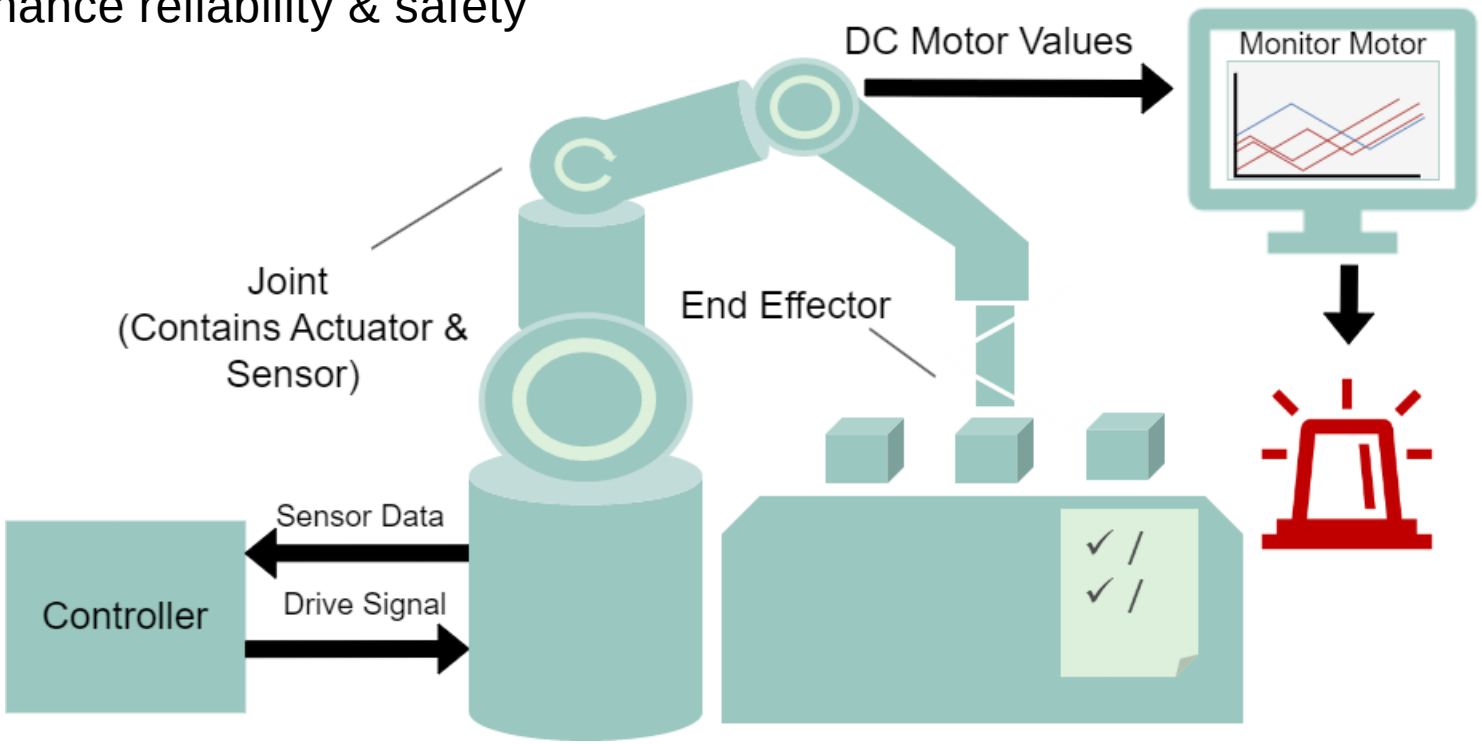
Motivation

- Faults can have significant impact on the overall production plant



Motivation

- Faults can have significant impact on the overall production plant
  - ➢ Fault Detection and Isolation (FDI) processes to avoid severe damage
  - ➢ Enhance reliability & safety



Carl von Ossietzky
Universität
Oldenburg

Key Aspects

- Early fault detection through simulation, fault injection and contract-based monitoring
- Combine the following concepts:

Carl von Ossietzky
Universität
Oldenburg

Key Aspects

- Early fault detection through simulation, fault injection and contract-based monitoring
- Combine the following concepts:
  - **Contract-based monitoring** to distinguish between desired and faulty behavior

Carl von Ossietzky
Universität
Oldenburg

Key Aspects

- Early fault detection through simulation, fault injection and contract-based monitoring
- Combine the following concepts:
  - **Contract-based monitoring** to distinguish between desired and faulty behavior
  - Map **FDI rules based on threshold verification** on contracts that can be evaluated in a co-simulation environment

Carl von Ossietzky Universität Oldenburg

OFFIS

Key Aspects

- Early fault detection through simulation, fault injection and contract-based monitoring
- Combine the following concepts:
  - **Contract-based monitoring** to distinguish between desired and faulty behavior
  - Map **FDI rules based on threshold verification** on contracts that can be evaluated in a co-simulation environment
  - A simulation-based **fault injection** procedure highlighting the principles of contract-based FDI rules

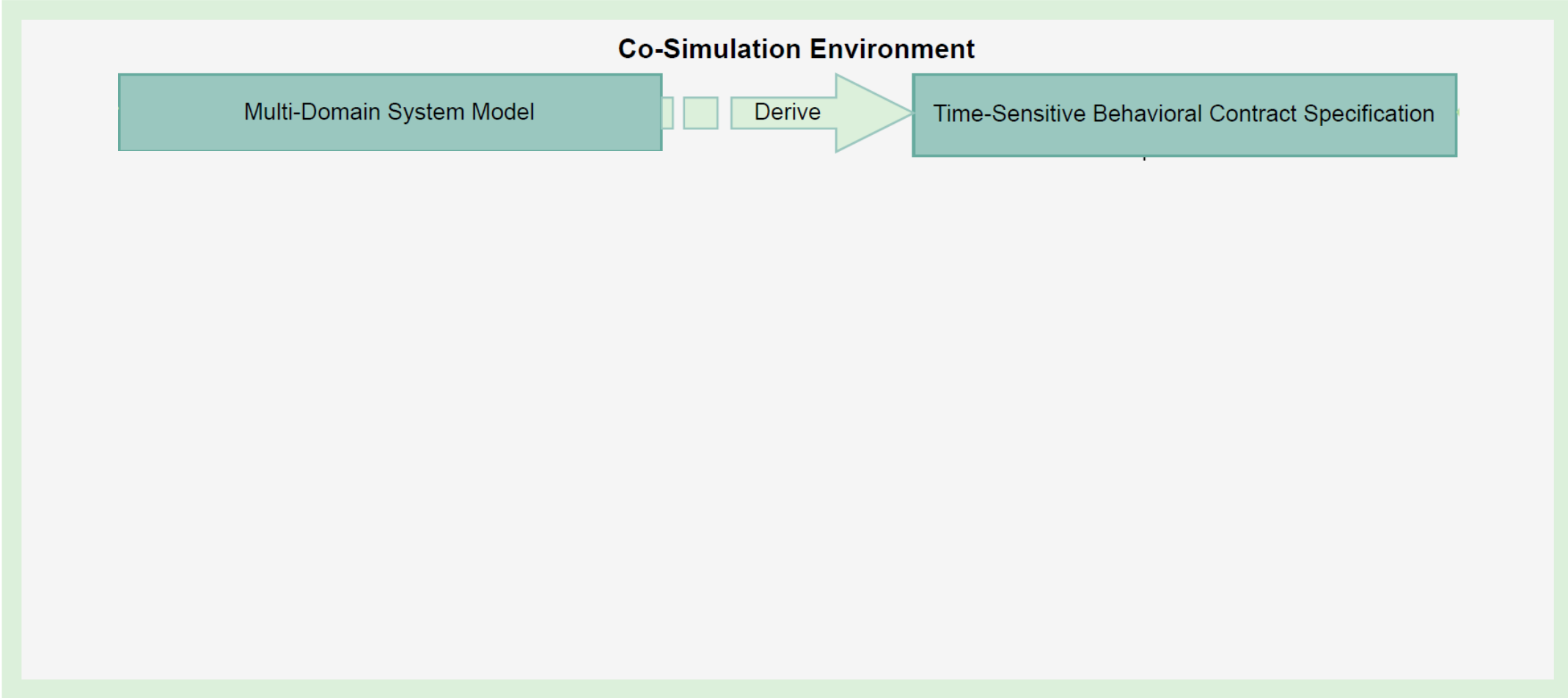
Carl von Ossietzky
Universität
Oldenburg

Key Aspects

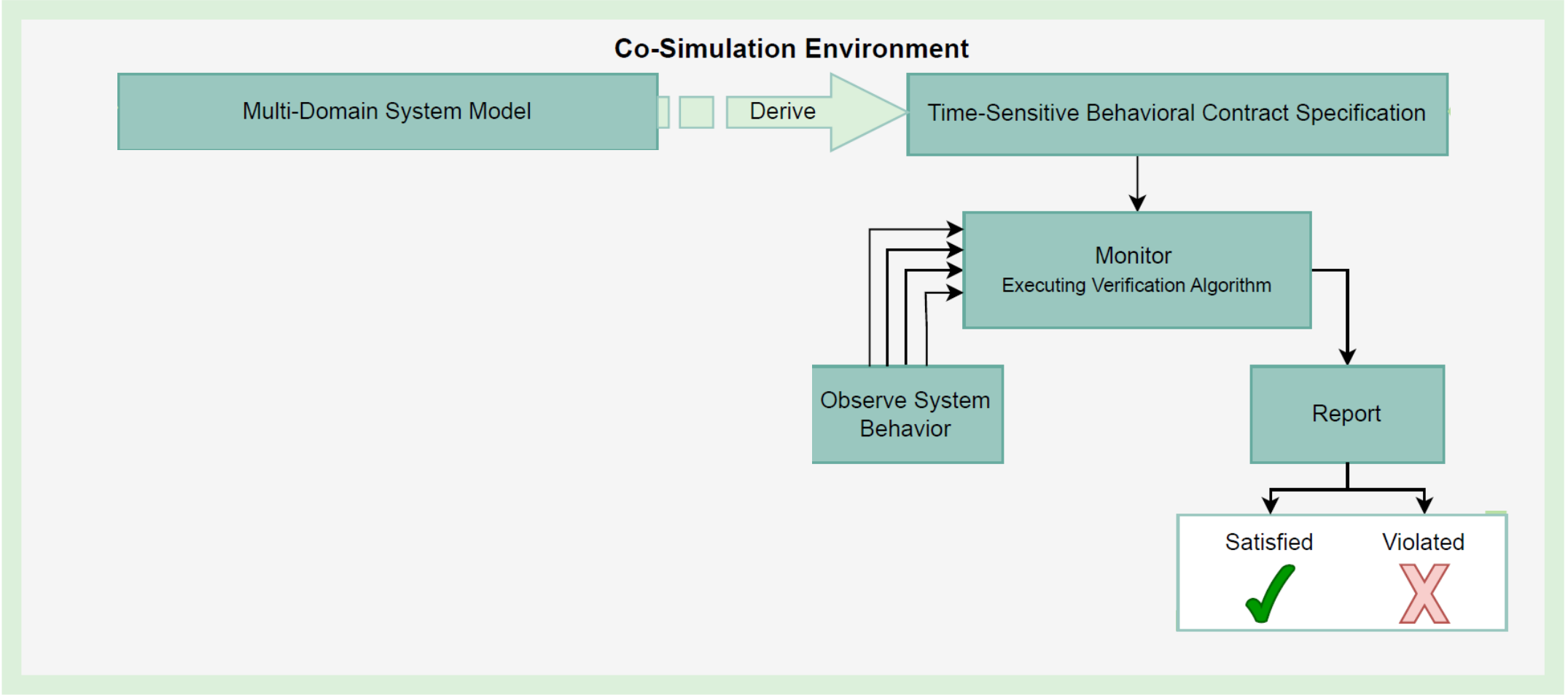
- Early fault detection through simulation, fault injection and contract-based monitoring
- Combine the following concepts:
  - **Contract-based monitoring** to distinguish between desired and faulty behavior
  - Map **FDI rules based on threshold verification** on contracts that can be evaluated in a co-simulation environment
  - A simulation-based **fault injection** procedure highlighting the principles of contract-based FDI rules
  - A **simulation of hardware monitors** based on time-sensitive behavioral contracts to detect faults, validating the applicability for use during system operation

Enhancing Multi-Fault Detection with Contract-Based Co-Simulation

Enhancing Multi-Fault Detection with Contract-Based Co-Simulation

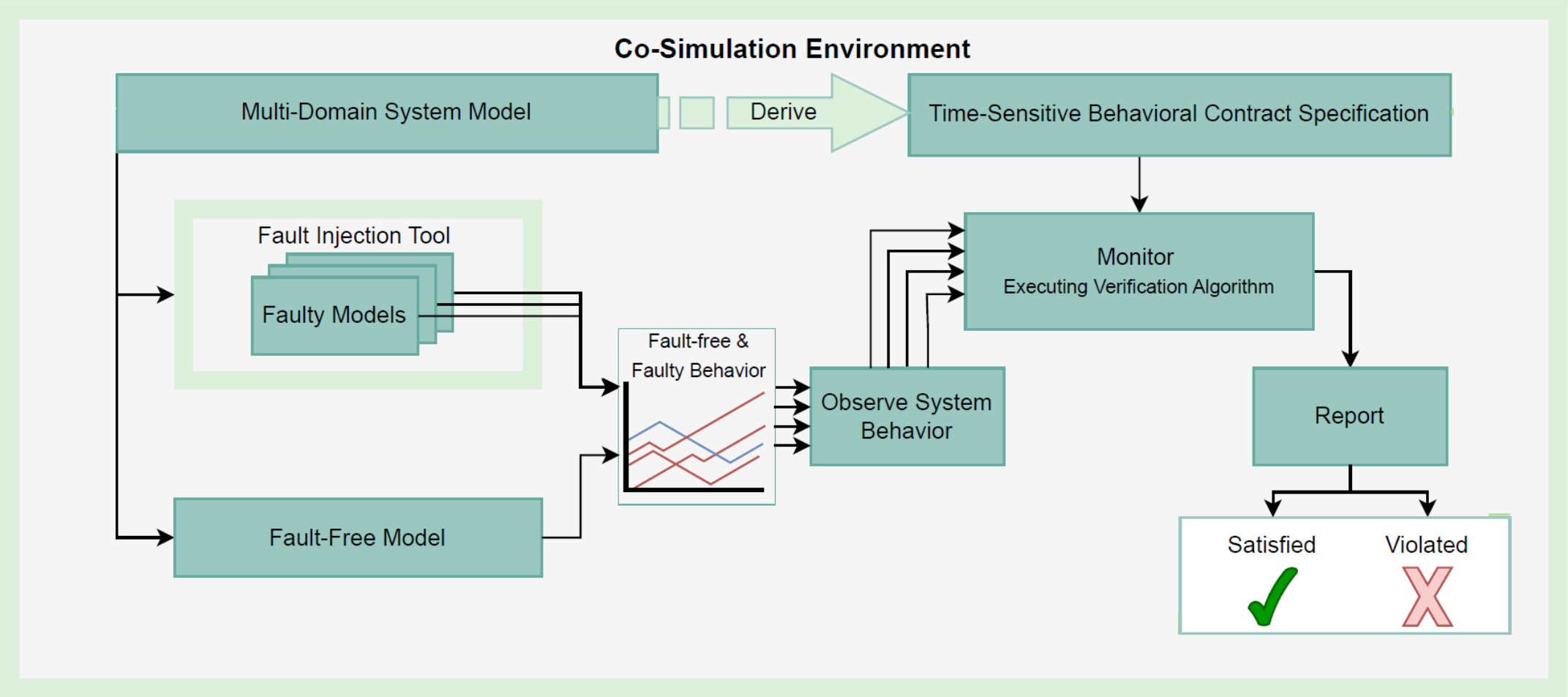


Enhancing Multi-Fault Detection with Contract-Based Co-Simulation



Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors
Friederike Bruns, Francesco Tosoni, Sven Mehlhop, Andreas Rauh, Franco Fummi and Frank Oppenheimer

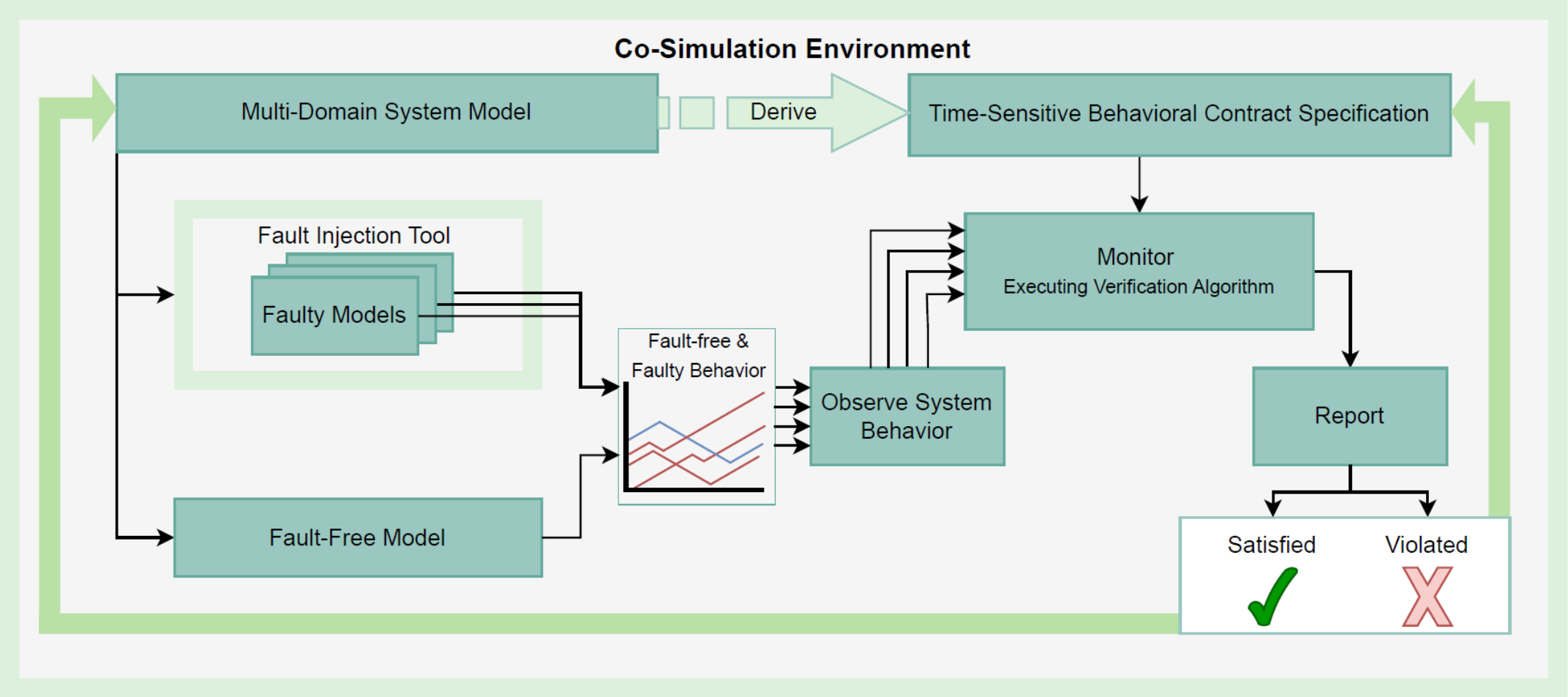
Enhancing Multi-Fault Detection with Contract-Based Co-Simulation



Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors

Friederike Bruns, Francesco Tosoni, Sven Mehlhop, Andreas Rauh, Franco Fummi and Frank Oppenheimer

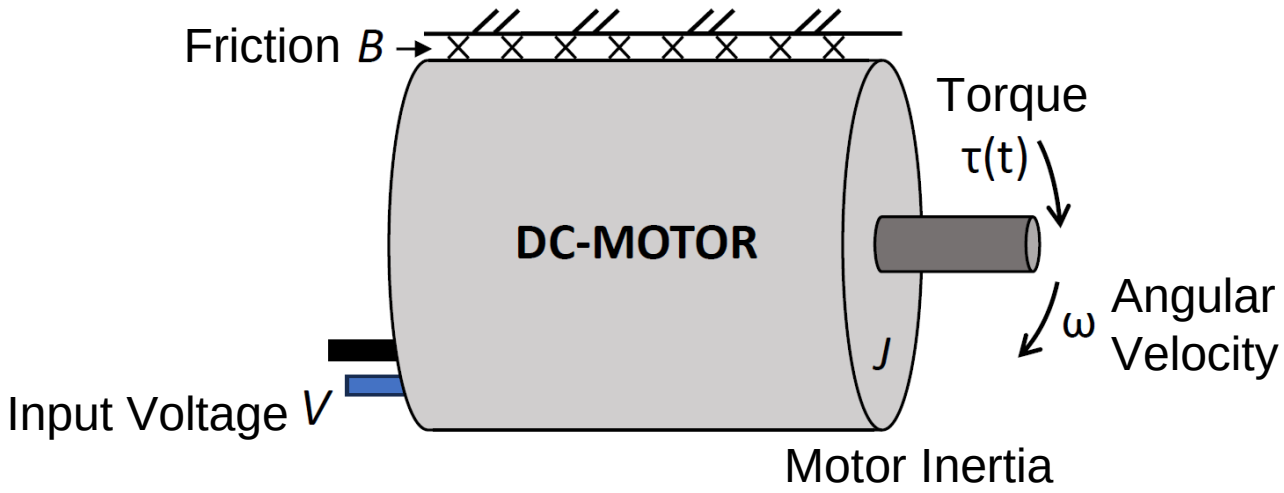
Enhancing Multi-Fault Detection with Contract-Based Co-Simulation



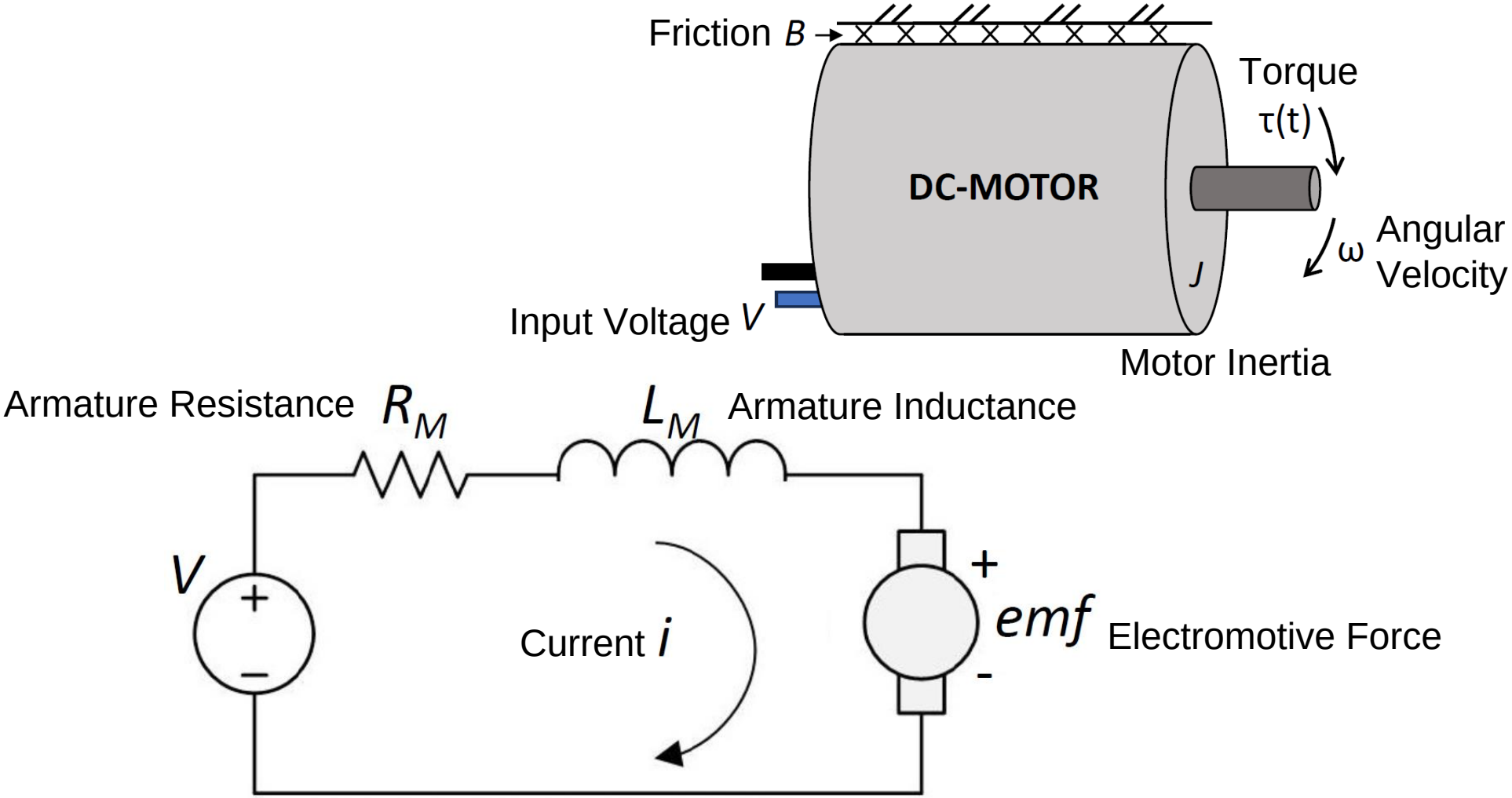
Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors

Friederike Bruns, Francesco Tosoni, Sven Mehlhop, Andreas Rauh, Franco Fummi and Frank Oppenheimer

Use Case Study: Physical Model of a DC Motor



Use Case Study: Physical Model of a DC Motor

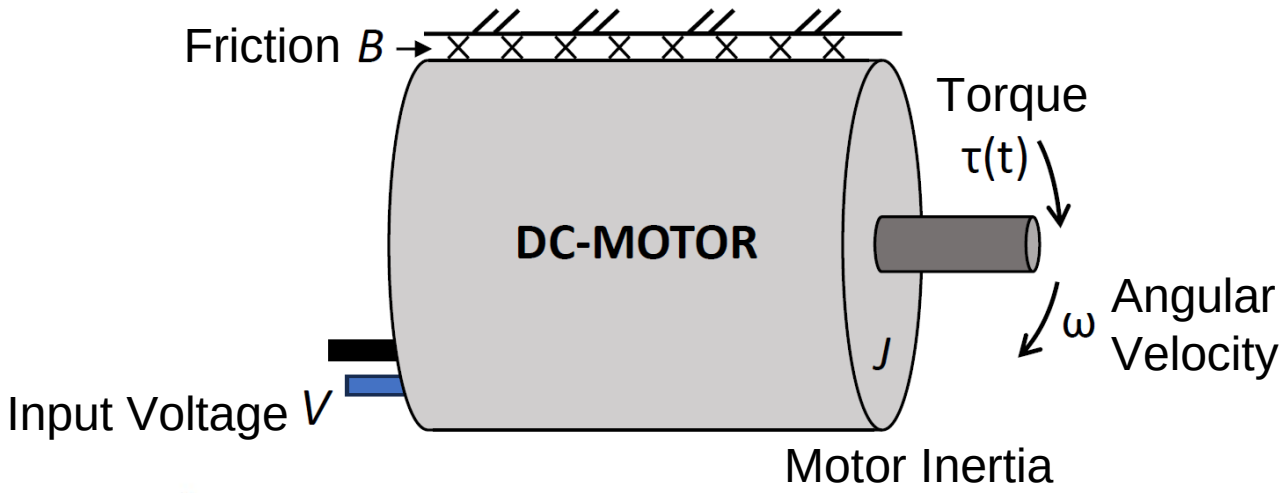


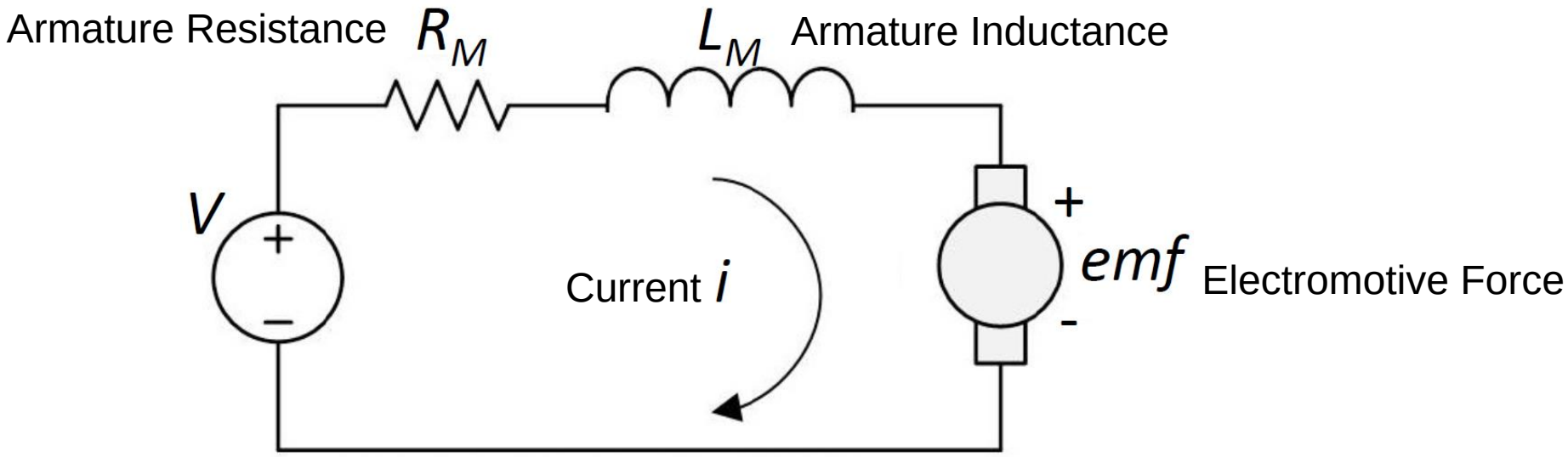
Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors
Friederike Bruns, Francesco Tosoni, Sven Mehlhop, Andreas Rauh, Franco Fummi and Frank Oppenheimer

Use Case Study: Physical Model of a DC Motor

Generate rotation of the shaft:

$$V = K_E \cdot \omega + R_M \cdot i + L_M \cdot \frac{di}{dt}$$





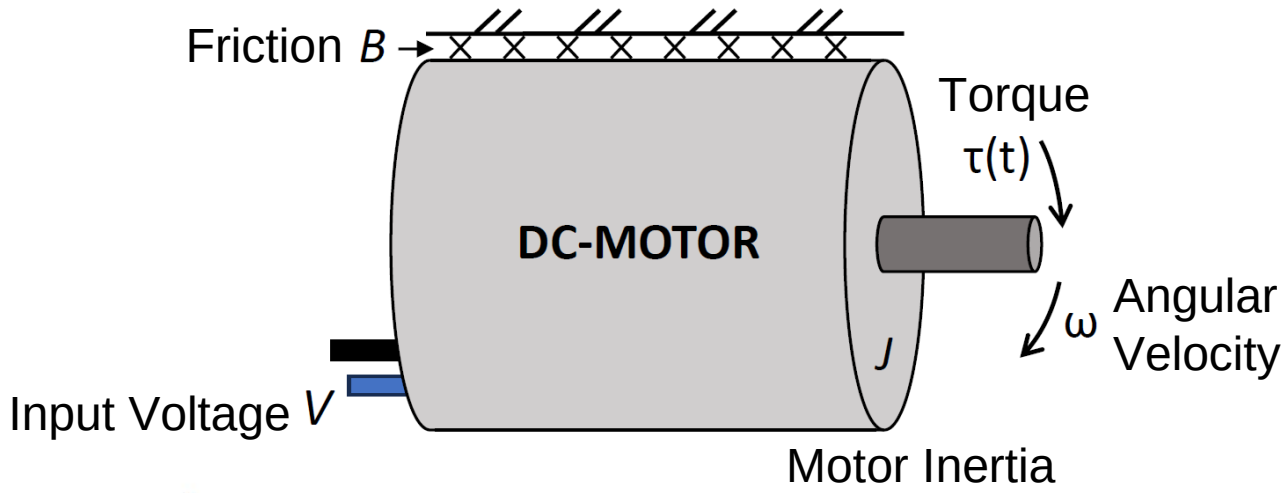
Use Case Study: Physical Model of a DC Motor

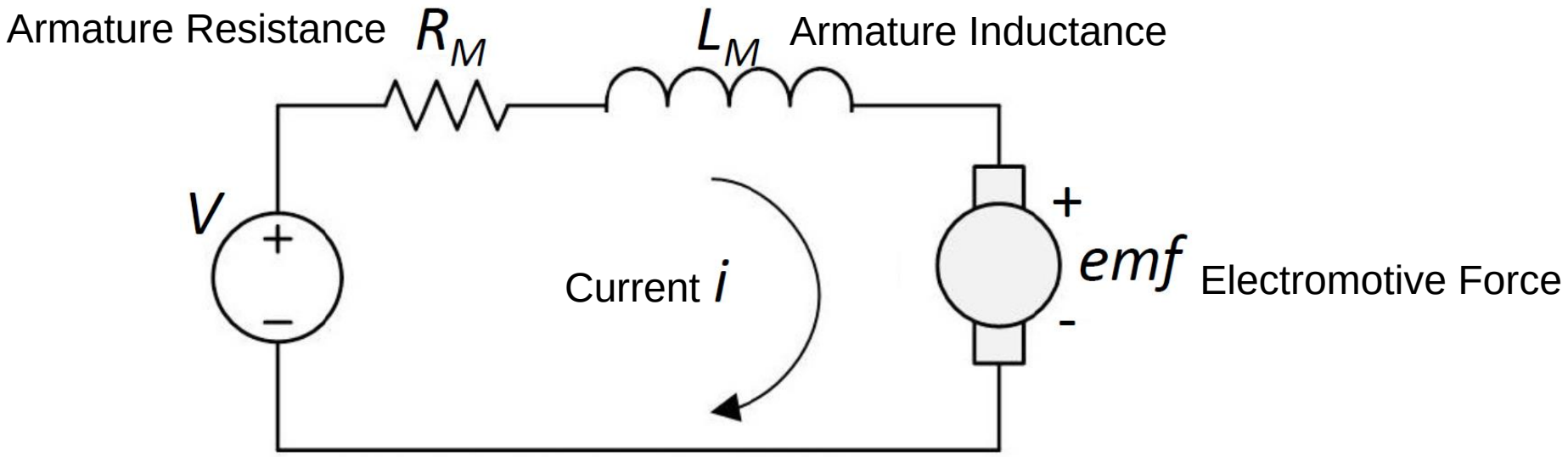
Generate rotation of the shaft:

$$V = K_E \cdot \omega + R_M \cdot i + L_M \cdot \frac{di}{dt}$$

Mechanical load behavior:

$$\tau = K_T \cdot i - B \cdot \omega - J \cdot \frac{d\omega}{dt}$$

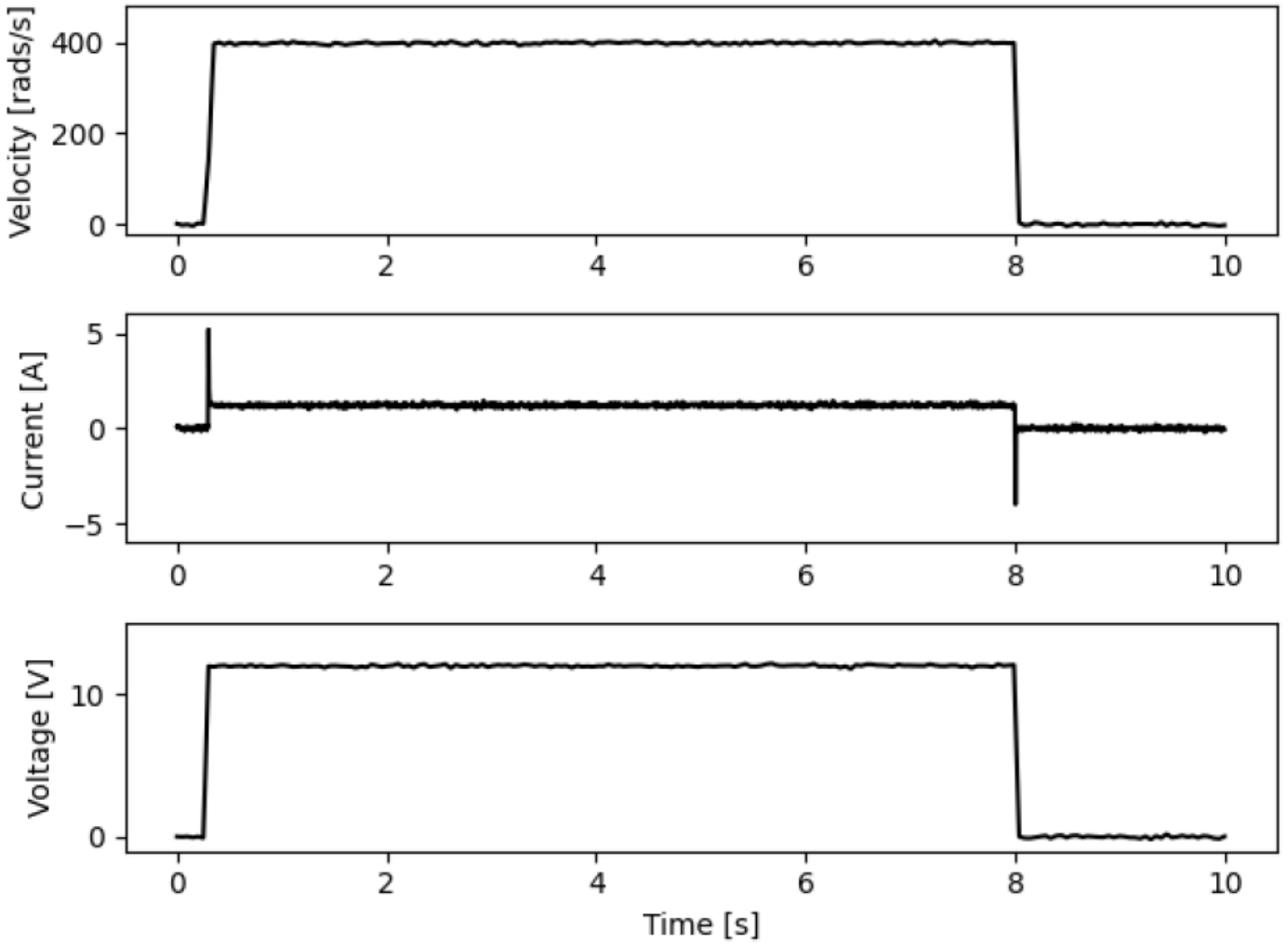




Analyzing Fault Behaviors in Multi-Domain Systems with Contract-Based Monitors
Friederike Bruns, Francesco Tosoni, Sven Mehlhop, Andreas Rauh, Franco Fummi and Frank Oppenheimer

Carl von Ossietzky
Universität
Oldenburg

Nominal Behavior of the DC Motor



Carl von Ossietzky Universität Oldenburg

Contract-Based Monitoring & Fault Injection

- Time-Sensitive Behavioral Contracts (TSBCs)
  - Assumption: Time point is within a specific interval
  - Guarantee: Corresponding data value is within specified interval

$$C_i : t \in [t_1; t_2] \; ? \; d \in [d_1; d_2]$$

Contract-Based Monitoring & Fault Injection

- Time-Sensitive Behavioral Contracts (TSBCs)
  - Assumption: Time point is within a specific interval
  - Guarantee: Corresponding data value is within specified interval

$$C_i : t \in [t_1; t_2] \; ? \; d \in [d_1; d_2]$$

- Electrical Fault

amount of resistance

```
V(p, n) <+ I(p, n) * open;
```

Contract-Based Monitoring & Fault Injection

- Time-Sensitive Behavioral Contracts (TSBCs)
  - Assumption: Time point is within a specific interval
  - Guarantee: Corresponding data value is within specified interval

$$C_i : t \in [t_1; t_2] \; ? \; d \in [d_1; d_2]$$

- Electrical Fault

amount of resistance

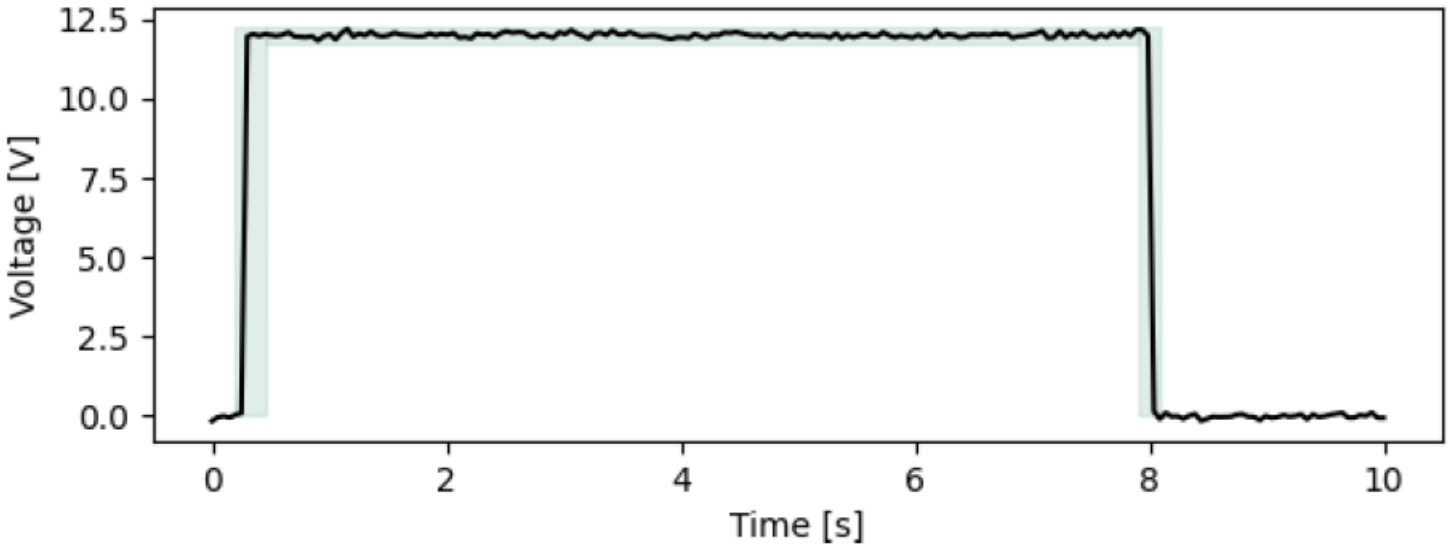
```
V(p, n) <+ I(p, n) * open;
```

- Mechanical Fault

slow down rotation

```
Tau(x, y) <+ Omega(x, y) * damp;
```

Valid Range & Contract Specification for Supply Voltage



White Gaussian noise was added

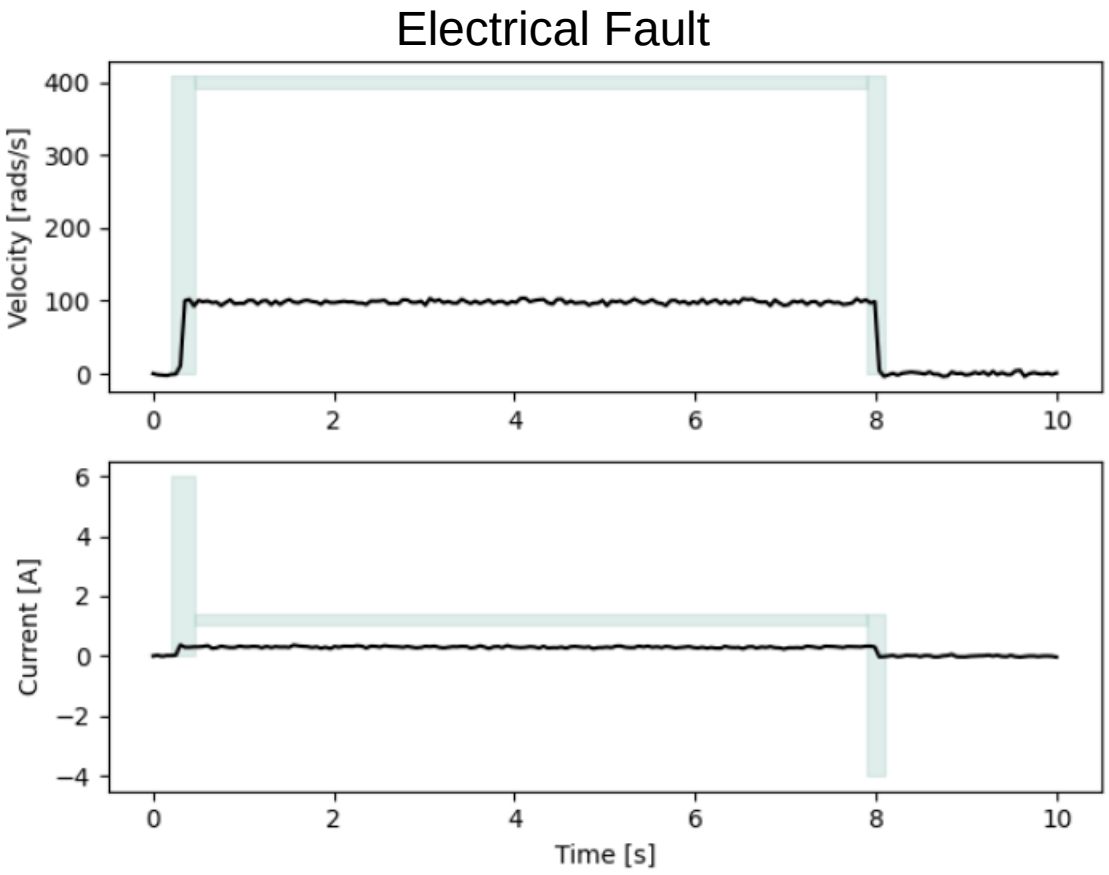
$$Contract\_C_1 : t \in [0.2; 0.45] \ ? \ d \in [0; 12.24]$$

$$Contract\_C_2 : t \in [0.45; 7.9] \ ? \ d \in [11.76; 12.24]$$

$$Contract\_C_3 : t \in [7.9; 8.1] \ ? \ d \in [0; 12.24]$$

$$Contract\_C_4 : t \in [8.1; 10] \ ? \ d = 0$$

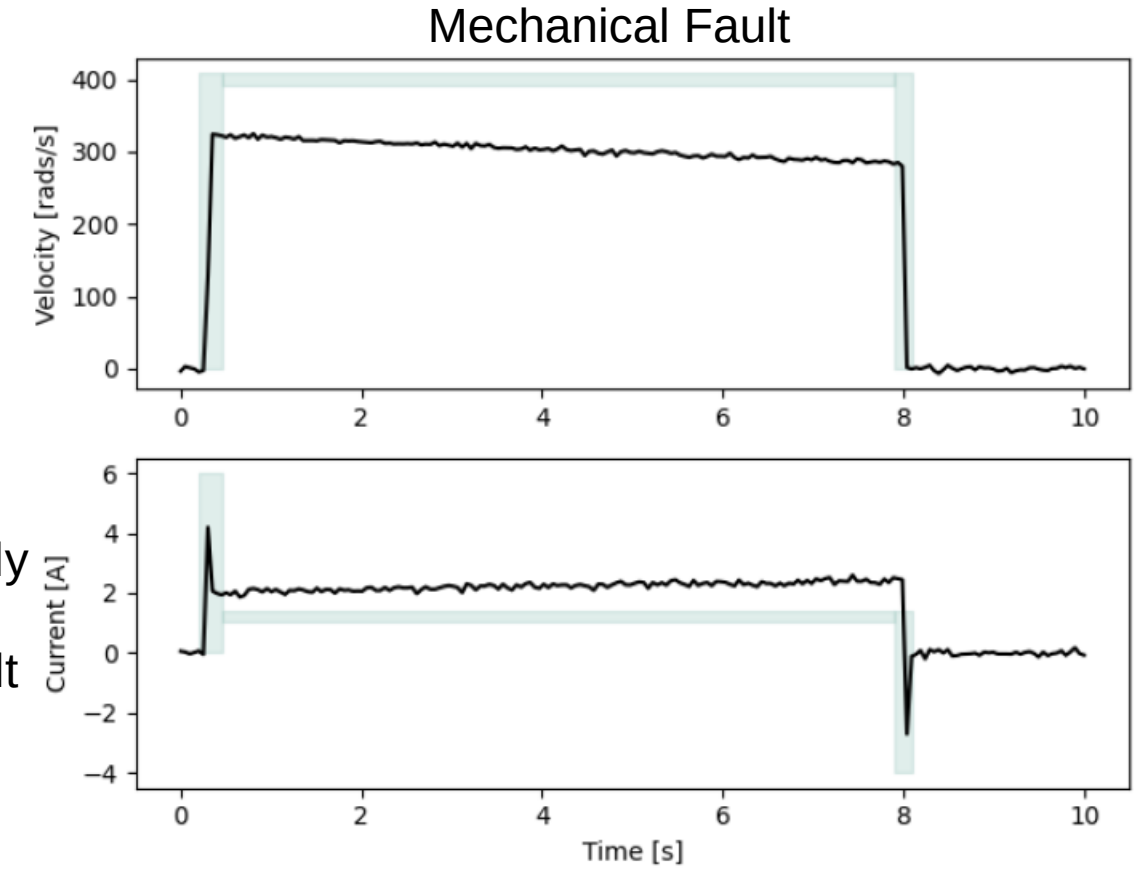
Possible Traces & Contract Violations



- Increased armature resistance
  - ➢ Wear and tear of electrical components
  - ➢ Badly placed connection
  - ➢ External electromagnetic interference
- Always active throughout simulation
  - ➢ Constant wear of the components
- Fault affects the electric current
- Fault affects angular velocity

Possible Traces & Contract Violations

- Additional friction to rotary components
  - ➢ Presence of debris or dust
  - ➢ External agents slowing down the shaft rotation
  - ➢ Deterioration of bearings due to motor aging
- Fault is incremental and increases slightly
  - ➢ Increasingly severe effect of the fault
- Larger braking force than normal friction
- Decreasing the angular velocity



Carl von Ossietzky Universität Oldenburg

Monitoring Results – A Detected Violation

- Recoverable monitors
  - Continue verification in case of being successful in the future
  - Monitors fail once may pass within the same request
- Unrecoverable monitors
  - Halt verification until subsequent request
  - Once violated they remain so for the duration of the current request
  - Suitable for critical fault conditions intolerant of any violations
- Find reason for critical fault and decide
  - Are corrections needed? Improvements to the model or monitors?

Carl von Ossietzky Universität Oldenburg

Monitoring Results – A Detected Violation

- Longer fault simulation
  - Analyze effect of a persistent fault
  - Reveal whether and how system controller mitigates the fault
- Based on severity user decides whether and how to intervene
- Simple change to the configuration: Correcting the input signal
- Changes to the contract specification
  - Relieve intervals and broaden spectrum of allowed values
  - This does not improve reliability – it prevents detection of smaller deviations
- Specify contracts systematically and consider precise requirements and behavior

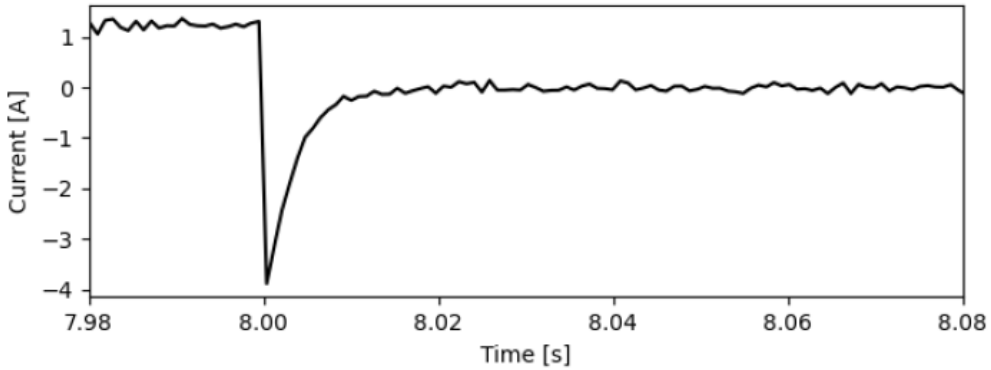
Carl von Ossietzky Universität Oldenburg

Discussion

- A suitable fault detection mechanism that can be tested during the design phase
- Applicable to several systems that contain a physical part
  - Establish system model and its nominal behavior
  - Derive contract specifications
- Motor model could be extended to generate data on other properties (temperature, …)
- Later fault detection requires more resources to rectify faults

Discussion

- Check valid behavior for signals that are not directly measured or measurable
- E.g. Besides pure threshold classifier, use extended specification to consider gradient within a contract
  - ➢ Finer granularity of monitoring
  - ➢ Earlier detection of potential violations
- Specifying more precise progression
  - ➢ TSBCs could do this by adding monitors (overhead)
  - ➢ A solution for this can improve fault detection
- Effect of faults might also be visible in software & extend fault detection to predictive maintenance



Carl von Ossietzky Universität Oldenburg

Summary

- A co-simulation environment that enables
  - ➢ Systematic approach for fault detection
  - ➢ Testing the behavior of a system under faulty conditions
  - ➢ Detect different faults through the use of TSBC monitors
- Faults are directly injected into the differential equations
- Reporting on the valid or invalid behavior of the system
- TSBC-based monitor specifications can be improved based on the provided results
- Monitors could be derived for application at run-time
- Extending the framework by a component for the control software