Challenges and Opportunities in Design and Operation of Intelligent Cyber-Physical Systems

Invited Talk, 19th International Conference on Runtime Verification (RV)
Part of the 3rd World Congress on Formal Methods
Porto, Portugal. October 10, 2019

Akshay Rajhans, PhD
arajhans@mathworks.com
https://arajhans.github.io

Talk outline

- ➢ Cyber-physical systems: a feature classification
- “Runtime” verification at design time: simulation as a proxy for run time
- Runtime analysis at operation time: From CPS to IoT and Digital Twins
- Challenges and future outlook

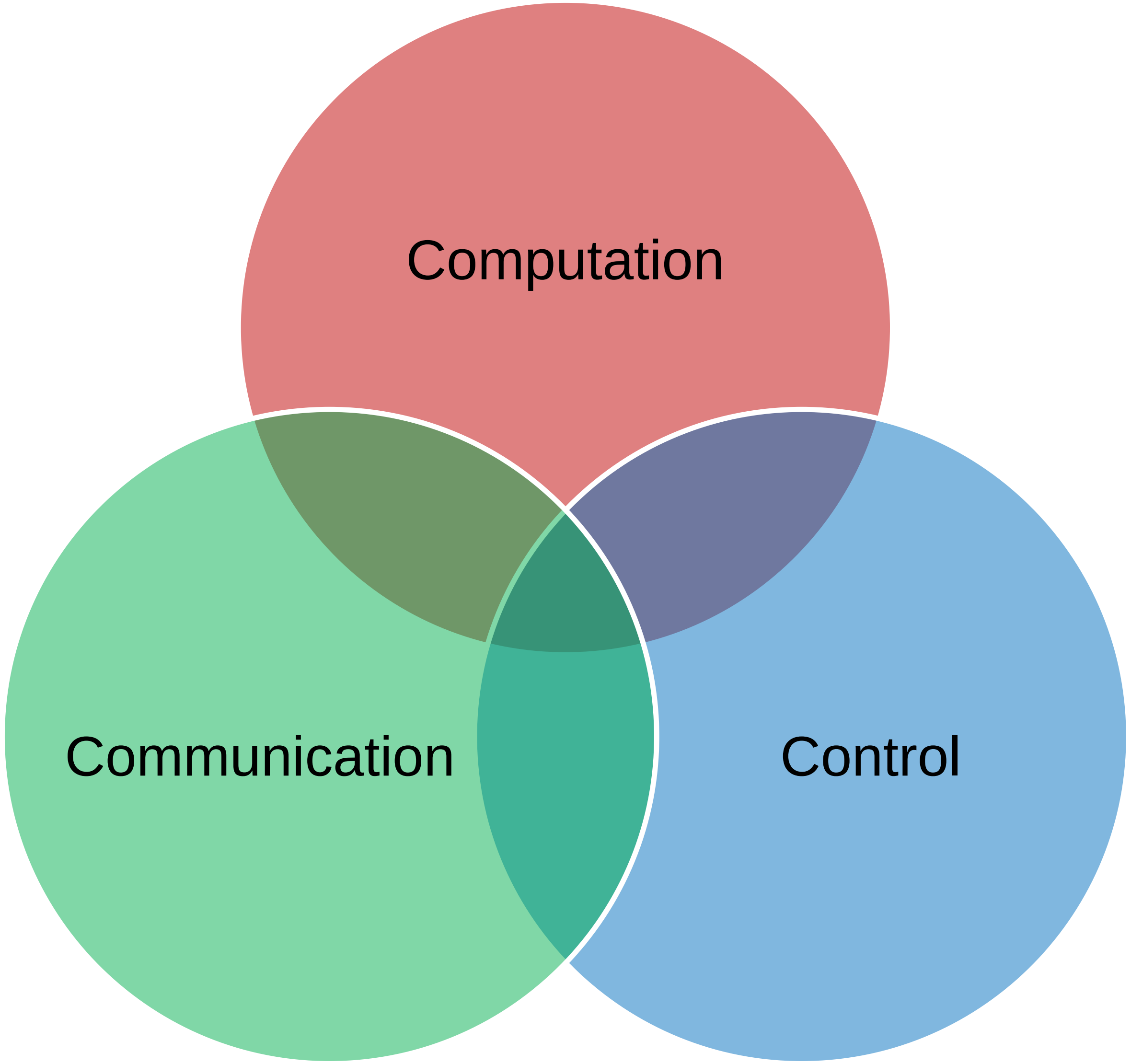
Cyber-physical systems: umbrella term, not a precise definition

“The term cyber-physical systems (CPS) refers to a new generation of systems with *integrated computational and physical* capabilities that can *interact with humans* through many new modalities.

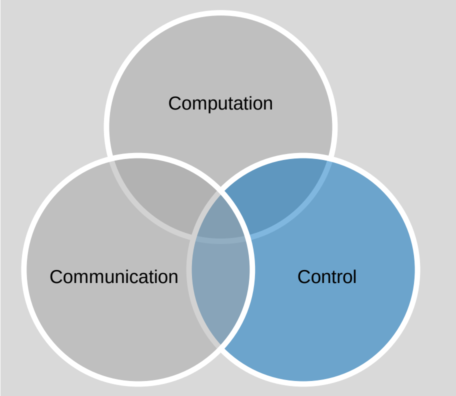
The ability to interact with, and expand the capabilities of, the physical world through *computation*, *communication*, and *control* is a key enabler for future technology developments.”

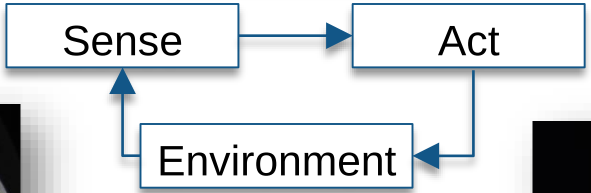
- Helen Gill and Kisan Baheti, NSF

IEEE Impact of Control Technology, T. Samad and A.M. Annaswamy (eds.), 2011. Available at www.ieeecss.org.

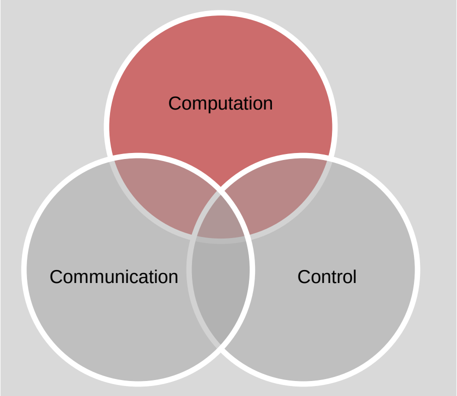


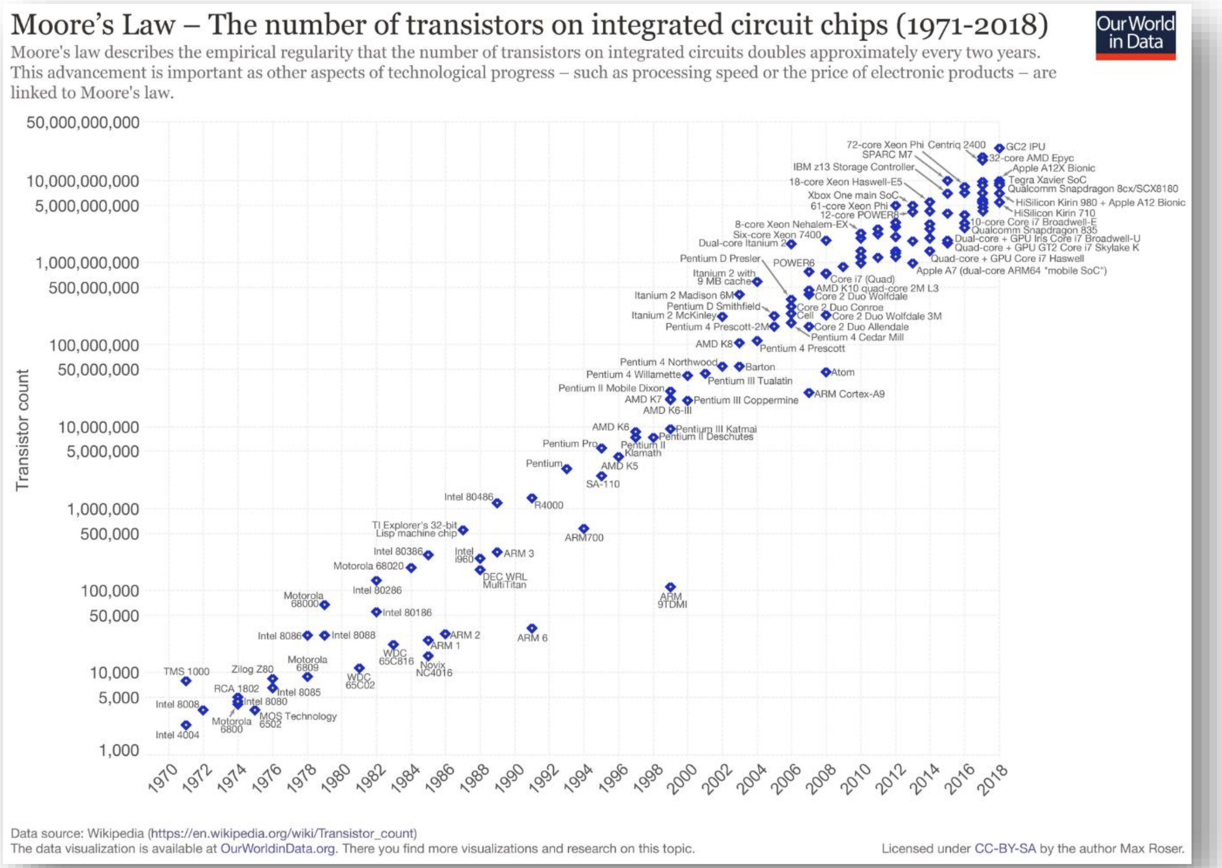
Control – closing the loop over the physical environment





Computation – fueled by Moore's law

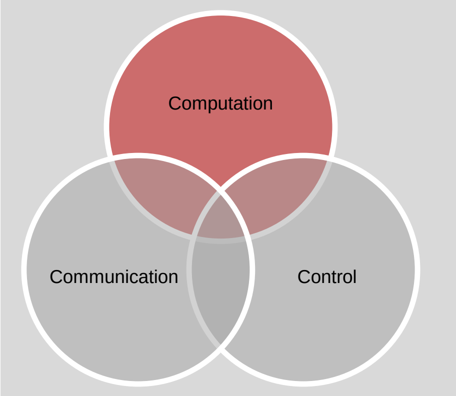




Source: Wikipedia

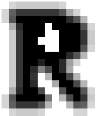
Computation Axis

Computation – fueled by Moore's law



Cost of Printing

Annual Production

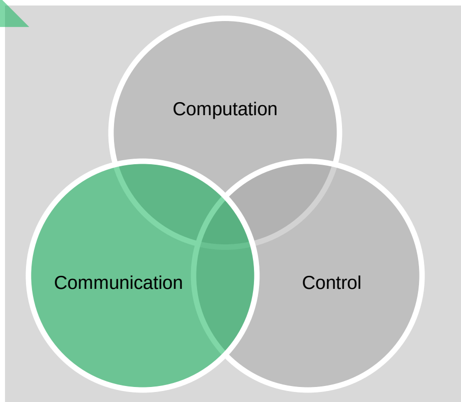
 >  > 

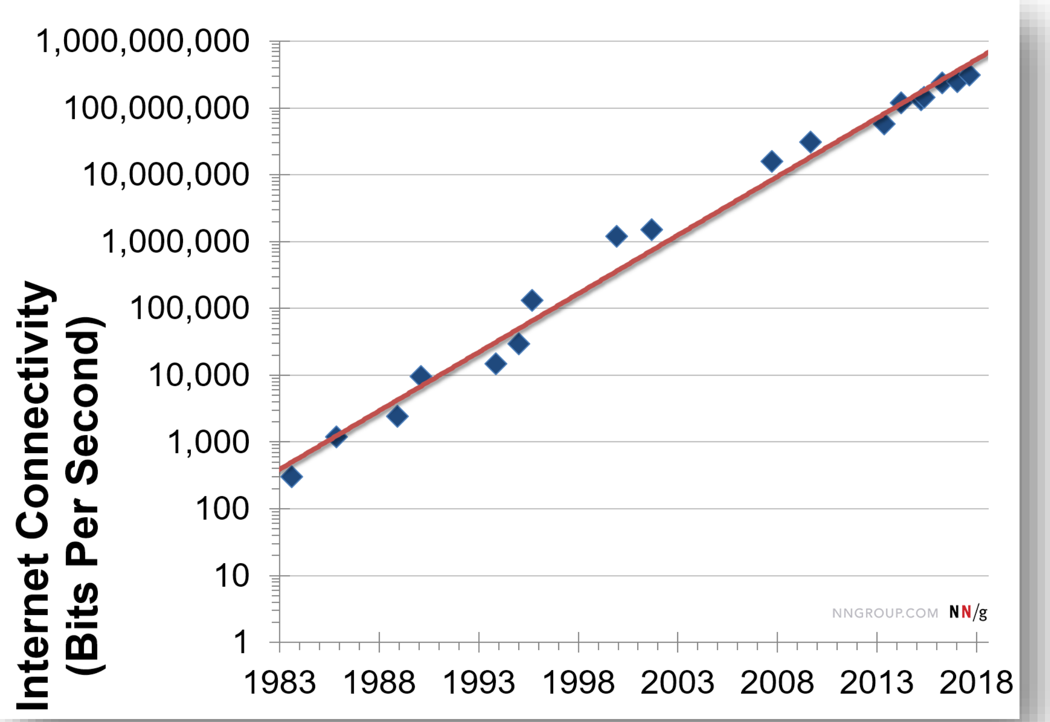
Source: Intel, IEEE

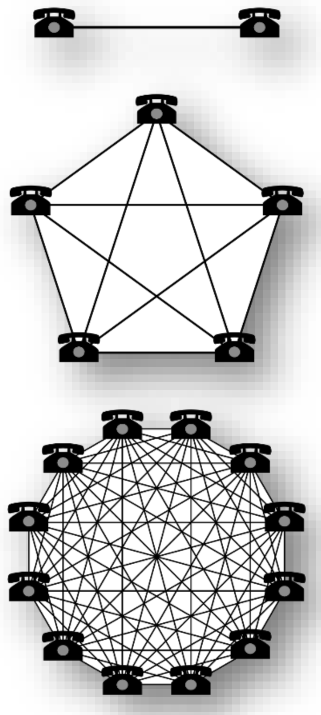
Computation Axis

Communication – Nielsen's law, Metcalfe's law

Communication Axis



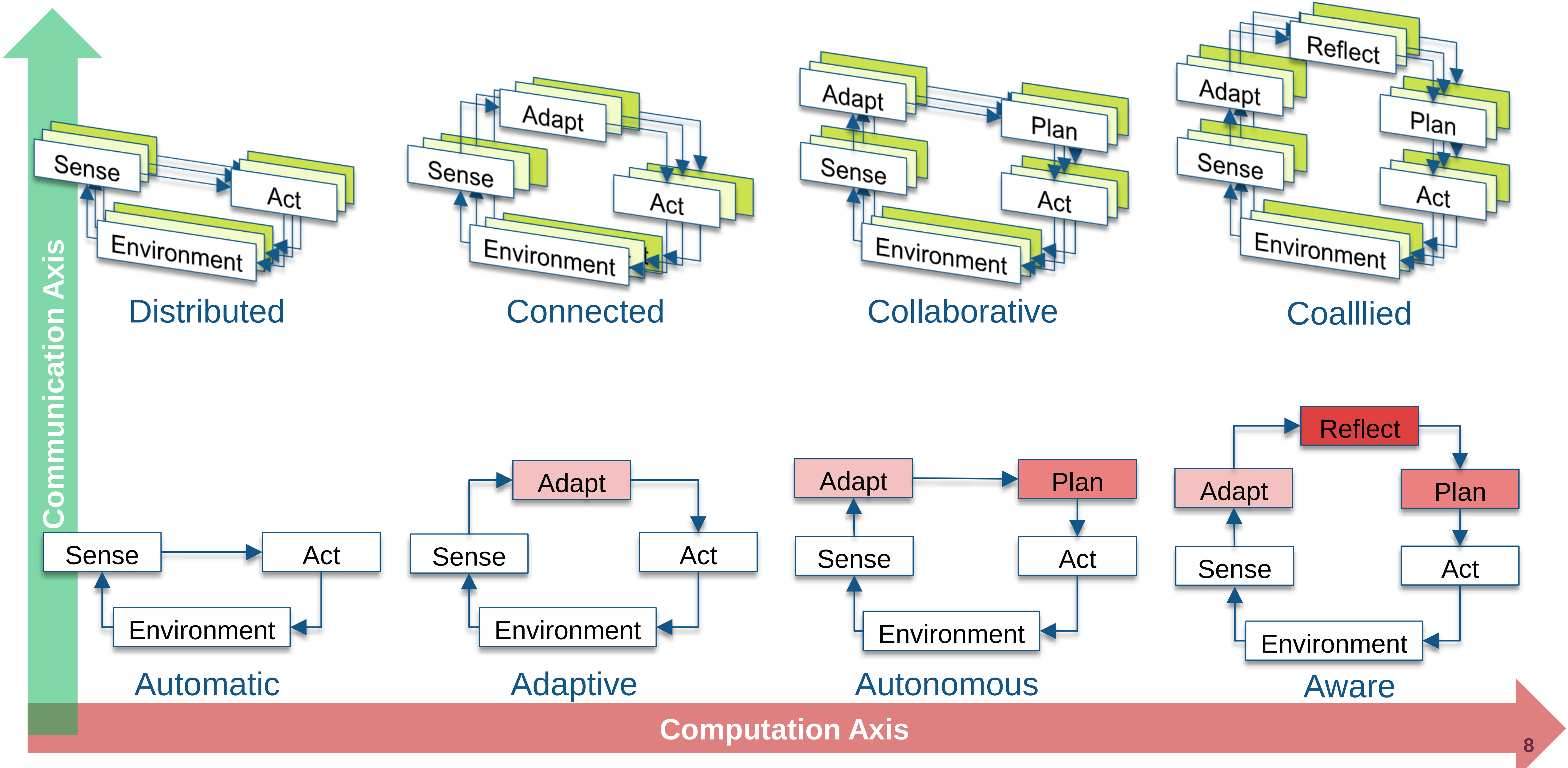




Source: nngroup.com

Source: Wikipedia

CPS feature classification



References

Configuration	Behavior			
	Reflexive	Reactive	Reasoned	Reflective
Individual	Automatic	Adaptive	Autonomous	Aware
Ensemble	Distributed	Connected	Collaborative	Coallied

[CMR+20] S. Castro, P. Mosterman, A. Rajhans, R. Valenti, "*Challenges in the Operation and Design of Intelligent Cyber-Physical Systems*", to appear.

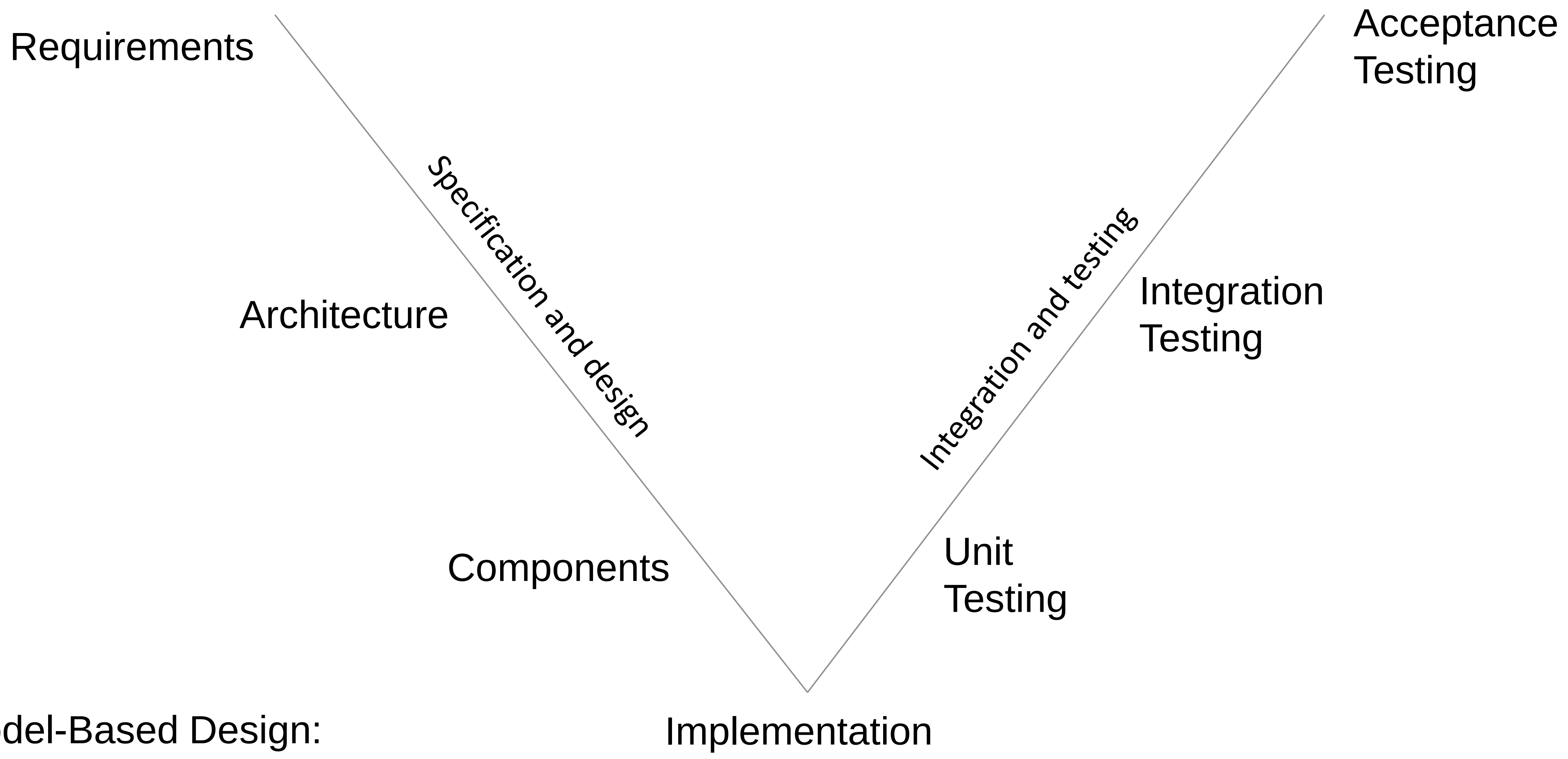
[ABK+19] F. Allgöwer, J. Borges de Sousa, J. Kapinski, P. Mosterman, J. Oehlerking, P. Panciatici, M. Prandini, A. Rajhans, P. Tabuada, P. Wenzelburger, "*Position paper on the challenges posed by modern applications to cyber-physical systems theory*", Nonlinear Analysis: Hybrid Systems, Volume 34, Pages 147-165, November 2019.

[TBD+18] A. Tolk, F. Barros, A. D'Ambrogio, A. Rajhans, P. J. Mosterman, S. S. Shetty, M. K. Traoré, H. Vangheluwe, and L. Yilmaz, "*Hybrid Simulation for Cyber Physical Systems – A Panel on Where are we Going Regarding Complexity, Intelligence, and Adaptability of CPS Using Simulation*," Spring Simulation Multi-Conference, 2018.

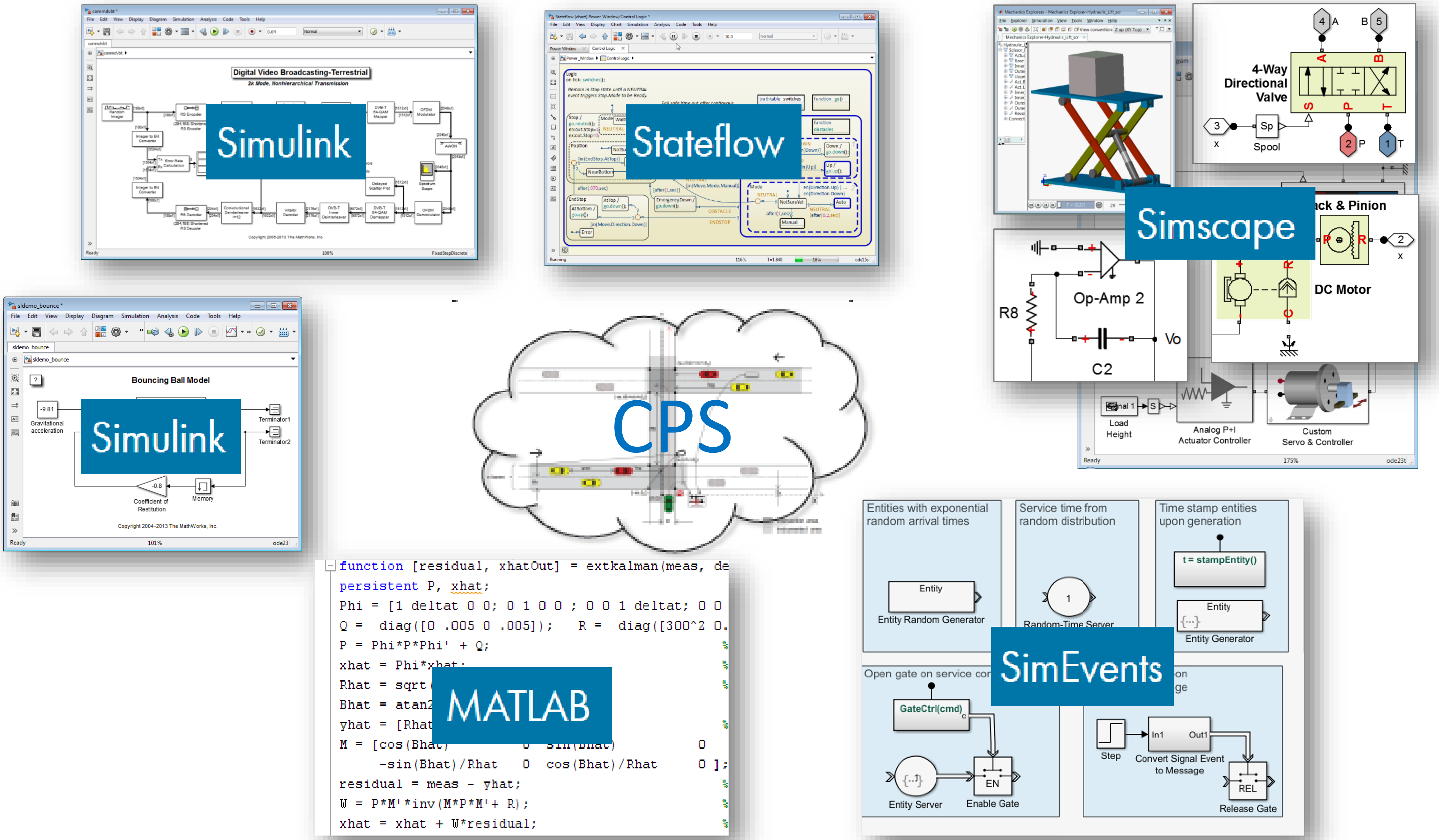
Outline

- CPS feature classification
- “Runtime” verification at design time: simulation as a proxy for run time
- From CPS to IoT and Digital Twins: runtime analysis
- Challenges and future outlook

Model-Based Design: Models as a proxy for the real system



Model-Based Design:
Use of computational models throughout


Simulink
Digital Video Broadcasting-Terrestrial
Stateflow
Simscape
4-Way Directional Valve
Spool
Rack & Pinion
DC Motor
Op-Amp 2
R8
C2
Vo
Load Height
Analog P+I Actuator Controller
Custom Servo & Controller
Simulink
Bouncing Ball Model
Gravitational acceleration
Coefficient of Restitution
Memory
Terminator1
Terminator2
CPS
MATLAB
function [residual, xhatOut] = extkalman(meas, de
persistent P, xhat;
Phi = [1 deltat 0 0; 0 1 0 0 ; 0 0 1 deltat; 0 0
Q = diag([0 .005 0 .005]); R = diag([300^2 0.
P = Phi*P*Phi' + Q;
M = [cos(Bhat) sin(Bhat) 0
-sin(Bhat)/Rhat 0 cos(Bhat)/Rhat 0];
residual = meas - yhat;
W = P*M'*inv(M*P*M'+ R);
xhat = xhat + W*residual;
SimEvents
Entities with exponential random arrival times
Entity Random Generator
Service time from random distribution
Random-Time Server
Time stamp entities upon generation
t = stampEntity()
Entity Generator
GateCtrl(cmd)
Entity Server
Enable Gate
Step
Convert Signal Event to Message
Release Gate

Simulations for increasingly faithful proxies of runtime behavior

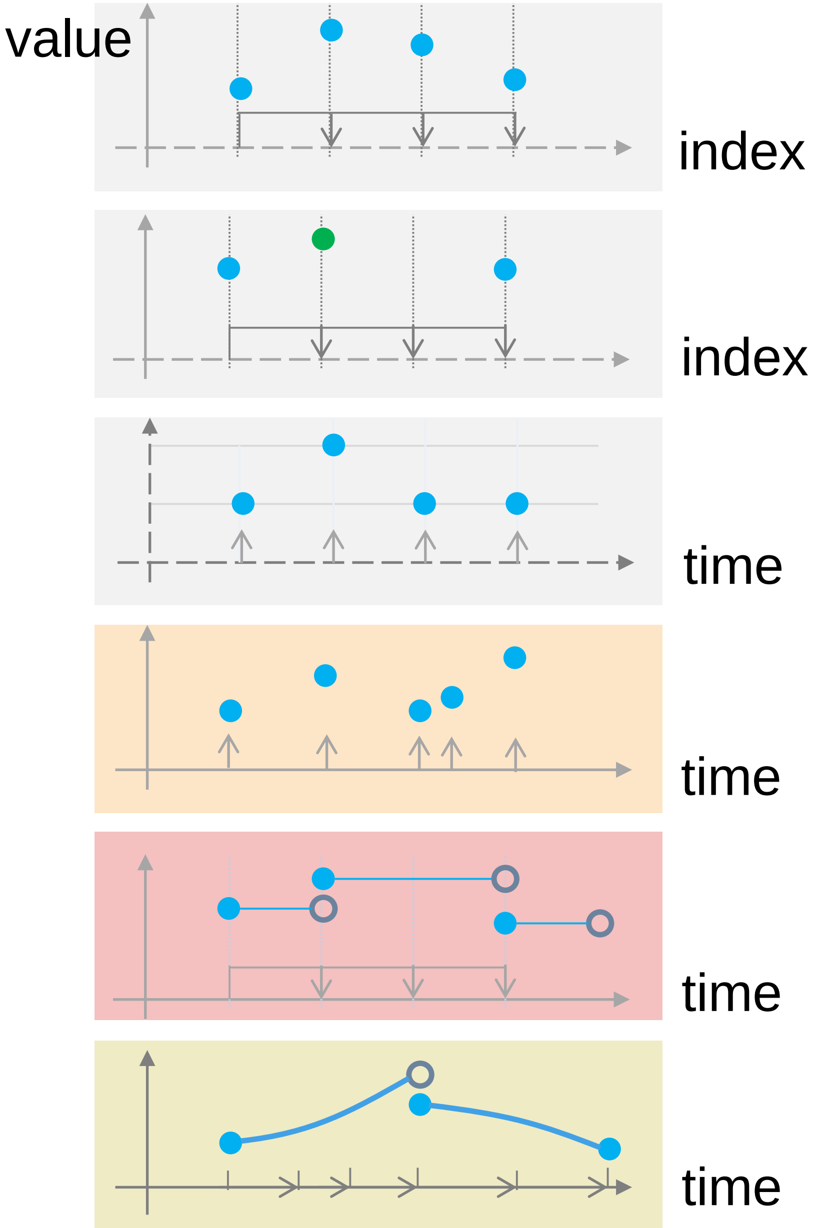
▪ Model-in-the-loop simulation	simulate / test	the model
▪ Software-in-the-loop simulation		the generated code
▪ Processor-in-the-loop simulation		code on the processor
▪ Hardware-in-the-loop simulation		plant on real-time h/w
▪ Gaming-engine-in-the-loop		visualization, physics

Ride & handling

Chassis controls

ADAS / AD

Microprocessor	Microprocessor	MATLAB	C code
		MATLAB	Multi-rate C code
		Stateflow	
Network		SimEvents	
Sensors	Actuators	Simulink	
Physics		Simulink	Simscape



Not today – how to address heterogeneity formally?

[MRM+20] P.J. Mosterman et al., "*Simulation of Hybrid Dynamic Systems*", Springer Encyclopedia of Systems and Control, Second Edition, to appear.

[RBR+14] A. Rajhans et al., "*Supporting Heterogeneity in Cyber-Physical System Architectures*", IEEE Transactions on Automatic Control, Special Issue on Control of CPS, Vol. 59, Issue 12, pages 3178-3193.

[R13] A. Rajhans, "*Multi-Model Heterogeneous Verification of Cyber-Physical Systems*," **PhD Thesis**, Carnegie Mellon University, 2013.

[RK13] A. Rajhans and B. H. Krogh, "*Compositional Heterogeneous Abstraction*," 16th ACM International Conference on HSCC, 2013.

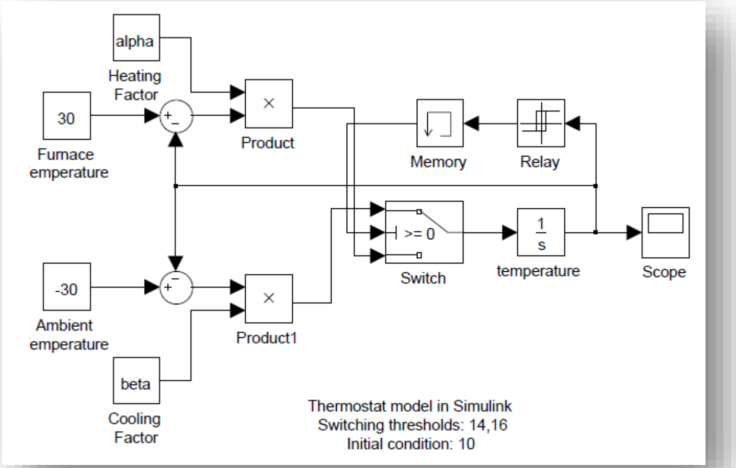
[RK12] A. Rajhans and B. H. Krogh, "*Heterogeneous Verification of Cyber-Physical Systems Using Behavior Relations*," 15th ACM International Conference on HSCC, 2012.

[RBL+11] A. Rajhans et al., "*Using Parameters in Architectural Views to Support Heterogeneous Design and Verification*," 50th IEEE CDC, 2011.

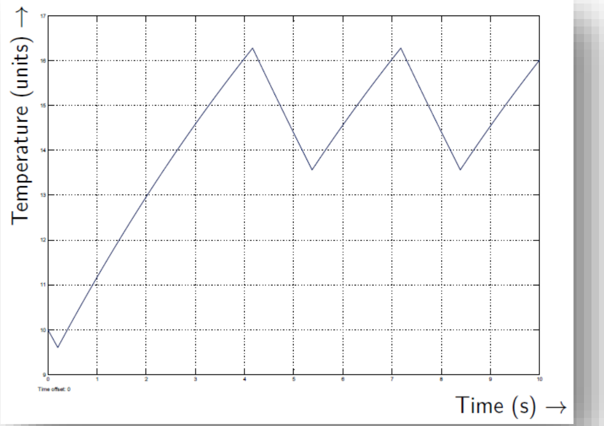
[BDK+10b] A. Bhave et al., "*Augmenting Software Architectures with Physical Components*," Embedded Real Time Software and Systems (ERTS^2), 2010.

[RCS+09] A. Rajhans et al., "*An Architectural Approach to the Design and Analysis of Cyber-Physical Systems*," Third International Workshop on Multi-Paradigm Modeling (MPM), 2009.

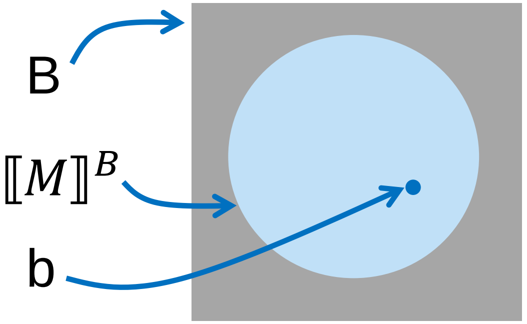
Models and Specifications



Model M

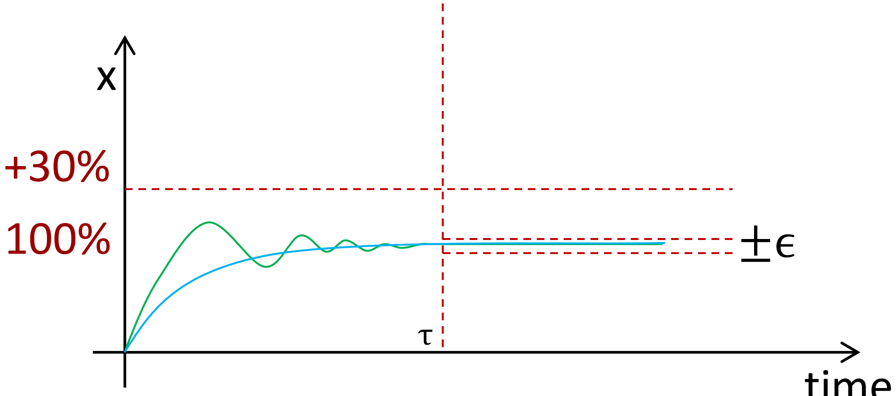


A behavior b that M exhibits

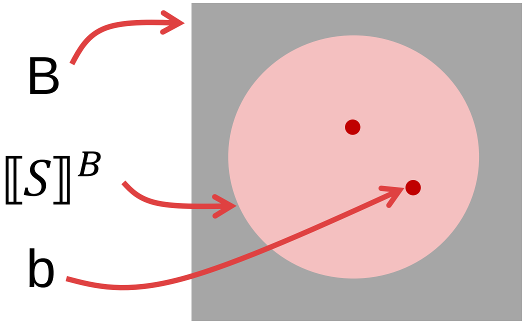


"overshoot is never more than 30% and settling time is less than τ"

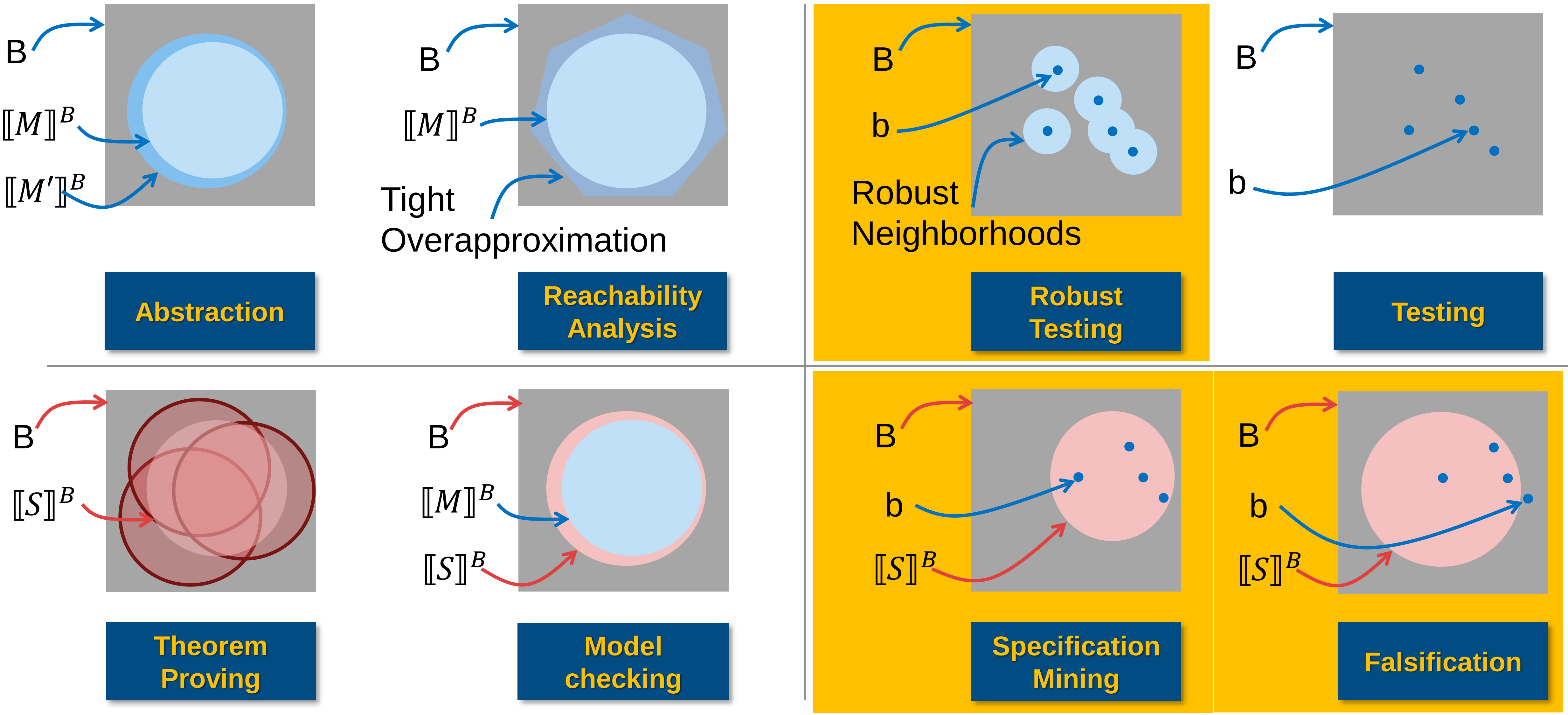
Specification S



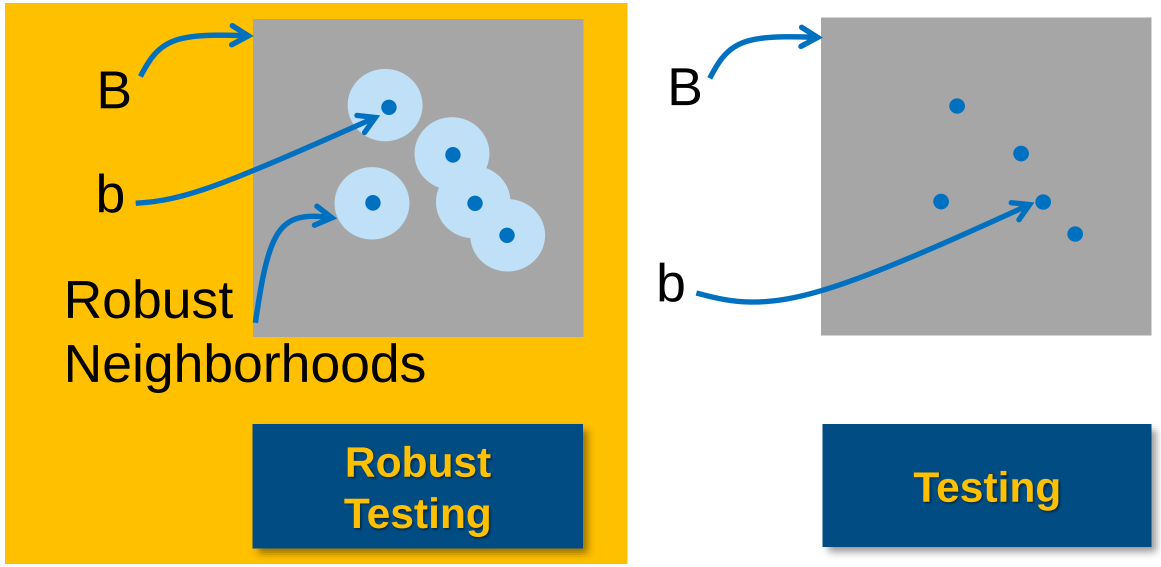
A behavior b that S allows



Various verification problems



Robust testing a.k.a. simulation-based reachability analysis



Robust testing a.k.a. simulation-based reachability analysis

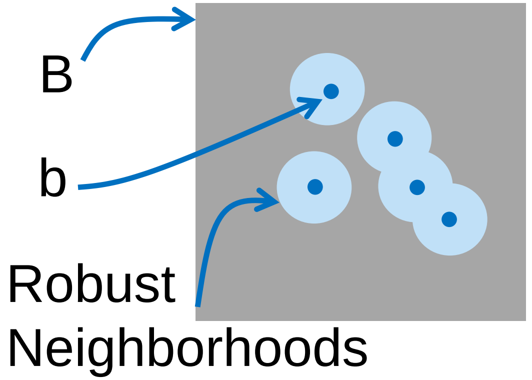
[R07] A. Rajhans, "*Development of Robust Testing Toolbox for Hybrid Systems*," MS Thesis, University of Pennsylvania, 2007.

[DRJ13] Y. Deng, A. Rajhans, and A. A. Julius, "*STRONG: A Trajectory-Based Verification Toolbox for Hybrid Systems*," 10th International Conference on Quantitative Evaluation of SysTems (QEST), 2013.

[DKR09] A. Donzé, B. H. Krogh, and A. Rajhans, "*Parameter Synthesis for Hybrid Systems with an Application to Simulink Models*," 12th IEEE/ACM International Conference on Hybrid Systems: Computation and Control, 2009.

Bisimulation functions

Sensitivity analysis



Related work by Fainekos, Pappas, Balkan, Tabuada, Zutshi, Sankaranarayanan, Kanade, Alur, …

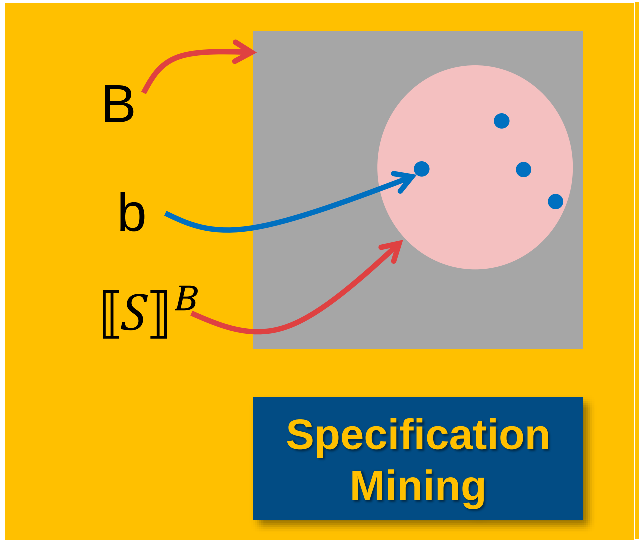
Lyapunov analysis, contraction metrics, barrier certificates, concolic testing …

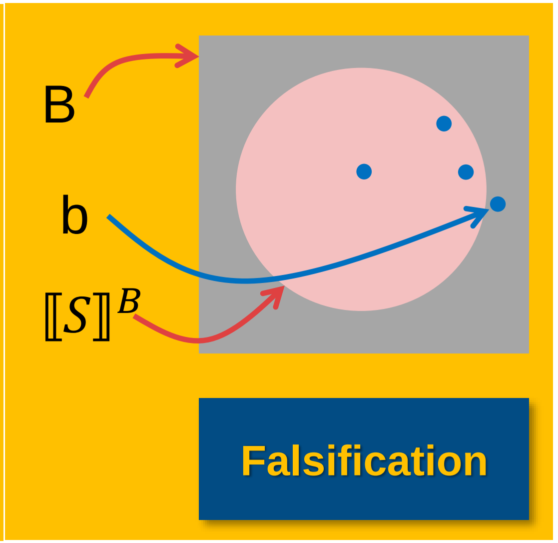
Toyota adoption a success story

Simulation-Based Approaches for Verification of Embedded Control Systems

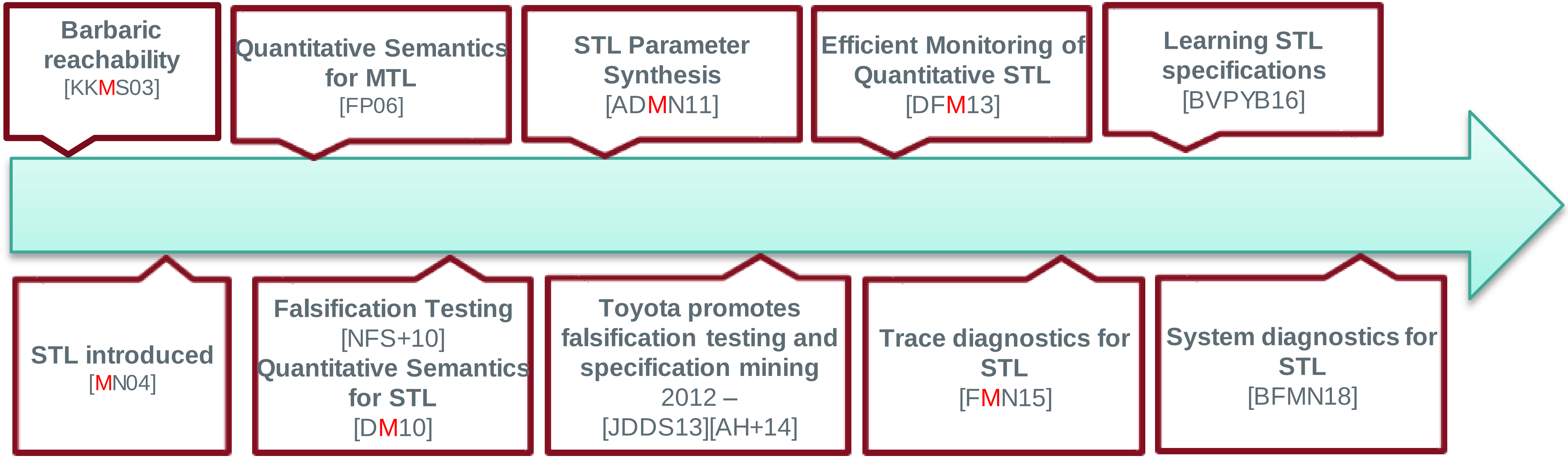
JAMES KAPINSKI, JYOTIRMOY V. DESHMUKH, XIAOQING JIN,
HISAHIRO ITO, and KEN BUTTS

Formalizing specifications to enable falsification



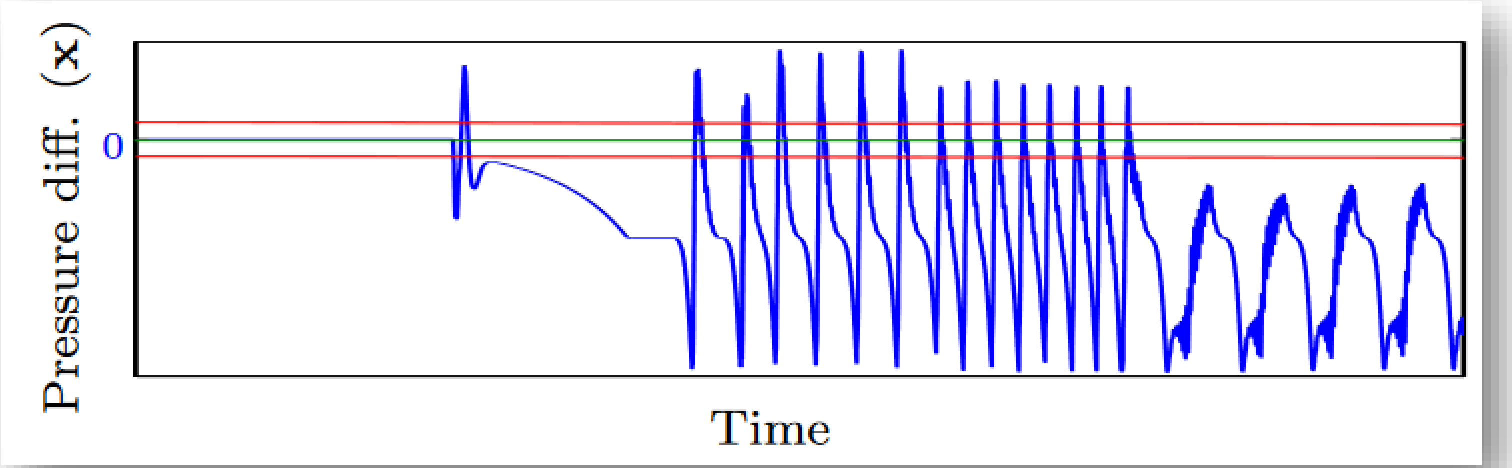


Signal Temporal Logic as a success story



Credit: Dejan Ničković (via Bruce Krogh), *Oded Maler: A memory box full of diamonds*, MT-CPS 2019.

An actual bug uncovered via falsification at Toyota



Mining Requirements from Closed-Loop Control Models

Xiaoqing Jin
Univ. of California Riverside
jinx@cs.ucr.edu

Alexandre Donzé
Univ. of California Berkeley
donze@eecs.berkeley.edu

Jyotirmoy V. Deshmukh
Toyota Technical Center
jyotirmoy.deshmukh@tema.toyota.com

Sanjit A. Seshia
Univ. of California Berkeley
sseshia@eecs.berkeley.edu

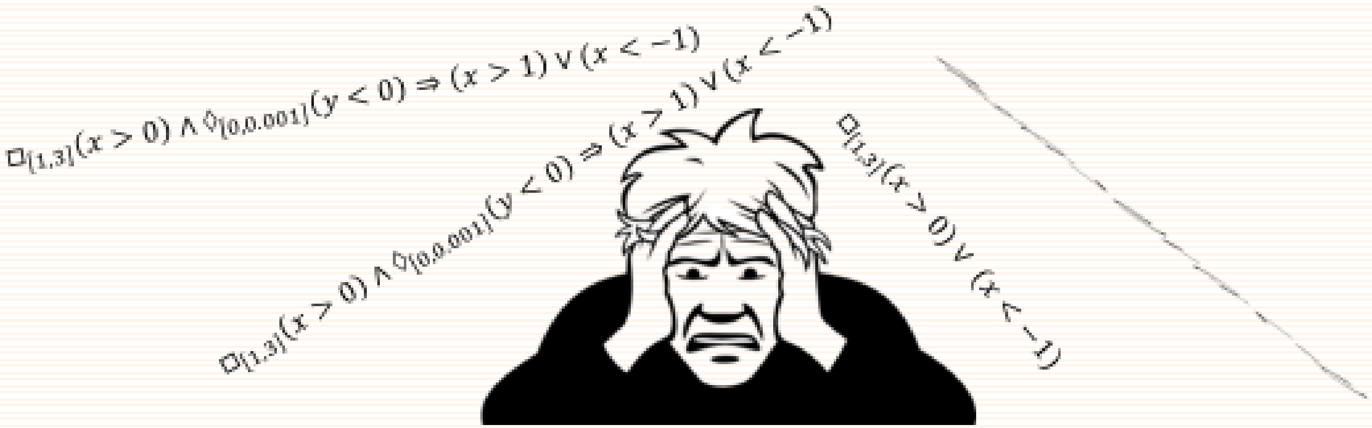
Considerations for engineering adoption of temporal logics

- Engineers are not logicians – logic vocabulary could be a challenge
- Simple engineering concepts may require complex logical formulas
- Multiple modeling formalisms that interact
- Multiple combinations of time/signal domains, data types, solver settings

HSCC 2015 Keynote, Jyotirmoy Deshmukh, (then) Toyota

Grand Challenge I: Requirement Engineering

- Key challenge for Toyota, Bosch, and others
  - How do you present requirements to control designers?
  - How do they convey their intention without using formalisms?
  - Is Temporal Logic the right requirement language?



$\square_{[1,3]}(x > 0) \Rightarrow \Diamond_{[1,3]}((y > 0) \wedge \Diamond_{[0,0.001]}(y < 0) \Rightarrow (x > 1) \vee (x < -1)$

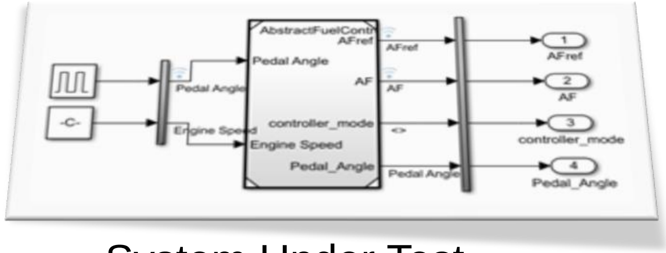
Logical and temporal assessments in Simulink Test

- Formalize and execute requirements directly as Test Assessments

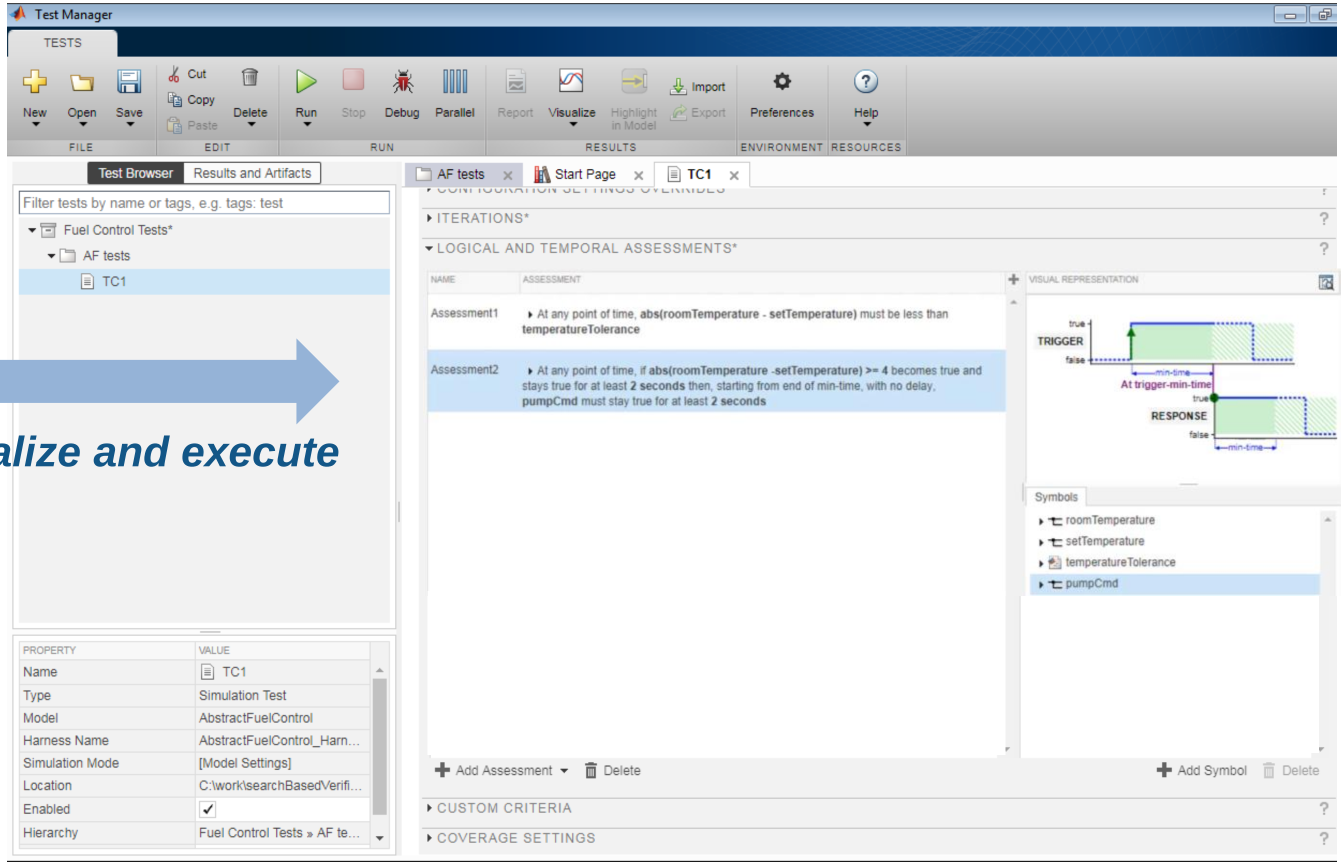
Requirements

1. The difference between the room temperature and the set temperature should never exceed 6 degrees.
2. If the temperature difference exceeds 4 degrees for more than 2 seconds, then the pump shall activate for at least 2 seconds

Formalize and execute

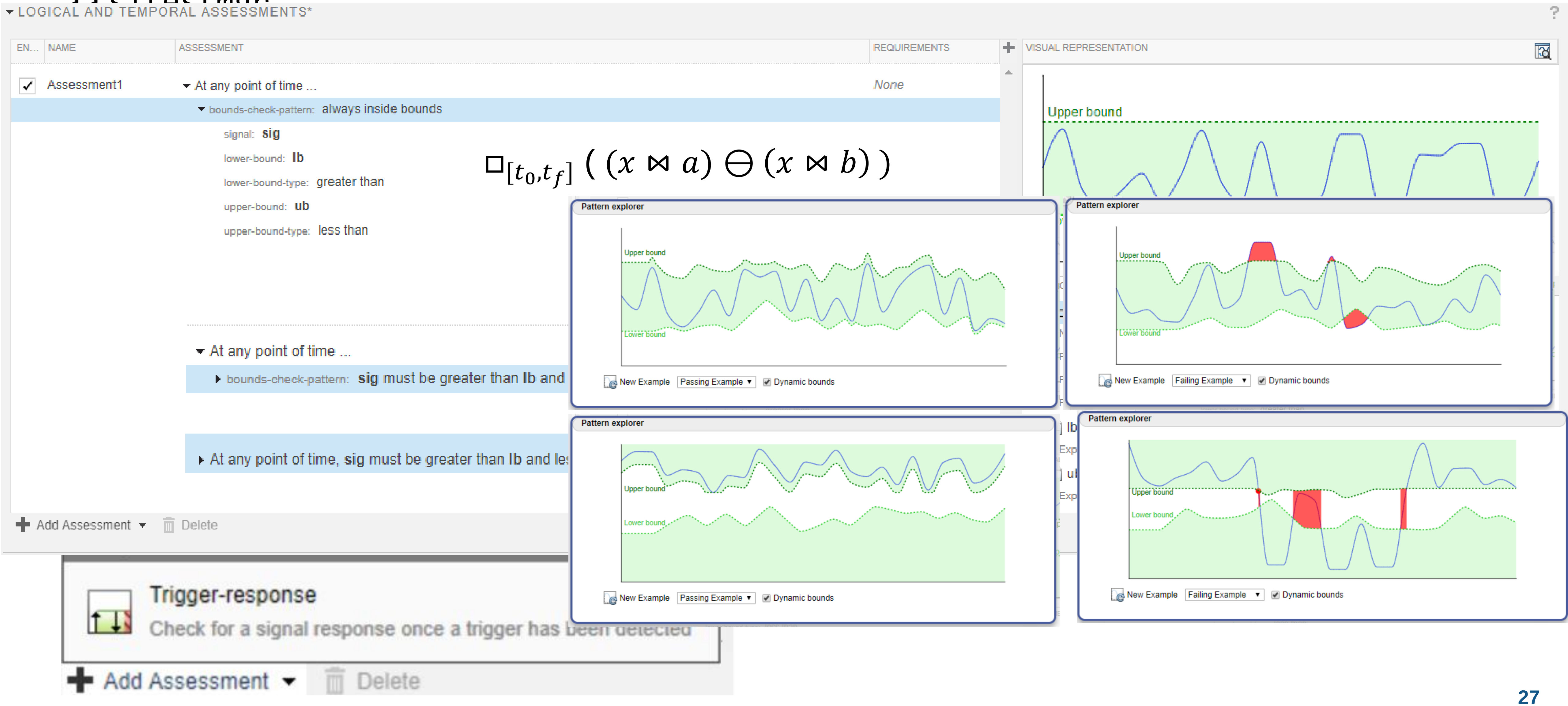


System Under Test



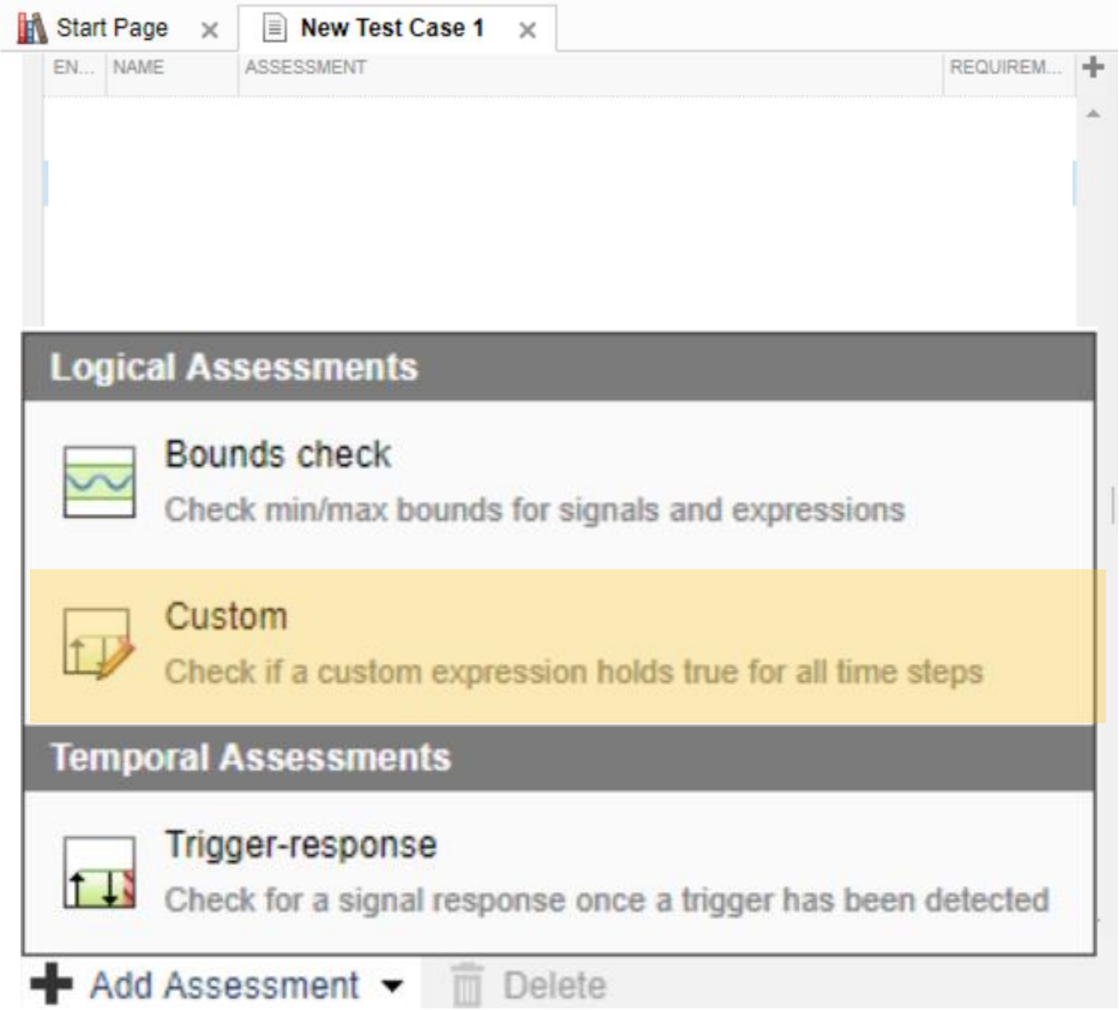
Authoring

```
>> sltestmgr
```



Authoring

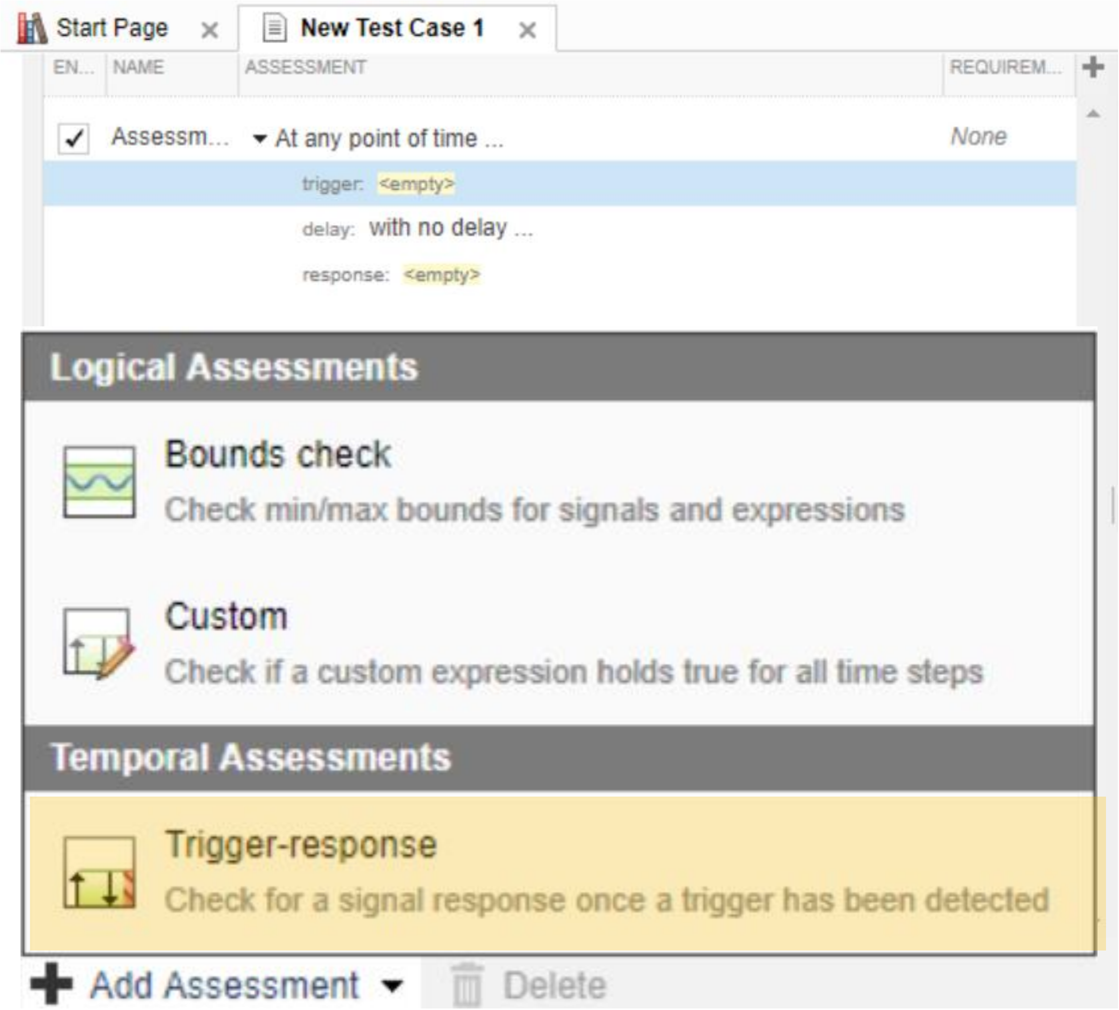
```
>> sltestmgr
```



$$\square_{[t_0,t_f]} \ \phi$$

Authoring

```
>> sltestmgr
```

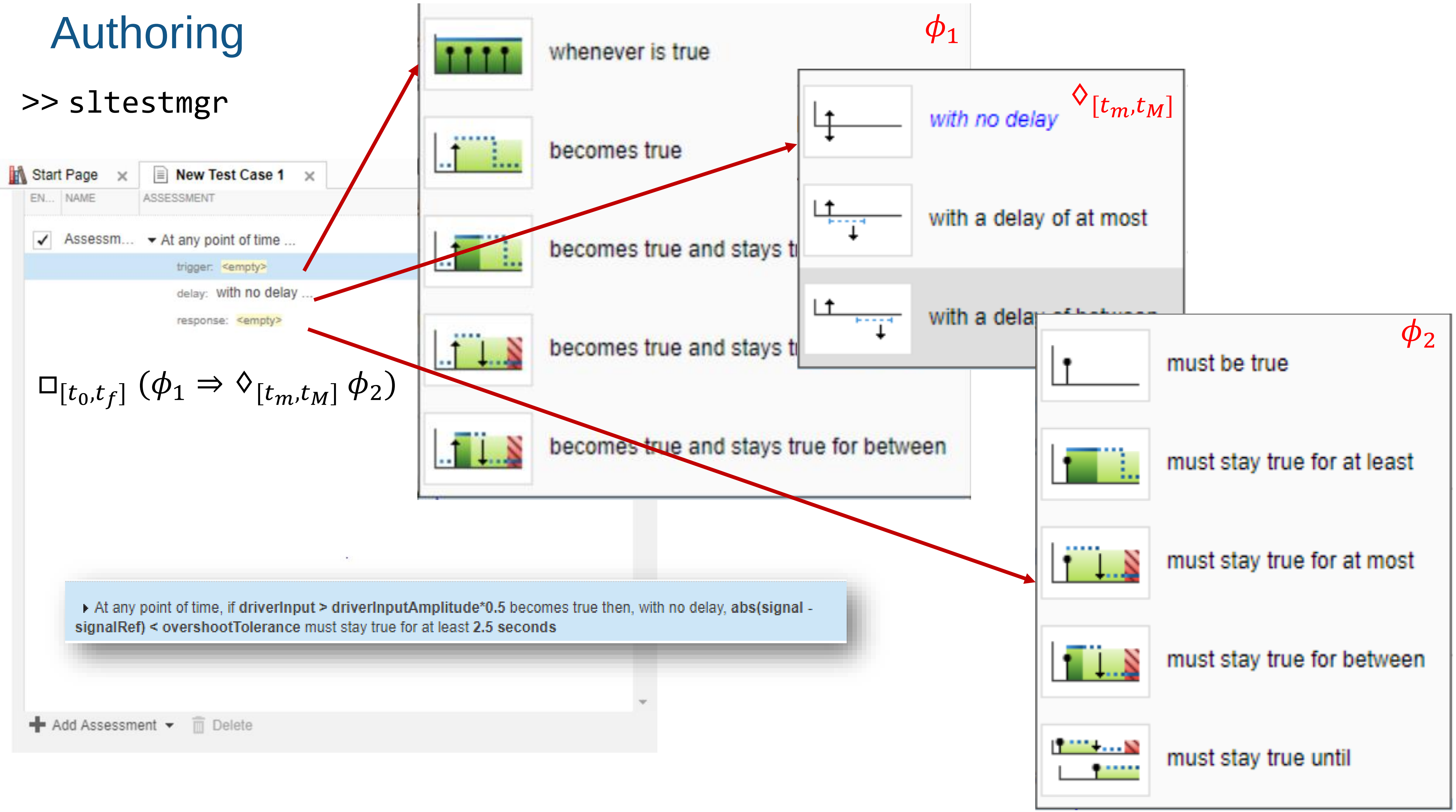


$$\Box_{[t_0,t_f]} \left(\phi_1 \Rightarrow \Diamond_{[t_m,t_M]} \phi_2\right)$$

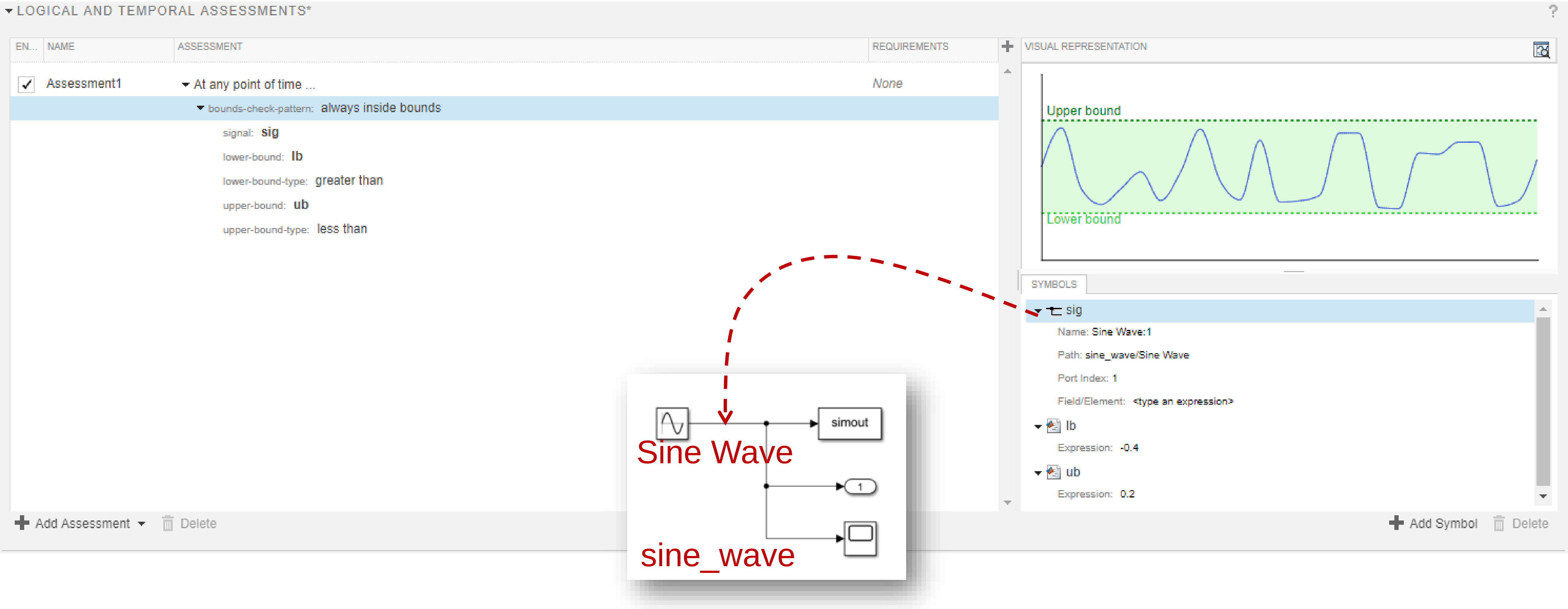
Authoring

```
>> sltestmgr
```

$$\square_{[t_0,t_f]}\,(\phi_1 \Rightarrow \Diamond_{[t_m,t_M]}\,\phi_2)$$

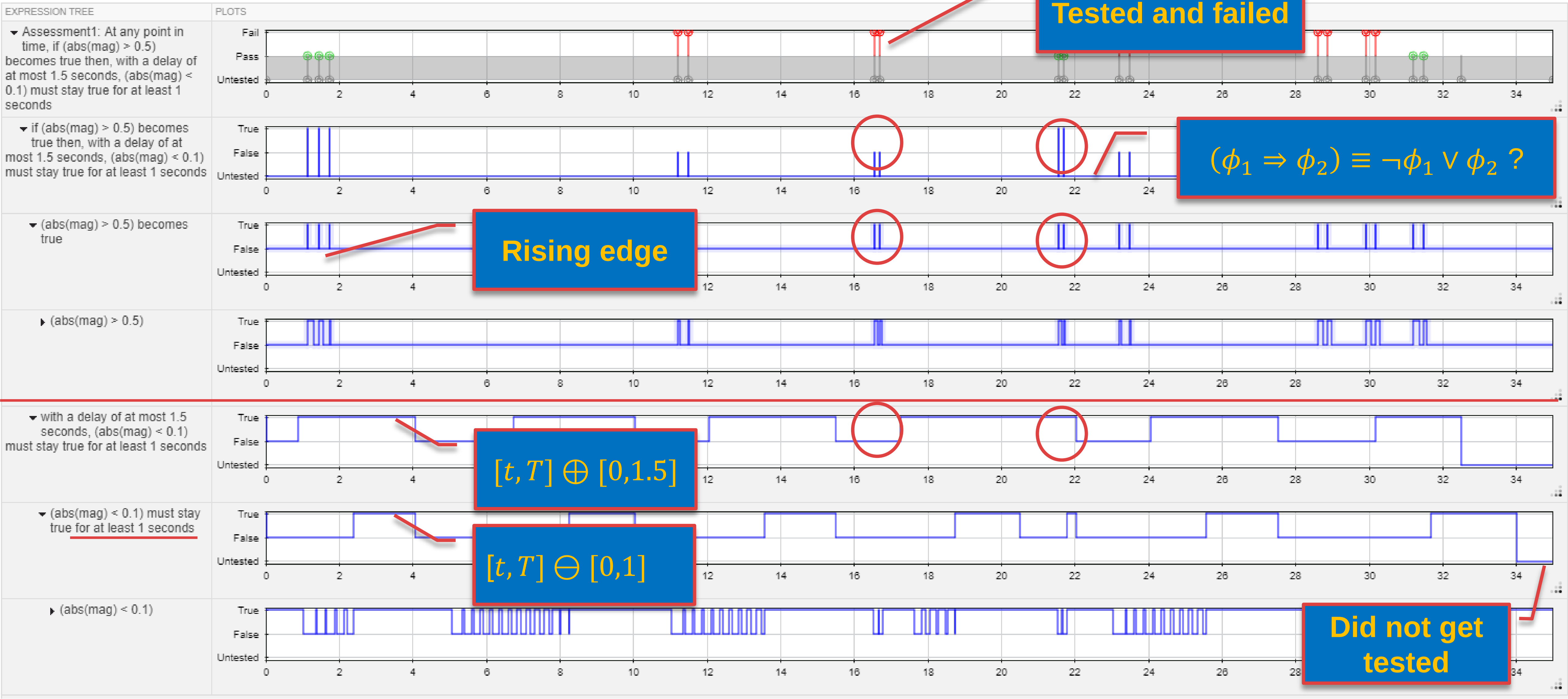


Symbol resolution and mapping

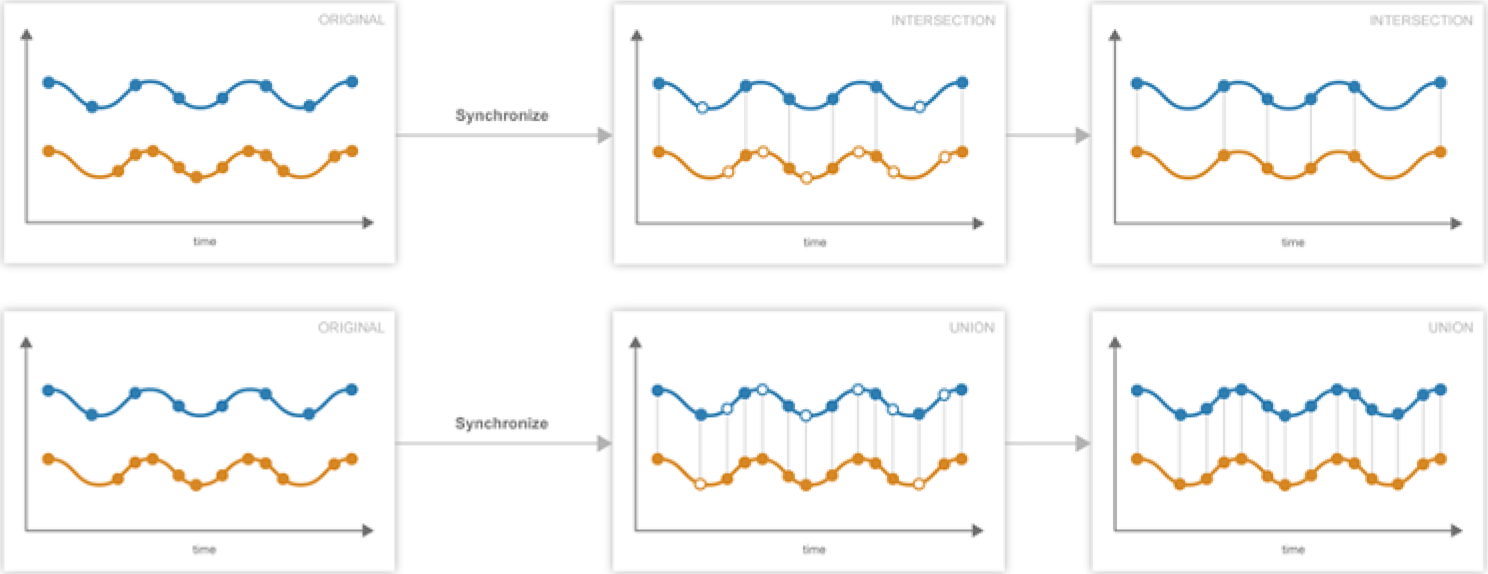


Assessment and explanation in case of failure

Expression tree $\Box_{[t_0,t_f]} (\phi_1 \Rightarrow \Diamond_{[0,t_M]} \phi_2)$



Synchronization and interpolation

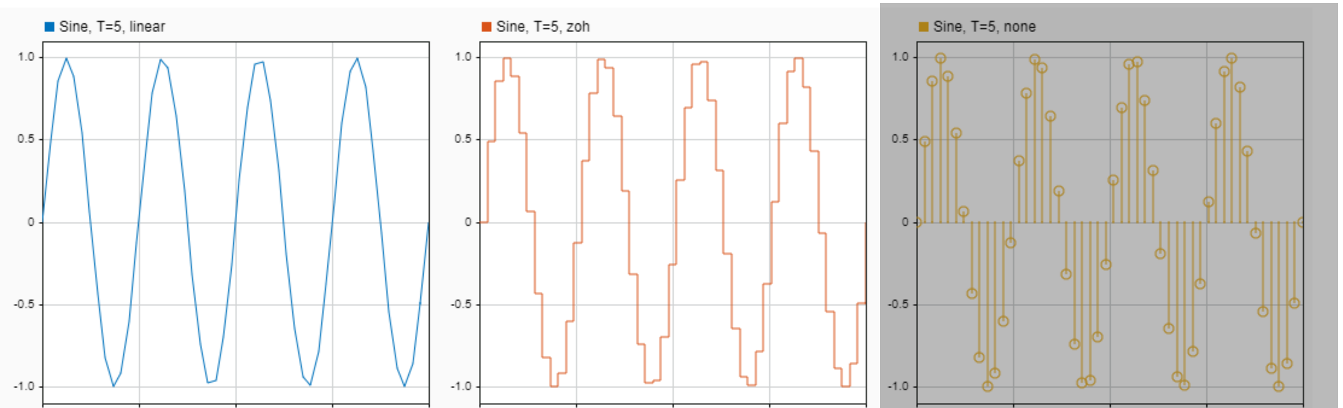


Research challenge: heterogeneity

- discrete and continuous time
- discrete and continuous value

STL ♡ LTL ?

- Needing to up/down-sample may impact frequency domain characteristics
- Dataflow domain: cannot insert or remove data points



Currently not supported

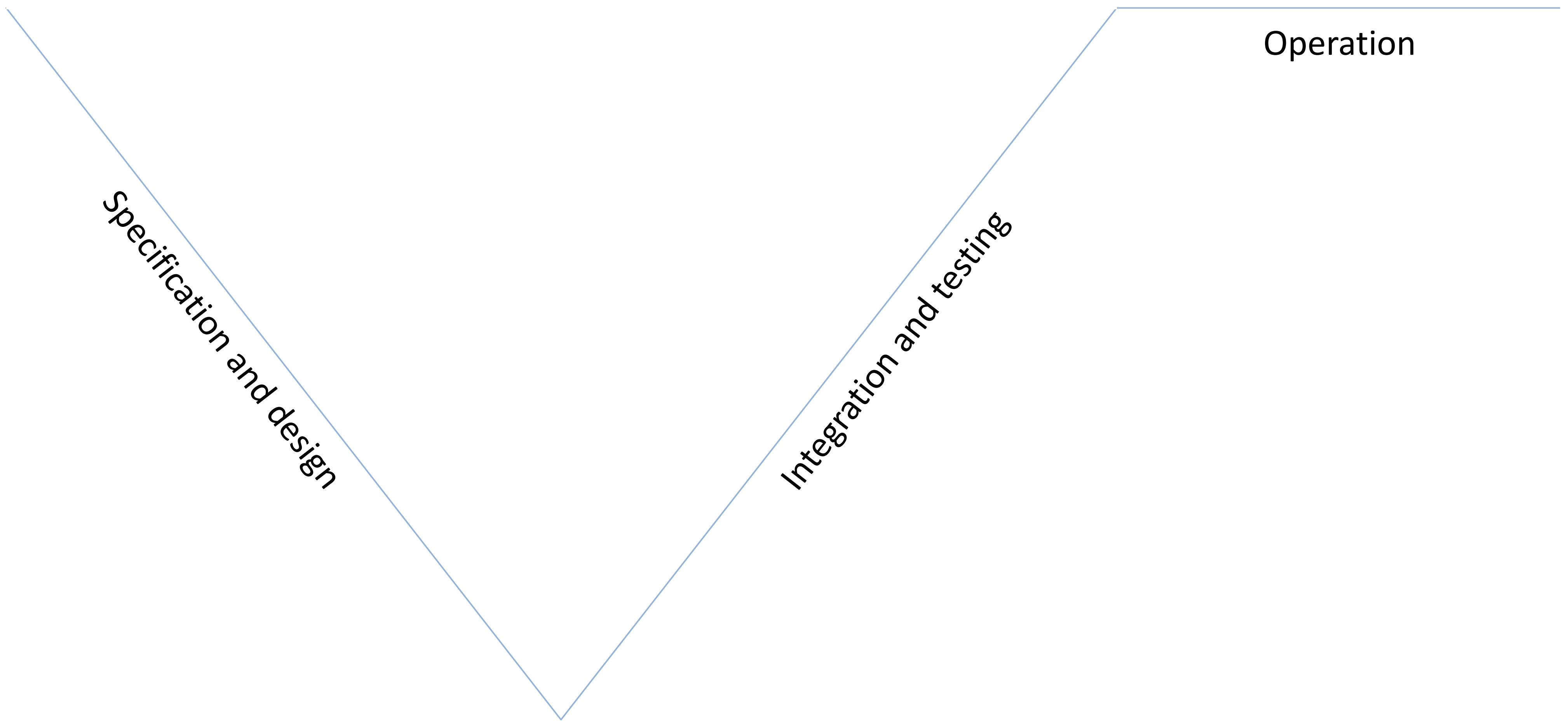
References

- [DMN19] A. Donzé and A. Rajhans, "*Tools Perspective*", J. V. Deshmukh, O. Maler, and D. Nickovic, eds., "*Specification Formalisms for Modern Cyber-Physical Systems (Dagstuhl Seminar 19071)*", 2019.
- [KKR19] J.-F. Kempf, Khoo Y. P., and A. Rajhans, "*Specification and Assessment of Temporal Requirements using Simulink Test*", Fourth International Workshop on Monitoring and Testing of Cyber-Physical Systems (MT-CPS 2019), part of CPS-IoT Week 2019.
- [ABB+18] S. Anderson, et al., "*On the Use of Modeling and Simulation in Robotics*," Workshop Report, NIST/NSF/DoD Workshop on Simulation and Machine Learning in Robotics, 2018.
- [DRJ13] Y. Deng, A. Rajhans, and A. A. Julius, "*STRONG: A Trajectory-Based Verification Toolbox for Hybrid Systems*," 10th International Conference on Quantitative Evaluation of SysTems (QEST), 2013.
- [DKR09] A. Donzé, B. H. Krogh, and A. Rajhans, "*Parameter Synthesis for Hybrid Systems with an Application to Simulink Models*," 12th IEEE/ACM International Conference on Hybrid Systems: Computation and Control, 2009.
- [R07] A. Rajhans, "*Development of Robust Testing Toolbox for Hybrid Systems*," MSE Thesis, University of Pennsylvania, 2007.

Outline

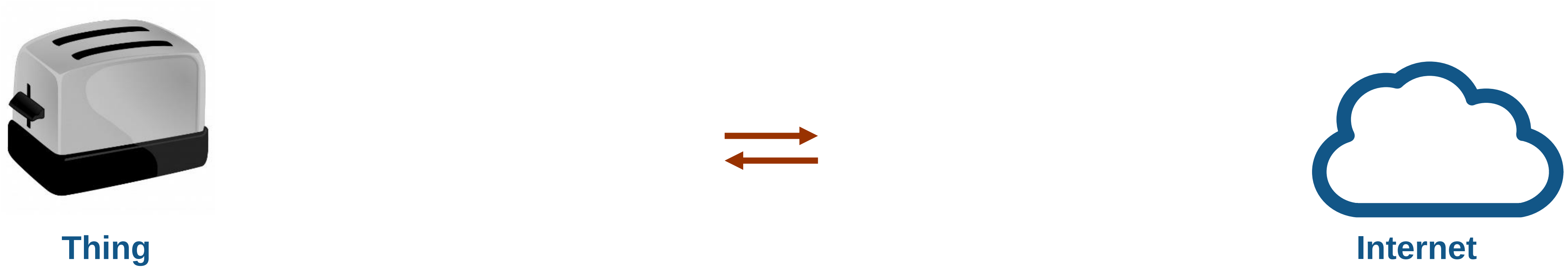
- Cyber-physical systems: a feature classification
- “Runtime” verification at design time: simulation-based approaches
- ➢ Runtime analysis at operation time: From CPS to IoT and Digital Twins
- Challenges and future outlook

Models are useful in both design and operation

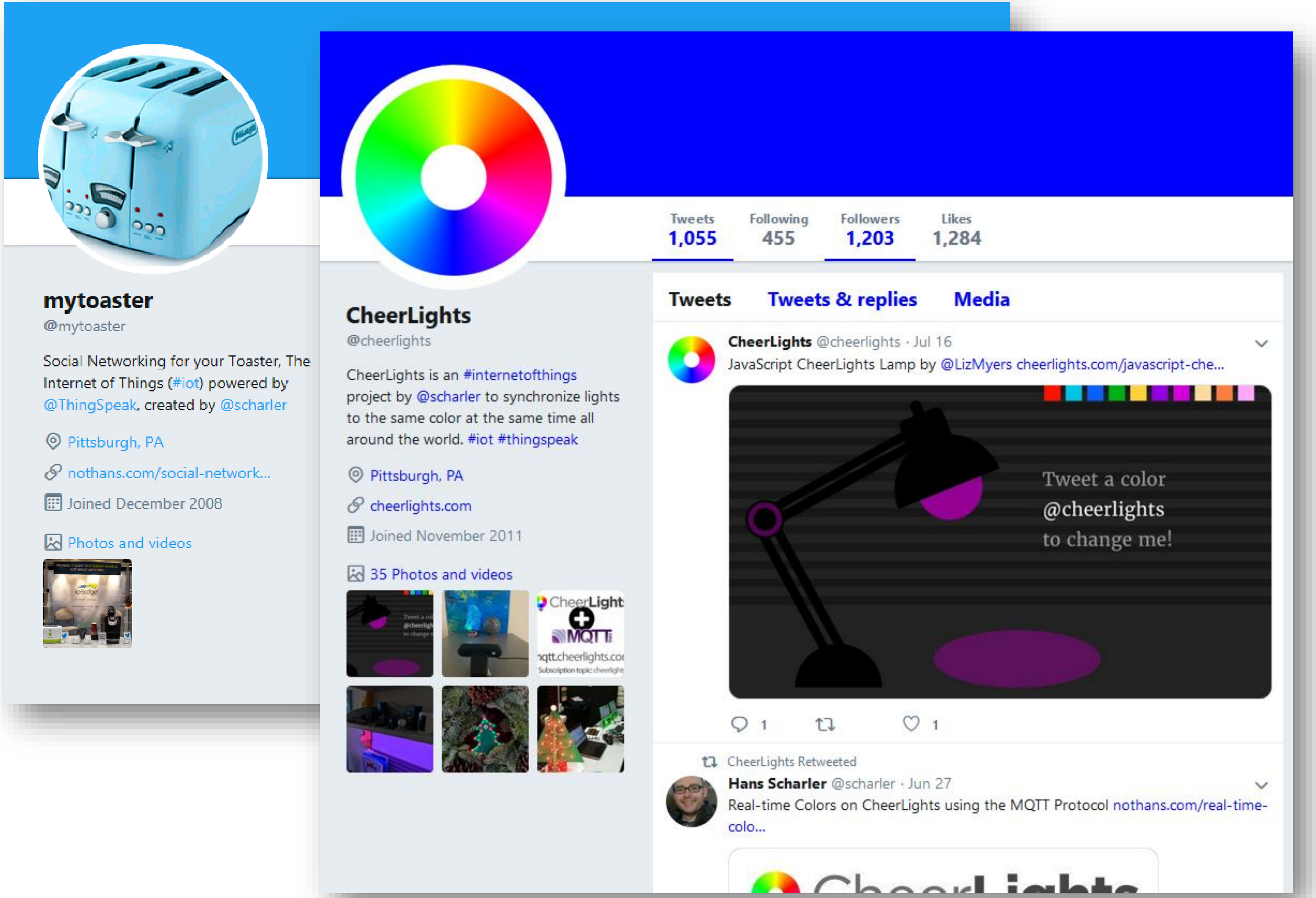


Challenges in the Operation and Design of Intelligent Cyber-Physical Systems, S. Castro, P.J. Mosterman, A.H. Rajhans, and R.G. Valenti, book chapter, *Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy*, S. Mittal and A. Tolk, eds., Wiley, 2019.

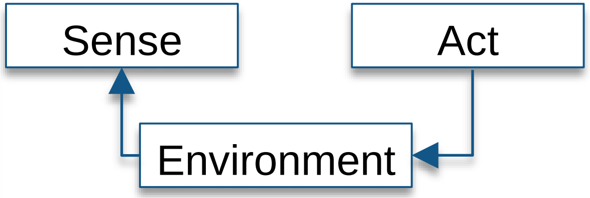
Internet of Things topology



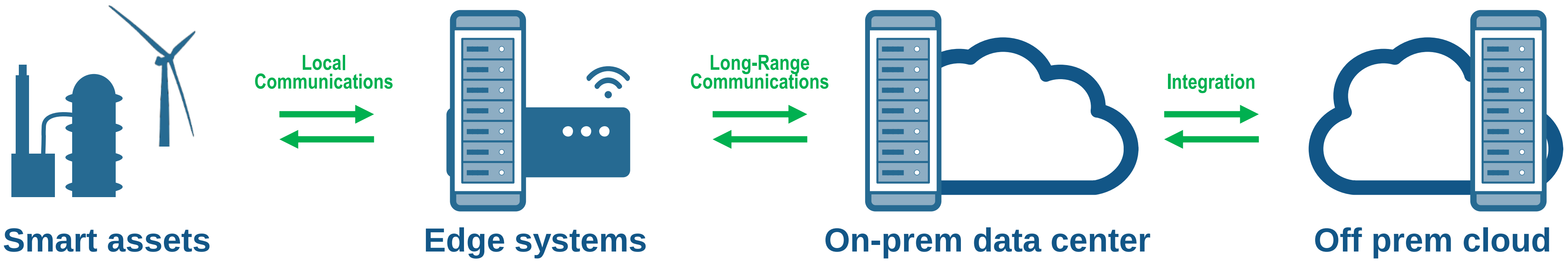
Internet of Things topology

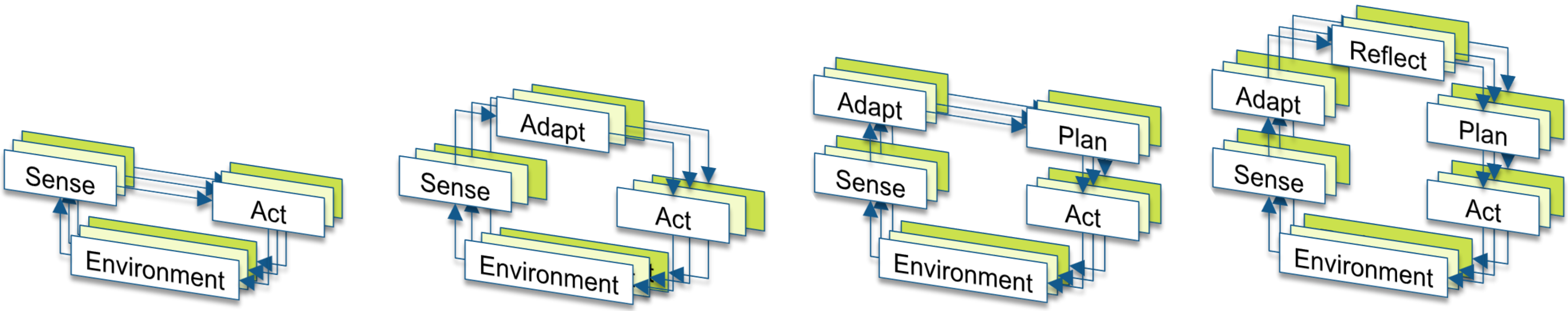


Internet

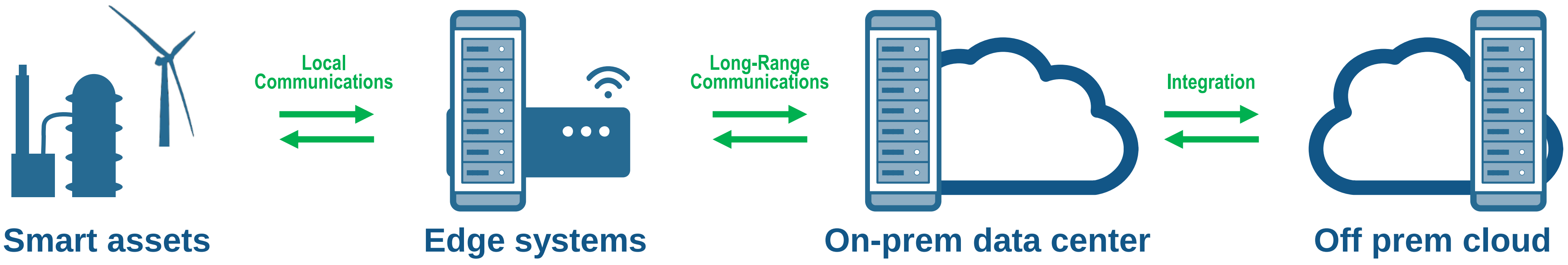


Industrial Internet of Things topology – Enterprise level operations





A complex collection of tools, platforms, and protocols

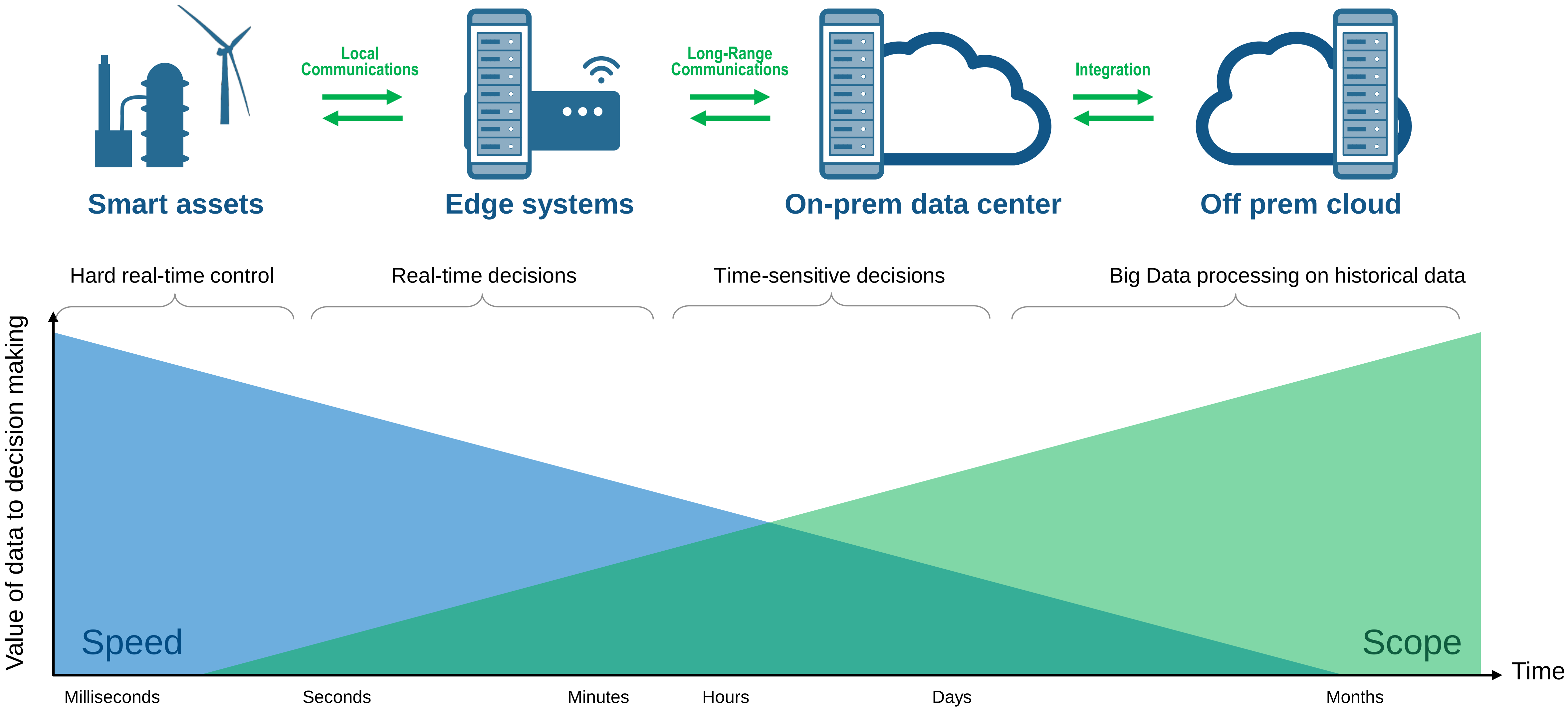


NXP
ARM
TCP/IP
MQTT
Azure Stream Analytics
Azure IoT Hub
Azure
TIBCO Spotfire
XILINX
NVIDIA
Rest APIs
amazon Kinesis
AWS IoT
amazon web services
tableau
intel
Windows
docker
Power BI
life.augmented
MindSphere
thingworx

- Chipmakers
- Transport protocols
- Operating systems running on edge or on-premises
- Cloud providers
- Streaming protocols for getting data in and out of the cloud platforms
- Services for managing data, timing, and other Industrial IoT requirements
- Dashboard tools for visualizing information in any area of the landscape

Analyst/Engineer

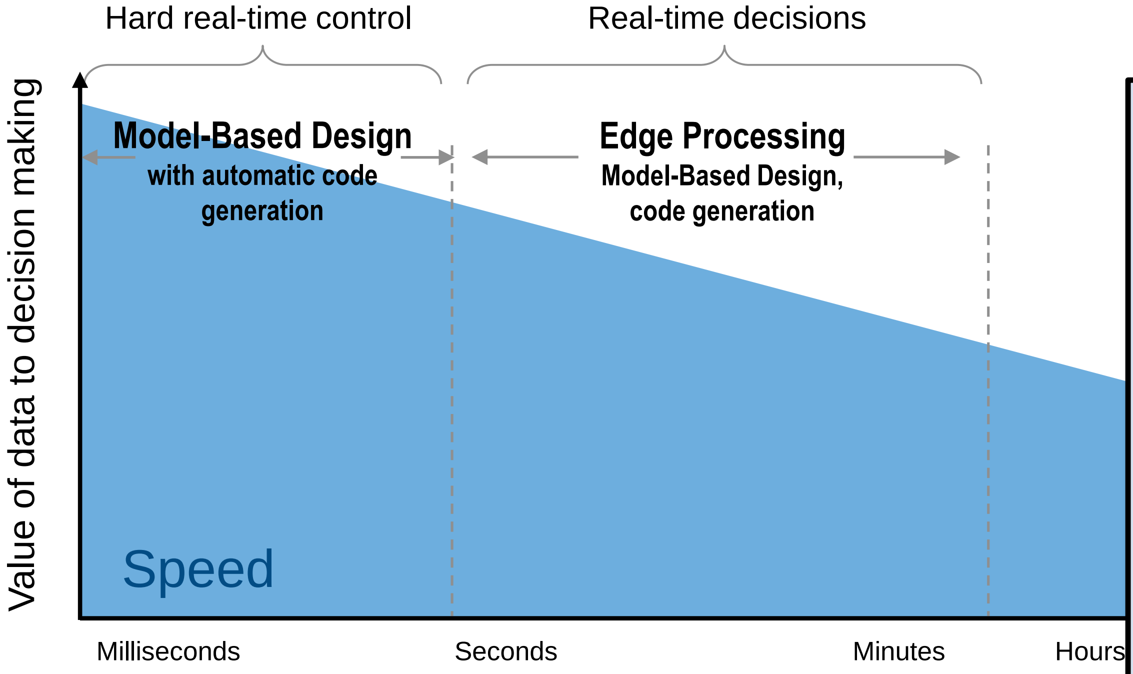
Applications at the Asset, the Edge, or Operational Technology Platform



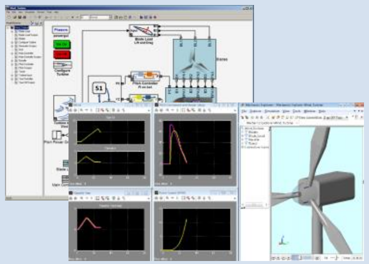
Development for Fast and Highly-Deterministic Systems

Smart assets **Edge systems**

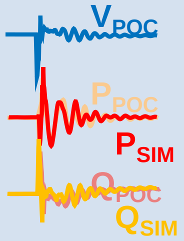
- Compute limited but have a choice
- Data usually as a memory read
- Product design focus



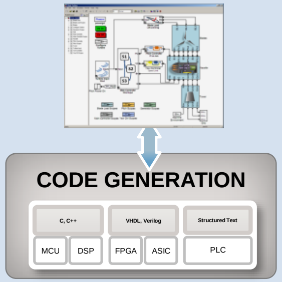
Model-Based Design



Multi-domain system modeling



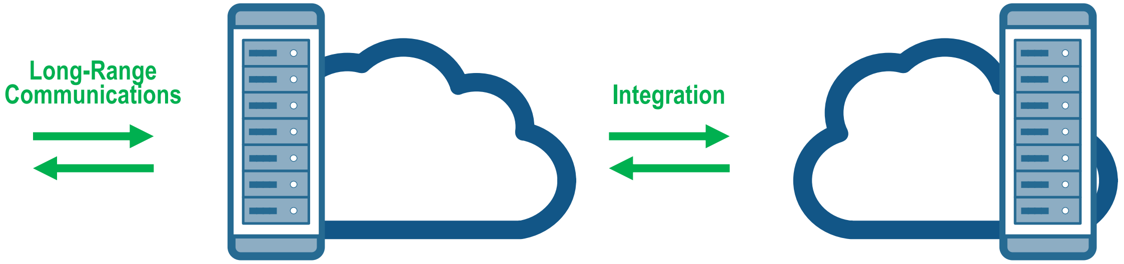
Parameter estimation



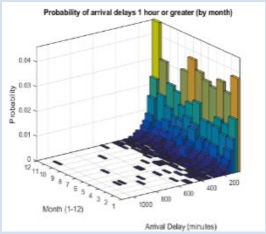
Automatic code generation

Development to OT/IT On-Prem and in Cloud

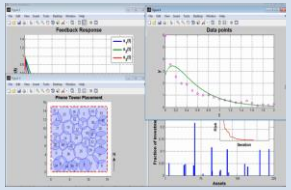
- Compute abundant but less control
- Data access as streaming messages
- Service focus



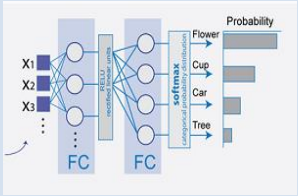
On-prem data center **Off prem cloud**



Variety and Volumes of Data

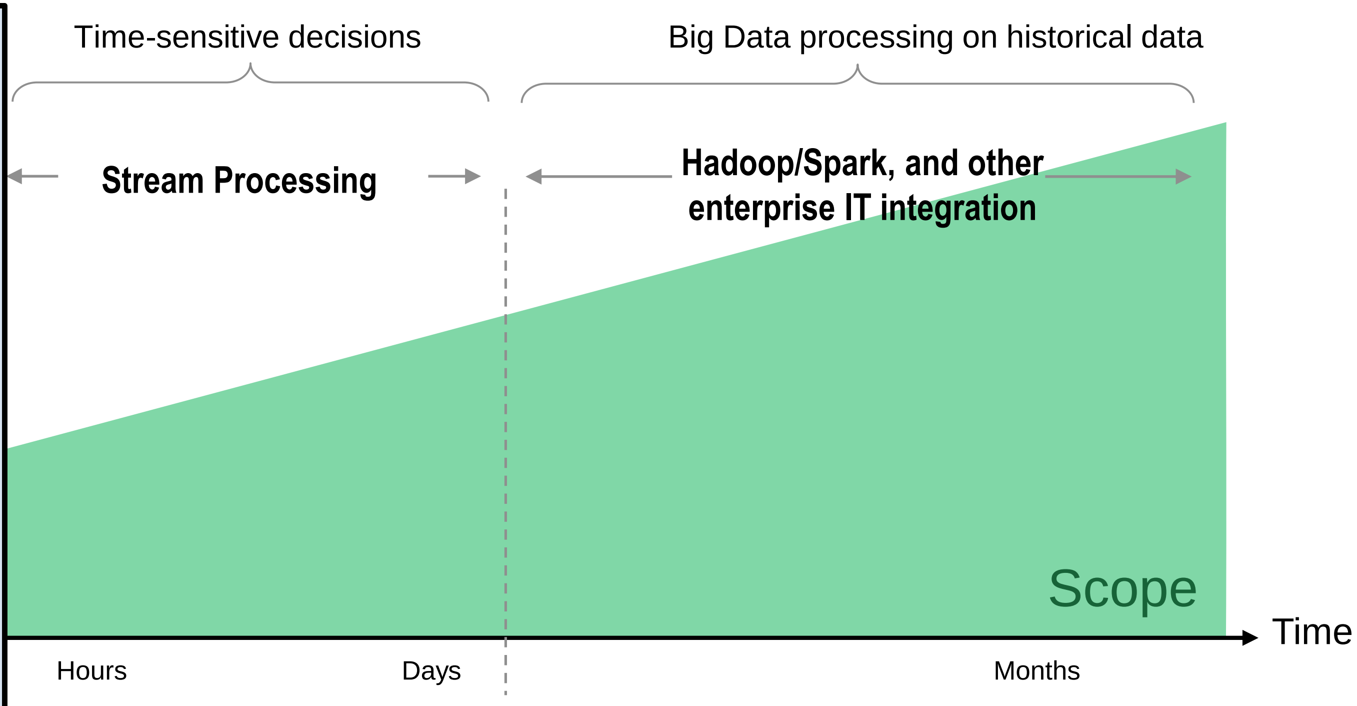


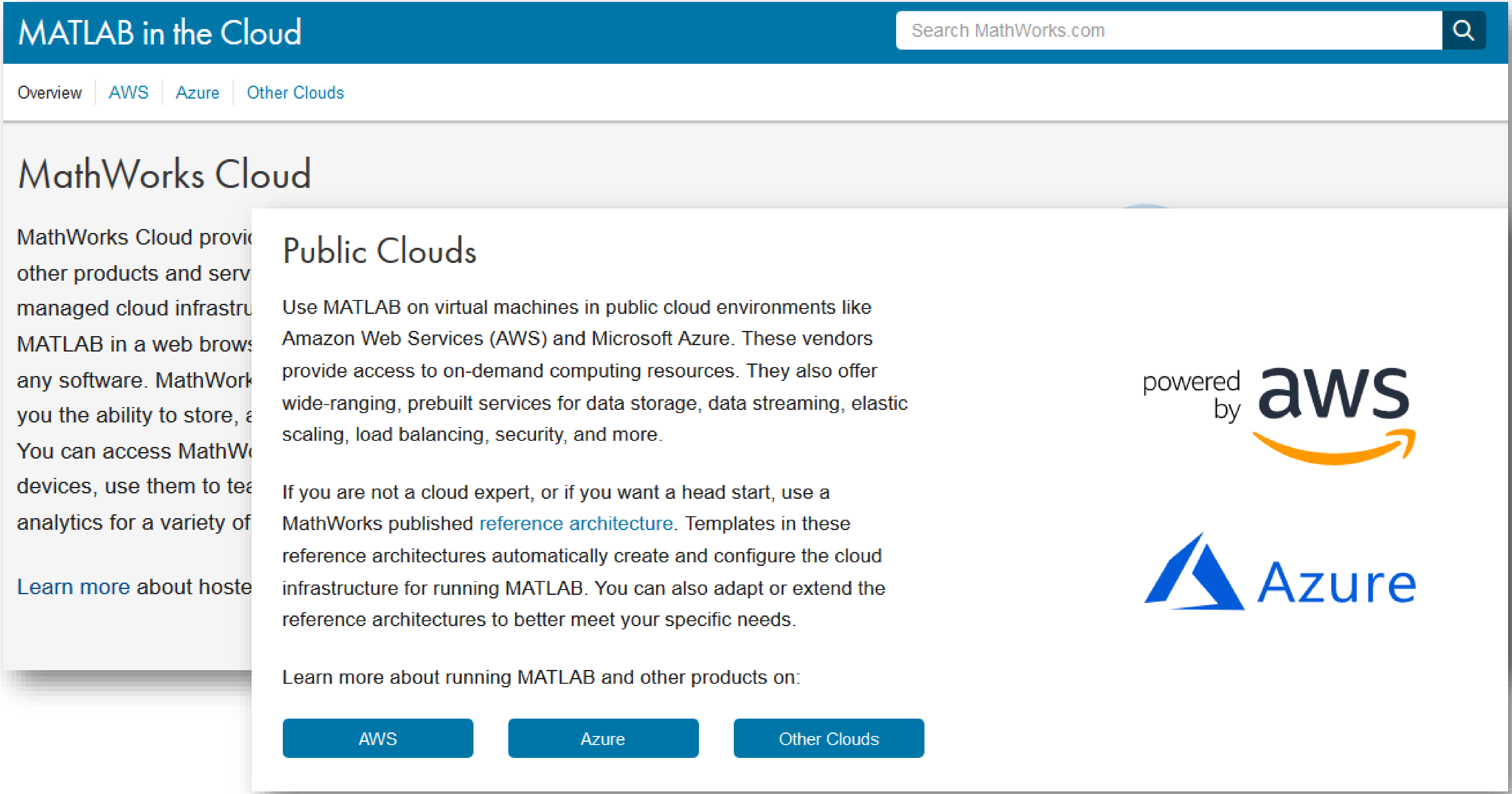
Optimization



Machine Learning and Deep Learning

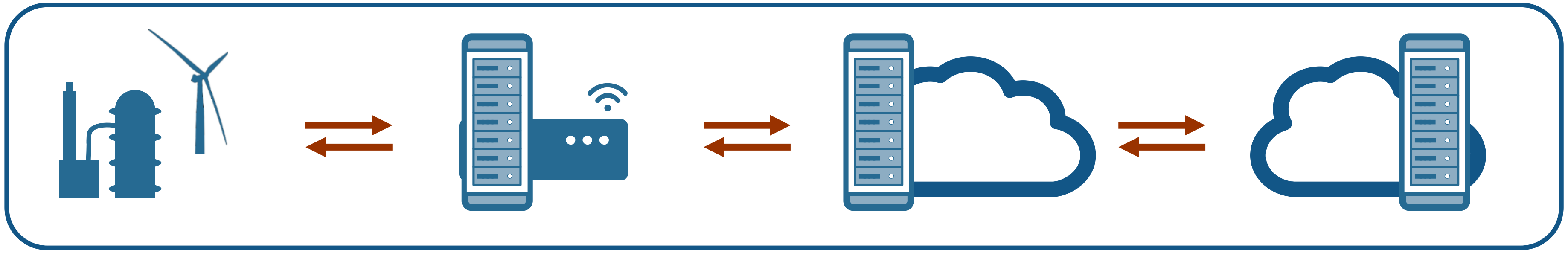
Enterprise system integration, (on-prem/cloud)

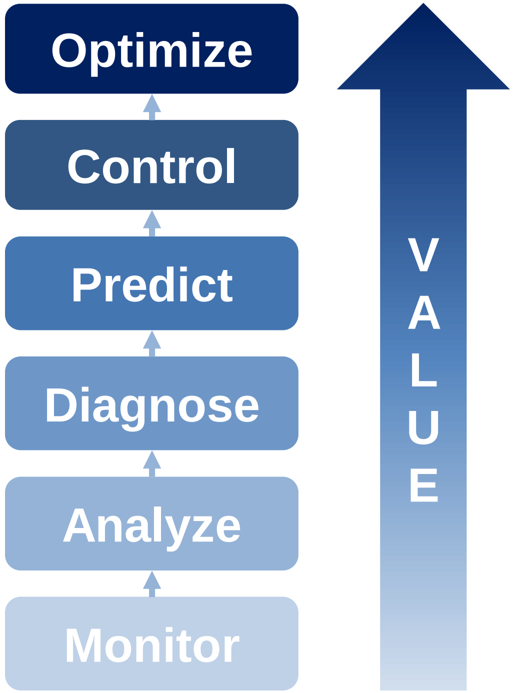




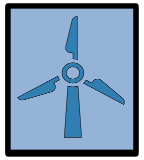
https://www.mathworks.com/cloud.html

Digital Twin





Create computational model of asset in operation



- Data-driven (MATLAB) or first-principles (Simulink) models
- Reuse models from development process (e.g. MBD)
- Kept up-to-date during asset operation (e.g. aging, wear, environment)

Use the computational model (digital twin) during operation

- Optimize fleet or system behavior
- Calculate control setpoints or parameters
- Predict future behavior or events

Reference example

Triplex Pump

1 *Fault Classification Using MATLAB*

kafka · Azure · kibana

Machine Learning fault classifier model ⟷ Visualization dashboard

- MATLAB
- Statistics & Machine Learning Toolbox
- MATLAB Production Server

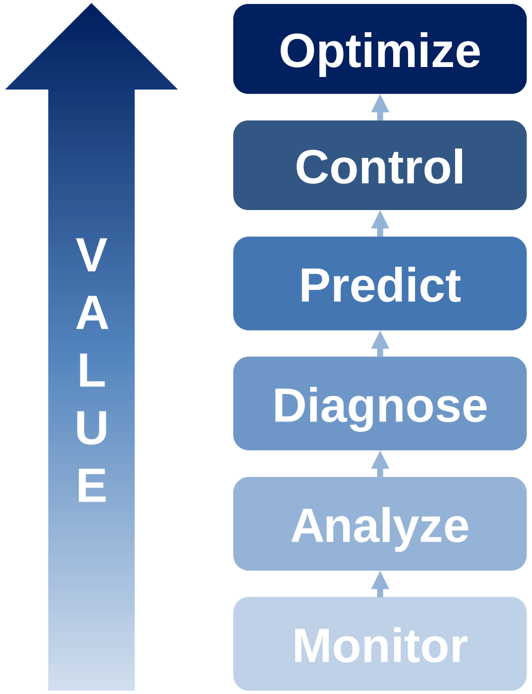
2 *"What-If" Analysis Using Simulink/Simscape Digital Twin*

Model tuned during operation ⟷ Parallel sims to explore scenarios

Azure Blob Storage · Windows · Azure

- Simulink/Simscape
- Simulink Design Optimization
- MATLAB Parallel Server

Research Connections



References

- [RD19] A. Rajhans and D. Lluch, "*A Digital Twin Approach to Online Monitoring in Industrial Internet of Things Applications*", Fourth International Workshop on Monitoring and Testing of Cyber-Physical Systems (MT-CPS 2019), part of CPS-IoT Week 2019

- Steve Miller (2019). Predictive Maintenance in Hydraulic Pump (https://www.mathworks.com/matlabcentral/fileexchange/65605-predictive-maintenance-in-hydraulic-pump), MATLAB Central File Exchange. Retrieved October 9, 2019.

- https://www.mathworks.com/cloud.html
- https://github.com/mathworks-ref-arch

In summary

- Cyber-physical systems continue to gain intelligence and autonomy
- CPS are open, interconnected, and change after deployment
- Formal specification and simulation-based approaches fill an important scalability gap w.r.t formal verification
- Model-Based Design approaches are being supplanted by model-based operation
- Scalability to enterprise-level system will be the value driver

Thank you!

- Thank you to the RV organizers, Leo, and Bernd
- Dagstuhl on Specification and Verification of CPS
- Jean-Francois Kempf, Khoo Yit Phang, Isaac Ito, and team
- Terri Xiao, Dan Lluch, Jim Tung, Pieter Mosterman, and team

MathWorks®

Accelerating the pace of engineering and science