INL/CON-24-78339-Revision-0

MFANS 2024 - Formally Proving Characteristics of Cyber-Physical Systems

April 2024

Changing the World's Energy Future

Daniel George Cole

Idaho National Laboratory

INL/CON-24-78339-Revision-0

MFANS 2024 - Formally Proving Characteristics of Cyber-Physical Systems

Daniel George Cole

April 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Formally proving characteristics of cyber-physical systems

Daniel G. Cole, Ph.D., P.E.

Associate Professor, University of Pittsburgh

Director, Cyber Energy Center

Faculty Researcher, Idaho National Laboratory

29 April 2024

Mathematically Formalized Assurance for National Security

Energy | Data Privacy | Regulatory Oversight | Governance | Grid & Infrastructure

US electric grid growing more vulnerable to cyberattacks, regulator says

By Laila Kearney

April 4, 2024 5:48 PM EDT · Updated 11 days ago

https://www.reuters.com/

TECH + ENGINEERING

Cyber Attack on German Steel Mill Leads to 'Massive' Real World Damage

A steel mill in Germany lost control of its blast furnace. Hackers had infiltrated the mill's control system, according to the German government's office for information security.

BY R.A. BECKER THURSDAY, JANUARY 8, 2015 NOVA NEXT

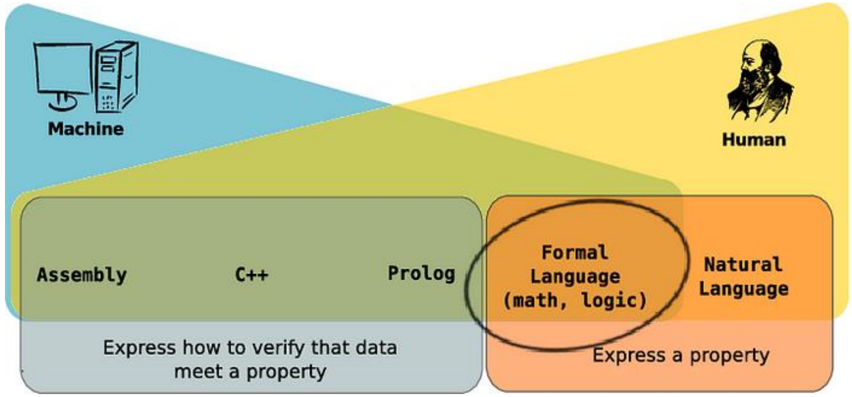
https://www.pbs.org/wgbh/nova/

For cyber systems, formal methods refer to rigorous techniques to specify, analyze, and verify software and hardware systems

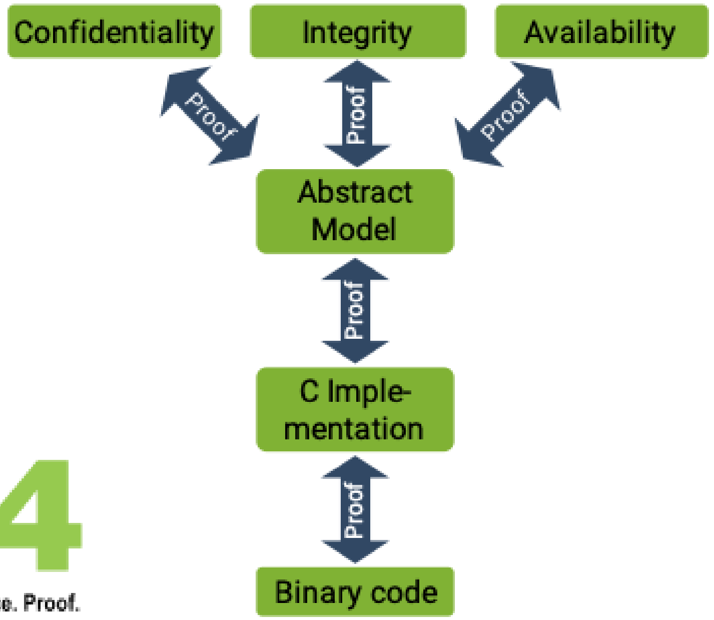
```
definition policy_wellformed where
  "policy_wellformed aag maySendIrqs irqs agent \<equiv>
     (\<forall>agent'. (agent, Control, agent') \<in> aag \<longrightarrow> agent = agent')
   \<and> (\<forall>a. (agent, a, agent) \<in> aag)
   \<and> (\<forall>s r ep. (s, Grant, ep) \<in> aag \<and> (r, Receive, ep) \<in> aag
               \<longrightarrow> (s, Control, r) \<in> aag \<and> (r, Control, s) \<in> aag)
   \<and> (maySendIrqs \<longrightarrow> (\<forall>irq ntfn. irq \<in> irqs \<and> (irq, Notify, ntfn) \<in> aag
                                  \<longrightarrow> (agent, Notify, ntfn) \<in> aag))
   \<and> (\<forall>s ep. (s, Call, ep) \<in> aag \<longrightarrow> (s, SyncSend, ep) \<in> aag)
   \<and> (\<forall>s r ep. (s, Call, ep) \<in> aag \<and> (r, Receive, ep) \<in> aag \<longrightarrow> (r, Reply, s) \<in> aag)
   \<and> (\<forall>s r. (s, Reply, r) \<in> aag \<longrightarrow> (r, DeleteDerived, s) \<in> aag)
   \<and> (\<forall>l1 l2 l3. (l1, DeleteDerived, l2) \<in> aag \<longrightarrow> (l2, DeleteDerived, l3) \<in> aag
                 \<longrightarrow> (l1, DeleteDerived, l3) \<in> aag)
   \<and> (\<forall>s r ep. (s, Call, ep) \<in> aag \<and> (r, Receive, ep) \<in> aag \<and> (r, Grant, ep) \<in> aag
               \<longrightarrow> (s, Control, r) \<in> aag \<and> (r, Control, s) \<in> aag)"
```

https://github.com/seL4/l4v/blob/master/proof/access-control/Access.thy

Coq



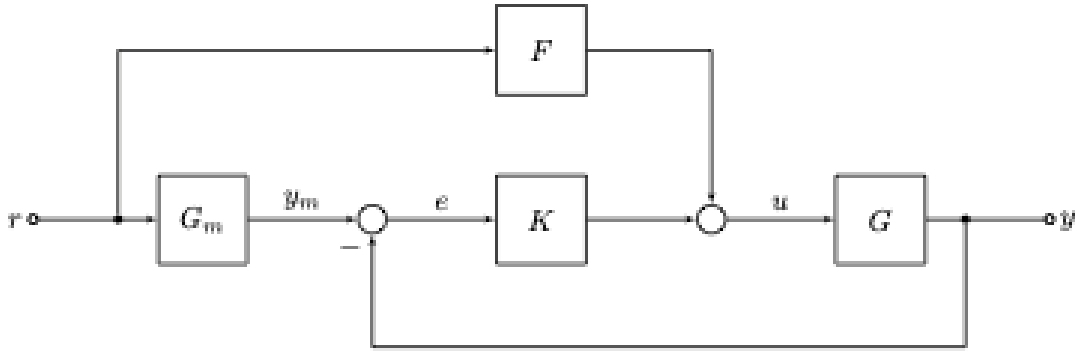
https://pratyaymondal.medium.com/formal-language-ee89efc44b52



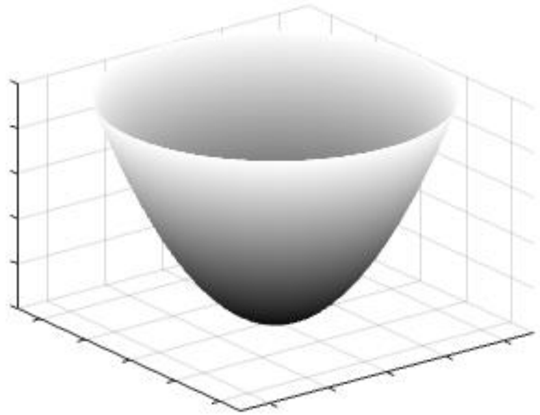
Security. Performance. Proof.

https://sel4.systems/About/seL4-whitepaper.pdf

For physical systems, dynamic and control theory has a history of using rigorous analytic techniques to prove functional correctness



Classical controls



Lyapunov theory

$$\dot{x} = Ax + Bu$$
$$y = Cx + Du$$
$$u = Kx$$

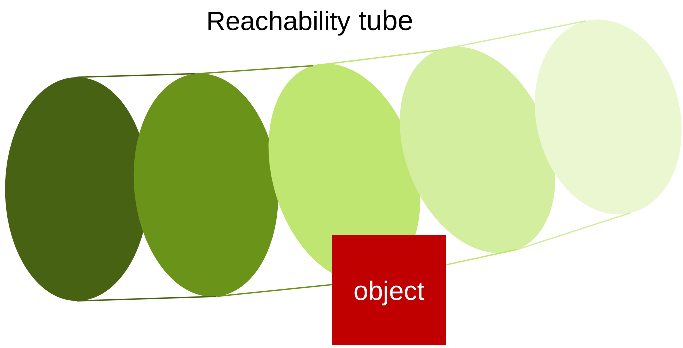
Modern controls

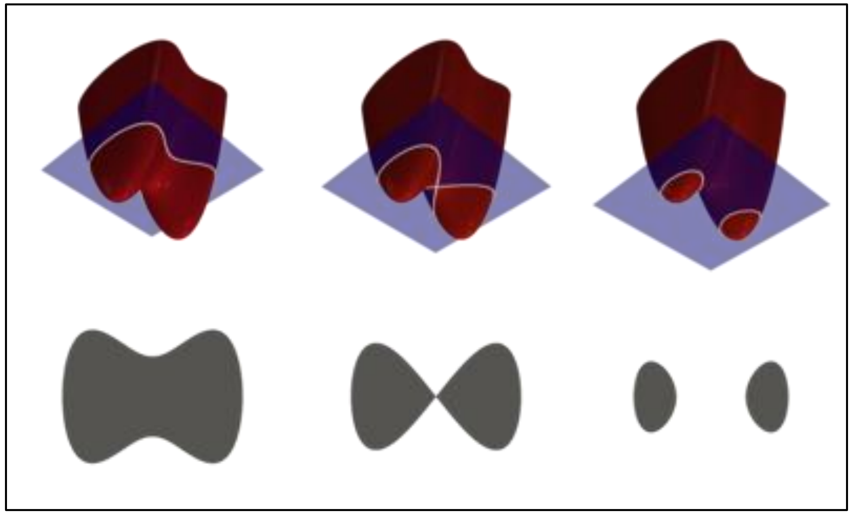
uncertainty $\quad G_t = G(1 + W_2\Delta), \quad \|\Delta\| < 1$

performance $\quad \left\| \begin{matrix} W_1 S \\ W_2 T \end{matrix} \right\| < \gamma$

Robust controls

Recent computational techniques like level-set theory and reachability analysis can assert that a system's state will avoid unsafe regions





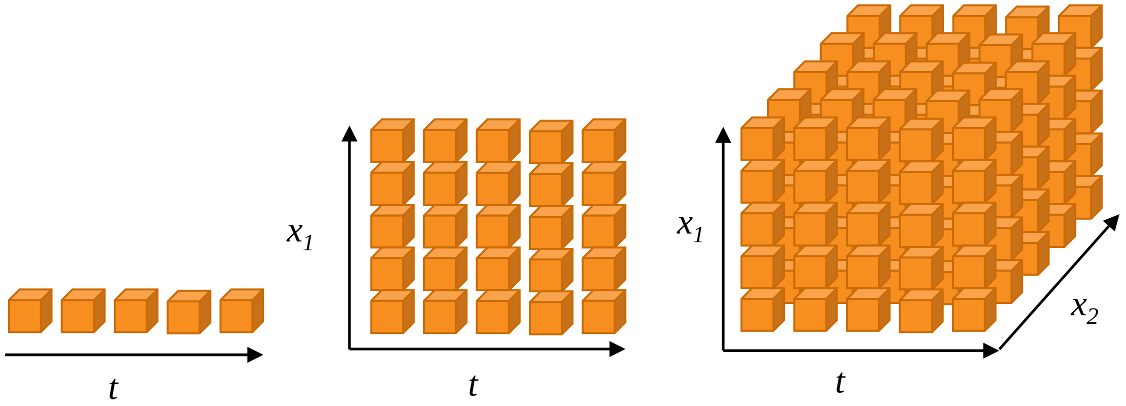
https://en.wikipedia.org/wiki/Level-set_method

$$\frac{\partial V}{\partial t} + \min_u \{f(x,t) \cdot \nabla V(x,t)\} = 0$$

final condition $\quad V(x(T),T) = D[x]$

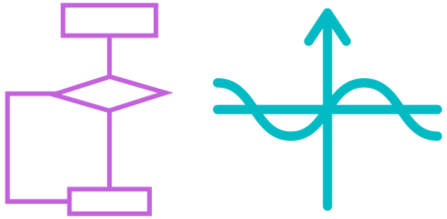
$$u^* = \min_u \{f(x,t) \cdot \nabla V(x,t)\}$$

Limitation: curse of dimensionality

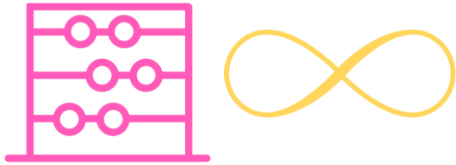


The integration of cyber and physical systems creates new challenges

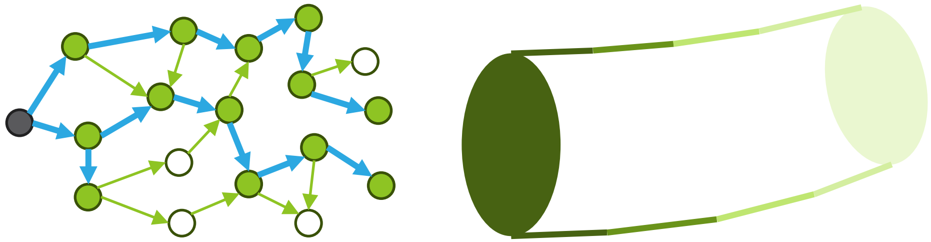
Discrete v. continuous time



Logic v. diff-eq based

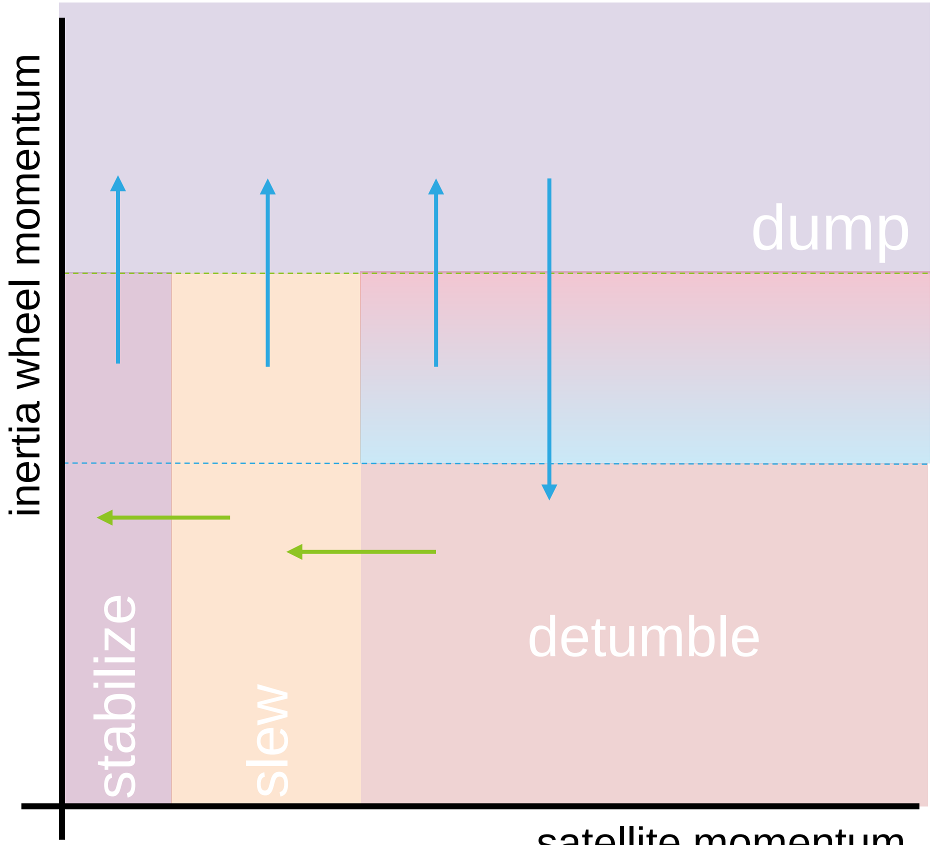


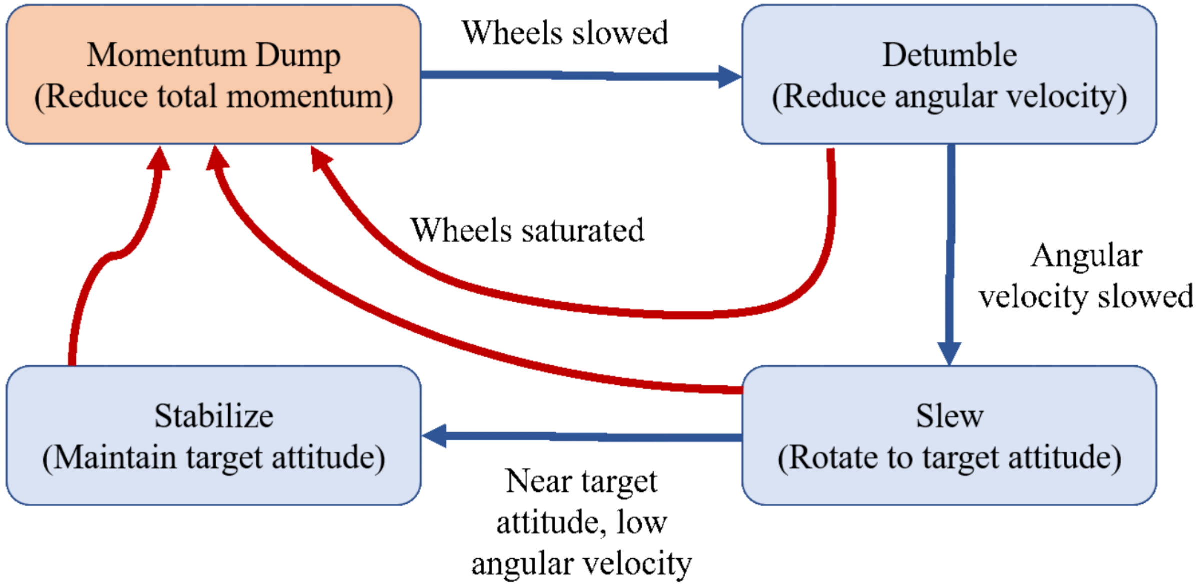
Finite v. infinite states



Model checking v. reachability

Satellites must manage the angular velocity of the satellite and the inertia wheels. Modes have different control laws, making it hybrid.

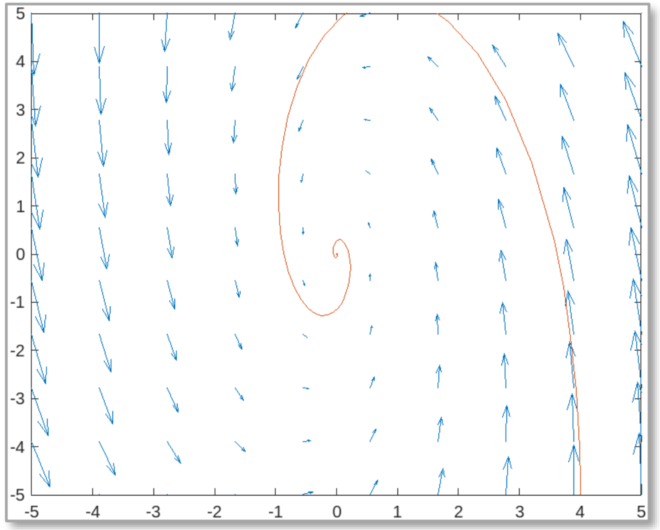




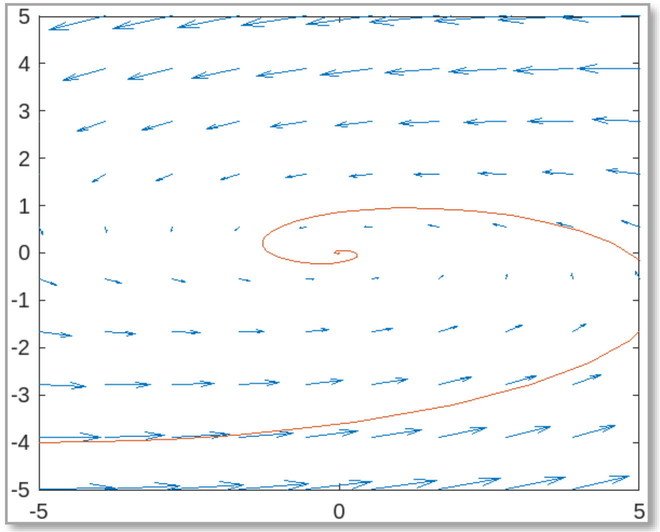
Idaho National Laboratory

Hybrid (switching) systems can result in unstable behavior even though the sub-systems are stable

stable, same eigenvalues

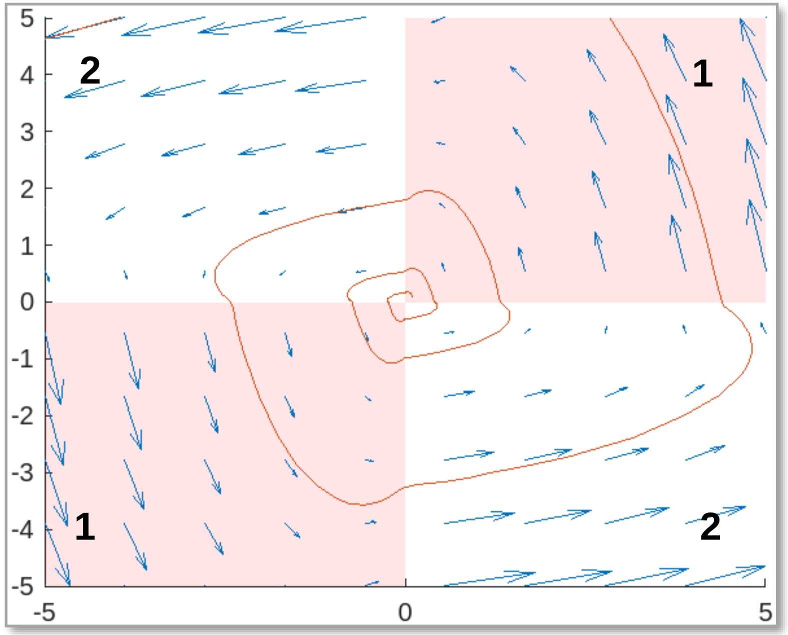


System 1

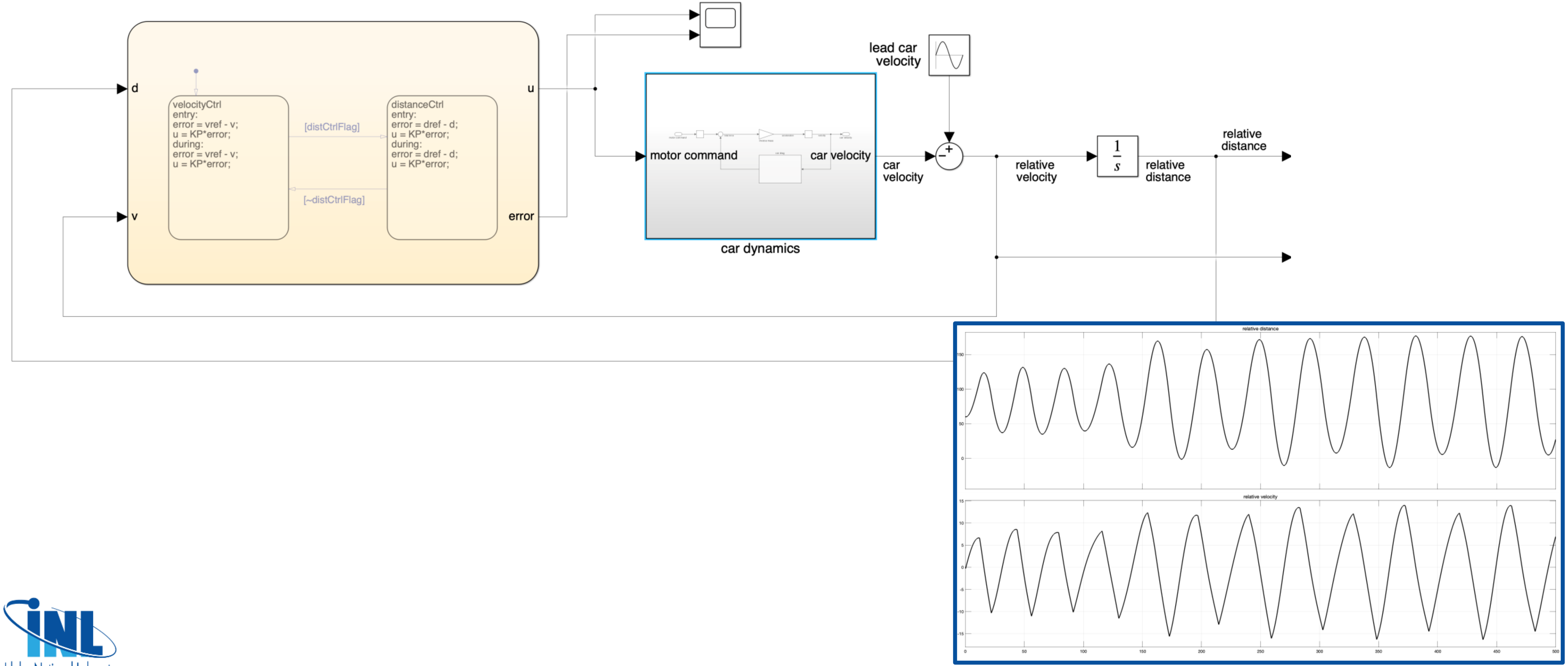


System 2

switched system



While it is possible to simulate hybrid systems, this provides only a demonstration of a performance and not proof



For hybrid systems, current formal methods and system analysis approaches require a workarounds to work on hybrid systems like CPS

Tool	Technique	Dynamics	Model Format
Level Set Toolbox	HJB PDEs	Nonlinear	MATLAB
Flow*	Taylor Models	Nonlinear hybrid	Flow*
CORA	Zonotypes	Linearization	MATLAB
C2E2	Simulated trajectories	Nonlinear hybrid	XML model
dReach	SMT solver	Nonlinear hybrid	dReach
CoCoSim	SMT solver	Linear hybrid	Simulink
KeYmaera X	DDL	Hybrid	KeYmaera X

Idaho National Laboratory

Research directions

- Systems analysis of hybrid systems
  - We need to close the gap between modeling and the capabilities of reachability for hybrid systems
  - We need standard methods to analyze stability, performance, and robustness for hybrid systems
  - The methods of reachability do not directly relate to specifications
- Curse of dimensionality
  - Approximate dynamic programming has strategies for the curse of dimensionality
  - The state-space can be reduced by analyzing components and then applying to the composite system
- Stochastic hybrid systems analysis

Formally proving characteristics of cyber-physical systems

Daniel G. Cole, Ph.D., P.E.

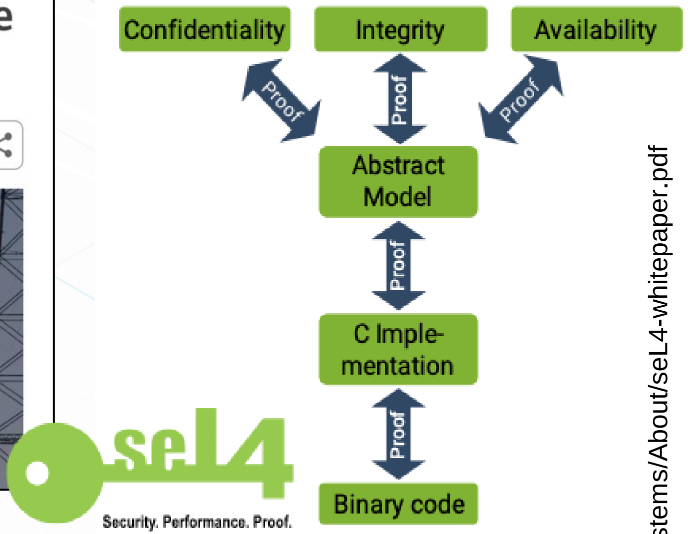
Associate Professor, University of Pittsburgh

Director, Cyber Energy Center

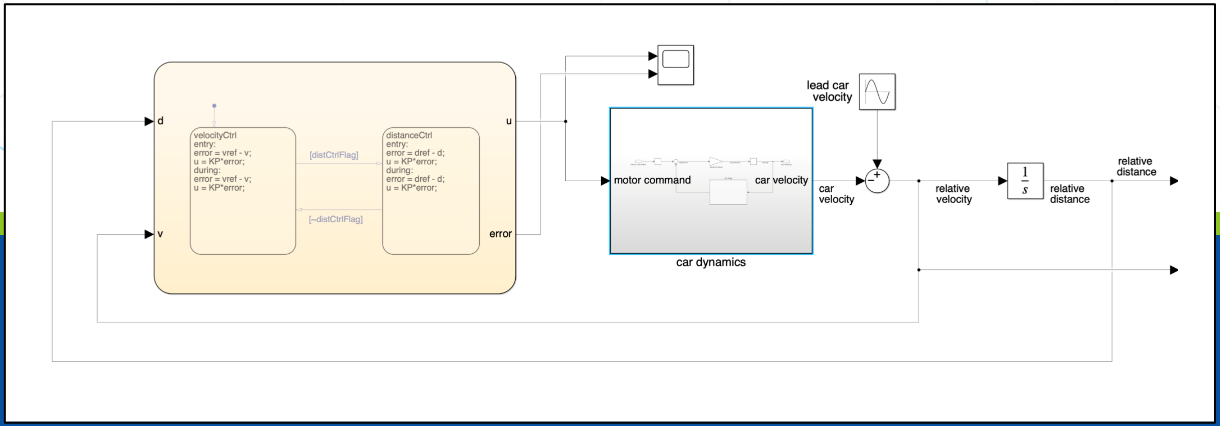
Faculty Researcher, Idaho National Laboratory

dgcole@pitt.edu

https://www.reuters.com/



https://sel4.systems/About/seL4-whitepaper.pdf



Idaho National Laboratory

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.