Building Trusted Systems from Untrusted Components

Bruce Krogh
Professor Emeritus of Electrical and Computer Engineering
SEI Research Staff

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0392

CMU Software Engineering Institute (SEI)

Federally funded research and development center (FFRDC) operated by Carnegie Mellon University.

Software Systems Division (SSD)

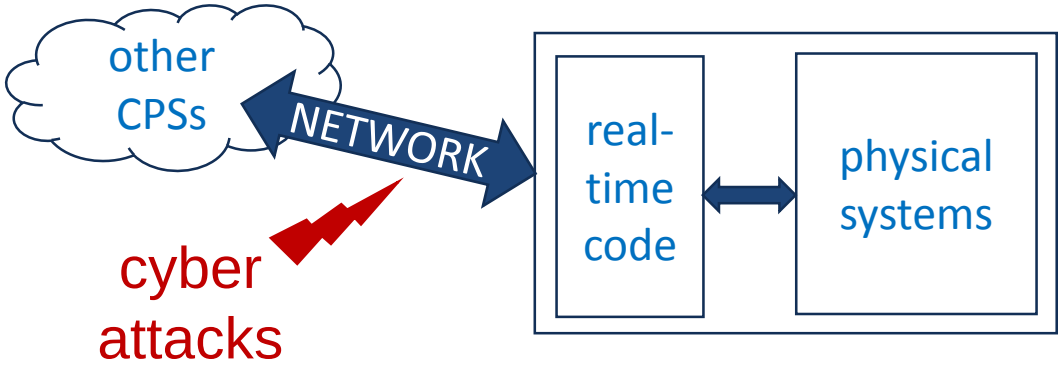
- Empowers the Department of Defense (DoD) to use software as a strategic advantage

Critical System Capabilities Directorate

- Focus: Complex autonomous systems
- Objective: Get unproven innovations into the field rapidly safely
- Projects:
  - Run-time enforcers for safe adaptation of AI/ML systems
  - IoT security framework to integrate untrusted devices

Today's Talk:
Security of Cyber-Physical Systems (CPS)

https://www.richardsilverstein.com/2010/11/22/iaea-inspectors-stuxnet-mayve-shut-down-iranian-enrichment-program//



https://www.sentryo.net/cyberattack-on-a-german-steel-mill/

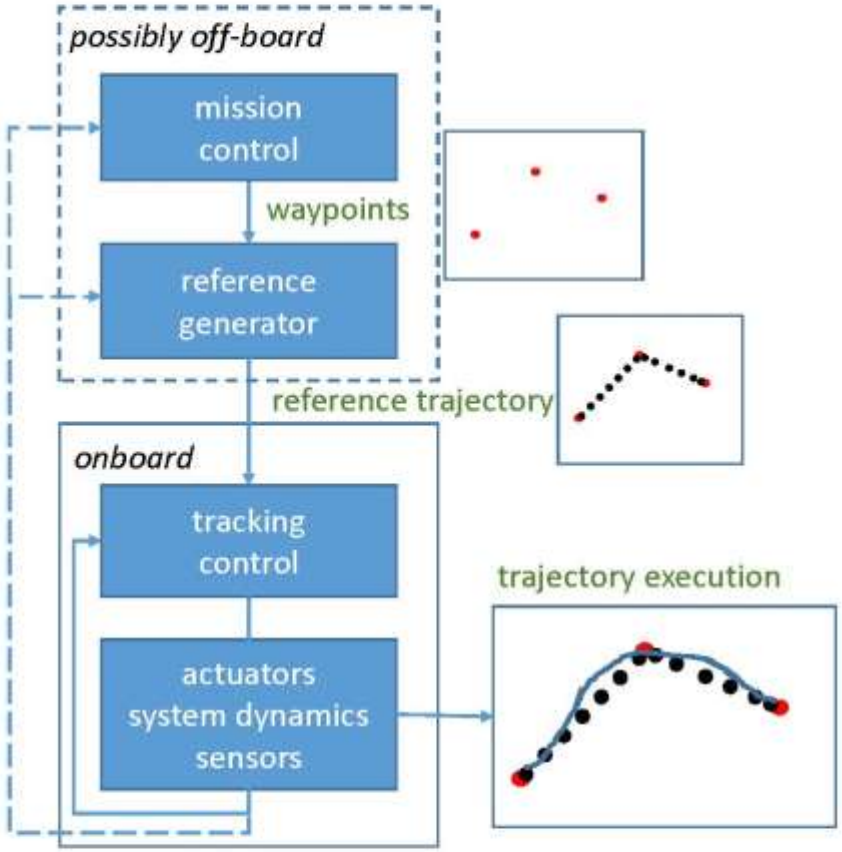
https://phys.org/news/2016-01-cyberattack-ukraine-power-grid.html//

Target CPS Application: Motion Control

store.dji.com

https://thestack.com/iot/2018/06/08/autonomous-vehicles-pedestrians-cities/

Motion Control Hierarchical



Why do you have to reboot your computers?

How-To Geek NEWS FEATURES SMART HOME REVIEWS CATEGORIES SUBSCRIBE

Why Restarting Your Phone Makes it Perform Better and Fixes Common Issues

CAMERON SUMMERSON @summerson
MAY 18, 2018, 9:00AM EDT

https://www.howtogeek.com/352460/why-restarting-your-phone-makes-it-perform-better-and-fixes-common-issues/

Small Business » Business Technology & Customer Support » Computers »

Reasons to Reboot Your Computer Nightly

by Thomas McNish

Turning off your computer at night has an obvious benefit: it saves electricity, which saves you money. Rebooting your computer, on the other hand, has less obvious benefits. Most laptops have the ability to go into sleep mode, which makes it easier to skip rebooting. Even though improved operating systems and more efficient computers have made rebooting less necessary, it still has advantages.

https://smallbusiness.chron.com

Why don't they just write code that will keep working?!

Software Rejuvenation: Periodically Reboot Automatically

Original proposal

Y. Huang, C. Kintala, N. Kolettis, and N.D. Fulton. Software rejuvenation: Analysis, module and applications. In Proceedings of 25th International Symposium on Fault Tolerant Computing, June 1995.

United States Patent
Gross et al.

(10) **Patent No.: US 7,100,079 B2**
(45) **Date of Patent: Aug. 29, 2006**

METHOD AND APPARATUS FOR USING PATTERN-RECOGNITION TO TRIGGER SOFTWARE REJUVENATION

Inventors: **Kenny C. Gross**, San Diego, CA (US); **Kishor S. Trivedi**, Durham, NC (US)

Assignee: **Sun Microsystems, Inc.**, Santa Clara, CA (US)

Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 571 days.

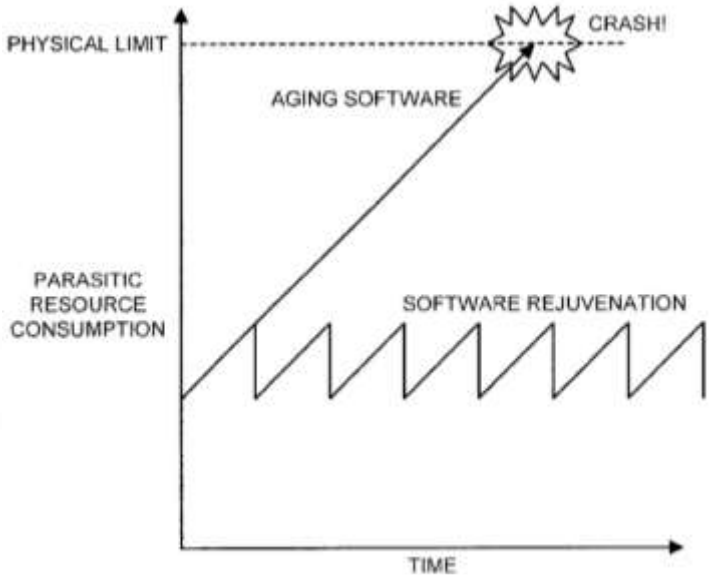
Appl. No.: **10/277,445**

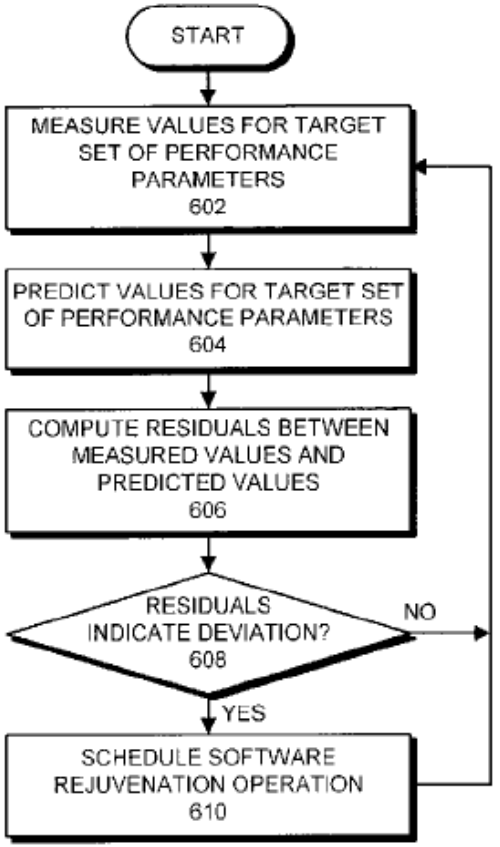
Filed: **Oct. 22, 2002**

Prior Publication Data

US 2004/0078657 A1 Apr. 22, 2004

Int. Cl.
G06F 11/00 (2006.01)
U.S. Cl. **714/23**; 714/47
Field of Classification Search 714/15, 714/23, 47
See application file for complete search history.





Software Rejuvenation for Secure CPS

United States
Patent Application Publication
ARROYO et al.

SECURED CYBER-PHYSICAL SYSTEMS

Applicants: **Miguel A. ARROYO**, New York, NY (US); **Lakshminarasimhan SETHUMADHAVAN**, New York, NY (US); **Jonathan WEISZ**, New York, NY (US)

Inventors: **Miguel A. ARROYO**, New York, NY (US); **Lakshminarasimhan SETHUMADHAVAN**, New York, NY (US); **Jonathan WEISZ**, New York, NY (US)

Assignee: **The Trustees of Columbia University in the City of New York**, New York, NY (US)

Appl. No.: **15/618,019**

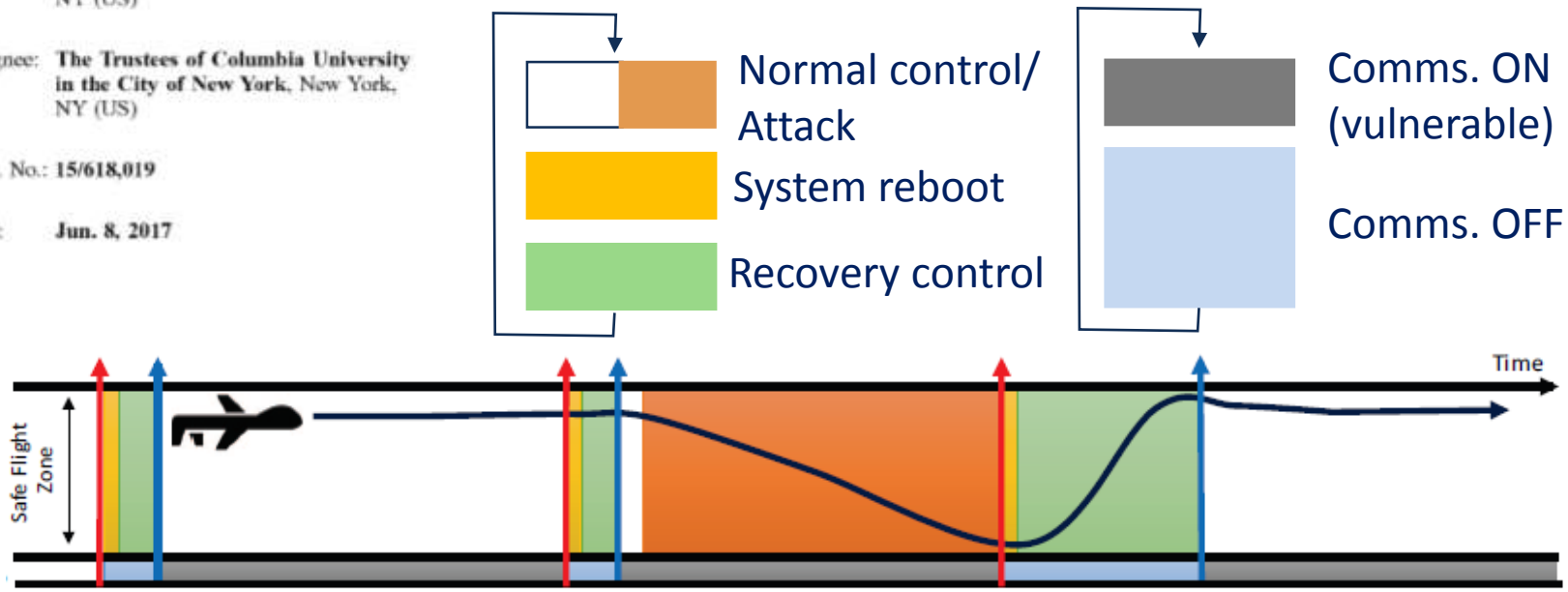
Filed: **Jun. 8, 2017**

- reboot to eliminate code/data changes from undetectable cyber attacks
- must reboot before attack could cause disaster

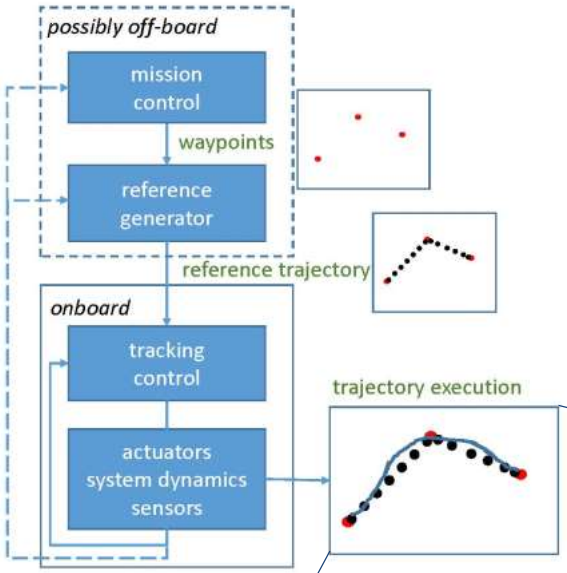
2018 9th ACM/IEEE International Conference on Cyber-Physical Systems

Guaranteed Physical Security with Restart-Based Design for Cyber-Physical Systems

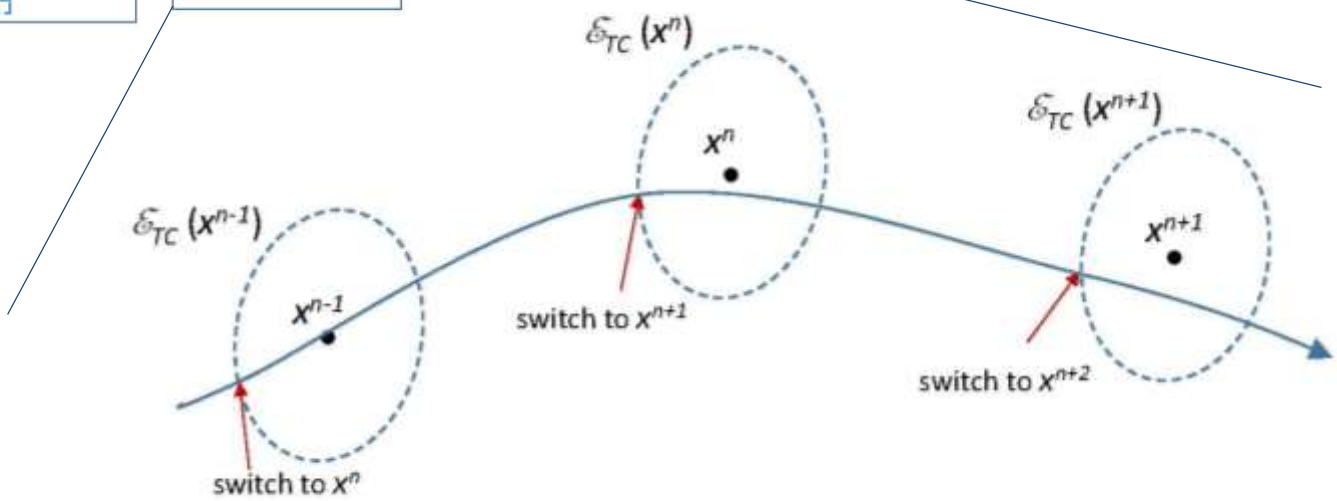
Fardin Abdi*, Chien-Ying Chen*, Monowar Hasan*, Songran Liu†, Sibin Mohan*, and Marco Caccamo*
*Department of Computer Science, University of Illinois at Urbana-Champaign, USA
{abditag2, cchen140, mhasan11, sibin, mcaccamo}@illinois.edu
†School of Computer Science and Engineering, Northeastern University, China



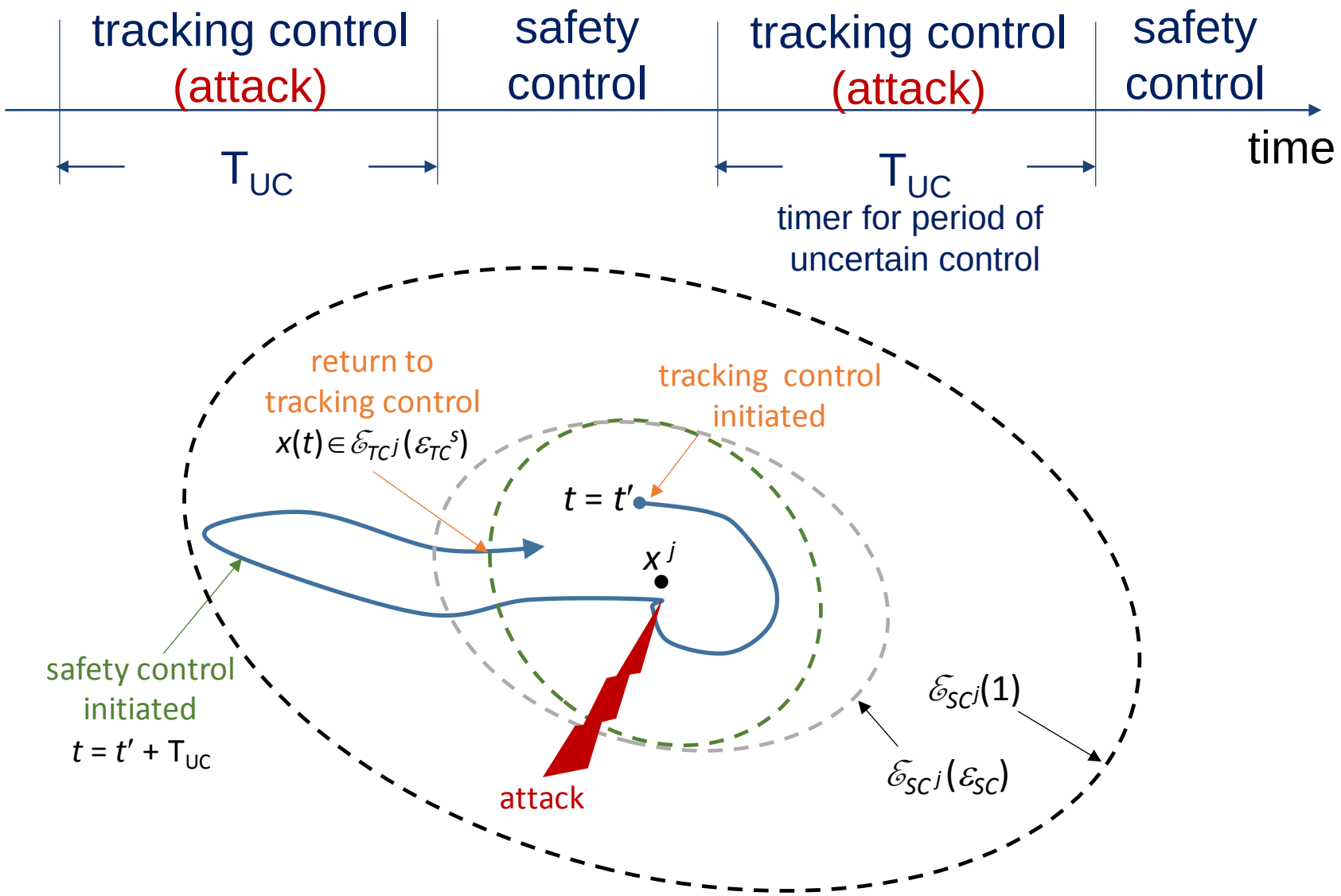
Tracking Control



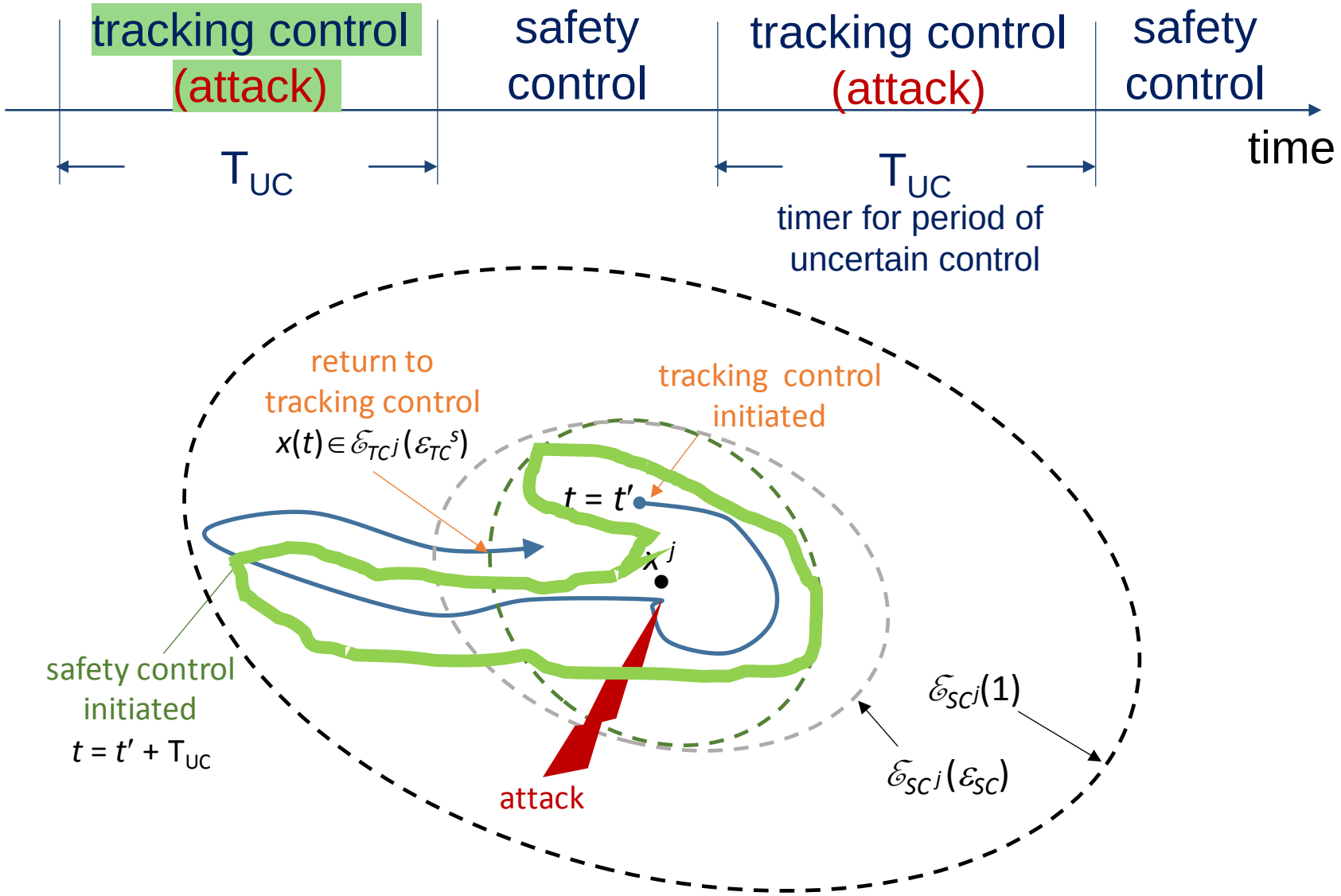
- design feedback controller to drive the system to a reference point
- switch reference points as the system is moving
- have reference points close enough to make switching viable



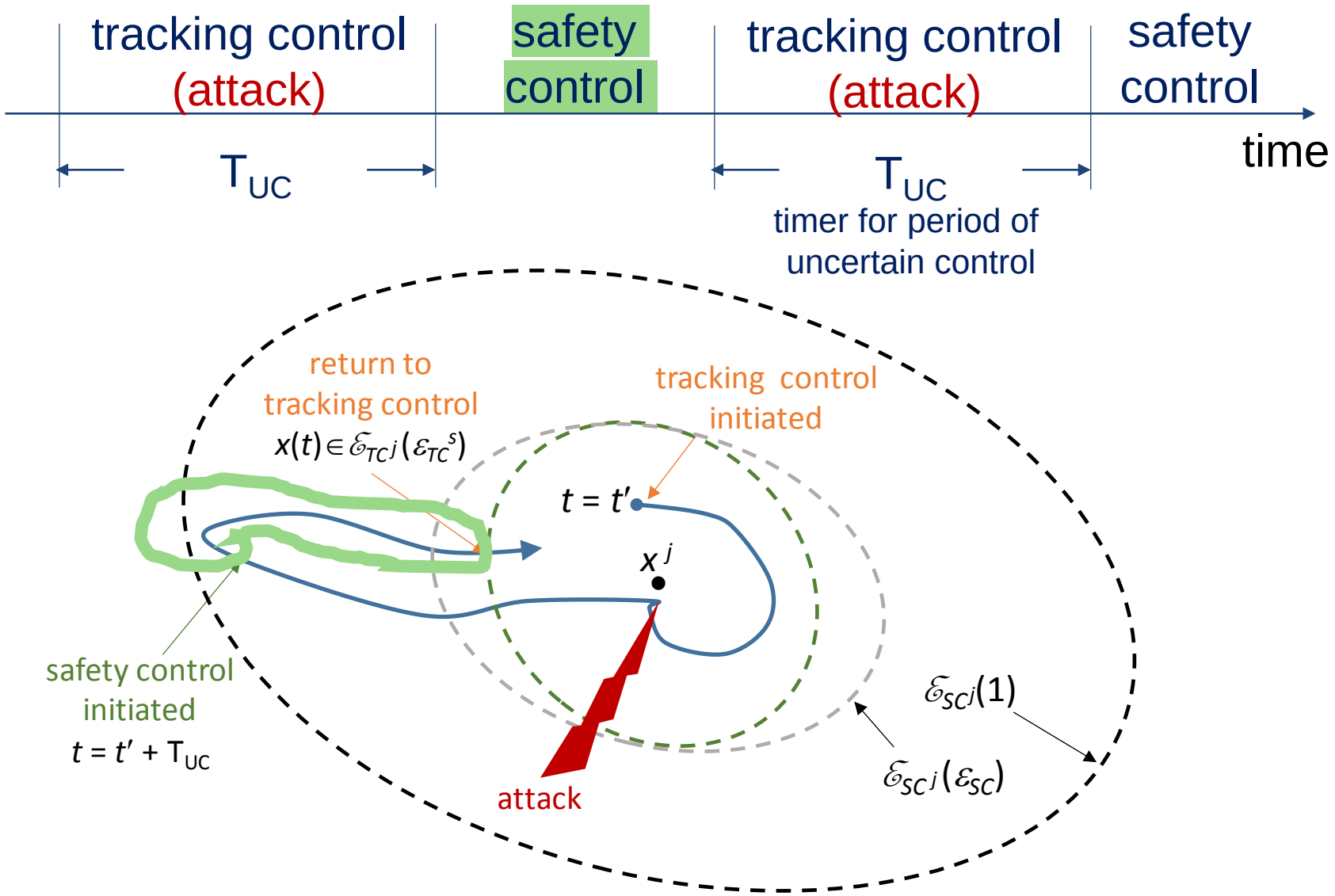
Safety Control



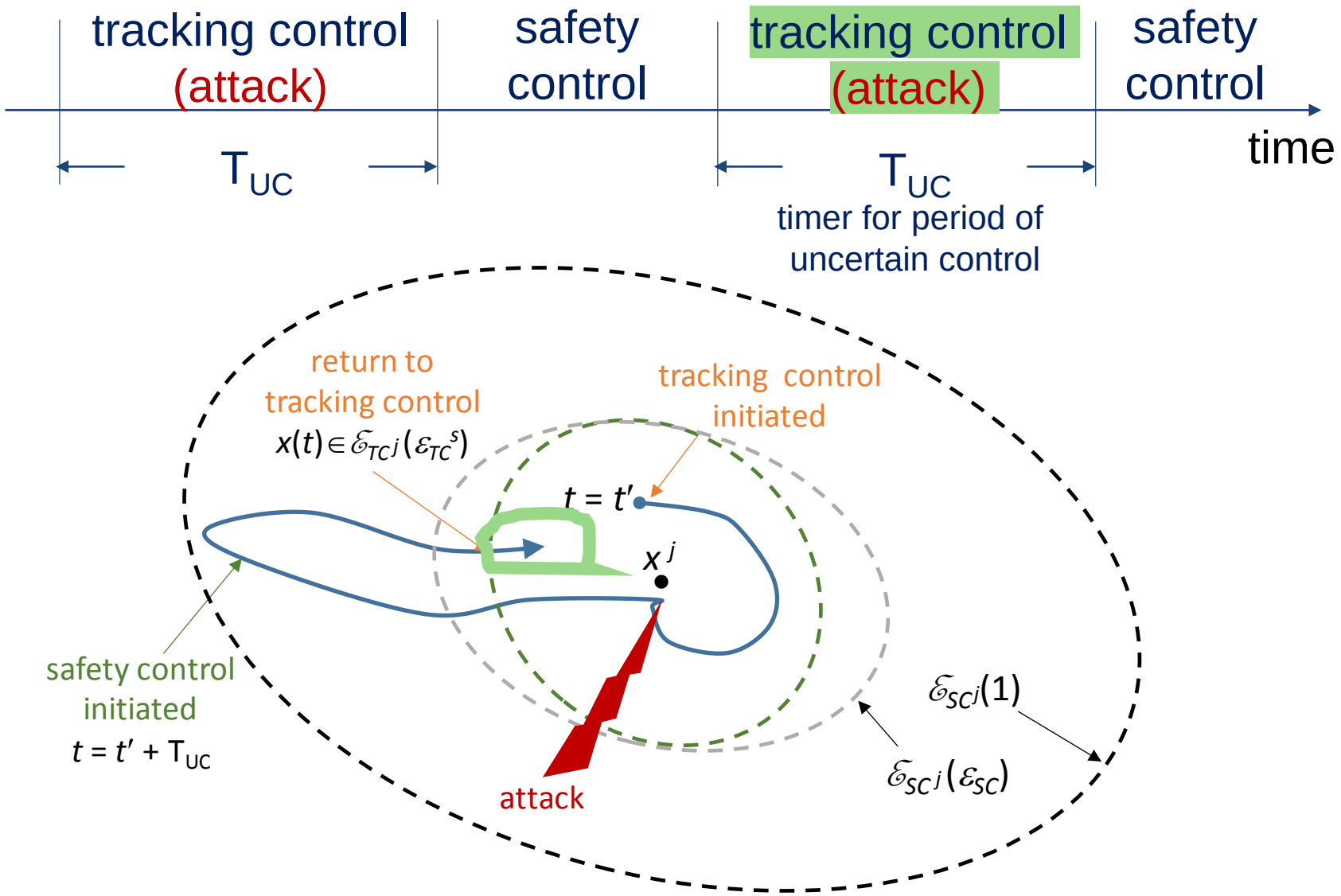
Safety Control



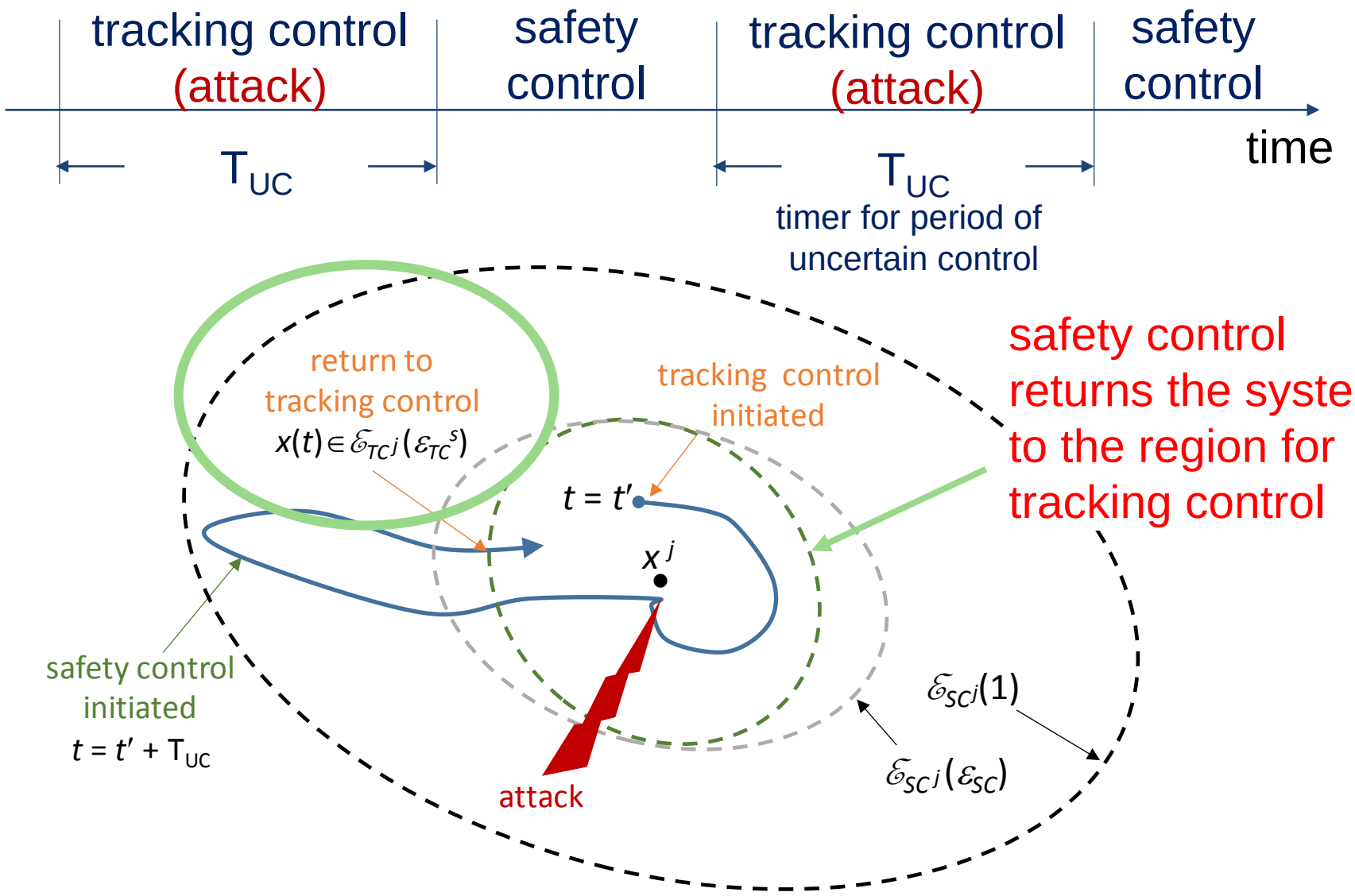
Safety Control



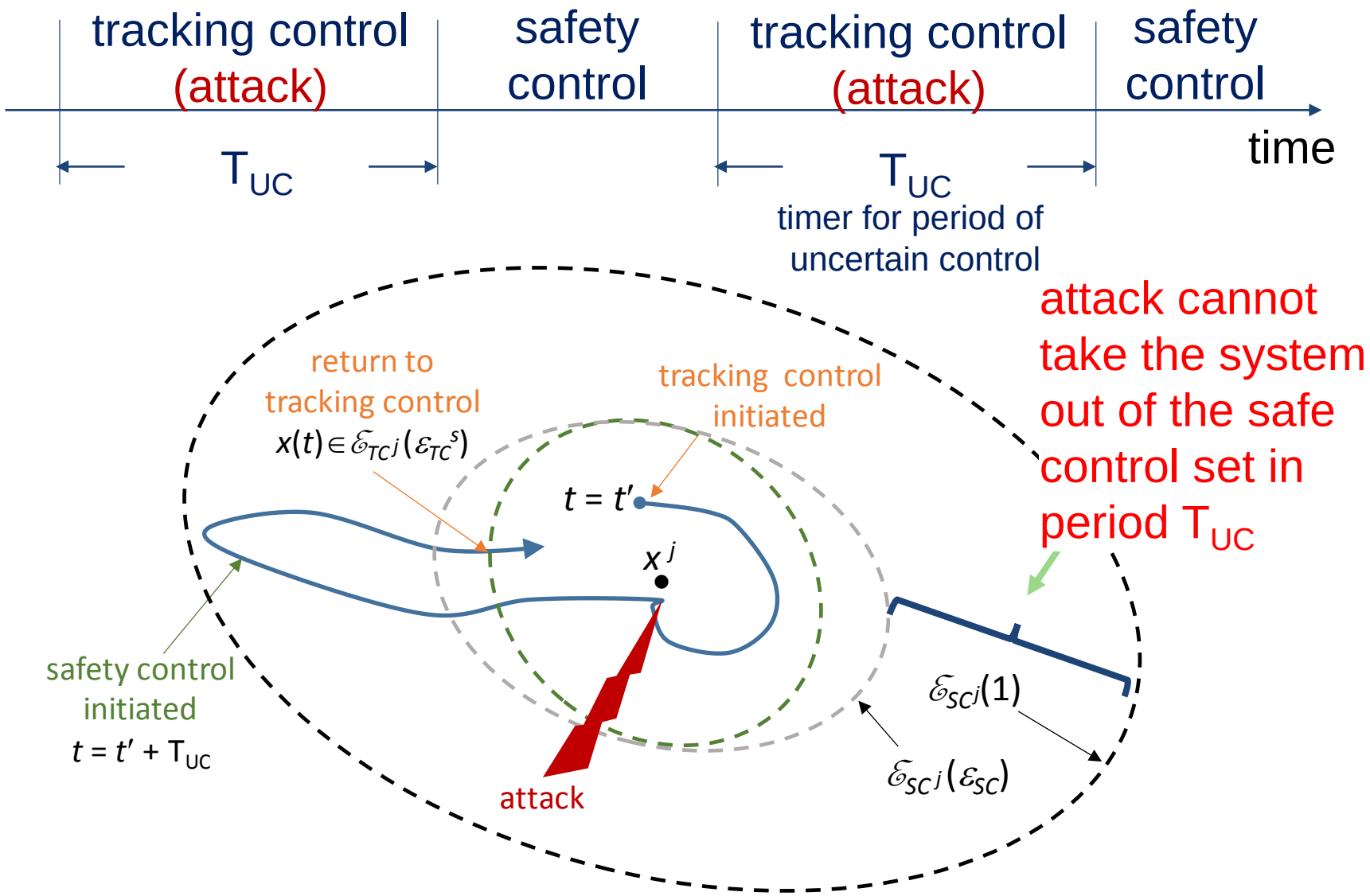
Safety Control



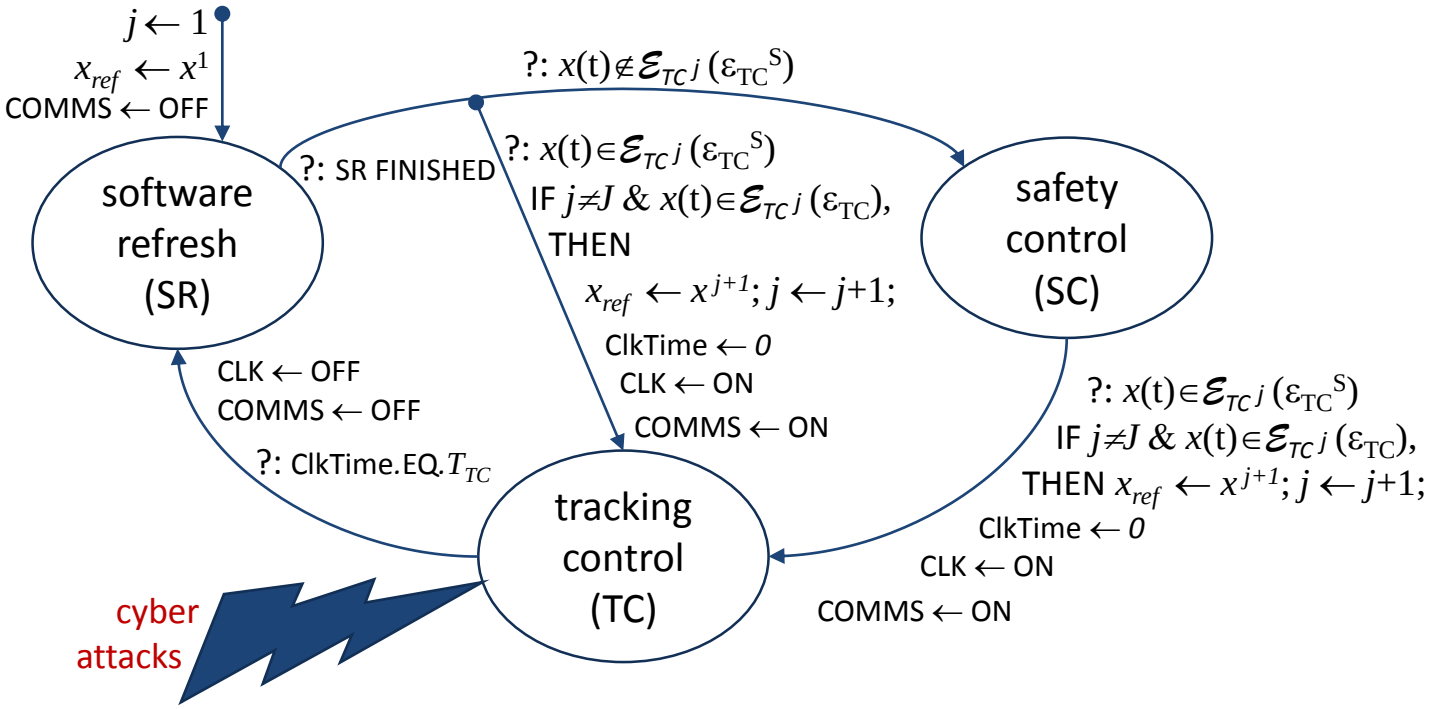
Safety Control



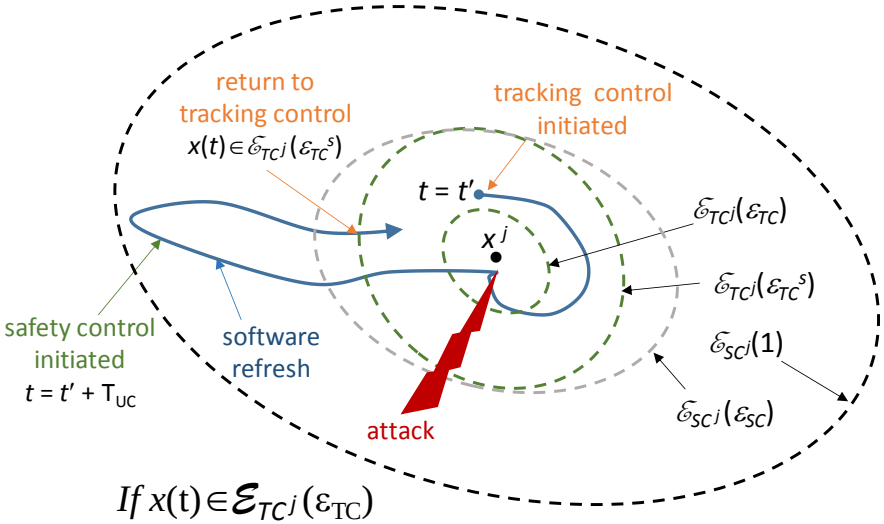
Safety Control

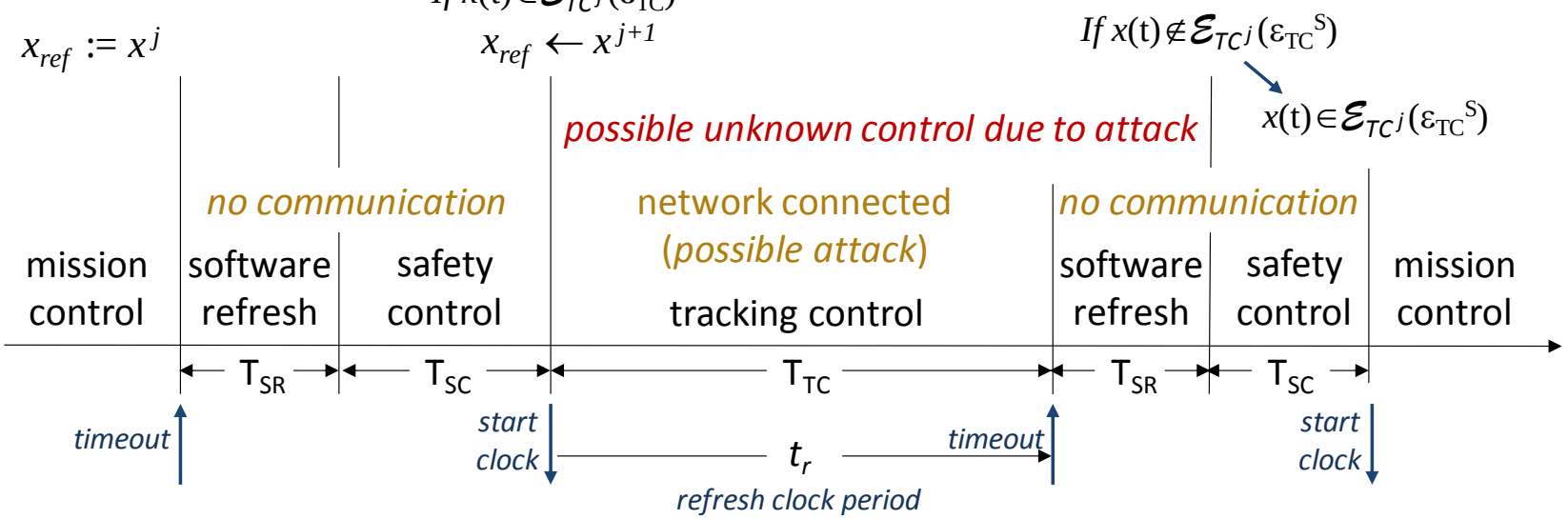


Software-Rejuvenation Control Modes

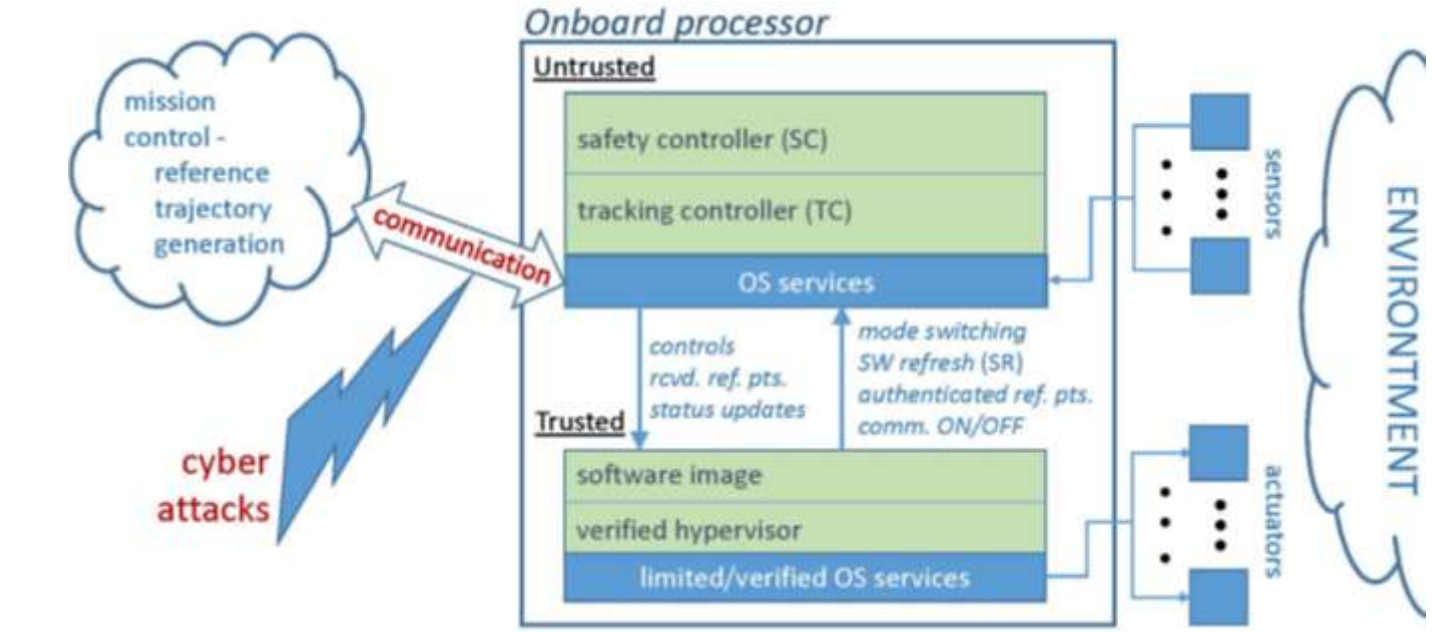


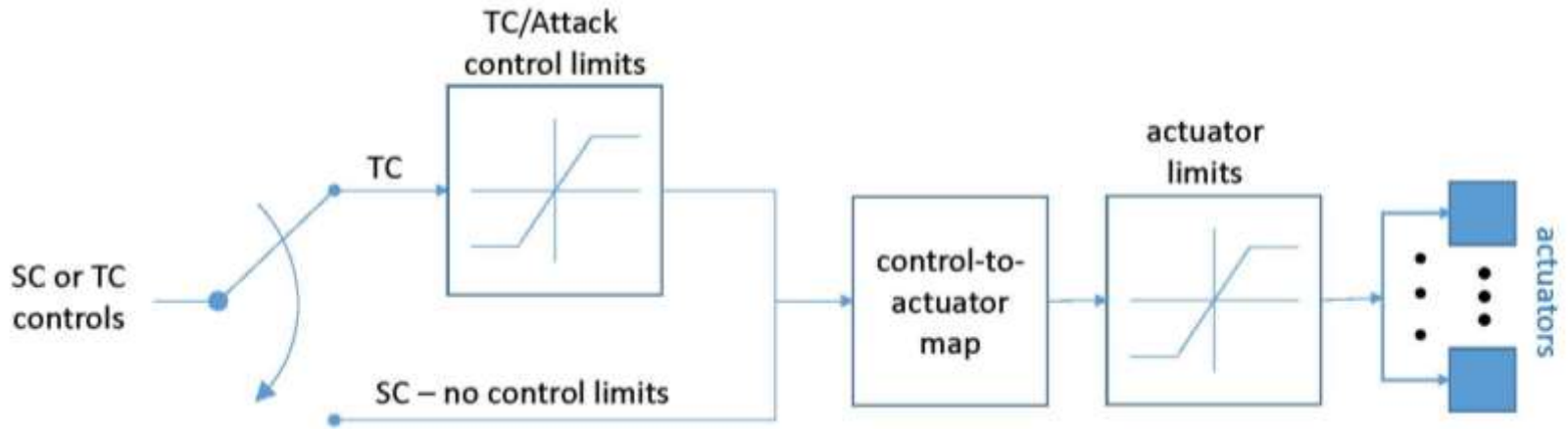
Software Rejuvenation for Tracking Control Systems: Combines Safety & Tracking Control





Implementation Architecture





Application of control theory for nonlinear systems

- Lyapunov functions & invariant sets used to find
  - safe region for safety control
  - maximum time required for safety control
  - attraction and switching regions for tracking control
- Reachability analysis use for
  - maximum time allowed for uncertain control (T_{UC})
- Proofs of algorithm guarantees
  - safety: the system always returned safely to tracking control, even if there are undetectable cyber attacks
  - liveness: if there are no cyber attacks, tracking control always progresses through the reference points

More Clearly …

$$\dot{x} = f(x, u), \tag{1}$$

$$\dot{x} = f_\varphi(x) \triangleq f(x, \varphi(x)), \tag{6}$$

and $x(t; x_0, \varphi)$ will denote the solution to (6) with initial condition $x(0) = x_0$. The set of states that are reachable for

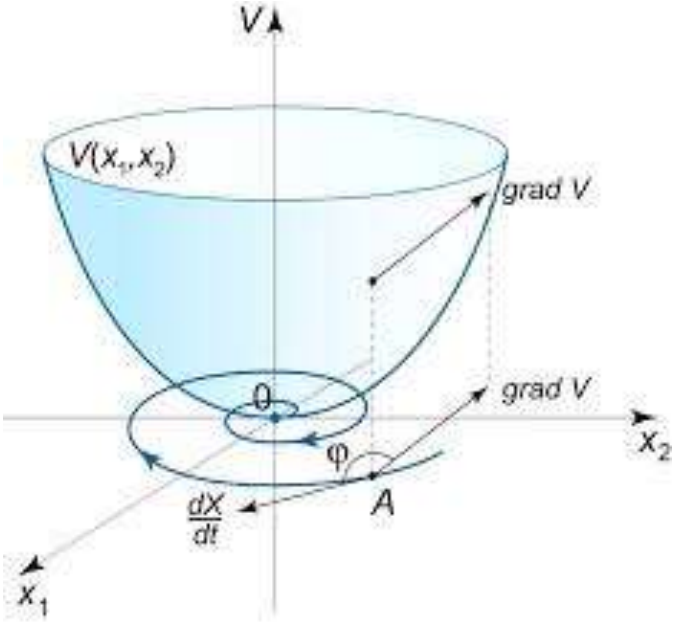
Suppose $V_\varphi : \mathbb{R}^n \to \mathbb{R}$ is a Lyapunov function for (6) in a neighborhood of x_{eq} denoted by $\mathcal{N}_{V_\varphi}(x_{eq}) \subseteq \mathcal{N}_\varphi(x_{eq})$, where $V_\varphi(x_{eq}) = 0$ and $\forall x \in \mathcal{N}_{V_\varphi}(x_{eq}) - \{x_{eq}\}$: (i) $V_\varphi(x) > 0$; and (ii)

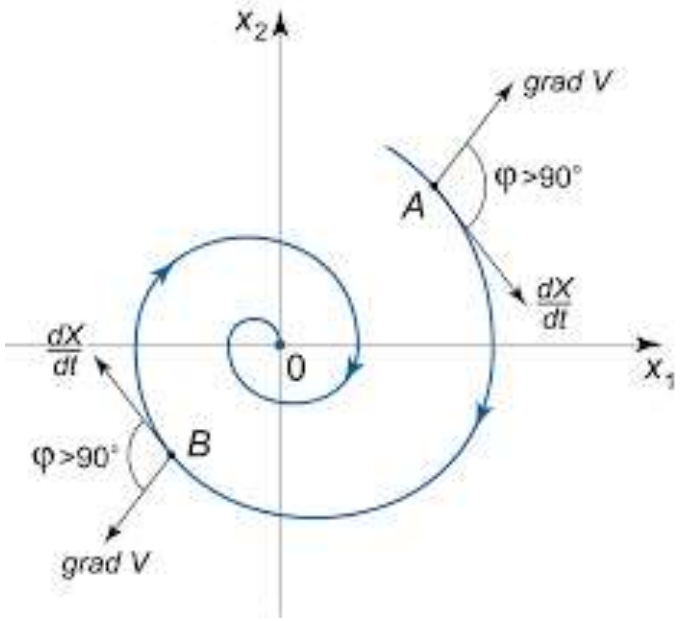
$$\dot{V}_\varphi(x) = \frac{\partial V}{\partial x} \cdot f_\varphi(x) < 0.$$

Then, $\forall\ x_0 \in \mathcal{N}_{V_\varphi}(x_{eq})$, $V_\varphi(x(t; x_0, \varphi) \downarrow_{t \to \infty} 0$, which implies $\lim_{t \to \infty} x(t; x_0, \varphi) = x_{eq}$.

Lyapunov functions

https://www.math24.net/method-lyapunov-functions/





$$\dot{V}_\varphi(x) = \frac{\partial V}{\partial x} \cdot f_\varphi(x) < 0.$$

Then, $\forall\ x_0 \in \mathcal{N}_{V_\varphi}(x_{eq})$, $V_\varphi(x(t; x_0, \varphi) \downarrow_{t\to\infty} 0$, which implies $\lim_{t\to\infty} x(t; x_0, \varphi) = x_{eq}$.

Invariants and Contraction

Proposition 2.1: Given system (1) with stabilizing controller φ for equilibrium state $(x_{eq}, \varphi(x_{eq}))$ and Lyapunov function $V_\varphi(x)$ as defined above, given $\epsilon > 0$ for any $\epsilon < \epsilon' \leq 1 \; \exists \; \gamma > 0 \; \ni \forall \; t \geq (\epsilon' - \epsilon)\gamma^{-1}$,

$$\mathcal{R}(t; \mathcal{E}_\varphi(\epsilon'), \varphi) \subseteq \mathcal{E}_\varphi(\epsilon). \tag{10}$$

Lyapunov Functions - implication

Proposition 2.1: Given system (1) with stabilizing controller φ for equilibrium state $(x_{eq}, \varphi(x_{eq}))$ and Lyapunov function $V_\varphi(x)$ as defined above, given $\epsilon > 0$ for any $\epsilon < \epsilon' \leq 1 \; \exists \; \gamma > 0 \; \ni \forall \; t \geq (\epsilon' - \epsilon)\gamma^{-1}$,

$$\mathcal{R}(t; \mathcal{E}_\varphi(\epsilon'), \varphi) \subseteq \mathcal{E}_\varphi(\epsilon). \tag{10}$$

$$\gamma \triangleq \inf_{x \in [\mathcal{E}_\varphi(\epsilon') - \mathcal{E}_\varphi(\epsilon)]} -\dot{V}_\varphi(x)$$

$$\mathcal{E}_\varphi(\epsilon) = \{x \in \mathcal{N}_{V_\varphi}(x_{eq}) | V_\varphi(x) \leq \epsilon\}$$

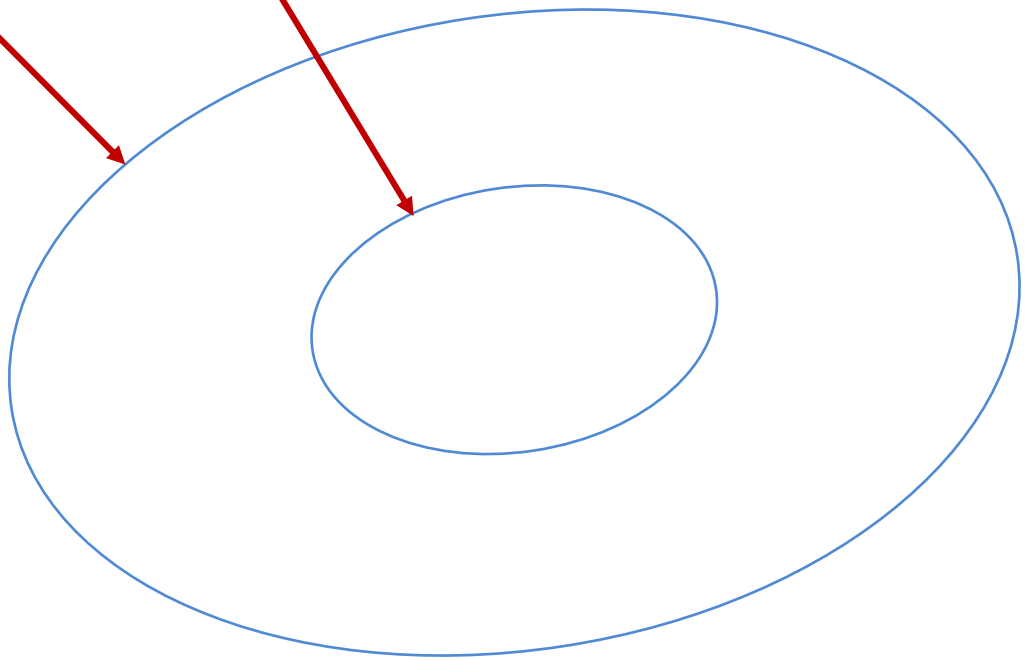
Lyapunov Functions - implication

Proposition 2.1: Given system (1) with stabilizing controller φ for equilibrium state $(x_{eq}, \varphi(x_{eq}))$ and Lyapunov function $V_\varphi(x)$ as defined above, given $\epsilon > 0$ for any $\epsilon < \epsilon' \leq 1 \; \exists \; \gamma > 0 \; \ni \forall \; t \geq (\epsilon' - \epsilon)\gamma^{-1}$,

$$\mathcal{R}(t; \mathcal{E}_\varphi(\epsilon'), \varphi) \subseteq \mathcal{E}_\varphi(\epsilon). \tag{10}$$

$$\gamma \triangleq \inf_{x \in [\mathcal{E}_\varphi(\epsilon') - \mathcal{E}_\varphi(\epsilon)]} -\dot{V}_\varphi(x)$$

$$\mathcal{E}_\varphi(\epsilon) = \{x \in \mathcal{N}_{V_\varphi}(x_{eq}) | V_\varphi(x) \leq \epsilon\}$$



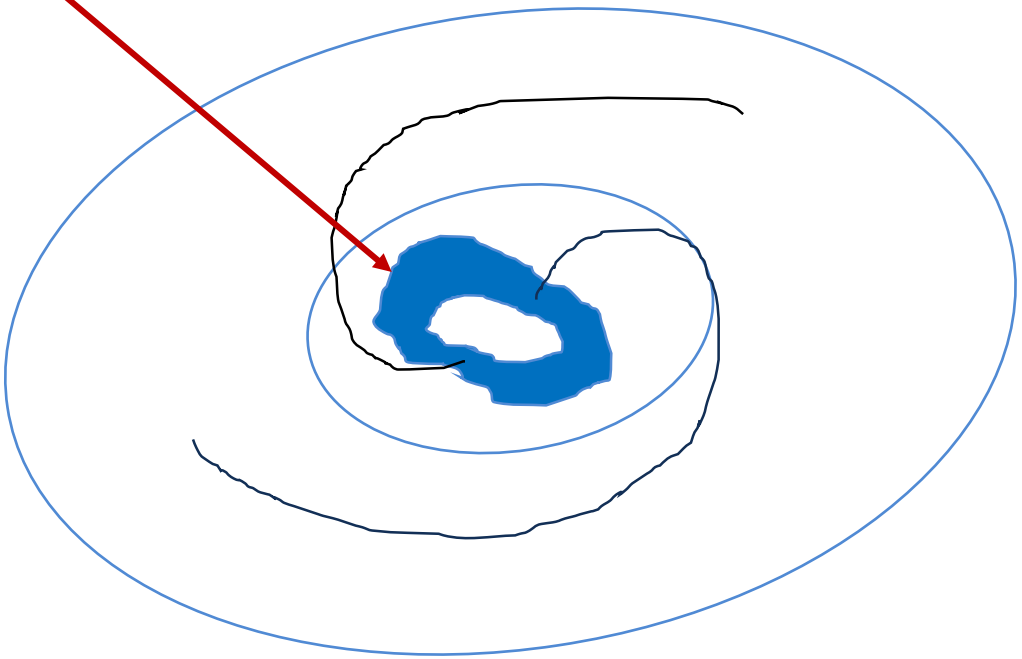
Lyapunov Functions - implication

Proposition 2.1: Given system (1) with stabilizing controller φ for equilibrium state $(x_{eq}, \varphi(x_{eq}))$ and Lyapunov function $V_\varphi(x)$ as defined above, given $\epsilon > 0$ for any $\epsilon < \epsilon' \leq 1 \; \exists \; \gamma > 0 \; \ni \forall \; t \geq (\epsilon' - \epsilon)\gamma^{-1}$,

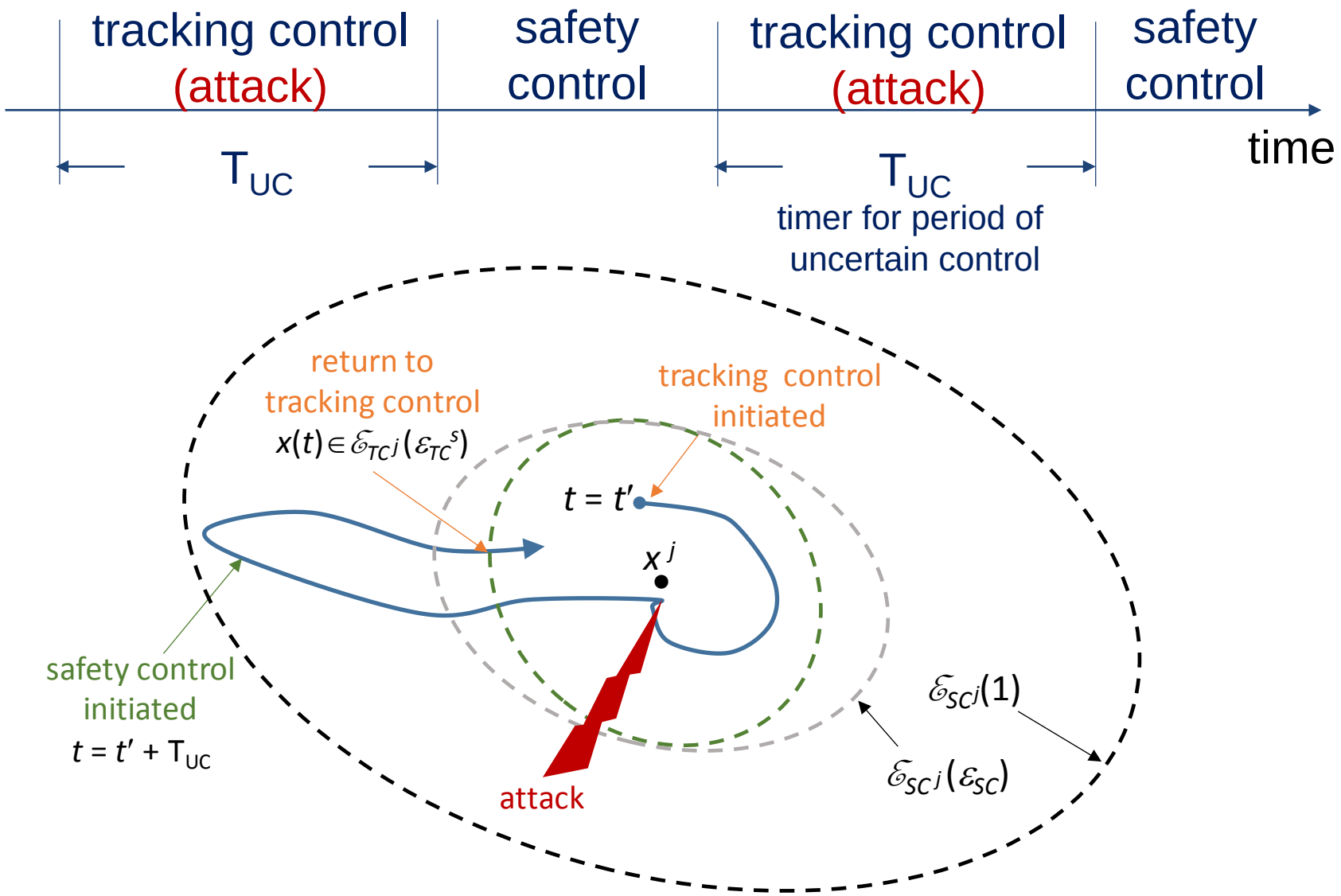
$$\mathcal{R}(t; \mathcal{E}_\varphi(\epsilon'), \varphi) \subseteq \mathcal{E}_\varphi(\epsilon). \tag{10}$$

$$\gamma \triangleq \inf_{x \in [\mathcal{E}_\varphi(\epsilon') - \mathcal{E}_\varphi(\epsilon)]} -\dot{V}_\varphi(x)$$

$$\mathcal{E}_\varphi(\epsilon) = \{x \in \mathcal{N}_{V_\varphi}(x_{eq}) | V_\varphi(x) \leq \epsilon\}$$

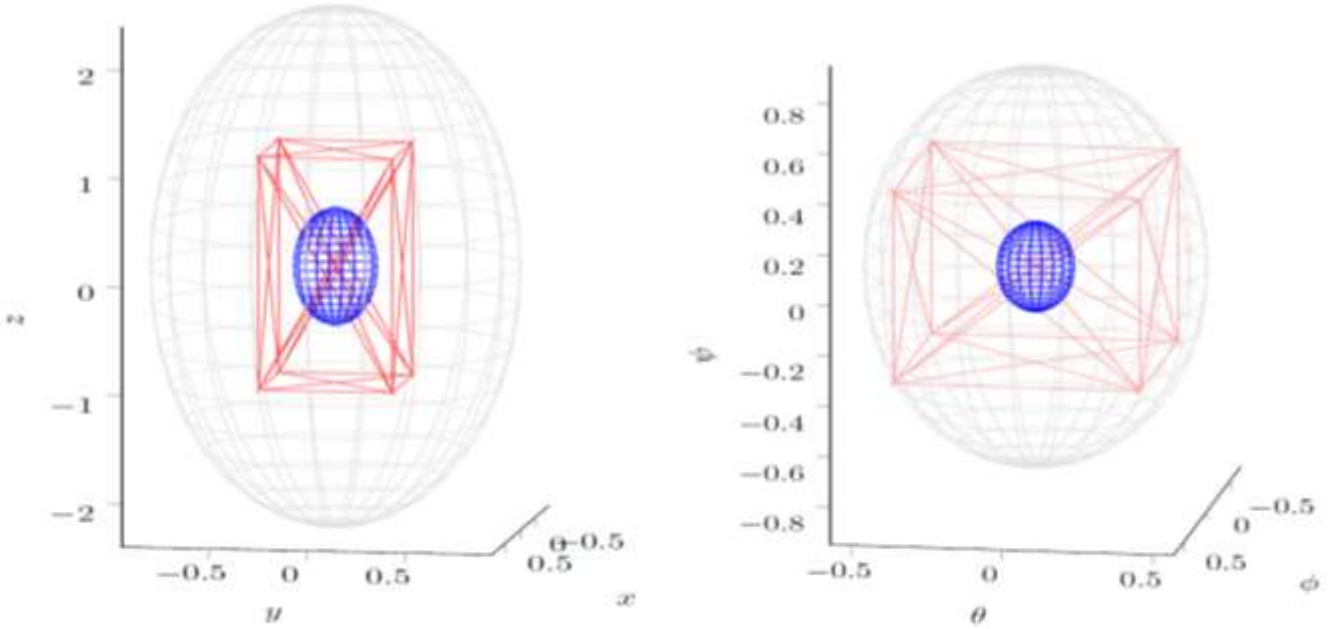


Safety Control



Application of control theory for linear systems

- Quadratic Lyapunov functions and ellipsoidal regions for safety and tracking control
- Linear-quadratic optimal control to design tracking and safety controllers
- Polyhedral reachable set computations to find T_{UC}



Application:
Secure tracking control for a quadrotor

6 DOF $\Rightarrow$ 12 state variables

$$\ddot{p}_x = -\cos\phi \sin\theta \frac{F}{m}$$
$$\ddot{p}_y = \sin\phi \frac{F}{m}$$
$$\ddot{p}_z = g - \cos\phi\cos\theta \frac{F}{m}$$
$$\ddot{\phi} = \frac{1}{J_x}\tau_\phi$$
$$\ddot{\theta} = \frac{1}{J_y}\tau_\theta$$
$$\ddot{\psi} = \frac{1}{J_z}\tau_\psi.$$

store.dji.com

Linear mapping from force & torques to propeller torques ($\propto$ currents)

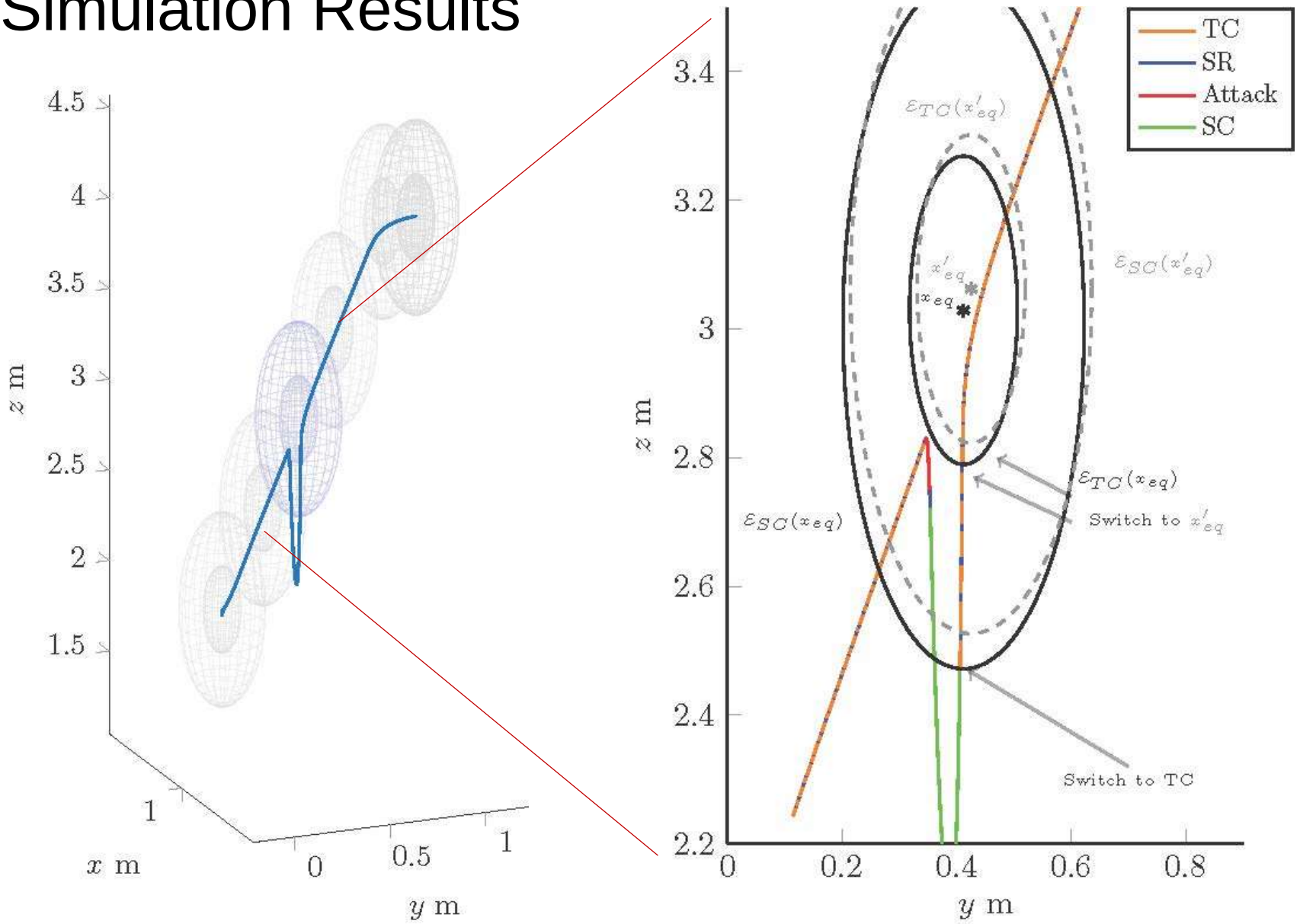
$$\begin{pmatrix} F \\ \tau_\phi \\ \tau_\theta \\ \tau_\psi \end{pmatrix} = \begin{pmatrix} k_1 & k_1 & k_1 & k_1 \\ 0 & -\ell k_1 & 0 & \ell k_1 \\ \ell k_1 & 0 & \ell k_1 & 0 \\ -k_2 & k_2 & -k_2 & k_2 \end{pmatrix} \begin{pmatrix} \delta_f \\ \delta_r \\ \delta_b \\ \delta_l \end{pmatrix}$$

Linear design:

- linearize at equilibrium
- assume full state available
- LQ state feedback design
- reference points = equilibrium states

Randal Beard. Quadrotor dynamics and control rev 0.1. All Faculty Publications. 1325. https://scholarsarchive.byu.edu/facpub/1325, 2008.

Simulation Results



Px4 flight controller: Generic 10" quad + geometry.
https://github.com/PX4/jMAVSim/blob/83bf400d71588131e2c6e179a6c63e8585271275/src/me/drton/jmavsim/Simulator.java#L314,
Last view: 09/2018.

Summary

- Overview of software rejuvenation
- Description of algorithm for tracking control systems
- Summary of theoretical results from control theory
- Demonstration in simulation for nonlinear drone application

References

R. Romagnoli, B.H. Krogh, and B. Sinopoli, Design of software rejuvenation for cps security using invariant sets, submitted to 2019 American Control Conference (ACC), arXiv preprint arXiv:1810.10484, 2018.

R. Romagnoli, B.H. Krogh, D. de Niz, and B. Sinopoli, Software rejuvenation for secure tracking control, submitted to 2019 International Conference on Cyber-Physical Systems, arXiv preprint arXiv:1810.10468, 2018.

R. Romagnoli, B.H. Krogh, and B. Sinopoli. Safety and liveness of software rejuvenation for secure tracking control, submitted to 2019 European Control Conference (ECC).

Current Research

- Implementing on a drone at SEI
- Extending theory to include
  - State estimation
  - Disturbances
- Additional applications
  - Smart grid
  - Smart vehicles