# Design of Software Rejuvenation for CPS Security Using Invariant Sets

Raffaele Romagnoli\*, Bruce H. Krogh\*\* and Bruno Sinopoli\*\*\*

\*Dept. of Electrical and Computer Engineering, Carnegie Mellon University \*\*Software Engineering Institute, Carnegie Mellon University \*\*\*Department of Electrical and Systems Engineering, Washington University in St. Louis

### 2019 American Control Conference, July 10-12, 2019, Philadelphia, PA.



Copyright 2019 Carnegie Mellon University. All Rights Reserved.

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. The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM19-0651

## Introduction to the Problem

Cyber-Physical Systems

### Attack Model



### Protected Hardware/Software Arch.



- 1-Motivation and Goal
- 2-Software Rejuvenation Operating Modes
- **3-Secure** Control
- 4-Tracking Control



## Motivation and Goal

## Software Rejuvenation

**Software rejuvenation** (SR) protects **cyberphysical systems** (CSPs) against **cyber attacks** on the run time code by **periodically refreshing** the system with an uncorrupted software image.



- e How often rebooting the system?
- e What are the effects on the control system?





- How often rebooting the system?
- e What are the effects on the control system?



## Goal

To propose a secure tracking control scheme based on software rejuvenation for nonlinear and linear systems and provide general conditions that guarantee the property of safety and liveness.



# Software Rejuvenation Operating Modes

- e Tracking Control (TC).
- e Software Refresh (SR).
- e Secure Control (SC).

## Timeline





#### **Carnegie Mellon University**



Recoverable set:  $E_{SC}^{j}(1)$ 



Carnegie Mellon University

7/19

[Distribution Statement A] Approved for public release and unlimited distribution.





Recoverable set:  $E_{SC}^{j}(1)$ 

Safety set:  $E_{SC}^{j}(s_{s}) \frac{3}{4} s_{s} E_{SC}^{j}$  (1)





Recoverable set:  $E_{SC}^{j}(1)$  Safety set:  $E_{SC}^{j}(s_{s}) \frac{3}{4} s_{s} E_{SC}^{j}(1)$ 

Find  $T_{UC}$ ,  $s_s \in R$ 

$$\mathsf{R}(\mathsf{T}_{\mathsf{UC}};\mathsf{E}_{\mathsf{SC}}^{j}(\mathsf{s}_{\mathsf{s}}),\mathsf{U})\subseteq\mathsf{E}_{\mathsf{SC}}^{j}(\mathsf{1}).$$

ENGINEERING

Carnegie Mellon University

### Controlled System:

 $\dot{x} = f_{\varphi}(x) \frac{3}{4} f(x, \varphi(x))$ 

where  $\phi(x)$  is the state feedback controller. Lyapunov Function:

 $\begin{array}{l} V_{\varphi} \colon R \xrightarrow{n} \to R, \ N \xrightarrow{}_{V_{\varphi}} (x_{e\!q}) \subseteq N \ (x \xrightarrow{}), \underset{e\!q}{\otimes} (x \xrightarrow{})_{p} = \underset{e\!Q}{\otimes} p \text{ and } \\ \forall x \in N_{V_{\varphi}} (x_{eq}) \ -\{x_{eq}\}: (i) \ V_{\varphi}(x) > 0, (ii) \end{array}$ 

$$\dot{V}_{0}(x) = \frac{\partial V}{\partial x} \cdot f(x_{0}) < 0$$

ENGINEERING

### Controlled System:

 $\dot{x} = f_{\varphi}(x) \frac{3}{4} f(x, \varphi(x))$ 

where  $\varphi(x)$  is the state feedback controller.  $\mbox{Lyapunov Function}:$ 

$$\begin{array}{l} V_{\varphi} \colon \mathbb{R}^{n} \to \mathbb{R}, \ \mathbb{N}_{\ \forall \varphi} \left( x_{eq} \right) \subseteq \mathbb{N} \ (x \ )_{eq} \in \mathbb{Q} \ \text{and} \\ \forall x \in \mathbb{N}_{\forall \varphi} \left( x_{eq} \right) \ - \{ x_{eq} \} \colon (i) \ \forall \varphi(x) > 0, (ii) \end{array}$$

$$\dot{V}_{0}(\mathbf{x}) = \frac{\partial V}{\partial \mathbf{x}} \mathbf{f} \quad (\mathbf{x}_{0}) < C$$
  
Lyapunov level set: For s>0,

$$\mathsf{E}_{\phi}(s) = \{ x \in \mathsf{N}_{V_{\phi}}(x_{eq}) | V_{\phi}(x) \leq s \}.$$

For any  $0 < s \le 1$ ,  $E_{\phi}(s)$  is an *invariant* set:  $\forall t > 0$ ,  $R(t; E_{\phi}(s), \phi) \subseteq E_{\phi}(s)$ 



### Proposition 1

Given  $\dot{x} = f_{\phi}(x) \sqrt[3]{4} f(x, \phi(x))$  with stabilizing controller  $\phi$  for equilibrium state  $(x_{eq}, \phi(x_{eq}))$  and Lyapunov function  $V_{\phi}(x)$  as defined above, given s > 0 for any  $s < s^{j} \le 1 \exists \gamma > 0 s \quad \forall t \ge (s^{j} - s)\gamma^{-1}$ ,

$$\mathsf{R}(\mathsf{t};\mathsf{E}_{\phi}(\mathsf{s}^{\mathsf{j}}),\phi)\subseteq\mathsf{E}_{\phi}(\mathsf{s}).$$

### Proposition 2

 $\begin{array}{l} \mbox{For any } U \subseteq U \mbox{and any } 0 < s < s^j \leq 1, \\ \exists \ T_U > 0 \ s \ R(t; \ E_{\phi}(s), U) \ \subseteq E_{\phi}(s^j) \ \forall t < T_U. \end{array}$ 



Idea: sequence of equilibrium points  $x_0, x_1, ..., x^{j-1}, x^j$ ,...



#### Carnegie Mellon University

Safety

$$x(t) \in \int_{j=0}^{[J]} E_{SCi}(1)$$

Theorem. The system is safe under software rejuvenation if the following conditions are satisfied:

i. 
$$x(0) \in E_{TC^1}(s^s_{TC});$$

ii. 
$$\mathsf{E}_{TC^{j}}(\mathbf{s}_{TC}^{s}) \subset \mathsf{E}_{SC^{j}}(\mathbf{s}_{SC});$$

iii.  $R(t; E_{SC}(s_{SC}), U) \subseteq E_{SC}(1) \forall t \in [0, T_{TC} + T_{SR}];$ 



**Carnegie Mellon University** 



iv.  $E_{TC^{j}}(s_{TC}) \subset E_{TC^{j+1}}(s_{TC}^{s})$ .





#### **Carnegie Mellon University**

### Liveness

Given reference points  $x^1, \ldots, x^J$ , the system is *live* if there exists a sequence of times  $t_1, \ldots, t_J$  where  $0 < t_1 < \cdots < t_J < \infty$  such that

 $x(t) \in E_{TC^j}(s^s_{TC}) \ \forall t \in [t_j, t_{j+1}), j = 0, \dots, J,$ 

where  $t_0 \frac{3}{4} 0$  and  $t_{J+1} \frac{3}{4} \infty$ .



**Assumptions**: no attack, the control input during  $T_{SR}$  is equal to the last value provided before software refresh.



**Theorem**. When there are no cyber-attacks, the system is live under software rejuvenation if, in addition to the conditions in Th. (safety),  $0 < s_{TC} < s^s_{TC}$  and  $\exists \delta > 0$  such that  $\forall x \in E^j_{TC} = T_{C^j}(s_{TC}^s) - E_{TC^j}(s_{TC})$  and  $\forall x^{jj} \in R(t; x(T_{TC}; x^j, TC^j), U)$ ,



 $\mathsf{V}_{TC^{j}}\left(\mathsf{x}^{j}\right) - \mathsf{V}_{TC^{j}}\left(\mathsf{x}^{jj}\right) \geq \delta$ 

14/19

[Distribution Statement A] Approved for public release and unlimited distribution.

### Linear Systems

$$E_{TC i}(s_{TC}) = x || (x - x)^{||}_{P_{TC j}} \le s_{TC}$$

### Safety

$$\forall x \in E_{TC^{j}}(s_{TC}) \Rightarrow x \in E_{TC^{j+1}}(s_{TC}).^{s}$$

.

### Liveness

$$\begin{split} & \tilde{A}_{j}^{\mathsf{T}}\mathsf{P}_{\mathsf{TC}^{j}} \tilde{A}_{j} - \mathsf{P}_{\mathsf{TC}^{j}} < 0. \\ & \text{where } \tilde{A_{j}^{3}}_{4} \tilde{A_{j}} \tilde{A_{j}}_{i} \tilde{A_{j}}, \tilde{A_{j}^{3}}_{4} e^{\mathsf{A}_{\mathsf{SC}^{j}} \mathsf{T}_{\mathsf{TC}}}, \tilde{A_{j}^{3}}_{4} (\mathsf{A}_{\mathsf{d}} - \mathsf{B}_{\mathsf{d}}\mathsf{K}^{j}). \\ & \mathsf{A}_{\mathsf{d}}^{3}_{4} e^{\mathsf{A}_{\mathsf{T}}} and \mathsf{B}_{\mathsf{d}}^{3}_{4} \int_{0}^{\mathsf{T}_{\mathsf{SR}}} e^{\mathsf{A}(\mathsf{T}_{\mathsf{SR}} - \mathsf{T})} \mathsf{B} \mathsf{d} \mathsf{T}. \end{split}$$

$$x(T_{UC})^{2} P_{TCj} < x_{j}(0)^{2} P_{TCj}$$

ENGINEERING



e 6DOF  $\rightarrow$  12 state variables

Linear design

- e Linearize at equilibrium;
- e Assume full state available;
- e LQ state feedback design;
- e Reference point = Equilibrium point.





e 6DOF  $\rightarrow$  12 state variables

Linear design

- e Linearize at equilibrium;
- e Assume full state available;
- e LQ state feedback design;
- e Reference point = Equilibrium point.

### Simulation

jMAVSim simulator. Turn-off attack.









**Tracking**. JMAVSim simulator. Turn-off attack. Projections of  $E_{TC^i}(s_{TC^s})$  and  $E_{TC^i}(s_{TC})$ 



ENGINEERING(a)

(b)

#### **Carnegie Mellon University**

18/19

[Distribution Statement A] Approved for public release and unlimited distribution.

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

### References

 R.Romagnoli, B.H. Krogh, B. Sinopoli. Design of SoftwareRejuvenation for CPS Security Using Invariant Sets. IEEE 2019 American Control Conference.

