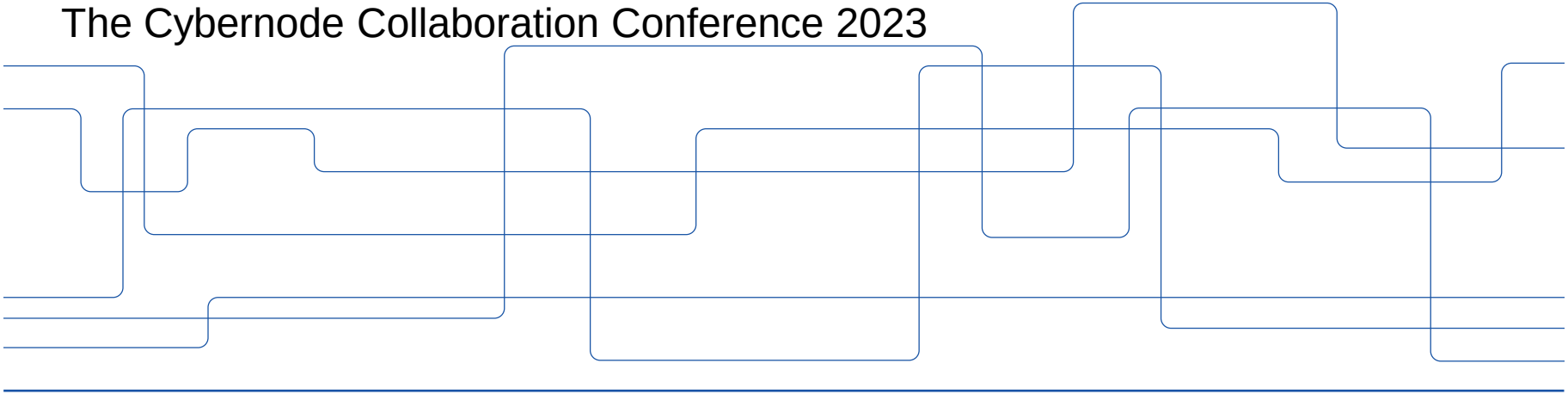
CERCES2:
Center for Resilient Critical Infrastructures

Henrik Sandberg (hsan@kth.se)

Decision and Control Systems, KTH EECS

The Cybernode Collaboration Conference 2023



CERCES2 in Short

- From MSB Research Framework Call 2014:
  - "…*forskning kring informationssäkerhet i industriella informations- och styrsystem*"
  - "*Då moderna industriella informations- och styrsystem ofta baseras på generella it-system leder detta ofta till att organisationen inte heller åtgärdar nyupptäckta eller kända it-säkerhetshål. Alternativt tar det mycket lång tid innan uppdateringar blir införda. Detta medför att industriella informations- och styrsystem oftast är sårbara för illasinnade angrepp.*"
- CERCES (2015-2020), CERCES2 (2020-2024)
- People
  - Mads Dam, Professor in Teleinformatics, KTH
  - Ragnar Thobaben, Associate Professor in Communication Theory, KTH
  - György Dán, Professor in Teletraffic Theory, KTH
  - Henrik Sandberg, Professor in Automatic Control, KTH
  - 6 PhDs → Ericsson Research (3), Scania (1), KTH (2)
  - 4 postdocs → TU/e (1), METU (1), KTH (2)

CERCES2 Research Areas

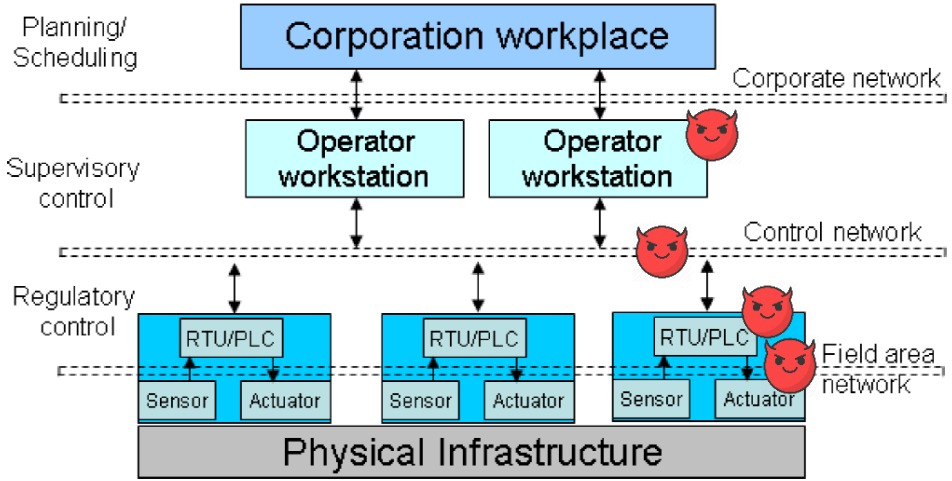


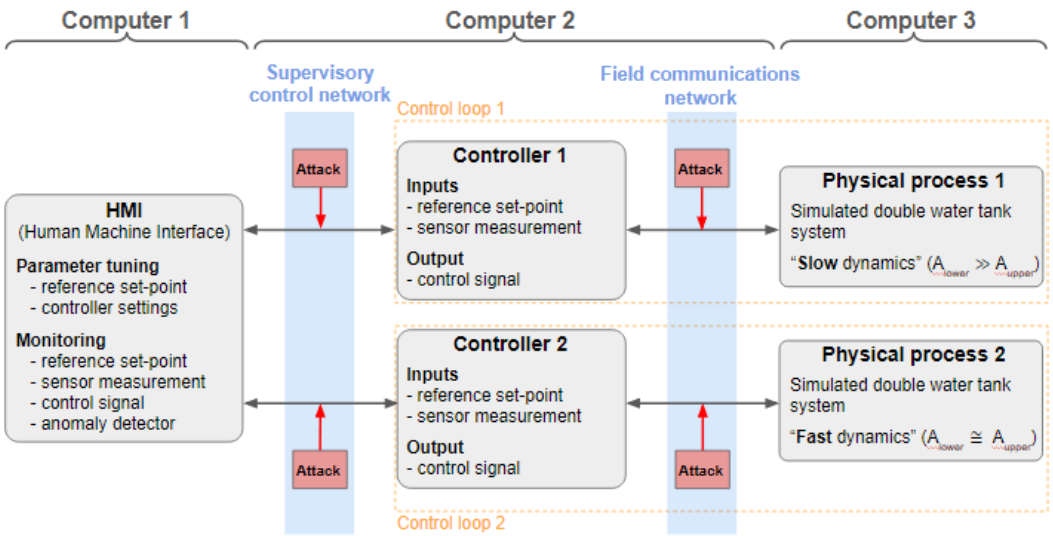
Figure 1. Architecture of control systems.

- Area 1: Embedded Software Platforms (Mads Dam)
- Area 2: Wireless Communication (Ragnar Thobaben)
- Area 3: Communication and Computation Infrastructure (György Dán)
- Area 4: Resilient Control of Cyber-Physical Systems (Henrik Sandberg)

CERCES2 Research Goals

- **Explore new and emerging research results and their possible adoption in the critical infrastructure/SCADA domain**
  - Area 1: Highly trustworthy execution platforms (PLCs/RTUs), validation of micro-architectural models
  - Area 2: Securing wireless transmissions, physical-layer intrusion detection in theory and practice
  - Area 3: Secure communication and computing infrastructures, resilient virtualized control systems, time synchronization
  - Area 4: Resilient networked control systems, cyber-physical anomaly detection and vulnerability/risk assessment

Virtual Testbed

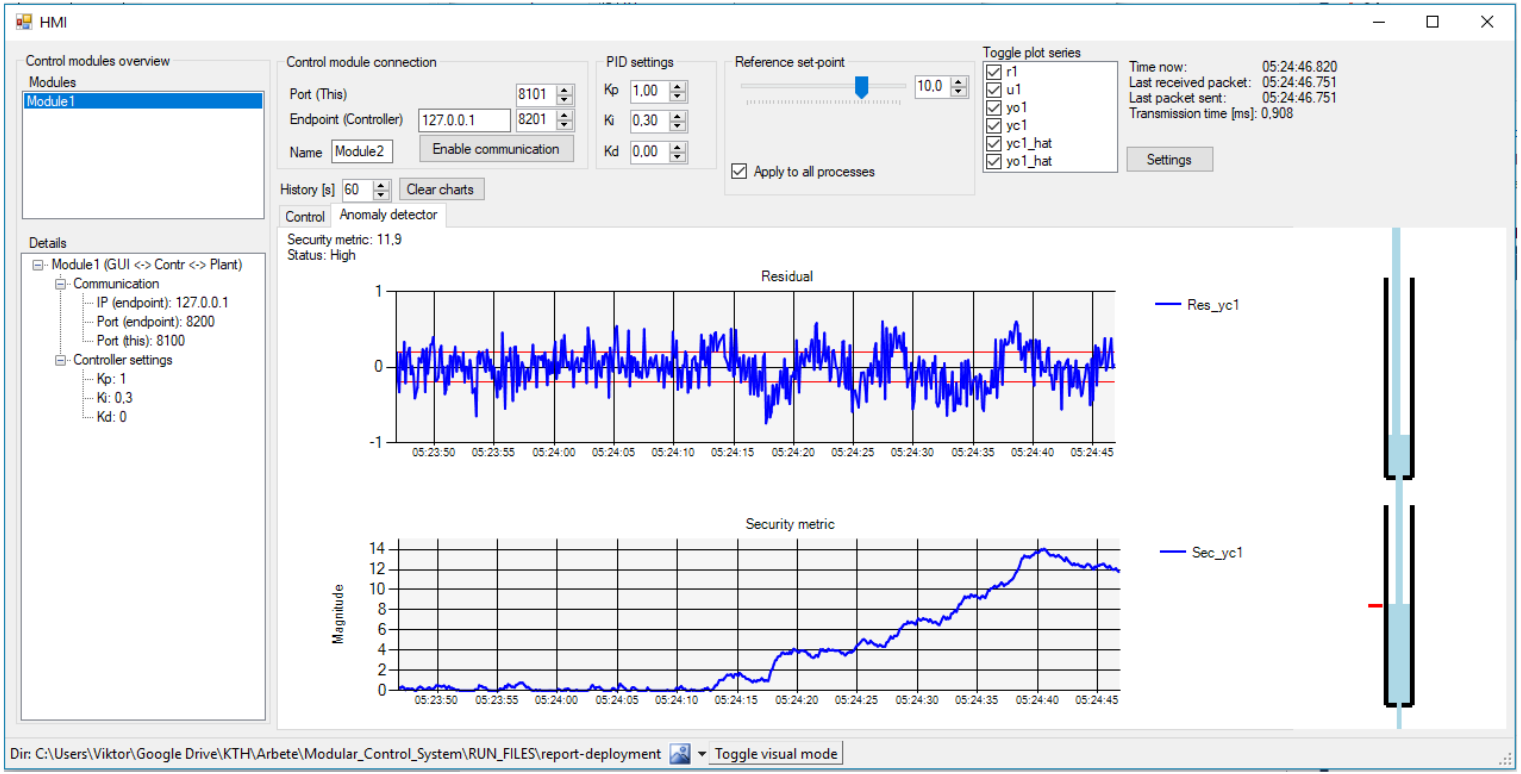


- Written in C#
  - Runs in standard IP-networks
  - Here: laptops or FOI CRATE

- Implemented modules:
  - Control center (HMI)
  - Controller (PID, see next)
  - Plant (simulated or real analog i/o)
  - Anomaly detector (Kalman filter + non-parametric CUSUM-test)
  - Channel (Supervisory control network, Field communication network, UDP/IP)

- GitHub: https://github.com/viktortuul/Modular_Control_System
- Tuul, Sandberg: "Testbed evaluation of DoS attacks on PID-controllers", CRITIS'19

Anomaly Detector Module Interface
(Ongoing DoS Attack Detected Using CUSUM-test)



Controller Module

- Supports digital implementation of the PID-controller

$$u(t) = K_P e(t) + K_I \int_0^t e(\tau)\,d\tau + K_D \frac{de(t)}{dt}$$

- Time-triggered PID

$$u_k = K_P e_k + K_I \sum_{i=1}^{k} e_i \Delta t + K_D \frac{e_k - e_{k-1}}{\Delta t} \qquad t_k = k\Delta t$$

- Event-triggered PIDplus (Emerson)

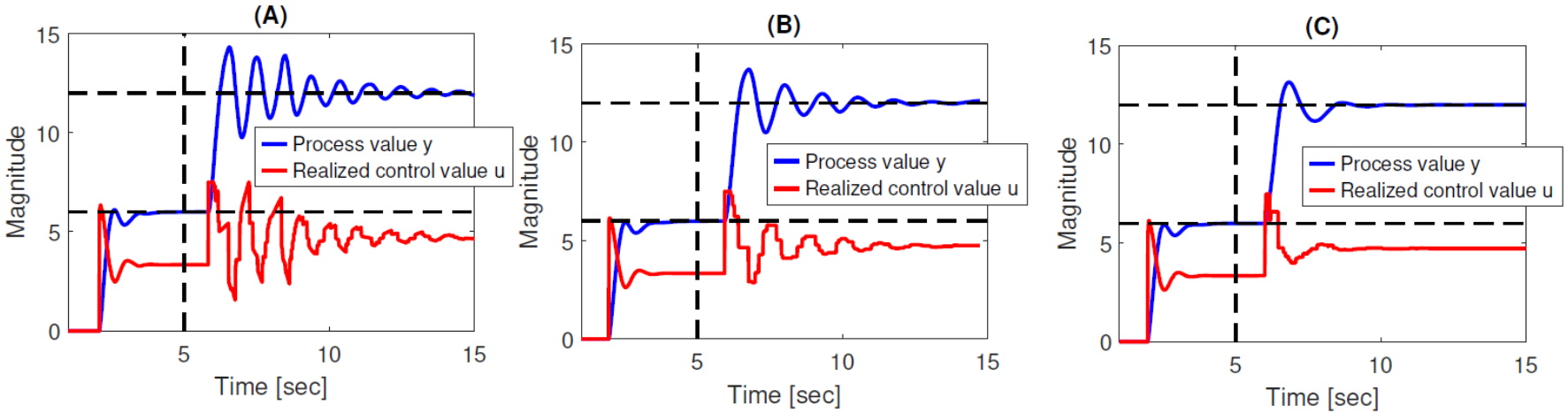
$$\begin{aligned} u_k &= P_k + F_k + D_k \\ D_k &= K_D(e_k - e_{k-1})/\Delta t_k && \Delta t_k := t_k - t_{k-1} \\ F_k &= F_{k-1} + (U - F_{k-1})(1 - \exp(-\Delta t_k / T_{\text{res}})) && T_{\text{res}} = K_P/K_I \end{aligned}$$

In case of outage (Δt_k large), $F_k \to U$ (last confirmed actuator setting)

- Event-triggered PIDsuppress (Tuul [new])

$$u_k = K_P \gamma_k e_k + K_I \sum_{i=1}^{k} \gamma_i e_i \Delta t_i + K_D \frac{e_k - e_{k-1}}{\Delta t_k}$$

DoS Attack Scenario: Change in Setpoint



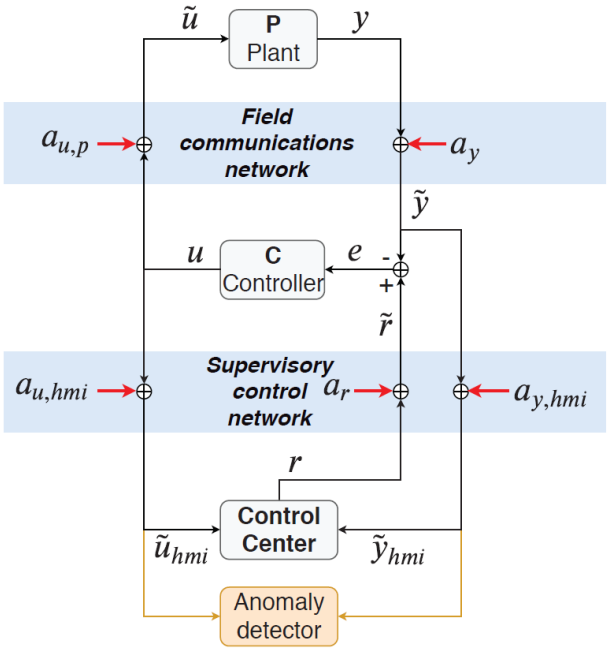
- (A) Time-triggered, (B) PIDplus, (C) PIDsuppress
- DoS attack starts at 5 sec, Pr(drop→pass) = 90%, Pr(pass→drop) = 10%
- Un-attacked performance similar
- PIDsuppress suppresses oscillations during attack, at the price of slight decrease of bandwidth

Contact Persons

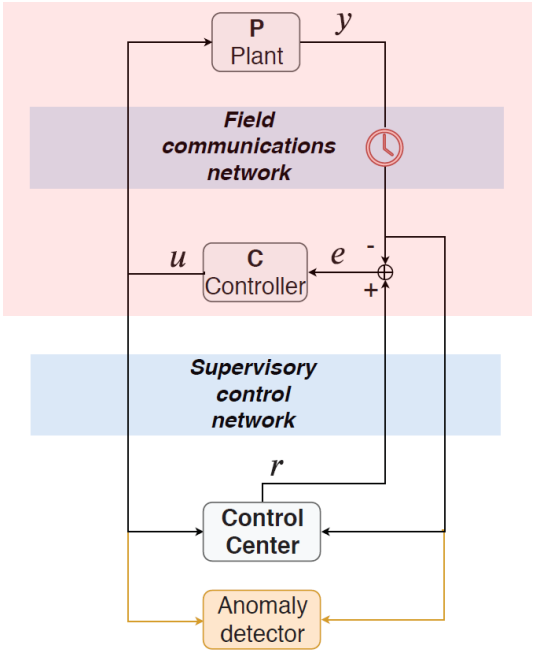
- Area 1: Embedded Software Platforms
  - Mads Dam (mfd@kth.se)
- Area 2: Wireless Communication
  - Ragnar Thobaben (ragnart@kth.se)
- Area 3: Communication and Computation Infrastructure
  - György Dán (gyuri@kth.se)
- Area 4: Resilient Control of Cyber-Physical Systems
  - Henrik Sandberg (project leader) (hsan@kth.se)

Supported Attack Types in Channel Module

Coordinated Data-injection Attacks (not today)



DoS Attacks (today)



Suppress Factor in PIDsuppress

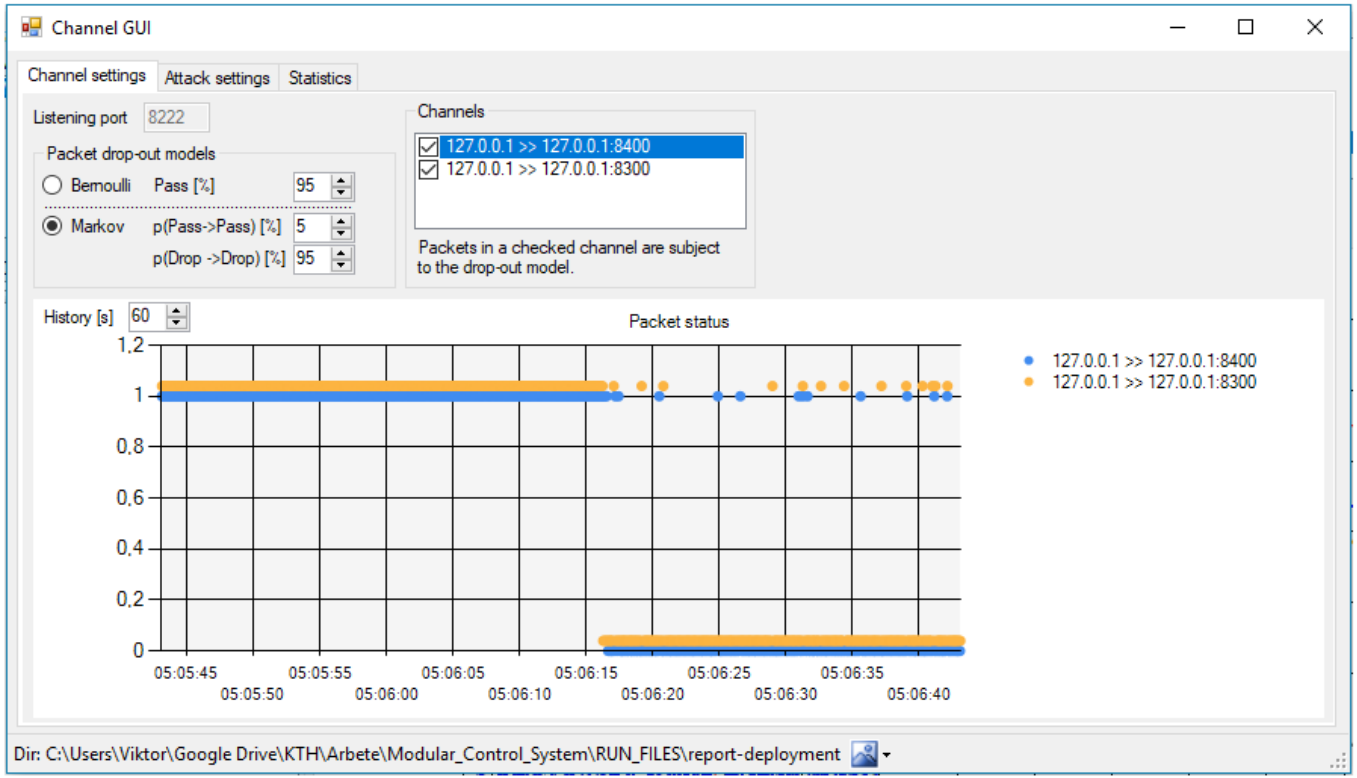
Algorithm 1 Suppress factor γ_k

function $\gamma_k(\gamma_{k-1}, \beta, \Delta t_k, T_{\text{supp}})$
  $\hat{\gamma}_k \leftarrow \exp(-\Delta t_k / T_{\text{supp}})$
  if $\hat{\gamma}_k \leq \gamma_{k-1}$ **then return** $\hat{\gamma}_k$
  else return $(1-\beta)\gamma_{k-1} + \beta\hat{\gamma}_k$

- Choose T_{supp} and order of magnitude larger than nominal sampling Δt_k

- Heuristic motivation
  - Sampling period Δt_k ~ time delay in loop gain $\Delta t_k/2$ ⇒ Phase loss and oscillations
  - Solution: Decrease the loop cross-over frequency $\omega_{\text{c,nom}}$ ~ system bandwidth ω_B
  - Role of suppress factor: $\omega_{\text{c}} = \omega_{\text{c,nom}}\, \gamma_k^{1/\alpha}$, $\alpha \approx 1.5$

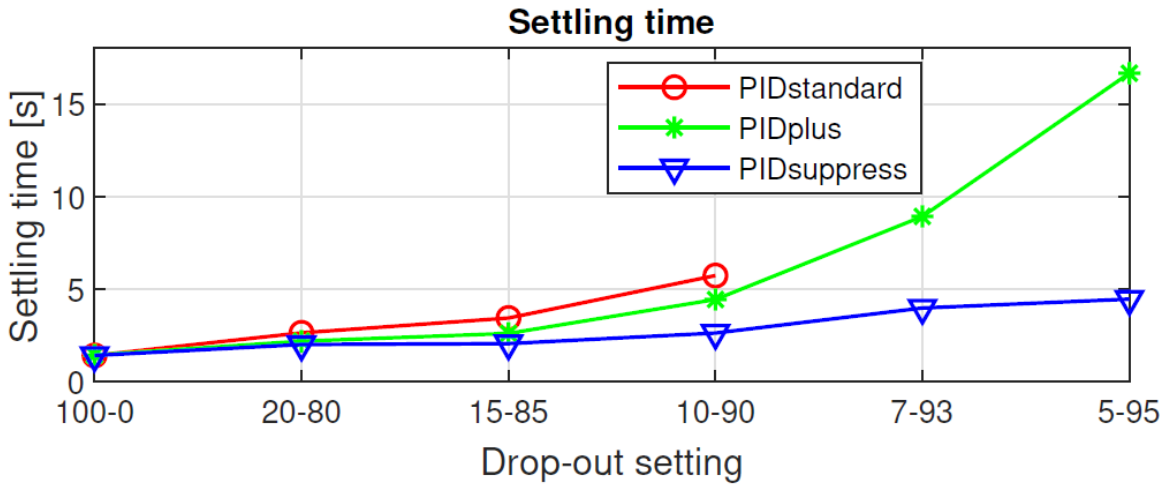
Channel Module (incl. Attack Configuaration)
(Channel Settings, Ongoing Gilbert-Elliott Packet Drop-out)



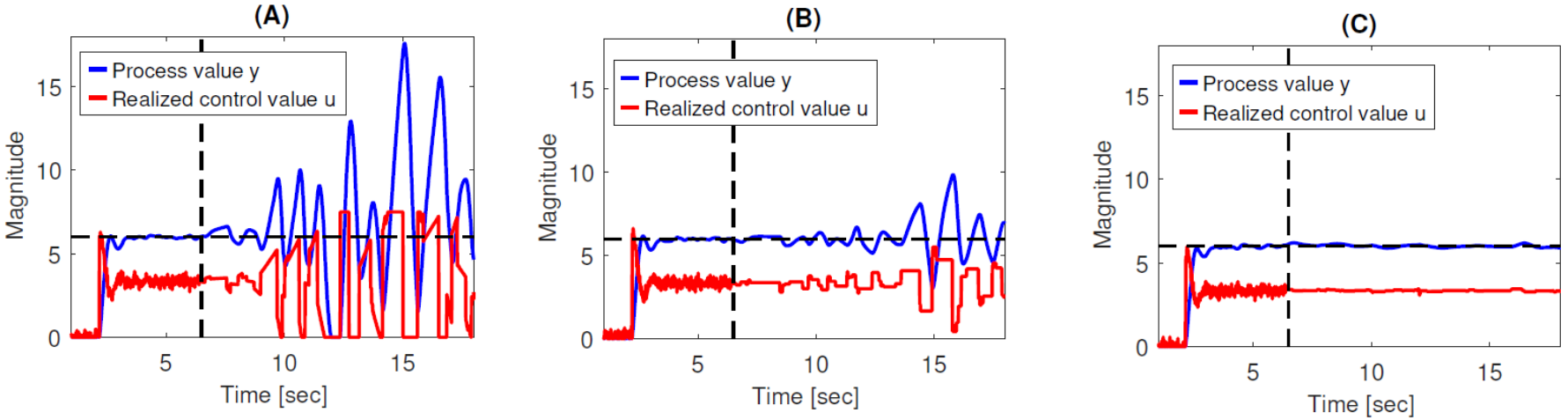
DoS Attack Scenario 2: Varying DoS Intensity

Drop-out setting [%]	100-0	20-80	15-85	10-90	7-93	5-95
Average pass time [sec]	-	0.25	0.24	0.22	0.22	0.21
Average drop time [sec]	-	1.00	1.34	2.00	2.86	4.00

Pr(drop→pass)-Pr(pass→drop)



DoS Attack Scenario 3: Measurement Noise



- (A) Time-triggered, (B) PIDplus, (C) PIDsuppress
- DoS attack starts at 6.5 sec, Pr(drop→pass) = 5%, Pr(pass→drop) = 95%
- Un-attacked performance similar
- PIDsuppress suppresses oscillations during attack, at the price of slight decrease of bandwidth

Summary Virtual Testbed

- Virtual testbed, download at GitHub: https://github.com/viktortuul/Modular_Control_System
- Also relatively benign physical processes exhibit potentially dangerous behavior under simple low-level DoS attacks. **Real-time control implementation matters!**
- New PID implementation: PIDsuppress
- Why did we do this?
  - Simple tool to evaluate the **physical effects** of attacks and defenses
  - Simulated as well as real lab processes
  - On networks of laptops as well real cyber ranges (FOI CRATE)
  - Educational effort, risk assessment, evaluation of anomaly detectors, and response mechanisms