Towards Trustworthy Data in Networked Control Systems: A Hardware-Based Approach

Thomas Ulz, Thomas Pieber, Christian Steger[1]
Rainer Matischek, Holger Bock[2]

[1]Graz University of Technology
[2]Infineon Austria AG

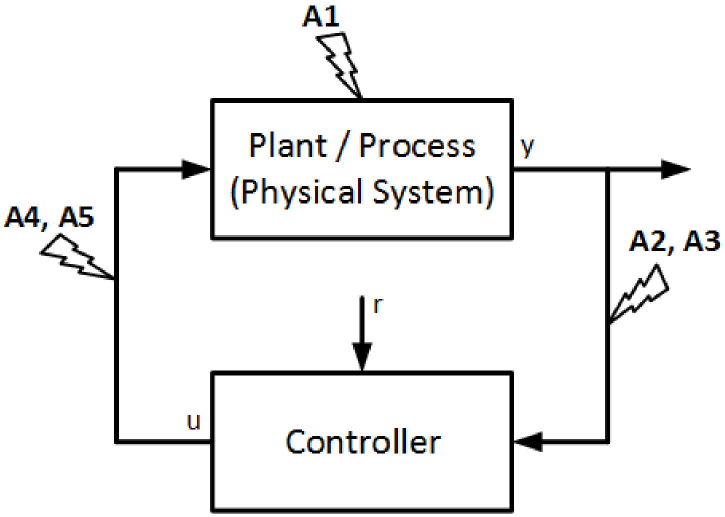
Outline

1. Introduction
2. State-of-the-Art
3. Approach Securing NCSs
4. Conclusion and future work

Introduction

- Networked Control Systems (NCS) are gaining popularity
  - E.g. Smart Factories and “Industrial Internet of Things”
- Increase in popularity entails higher interest of attackers
  - Attacks targeting NCS become more frequent
- Proper functionality of the NCS must be ensured
  - Malfunctioning NCS might have severe consequences for the system or the controlled process
  - Or even threaten human lives

Introduction



- By introducing network interfaces between sensor, controller, and actuator
- Also new potential attacking points introduced
- → Network communication must be secured!

– **A1**: Attacks directly targeting physical process

– **A2**: *Deception attacks*, attacker injects false information $\tilde{y} \neq y$

– **A3**: Denial-of-Service Attacks

– **A4**: Attacker induces false control commands $\tilde{u} \neq u$

– **A5**: Denial-of-Service Attacks

Outline

1. Introduction
2. State-of-the-Art
3. Securing NCSs
    1. Authenticated encryption
    2. Joint encryption and error correction
    3. Hardware support
4. Conclusion and future work

State-of-the-Art

- There are several research challenges for NCS
  - Network delays
  - Packet loss
  - Information security
- Regarding information security, the following properties must be protected for data transferred in an NCS
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity

State-of-the-Art

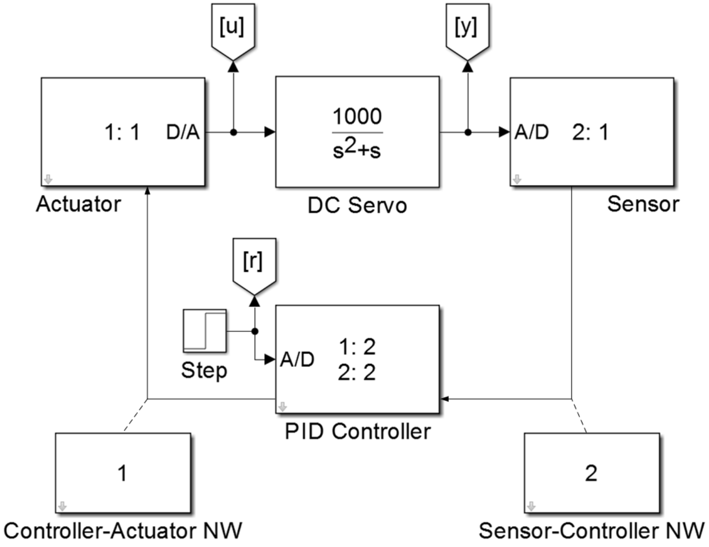
- No current work aims to protect all 4 of these properties
- Most often, DoS attacks are mitigated (Availability)
  - By considering the ensuing packet loss in the NCS
- To protect data confidentiality, encryption is applied
  - However, data integrity and authenticity not considered
  - We will show in this presentation why applying plain encryption in an NCS is not a good idea

Outline

1. Introduction
2. State-of-the-Art
3. Securing NCSs
   1. Authenticated encryption
   2. Joint encryption and error correction
   3. Hardware support
4. Conclusion and future work

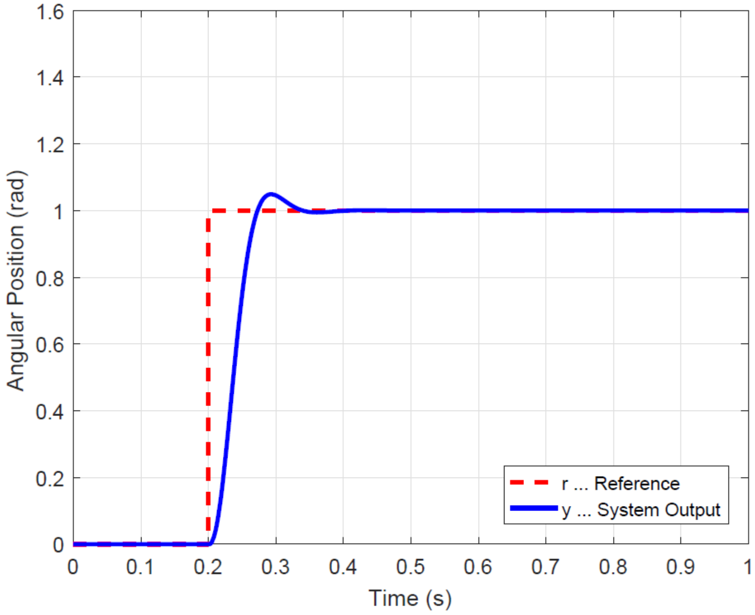
Securing NCSs – Simulation Model

- To evaluate the presented approaches, a DC Servo with a transfer function $G(s) = \frac{1000}{s\,(s+1)}$ was used.
- The model was simulated in Matlab/Simulink and the TrueTime toolbox



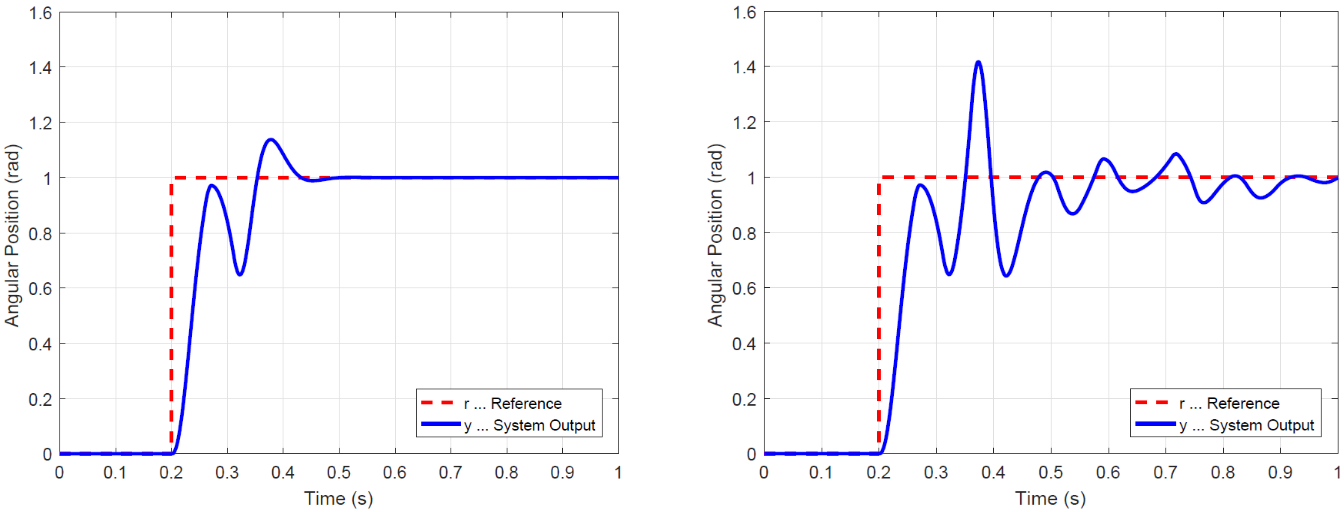
Securing NCSs – Simulation Model

- For this model, we applied a simple PD-controller
- This leads to the following step response for a system without any network delays or errors



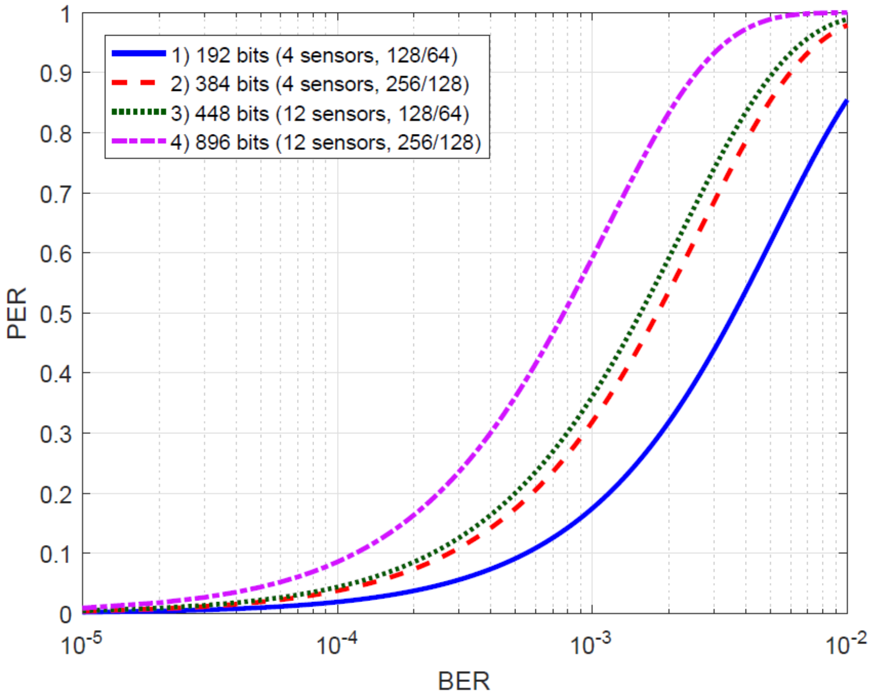
Securing NCSs – Authenticated Encryption

- Instead of currently used basic encryption
- Applying “Authenticated Encryption” (AE), where data “Confidentiality, Integrity, and Authenticity” can be provided
- But, a single bit-error renders the data packet useless!
- The following step responses were simulated for bit-errors of 25% and 50% respectively



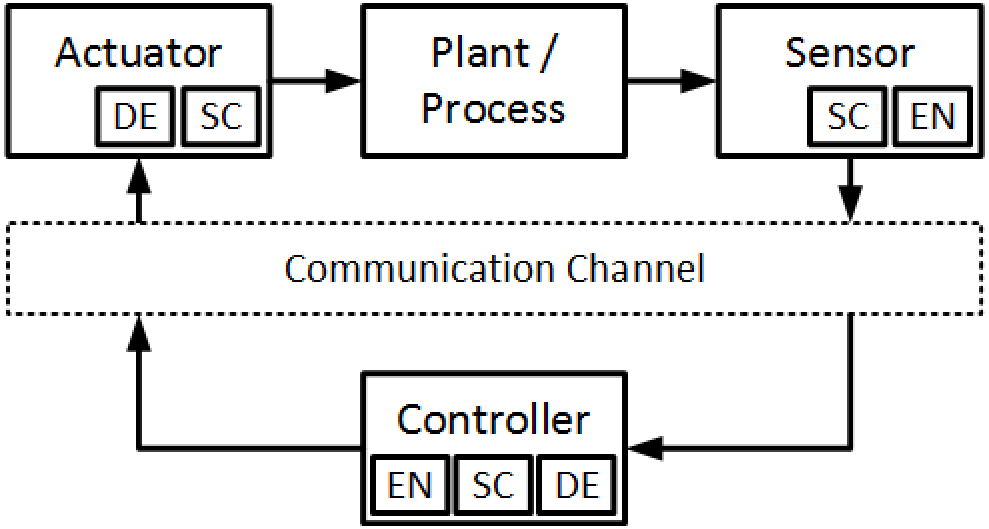
Securing NCSs – Authenticated Encryption

- Low bit-error rates already lead to high packet-error rates
- Suddenly, DoS attacks are easier to perform for attackers!



Securing NCSs – JEEC

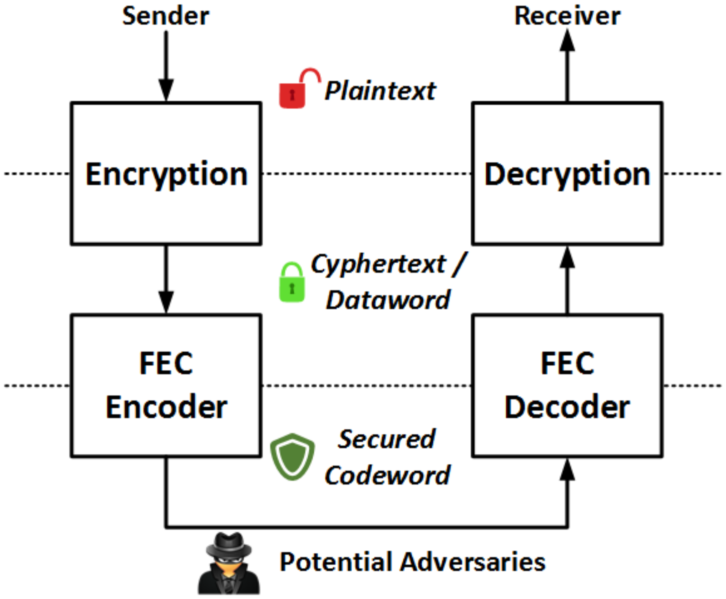
- To mitigate this self-induced problem, we apply “Joint encryption and error correction” (JEEC)
  - Well established principle from satellite communication
- Additionally combine with HW-Security-Controllers (SC)



Securing NCSs – JEEC

- By applying forward error correction (FEC), also DoS attacks are harder to perform for potential adversaries (“Availability” aspect)

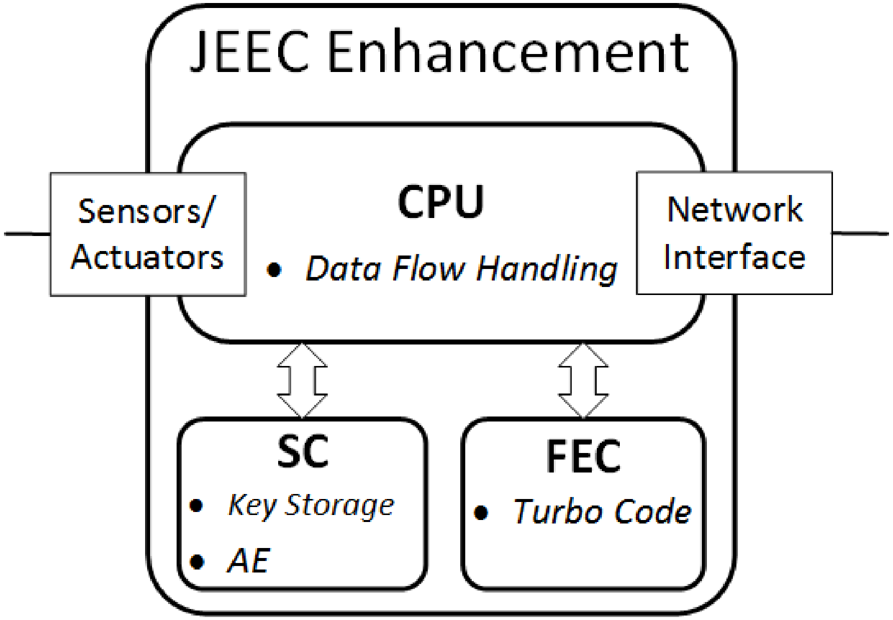
- The encrypted information with additional error correction data is transferred



- In addition, JEEC can be used for anomaly detection in the NCS

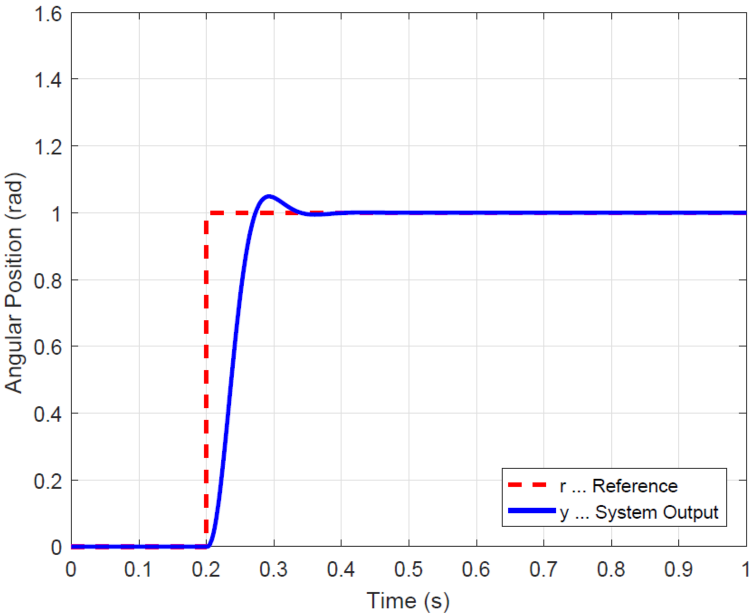
Securing NCSs – JEEC System Design

- In order to guarantee low additional delays due to the applied JEEC principle, and to be robust against potential SW-Attacks
- We propose a system design using dedicated hardware components (SC) to perform security related operations



Securing NCSs – Evaluation

- Using a low-delay JEEC enhancement, the initial step response for our simulation model can be achieved



Outline

1. Introduction
2. State-of-the-Art
3. Securing NCSs
   1. Authenticated encryption
   2. Joint encryption and error correction
   3. Hardware support
4. Conclusion and future work

Conclusion

- In this paper, we highlight the security risks of NCSs
- We show, why simply applying pure encryption or authenticated encryption is not sufficient to provide confidentiality, integrity, authenticity, and availability for the system
- We propose to use JEEC to mitigate the problems induced by (authenticated) encryption
- To induce only minimal overheads, we propose a dedicated hardware enhancement for NCSs

Future work

- In our approach, we applied sequential JEEC
- However, there is also research aiming to combine (authenticated) encryption and forward error correction into one step
- In theory, this should allow to build smaller and faster hardware extensions to perform this step
- Currently, we are investigating such algorithms in SystemC simulation models

Acknowledgements IoSense

This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia.

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

IoSense is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2016 and April 2019. More information: https://iktderzukunft.at/en/

bmvit
Austrian Ministry
for Transport,
Innovation and Technology

Questions?

Thank you!

For detailed questions please contact main author:
Thomas Ulz <thomas.ulz@tugraz.at>