Master's Thesis
Topic: Intrusion Detection in Control Systems

SIEMENS
Ingenuity for life

Master's Thesis at Siemens

Master's Thesis Topic: Intrusion Detection in Control Systems

Location: The Master's work will be carried out at and financed by Siemens Corporate Technology in Munich

Working conditions:

- This opening is only for TUM students, preferably from Electrical Engineering or Computer Science
- The selected student will conduct the work at Siemens Corporate Technology in Munich (last stop of U5 in Neuperlach Süd)
- From the TUM side, this work will be supervised by Prof. Sandra Hirche
- The duration of the work will be 6 months
- The selected student will be paid by Siemens according to its regulations for financing Master's students
- The student will have an opportunity to interact with different Siemens internal groups working on IT Security and Industrial Automation
- The work will be carried out and the thesis written in English
- Starting date: as soon as possible

Contact person at Siemens: Dr. Dragan Obradovic

The application documents should be sent to: dragan.obradovic@siemens.com. They should include a CV and copies of transcripts / grades.

Master's Thesis at Siemens
Topic: Intrusion Detection in Control Systems

SIEMENS
Ingenuity for life

Topic Description:

Classical Internet security methods such as authentication, access control, firewalls and encryption are applied to a variety of applications including automation and control systems. But in contrast to other applications, control systems are typically used in a very well planned and optimized manner, where the knowledge about their dynamics and underlying communication are stored in different engineering tools. Having access to this knowledge enables planning very sophisticated cyber-attacks such as Stuxnet, but it also enables the development of control-theory-based mechanisms for early detection and stopping of these attacks.

In the Stuxnet attack, the parameters of the controller were changed to make the closed-loop unstable. Simultaneously, to make this controller changes undetected, the intrusion program has identified typical steady state of the system, recorded its data and continued sending these data to the monitoring station during the attack.

The goal of this Master's thesis work is to investigate different attack/intrusion detection mechanisms relying on diverse levels of the control system knowledge and control theoretical concepts. The available information about the control system can vary from knowing only the basic properties of the signals in the closed loop to having comprehensive system dynamic models including the information about the built-in redundancy in communication between control loop elements such as sensors, actuators and controllers.

The derived concepts, if time allows, might be tested and demonstrated on two small production systems available at Siemens in Munich which are controlled by Siemens automation hardware and software.

References:

1) D. Umsonst, H. Sandberg; "A Game-Theoretic Approach for Choosing a Detector Tuning Under Stealthy Sensor Data Attacks", 2018 IEEE Conference on Decision and Control (CDC), Miami, USA

2) P. Hespanhol, et al.; "Statistical Watermarking for Networked Control Systems", 2018 Annual American Control Conference (ACC), Milwaukee, USA

3) Y. Mo, S. Weerakkody, B. Sinopoli; " Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs", 2015, IEEE Control Systems Magazine