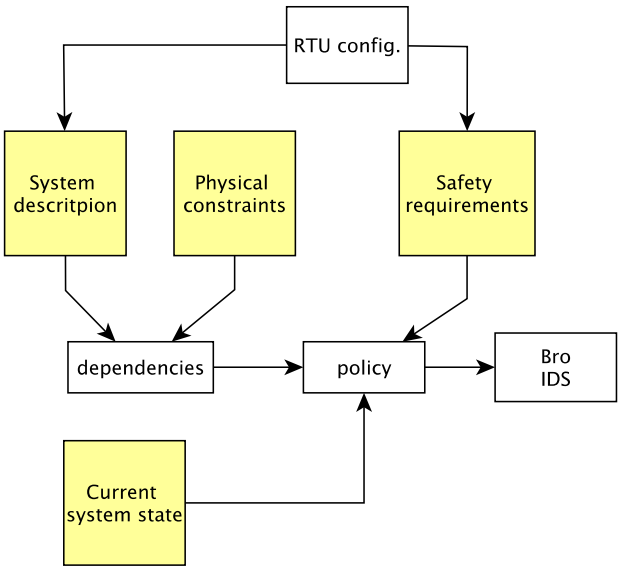
DACS
Design and Analysis of Communication Systems

UNIVERSITY OF TWENTE.

Automatic Generation of Bro Intrusion Detection Rules based on Physical System Description

SCADA (Supervisory Control and Data Acquisition) systems are systems which monitor and control geographically distributed physical systems, such as power distribution systems. These networks were not designed with security in mind, and they have had become a popular target for attacks, for example with CrashOverride malware[1]. A possible way to secure these networks is by introducing Intrusion Detection Systems (IDS). IDSes, such as Bro[2] or Snort[3] monitor the network traffic and analyse the content of the packets. They can detect intrusions based on anomalies from regular traffic behaviour or based on pre-defined signatures.

For networks, which directly control the physical system, it is worthwhile to include the information about that system into the rules. For example, if a system controls a solar panel, and the traffic shows non-zero electricity production during the night time, it is possible to raise an alert about false production information.



In more general case, the input information for rules are:

(i) System description (e.g., PV panel is an energy source; controller has a configuration about the stored values)

(ii) Physical constraints (e.g., production happens during the day; depending on the weather information we expect certain production profile)

[1] https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[2] https://www.bro.org
[3] https://www.snort.org

(iii) Safety requirements (e.g., if the current on a power line exceeds certain amount, an alert must be raised; information can be given by a controller such as RTU)

(iv) Current system state

The goal of the assignment is to automatically derive Bro rules based on information listed above. Automatic, one-time generation of rules, based on the RTU configuration was considered before, e.g., by Nivethan and Papa [1]. However, as opposed to the work of Nivethan and Papa, the rules should be **updated** based on the **current state** of the physical system. For example, if the energy load on a power line is low, it is allowed to disconnect it, because this load can be handled by other lines. However, if it is high, it might be not allowed to open such a power line.

The system description, physical constraints and safety requirements can be determined based on our previous work [2-4].

This master assignment will be performed at the **DACS** (Design and Analysis of Communication Systems) group. It is applicable for the following Master Programs:

- Technical Computer Science
- Internet Science & Technology
- Electrical Engineering
- Embedded Systems

For more information, please contact Justyna Chromik (j.j.chromik@utwente.nl).

[1] Jeyasingam Nivethan and Mauricio Papa. 2016. A SCADA Intrusion Detection Framework that Incorporates Process Semantics. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference* (CISRC '16). ACM, New York, NY, USA, Article 6, 5 pages. DOI: https://doi.org/10.1145/2897795.2897814

[2] Chromik, J. J., Remke, A. K. I., & Haverkort, B. R. H. M. (2016). Improving SCADA security of a local process with a power grid model. In *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, ICS-CSR 2016* (pp. 114-123). (Electronic Workshops in Computing). UK: BCS Learning & Development Ltd..
DOI: 10.14236/ewic/ICS2016.13

[3] Chromik, J. J., Remke, A. K. I., & Haverkort, B. R. H. M. (2016). What's under the hood? Improving SCADA security with process awareness. In *Proceedings of the Joint Workshop on Cyber-physical Security and Resilience in Smart Grids (CPSR-SG 2016)* (pp. -). USA: IEEE.
DOI: 10.1109/CPSRSG.2016.7684100

[4] Chromik, J. J., Haverkort, B. R. H. M., Remke, A. K. I., et al. (2017). *Context-aware local Intrusion Detection in SCADA systems: a testbed and two showcases*. Paper presented at 8th IEEE International Conference on Smart Grid Communications, SmartGridComm 2017, Dresden, Germany.