Anomaly Detection in ICS based on Data-history Analysis

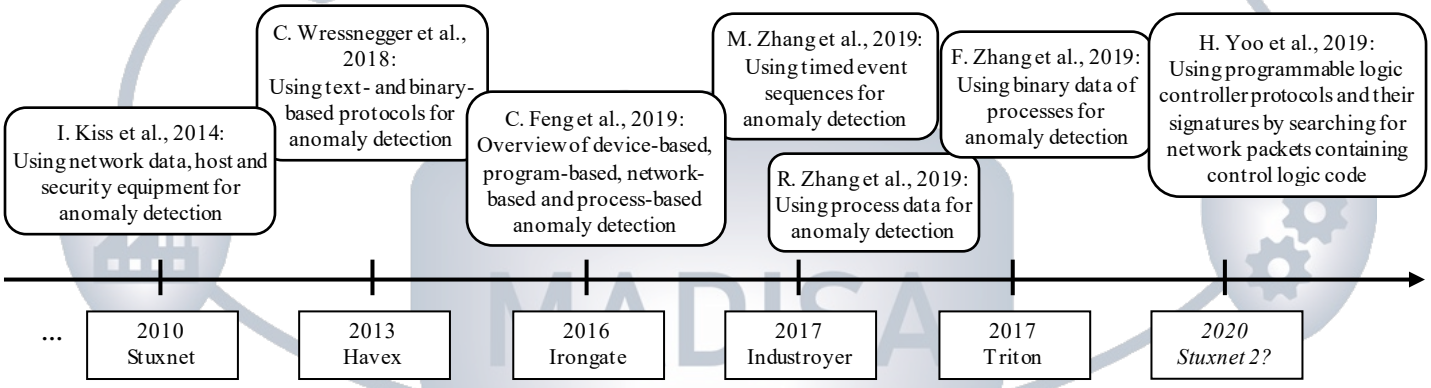
Laura Hartmann and Steffen Wendzel

University of Applied Sciences Worms, Germany

Since anomaly detection on the historical data of industrial control systems (ICS) is nearly unexplored, the project MADISA (*Machine Learning for Attack Detection Using Data of Industrial Control Systems*) deals with a data-based approach on those data-sets. This poster provides an overview of the data investigated in this research.

MADISA – The idea

The project analyses code and configuration files that were potentially modified to damage product, machine or surrounding environment due to incorrect entries or changed values by cyber attacks. Anomalous values should first be described as features and later be found and reported by a supervised machine learning system. To train this system, malicious configurations will be simulated based on our found heuristics and interviews with the manufacturer. For this purpose we received real-world project data from a German car manufacturer. The meta-data that can be affected by malicious changes are briefly highlighted in this early-work poster to show a potential path for ICS-focused anomaly detection. The folder and file structure of the projects can also give an indication of whether an attack is present on the system, since, for example, code snippets have been stored in the system whose execution causes malicious changes. The different types of ICS data are physical process data, code, configuration and meta-data of files. The focus of the MADISA project is on the latter three.



This research was funded by the European Union from the European Regional Development Fund (EFRE) and the State of Rhineland-Palatinate (MWWK), Germany. Funding content: P1-SZ2-7 F\&E: Wissens- und Technologietransfer (WTT), Application no 84003751.

madisa.ztt.hs-worms.de
hartmann@hs-worms.de
wendzel@hs-worms.de