Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control Systems

Title	Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control Systems
Publication Type	Conference Paper
Year of Publication	2017
Authors	Sugumar, G., Mathur, A.
Conference Name	2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)
Date Published	jul
ISBN Number	978-1-5386-2072-4
Keywords	6-stage operational water treatment plant, and Cyber Physical Systems, attack detection, attack detection mechanisms, Automata, automata theory, Clocks, coding theory, compositionality, computer security, critical infrastructure , cryptography, Cyber Attack Detection, cyber attack prevention, cyber security, formal methods, formal verification, ICs, industrial control, industrial control systems, Integrated circuit modeling, legacy systems, Metrics, process invariants, pubcrawl, resilience, Resiliency, security, security of data, security requirements, security specifications, software maintenance, timed automata, UPPAAL, Valves, water supply, water treatment

Abstract

Industrial Control Systems (ICS) are found in critical infrastructure such as for power generation and water treatment. When security requirements are incorporated into an ICS, one needs to test the additional code and devices added do improve the prevention and detection of cyber attacks. Conducting such tests in legacy systems is a challenge due to the high availability requirement. An approach using Timed Automata (TA) is proposed to overcome this challenge. This approach enables assessment of the effectiveness of an attack detection method based on process invariants. The approach has been demonstrated in a case study on one stage of a 6- stage operational water treatment plant. The model constructed captured the interactions among components in the selected stage. In addition, a set of attacks, attack detection mechanisms, and security specifications were also modeled using TA. These TA models were conjoined into a network and implemented in UPPAAL. The models so implemented were found effective in detecting the attacks considered. The study suggests the use of TA as an effective tool to model an ICS and study its attack detection mechanisms as a complement to doing so in a real plant-operational or under design.

URL http://ieeexplore.ieee.org/document/8004305/
DOI 10.1109/QRS-C.2017.29
Citation Key sugumar_testing_2017

6-stage operational water treatment plant and Cyber Physical Systems Attack detection attack detection mechanisms automata automata theory Clocks coding theory Compositionality computer security critical infrastructure Cryptography Cyber Attack Detection cyber attack prevention cyber security formal methods formal verification ICs industrial control Industrial Control Systems Integrated circuit modeling legacy systems Metrics process invariants pubcrawl resilience Resiliency security security of data security requirements security specifications software maintenance timed automata UPPAAL Valves water supply water treatment