CASE STUDIES

We provide Python NetworkX graph data (JSON format) for boiler system along with the release of a HAI 23.05 and HAIEnd 23.05. You can create the separate graphs for the two subsystems: the digital subsystem and physical subsystem and also merge them by connecting the sensor and actuator nodes of the two subsystems. The NetworkX graphs helps in analyzing and optimizing anomaly detection performance. Several case studies with this tool are as follows.

Data flow graph for digital subsystem

PCL-based data flow graphs are suitable for user purposes using typical graph analysis methodologies.

For example, when analyzing attack scenario initiated by the digital subsystem (DCS, HMI, EWS and

so on), the reachability to all traversal results from the start node (attack initiation) to the end node (attack target) can be used, and extracts and selects all reachable paths as traversal results. Furthermore, an attack propagation chain (APC), a path composed of nodes and edges affected by the attack, is provided for sophisticated analysis for anomaly detector.

CASE I: ATTACK PROPAGATION CHAIN

An APC describes a path composed of nodes and edges being attacked and applies forward analysis

to the graph to determine the propagation path in the forward direction with the analysis target node as the starting point. It then determines which nodes and edges are situated along the propagation path affected by the attack. APCs can also be used to identify hidden targets and scopes when constructing an attack scenario.

When HMI is compromised by an attacker, the impact can be identified using an APC as indicated by

the bold path as shown in Figure 16. Attack propagation chain is derived as two distinct paths. The first path (In order of path: 1001.7, 1001.8, 1001.20, 1001.21, 1001.22/1001.23, and 1001.24) refers to a situation in which an attacker spreads the influence through keyboard manipulation of the HMI. The second path (In order of path: 1001.5, 1001.14, 1001.15, 1001.16, 1001.17, 1001.18, and 1001.19) indicates the effect of manipulation the setpoint. In particular, here is an APC for one of the attack scenarios described in previous section. When manipulating internal point at DM-PCV01-D in 1001.21 (i.e., ATTACK SCENARIO AE05), the impact can be identified using an APC as indicated by the bold path as shown in Figure 17. Once the attack proceeds at entry point, related data (control and measurement values) of PCV01 and PCV02 are affected as well.

CASE II: ROOT-CAUSE ANALYSIS

In contrast to APC, backward analysis of a graph can elucidate the root-cause of an attack. The attack entry point can be identified from the node corresponding to the path end by tracing the path backward from a specific node. For example, when backward analysis is applied to the graph for anomaly of PIT01 as shown in Figure 18, root-cause (HMI, HIL, EWS) can be provided.

Physics-related flow graph for physical subsystem

A Physics-related flow graph is a visual representation of the interconnected components and processes within a physical subsystem. It provides a clear and organized overview of how energy and information flow through different elements of the system, enabling the analysis and understanding of its behavior.