Faculty and PostDoc, Science and Engineering

CYBER-PHYSICAL INDUSTRIAL CONTROL SYSTEM TESTBED: A CYBER-SECURITY SOLUTION

By Mohammad Noorizadeh, Mohammad Hussein Shakerpour, Nader Meskin, Devrim Unal

INTRODUCTION

In this project, the hybrid testbed architecture is selected for the development of ICS testbed where the Tennessee Eastman (TE) plant is simulated inside PC and the remaining components are implemented using real industrial hardware. TE plant is selected as the industrial process for the developed cybersecurity testbed due to the following reasons. First, the TE modTheel is a well-known chemical process plant used in control systems research and it dynamics is well-understood. Second, it should be properly controlled otherwise small disturbance will drive the system toward an unsafe and unstable operation. The inherent unstable open-loop property of the TE process model presents a real-world scenario in which a cyber-attack could represent a real risk to human safety, environmental safety, and economic viability. Third, the process is complex, coupled and nonlinear, and has many degrees of freedom by which to control and perturb the dynamics of the process.

ATTACK HISTORY

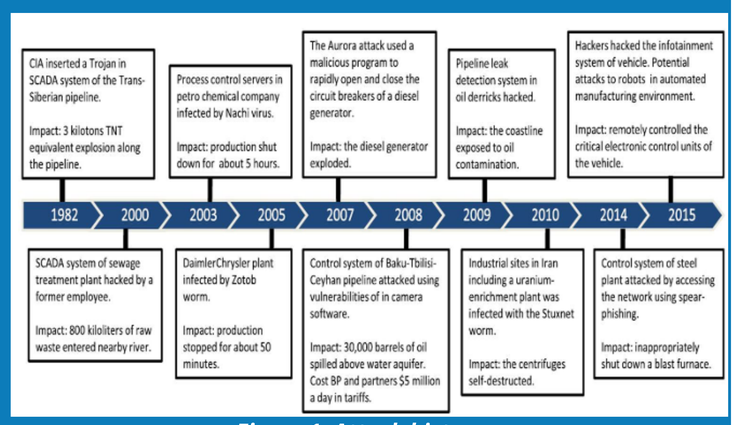

Figure 1: Attack history

OBJECTIVE

In this project, a hybrid testbed was implemented. An physical attack is injected into the system, and by the use of a machine learning algorithm, namely isolation forest, the attack is detected as an anomaly. The main objective is to detect the anomaly before system goes to the shutdown condition.

TENNESSE EASTMAN PROCESS SIMULATION

TE process is first described by Down and Vogel in 1993. The process is modeled through fifty nonlinear and coupled differential equations and it consists of five major operation units: chemical reactor, product condenser, recycle compressor, vapor-liquid separator, and product stripper . Two liquid products (G, H) are produced using A, C, D, E gaseous reactants with B and F as inert and byproduct, respectively.The chemical reactions are irreversible and can be presented as follows:

$$A(g) + C(g) + D(g) \rightarrow G(l), \text{ Product 1,}$$
$$A(g) + C(g) + E(g) \rightarrow H(l), \text{ Product 2,}$$
$$A(g) + E(g) \rightarrow F(l), \text{ Byproduct,}$$
$$3D(g) \rightarrow 2F(l), \text{ Byproduct.}$$

The control objectives of TE process are listed below

Maintain process variables at desired values,

Keep process operating conditions within equipment constraints,

Minimize the variability of product rate and product quality during disturbances,

Minimize the movement of valves which affect other processes,

Recover quickly and smoothly form disturbances, production rate changes or product mix changes.

SYSTEM STRUCTURE

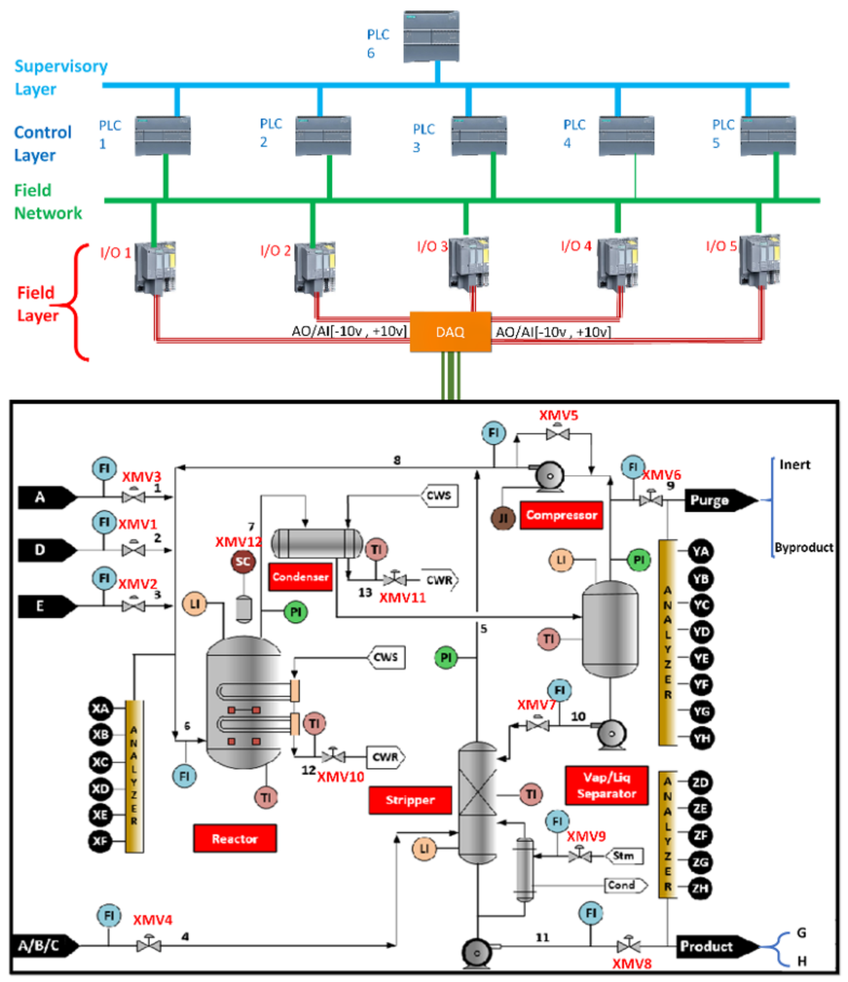

Figure 1: System Architecture

Table 1: Sensor measurements

Variable name	Variable number	Units
A feed	XMEAS 1	kscmh
D feed	XMEAS 2	kg/h
E feed	XMEAS 3	kg/h
A and C feed	XMEAS 4	kscmh
Reactor pressure	XMEAS 7	kPa gauge
Reactor level	XMEAS 8	%
Reactor temperature	XMEAS 9	C
Purge rate	XMEAS 10	kscmh
Prod. separator temperature	XMEAS 11	C
Prod. separator level	XMEAS 12	%
Prod. separator underflow	XMEAS 14	m3/h
Stripper level	XMEAS 15	%
Stripper underflow	XMEAS 17	m3/h
A Concentration	XMEAS 23	mol %
C Concentration	XMEAS 25	mol %
G Concentration	XMEAS 40	mol %

Table 2: Actuator measurements

Variable name	Variable number	Units
D-feed flow	XMV 1	kg/h
E-feed flow	XMV 2	kg/h
A-feed flow	XMV 3	kscmh
A and C feed flow	XMV 4	kscmh
Purge valve	XMV 6	%
Separator pot liq. flow	XMV 7	m3/h
Stripper liq. prod. flow	XMV 8	m3/h
Reactor cw. flow	XMV 10	m3/h
Condenser cw. flow	XMV 11	m3/h

RESULTS

The results shows that the ML algorithm successfully detected the different attacks before the system goes to the shutdown condition illustrated in Table 3:

- Reactor pressure exceeds 3000 pa
- Reactor temperature exceeds 175 ^oC
- Reactor level exceeds 24.0 m^3 or decreases below 2.0 m^3
- Stripper level exceeds 8.0 m^3 or drops below 1.0 m^3
- product separator level exceeds 12.0 m^3 or drops below 1.0 m^3

Table 3: ML performance

ATTACK	DETECTION TIME
PLC1_DEC	2 min
PLC1_INC	57 min
PLC2_DEC	32 min
PLC4_DEC	50 min
PLC5_INC	45 min

CONCLUSION

To sum up, the hybrid testbed has been implemented successfully. Hence, by generating a realistic data-set that can be considered thanks to using hardware-in-the-loop. By training the algorithm based on the data-set, attacks were detected timely before the shutdown condition. Future work includes extending the testbed to higher levels of automation hierarchy in addition to connecting with the CyberRange at Qatar University.

ACKNOWLEDGMENT

This publication was made possible by NPRP grant No. NPRP10 – 0105 – 170107 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

HYBRID ICS TESTBED

As shown in Figure 1, the developed testbed is split into three layers: Tennessee Eastman plant simulated inside PC, field devices emulated using DAQ and Siemens distributed I/O, and the control layer implementation using Siemens PLCs.

Accordingly, the mathematical model of the TE process is implemented and simulated in Matlab/Simulink environment and the controllers are implemented inside PLCs. The interface between the plant simulation and PLCs is done using DAQ boards and distributed I/O module. The distributed I/O modules provide the interface between the plant sensors/actuators and PLCs. Consequently, the DAQ boards and distributed I/O modules emulate layer 1 in the industrial automation hierarchy, namely the field layer.

NETWORK ARCHITECTURE

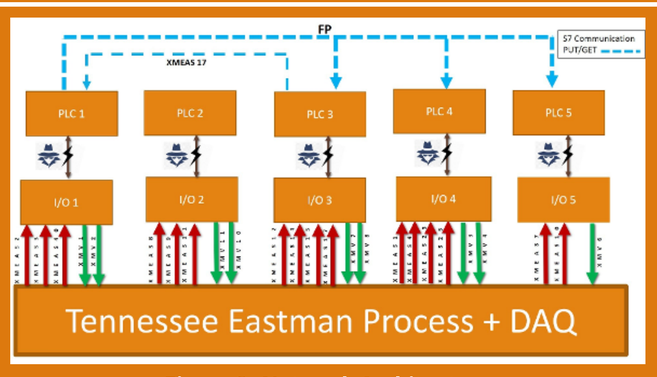

Figure 2: Network Architecture

TESTBED OVERVIEW

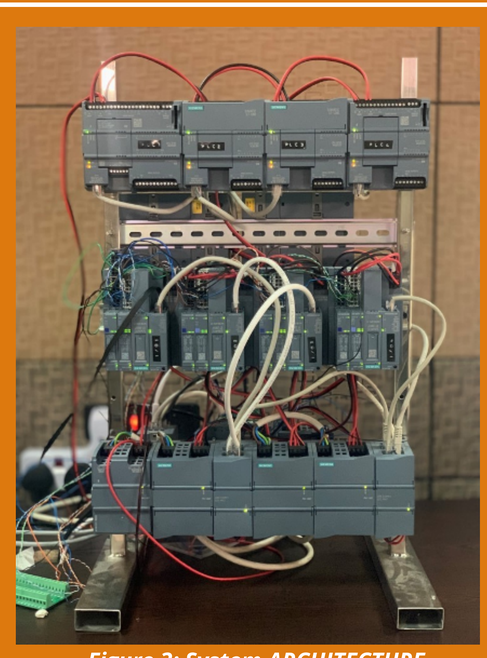

Figure 3: System ARCHITECTURE

ATTACK

In this section, our methodology for injecting cyber-attacks on the developed testbed is presented. Generally, different protocols enable various attack surfaces such as Data integrity attack (e.g. manipulating sensor measurement), and Denial-of-Service (DoS) which causes the disruption of communication flow between entities. In an ICS architecture, attacks can be generally categorized into two general types as configuration and operational attacks. In the configuration attack, the attacker targets the configuration protocols of ICS and consequently gets the full control of the system. On the other hand, in the operational attacks, the attacker mainly targets the operational communication protocol such as PROFINET IO Real-time data, in which critical field data are transferred. For this attack to take place, it is assumed that:

The attacker has field level access to IO Module and PLCs.

Attacker has knowledge of the physical system, meaning that, he/she is aware of what is being transmitted from sensor and what is being transferred to actuators.

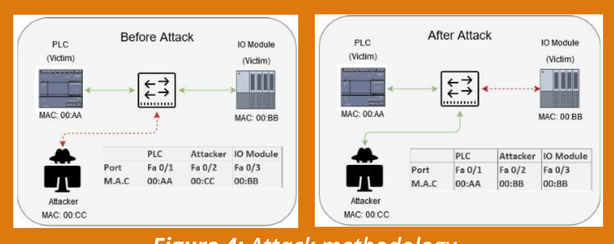

Figure 4: Attack methodology