WiP Abstract: KRS-DGIST: A Resilient CPS Testbed for Radio-Based Train Control

Yuchang Won
DGIST
Republic of Korea
yuchang@dgist.ac.kr

Buyeon Yu
DGIST
Republic of Korea
yubuyeon@dgist.ac.kr

Jaegeun Park
DGIST
Republic of Korea
jaegeun2@dgist.ac.kr

In-Hee Park
DGIST
Republic of Korea
inhee@dgist.ac.kr

Haegeon Jeong
Hanyang Univ.
Republic of Korea
haegeonj@hanyang.ac.kr

Jeanseong Baik
Hanyang Univ.
Republic of Korea
jsbaik@hanyang.ac.kr

Kyungtae Kang
Hanyang Univ.
Republic of Korea
ktkang@hanyang.ac.kr

Insup Lee
Univ. of Pennsylvania
PA 19104 USA
lee@cis.upenn.edu

Kyung-Joon Park
DGIST
Republic of Korea
kjp@dgist.ac.kr

Yongsoon Eun
DGIST
Republic of Korea
yeun@dgist.ac.kr

***Abstract*—This paper presents an architecture for cyber-physical systems resilient against external attacks and internal faults. The target CPS consists of multiple physical systems equipped with local embedded systems, a supervision module that oversees operations of the physical systems, and communication network connecting each physical system to the supervision module. We give an instantiation of the architecture on a radio-based train control system to demonstrate the resiliency under various safety critical scenarios. The testbed entitled KRS-DGIST includes a commercial train control and supervision software deployed in the Philippines. The railway installed sensors and other mechanisms are implemented reflecting the actual train control and supervision system, and the dynamics of the trains is computer simulated. Demonstrations are given with attacks on sensors, communication network, and embedded systems.**

I. Introduction

Cyber-physical systems (CPS) refers to next generation engineered systems that require tight integration of computing, communication, and control technologies to achieve stability, performance, and efficiency with a higher level of coordination between physical and cyber entities [1], [2], [3]. Because many critical infrastructures of our society are constructed in the framework of CPS, the importance of resiliency has received increasing attention. By the term 'resiliency' we imply systems that can tolerate a level of malicious external attacks or internal faults; maintain core functionalities if continued normal operation is not possible; and fail gracefully if inevitable.

This paper presents an architecture for resilient CPS on radio-based train control systems. The target CPS is assumed to have multiple physical systems equipped with local embedded systems, a supervision module that oversees and coordinates the operation of the physical systems and communication network connecting each physical system to the supervision module as shown in Fig. 1. In particular, metro railway systems consist of trains with embedded local controller with sensors and actuators, an operation control center that schedules, monitors and coordinates the movement of trains at and between stations, and communication network over which the center and each train send and receive information. In fact, not only train systems, but also many CPS applications such as drones, airplanes, and ground vehicles fall into the described architecture.

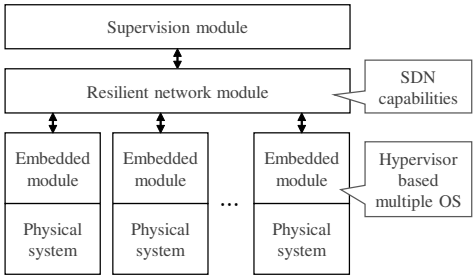

Figure 1. Resilient CPS architecture.

Here, we focus on a radio-based train control system to demonstrate the resiliency under various safety critical scenarios. The trend of adopting advanced communication technologies including Wi-Fi to improve train operation efficiency is on the way and several new systems have been built in this manner. We expect that the opening of the system to radio-based communication will increase the importance of system resiliency against malicious attacks.

The testbed entitled KRS-DGIST consists of a supervision module, radio-based communication network, embedded systems on the train, and railway train dynamics simulator. Details of each component are given in the next section. We demonstrate improved resiliency of the proposed architecture under various feasible safety critical scenarios.

II. Radio-Based Train Control Systems

Conventional metro systems consist of the automatic train supervision (ATS), automatic train protection (ATP), automatic train operation (ATO), trains, railways and tracks with installed sensors, stations, and a wired communication system.

The ATS schedules, monitors, and coordinates the operation of trains, which corresponds to the supervision module

0-7695-6378-3/18/$31.00 ©2018 IEEE
DOI 10.1109/ICCPS.2018.00043

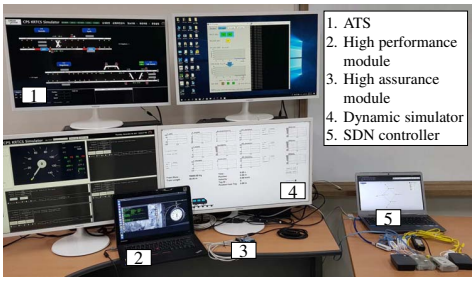

Figure 2. Radio-based train control system testbed.

in Fig. 1, the train equipped ATO, ATP and other communication devices that correspond to the local embedded systems, trains themselves, railway and tracks with sensors corresponding to the physical systems, and finally the wired communication systems corresponding to the communication network. In our testbed, the ATS is constructed with commercial software and the track data for a certain line in the Philippines.

The embedded systems, i.e., train onboard ATP and ATO are similar to the conventional one, but the train controller in the ATO is made with simplex architecture [4], consisting of high performance module and high assurance module. The two are, respectively, installed on a laptop computer and an embedded Odroid XU4 board. The high assurance module runs multiple copies of Ubuntu on a kernel-based virtual machine (KVM). The high performance module has train motion control algorithm, and additional algorithms that provide resiliency including sensor attack detection algorithms and attack-resilient state estimation algorithms.

Communication network is constructed with software define networking (SDN) technology so that network intelligence and state are logically centralized in the SDN controller. Specifically, an ONOS SDN controller is installed on a laptop and the SDN switches are implemented using an embedded Raspberry Pi. One of the switches is wired to ATS, other switches are wirelessly connected to the train onboard embedded systems. Both wired and wireless communication protocols follow KRS-SG-0069 standard [5] that has been developed for radio-based train control in Korea, which closely follows the international standard.

The physical systems, e.g., the trains and the topology of the tracks are constructed using a dynamic simulator. This includes train dynamics from force to position, sensors such as encoders on trains, position tags on the tracks.

III. Demonstration

We consider various attack scenarios on the radio-based train control testbed and demonstrate resiliency of the proposed architecture. The scenarios are described as follows:

Attacks on physical systems: Attacks on encoders in the form of bias injection on the velocity can cause a train to collide with the preceding train. In order to avoid the collision, an attack detection algorithm [6] is implemented to monitor individual sensors. This algorithm enables the system to tolerate sensor failure as long as at least one sensor remains intact. Otherwise, the train stops gracefully. Other algorithms for sensor attack detection can be implemented in the module. We point out that in the conventional systems, the only way to avoid collision is for the train operator to manually apply emergency brake.

Attacks on local embedded systems: Upon detection of the high performance module failure using a monitoring mechanism, the high assurance module implemented in the Odroid XU4 takes over the train control, and stops the train gracefully.

Attacks or faults on the operating systems (OS) of the embedded module: Assuming that failure of an OS is detected, a critical application on the failing OS, in our testbed the train velocity controller, is migrated to another OS on the KVM. While this is done by sequencing the KVM commands, employment of advanced techniques such as container based migration is underway.

Attacks on the network: We analyze the KRS-SG-0069 standard and discover that ARP-spoofing attack is possible. The discovered attack can change the data transmitted from the ATS to a train, and can make the train collide with the preceding one. This attack is neutralized by functional-level hot-patching method [7] or by rerouting network traffic around the compromised node upon detection using SDN capabilities.

Acknowledgment

Three leading authors contributed equally on this work. Yongsoon Eun and Kyung-Joon Park are the co-corresponding authors. This work was partially supported by an IITP grant, funded by the Korea government (MSIT) (2014-0-00065, Resilient Cyber-Physical Systems Research) and by GRL grant (NRF-2013K1A1A2A02078326).

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-Physical Systems: The Next Computing Revolution," in *Proc. 47th Design Autom. Conf.* (DAC), pp. 731–736, 2010.

[2] K.-D. Kim and P. R. Kumar, "Cyber-Physical Systems: A Perspective at the Centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, 2012.

[3] K.-J. Park, R. Zheng, and X. Liu, "Cyber-Physical Systems: Milestones and Research Challenges," *Computer Communications*, vol. 36, no. 1, pp. 1–7, December 2012.

[4] L. Sha, "Using Simplicity to Control Complexity," *IEEE Software*, vol. 18, no. 4, pp. 20–28, 2001.

[5] KRS-SG-0069: Korean Radio Based Train Control System for Urban Rapid Transit. [Online]. Available: http://krs.krri.re.kr/MultiViewer/ViewStartFrame.aspx?cid=72548&gubun=K&xSize=1890&ySize=930 (in Korean).

[6] B. Yu and Y. Eun, "Sensor Attack Detection for Railway Vehicles Using Topographic Information," in *Proc. 17th Int. Conf. Control, Autom. and Sys.* (ICCAS), pp. 149–154, 2017.

[7] H. Jeong, J. Baik, and K. Kang, "Functional Level Hot-Patching Platform for Executable and Linkable Format Binaries," in *Proc. IEEE Int. Conf. Sys., Man, and Cybernetics* (SMC), pp. 489–494, 2017.