Introductory to Cyberphysical System Integration Security (CSIS)

Michael John Curnow II

CPS Security SME,

Defiant Networks, Inc.

North Carolina, USA

Table of Contents

Purpose

This document serves as the inception and introductory to the field of cybersecurity study, research and development titled “Cyberphysical System Integration Security” (CSIS), and substantiate the significance of it’s existence and efforts to secure communications between cyberphysical systems (CPS) and informational technology (IT) systems in scalable and robust fashions.

Design & Methodology

This document makes use of identifying security gaps in connectivity methods between CPS and IT systems coupled with use of graphical representations, threat models, and cases.

Practical Implications

Readers of this document will learn about how CPSs integrate with IT systems for data-collection and management purposes in regards to the context of Industry 4.0, many of the inherent insecurities in modern practices, and the further downstream implications of insecure CPS integrations. In addition to this, readers will learn what it takes to commit meaningful contributions to the CSIS field and overall secure the underpinnings of Industry 4.0.

Goal

The goal of CSIS as a field is to ensure transcendent and robust methods of defense for the cyberphysical transport layer that’s purpose-built to meet the needs of varying integrations and use cases. CSIS promotes achieving this through any of the following methods defined herein (but not necessarily limited to):

- Research
  - Security
    - Uncover connectivity vulnerabilities in defined CPS
    - Collect and/or generate intelligence on any compromise or exploit making use of CPS connectivity as an attack vector
    - Collect and/or generate intelligence of APT groups employing aforementioned compromises or exploits

    - Academic Papers
        - Papers illustrating cases regarding the security standing of a connectivity practice a broad or defined CPS employs
        - Papers proposing solutions or practices (technical, procedural, or both) to secure either broad or defined CPS
- Development
    - Engineering
        - Protocols to secure a broad or defined CPS connectivity with related assets
        - Tools to bolster security of CPS and how it integrates with outside systems
    - Methods
        - Tactics, techniques, and procedures (TTPs) to secure and harden your CPS communication over traversed distances
        - Frameworks for deploying technology or methods to secure broad or defined CPS
- Content
    - Policies, standards, and guidelines to bolster operations around securing CPS to protect it when interacting with integrated systems
    - Multimedia covering:
        - State of security of a broad or defined CPS
        - Techniques to secure broad or defined CPS
        - Techniques to infiltrate broad or defined CPS

Introduction to CSIS

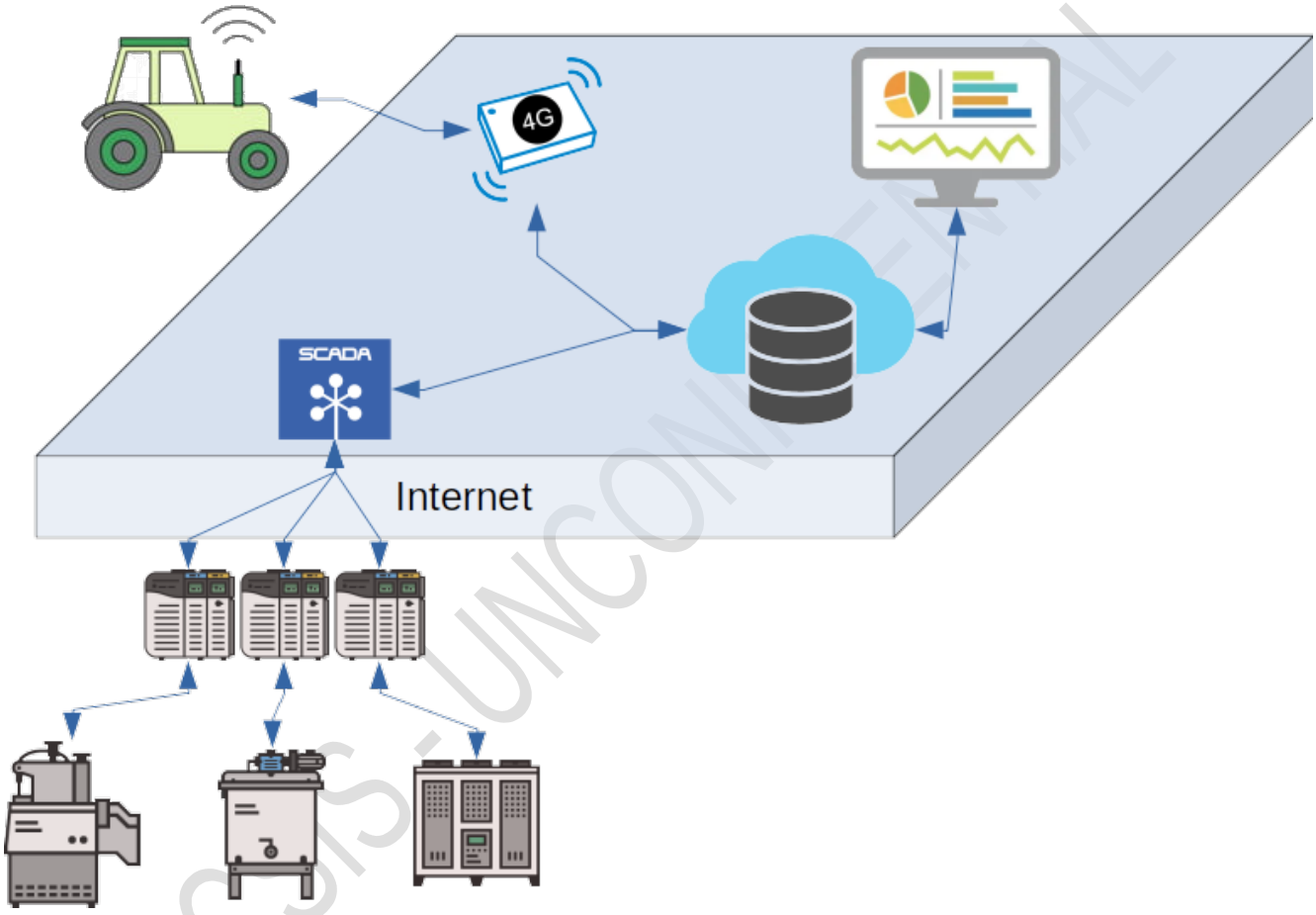
Due to rapidly increasing inter-connectivity between Operational Technology (OT) and cloud or remote/off-premises systems as a result of the 4th Industrial Revolution (Industry 4.0) and the Internet-of-Things (IoT) paradigm shift, the cyberphysical attack surface has grown exponentially. Expanding management and analysis capabilities to remote manufacturing facilities, IOT, connected-vehicles, and other semblance of CPS requires system integration to otherwise coalesce geographically distant devices for unified command and control over digital systems and CPS. This can take place over the internet or in closed private networks via:

- direct cabled connections
  - RJ-45
  - fiber
  - serial
- wireless connections:
  - bluetooth/BLE
  - WiFi
  - cellular 4G LTE (5G upcoming)
- some combination of 2 or more mediums
- Something novel and not listed above

And though the connectivity mediums may differ, advance, or change entirely, the practice of securing such will remain paramount in bolstering the foundations of Industry 4.0, and allow for a safer yet quicker advancement into further states of industrial revolution and societal progression worldwide.

Current problem

In modern practice it's quite prevalent to expose and open OT assets to the public internet to facilitate some sort of remote connectivity, be it for remote access & maintenance, or to interface omnidirectionally with a myriad of tools or platforms. In this deployment model, the device openly broadcasts to the worldwide internet which protocols it's likely using, on which port it's operating on, and in some cases it's actual location.



In industry, this is often referred to as the known and prolific terms of "IT/OT Convergence", "hyperconnectivity", or "digital transformation". This serves a business use-case (and need in most cases) to optimize factories, manufacturing facilities, smart farms/cities/roadways, and the many forms of IoT.

The threat to this model comes in the form of potential interference to the OT assets or other systems related to the CPS itself. This can occur in a number of ways, to include (but not limited to):

1. Denial of Service
    1. OT assets in a CPS, like Programmable Logic Controllers (PLCs) for example, are widely susceptible to overwhelming their throughput, especially on ports for industrial specific protocols like ModBus, S7, DNP3, etc.
2. Man in the Middle
    1. An attacker may misappropriate the identity of an intended recipient in CPS's upstream/ communication(s) to a collection service in efforts to identify useful artifacts from captured traffic.
3. Fuzzing
    1. An attacker can deduce which protocol these exposed devices are using to ascertain the level of input validation and robustness of it's throughput through randomized interactions.
4. Misuse of device specific protocols
    1. A device's native protocol(s) can be exploited to conduct unauthorized actions.

Many critical assets spend many years in an air-gapped environment, using physical controls to ensure that no network connectivity exists with the outside world. But this isn't sustainable when today digital transformation is almost a necessity for a business's success, though the degree of such can rest entirely on the myriad of unique use cases. But once a critical asset is internet exposed, be it a SCADA system, any industrial PC (IPC), or any other kind of management layer tooling, becomes fallible to the same vulnerabilities that any other computer with internet access is. And in the case for SCADA systems, Human Machine Interfaces (HMIs) and IPCs, these are often legacy operating systems with many unpatched vulnerabilities.

Implications

CPS & IoT are already here, and they're here to stay. The future of society that's being built right now is centered around automation & control in CPS and telemetry analysis to better increase efficiency and capabilities of that very same automation and control. This is necessary for smart-cities and smart-roadways and any other connected infrastructure to function in an optimal capacity, and grow in a sustainable fashion. Many other semblances of CPS share the same aforementioned necessities, whether it be an IoT home alarm & security system you can monitor and control from a mobile device to an administrative dashboard to gain clarity of your facilities industrial processes and overall equipment effectiveness (OEE).

The common denominator amongst these technologies is that one or more components in any CPS carries impact in the physical world (albeit to varying degrees). If any of these systems were to be compromised, this carries with it high probability of damage to property and loss of human life. The following examples illustrate the aforementioned implications of potential compromise:

1. A streetlight is compromised to produce 2 green lights on adjacently angled streets of an intersection, motorists will suffer injury and deaths will likely occur, coupled with mass property damage.
2. An internet connected vehicle drives in range of a fake base-station/cellular-site-simulator, and can successfully trick the vehicle into a faulty Firmware Over The Air (FOTA) update to flash ECUs with malicious firmware. This may put the motorist's life at risk.
3. Internet exposed industrial devices like PLCs and control systems are susceptible to multiple low complexity attacks that can have hazardous effects on equipment it controls, putting the safety of those in range of that managed piece of equipment in potentially immediate risk.
4. A wearable insulin pump that interfaces wirelessly via radio, bluetooth, or a phone/web application can be compromised to accept a malicious replayed interactions captured, which tells the pump to release the entirety of it's contents into the wearer, resulting in an insulin overdose.

Digital transformation of CPS suffers many current vulnerabilities due to it's omnipresent connectivity, many of which aren't given attention to in the early stages of conception. So when new vulnerabilities are discovered in a component(s) of a CPS, subsequent patching very well may require an inordinate timeframe to employ due to potential up-time, availability, and safety concerns involved with patching of CPS. This does depend on the type of system though. Longer timeframes are typically present in manufacturing and infrastructure environments, whereas deployed CPS at a small scale (considering volume and management) may take considerably less time to properly patch and test changes. However a single discovered compromise might be relevant to a component that's quite prevalent in major connected-infrastructure, thus resulting in many systems susceptible to the same attack and won't be able to deploy changes in the short-term that'd effect that particular process's up-time.

Much in the way that poor security practice in the digital transformation of industrial control systems and infrastructure expand the overall cyberphysical attack surface, the same can be said for the ubiquitous IoT presence in the home, though the attack vector and implied impact would differ contextually from the aforementioned example, in that the threat model itself would be of a different context. These compromises would have an effect much "closer to home". If your smart-thermostat in your home is compromised then it can be used to directly effect the climate of your residence/domicile, or if your connected home security and alarm system is compromised then unlocking doors and traversing your home would be an easy feat for one wishing to burglarize your home.

CSIS Hard-Challenges

Some text about what these hard-problems are.

1. Policy & Governance

    Challenge: Develop processes to enforce standardized requirements of identified and proven methods proposed to secure communications of integrated CPS, and to do such in a way that's intuitive enough to compliment (or at least not entirely hinder) current industry security guidelines.

2. Robustness & Resilience

    Challenge: Tactics, techniques & procedures (TTPs) employed, whether policy driven or those of a technical nature (or both), MUST be built for long term persistence to withstand a variety of interference and unexpected changes, all the while be resilient enough to quickly recover from whatever scenario that could put the integrity or up-time of the integration in jeopardy.

3. Scalable Solution Architecture

    Challenge: Solutions purpose-built or crafted to meet the need of securing connectivity in a CPS MUST account for an inevitability that component and connectivity volume isn't a static metric, and should allow the system, which the solution is applied to, to retain it's operability when faced with changes in size.

4. Integrability & Adaptability

    Challenge: Applying solutions to secure connectivity in a CPS MUST NOT hinder operation or integrity of the CPS component(s) when introduced into the environment. Any solution designed and proposed as a method for securing CPS connectivity MUST accommodate all industrial, operational, informational and communication protocols necessary for CPS component(s) to function independently and also as a constituent of a larger system (this is to include functionality with third-party solutions).

5. Human/Operator Element

    Challenge: In Industry 4.0's forseeable future, there will always be a human influence or presence somewhere in a CPS. This is true for someone to manage, monitor, integrate, and troubleshoot. Any solutions proposed for securing CPS connectivity should account for a human-driven margin of error, with proper measurements and redundancies in place.

Conclusion

For Industry 4.0 to grow, (vertical & horizontal) system integration is a key factor. It allows the otherwise arguably separate silos of Industry 4.0 (*big data, autonomous robots, simulation, systme integration, IoT/IIoT, cloud computing, additive manufacturing, augmented reality, and cybersecurity*) to work closely with one another in a seemingly unified mesh of I/O and capability. And in order for Industry 4.0 to advance and transcend to higher levels of industrial revolution, securing the connectivity between IIoT/IoT and the CPS components they're integrated with is paramount. Without it, further introduction of CPS Industry 4.0 may very well serve to rapidly expand the cyberphysical attack surface, and put even more lives at risk from insecure IoT/IIoT deployments. As these insecure CPS are ubiquitous today, we need to start tackling the challenges set forth in this document in order to assure a sense of preparedness, both technical and procedural, to ensure a safe, secure, and optimal advance in industrial and societal advances. CSIS serves as that effort to build the proper foundations for safety and security that will further our sustainable progress now and in the future.