Security Application Brief
SPRACO8–October 2019

Programmable Logic Controllers — Security Threats and Solutions

Amrit Mundra, security architect and VC Kumar, marketing manager *Processors*

ABSTRACT

This security application brief provides an example security analysis for programmable logic controllers. The intent is to highlight various potential threat scenarios and corresponding steps to help combat them. This process includes the identification and ranking of potential threats and exploring relevant TI security enablers.

This brief leverages the first.org CVSS 3.1 calculator. All scoring in this brief is based on TI's assessment. Readers should adjust each parameter according to their targeted applications and system designs.

Contents

1 Introduction 2
2 Reinventing the PLC for Industry 4.0 2
3 Security implications 3
4 TI security frameworks 4
5 TI devices with security enablers 6
6 Conclusion 7
7 References 7

Trademarks

1 Introduction

A programmable logic controller (PLC), also known as a programmable controller, serves as a computer for industrial manufacturing. PLCs bring flexibility (ability to reprogram quickly) with reliability (minimal power down and maintenance) and ease of use in a standalone factory environment. Originally conceived for the auto manufacturing industry in the 1960s to replace hard-wired options such as relays and enable programmable, real-time control of equipment, PLCs are now ubiquitous in the manufacturing industry. They are a necessary component of factories of today and of future, and instrumental to safety, reliability and continuous operation.

Over the past five decades, PLCs have evolved to meet the ever-growing needs of more automation and more data handling. This includes miniaturization, deterministic communication, moving to distributed control systems and cloud connectivity.

Figure 1. A typical PLC

2 Reinventing the PLC for Industry 4.0

Industry 4.0, also known as the Fourth Industrial Revolution, typically refers to the digitization of the manufacturing industry and the collection and use of information in real time to create smart factories. The goal is to sense, share and control health data, status and operation of factory equipment and product in real time while enabling intelligent and self-aware machines such as robots to drive increased efficiency and flexibility.

The digitization of the factory requires communications, information technology (including cloud storage and interaction), and data and physical elements like PLCs in factories, where machines interact with humans, other machines and the products being manufactured. Integrated sensing delivers decision-critical data, and real-time information processing, control and communication are driving profound changes in the entire industrial ecosystem [1].

Industry 4.0 is depending on PLC technology to be a key factor in this transformative evolution.

3 Security implications

Before looking at the security threats and possible solutions, quickly review how PLCs fit into the factory/Industry 4.0 world. In Figure 2, PLCs are in each element.

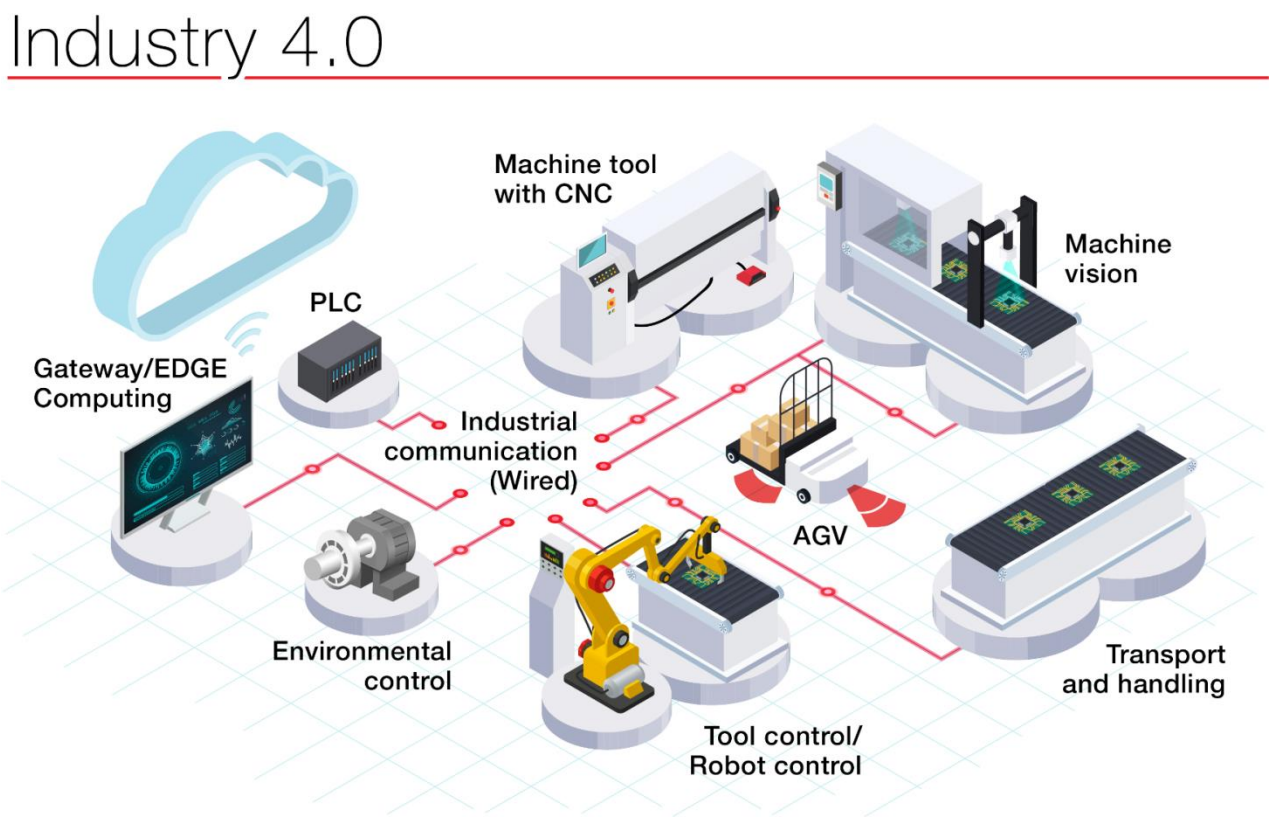

Figure 2. Factory floor setting

As factories have evolved, a few trends are worth considering for PLCs in the context of security [2]:

- Networked environments. In today's automated factories, PLCs are no longer stand-alone components. They need to interact in real time with each other within different systems in a factory, and potentially with cloud metadata to make control decisions in real time. Network reliability and is a priority.
- Distributed control. The world has moved from centralized control brains in factories to a more distributed control model of several autonomous subsystem brains, sometimes even within the same machine. This places a premium on real-time communication integrity and network reliability.
- Deterministic communication. The need to respond to faults or failures, especially in an automated environment, places a premium on communication and processing reliability with low latencies.
- Minimal downtime. The push to minimize downtime has driven the demand for hot-plug features. A need exists for trust and integrity checks to potentially span multiple sessions, not just within the same session.

3.1 Threat descriptions and risk assessment

Given the critical role that PLCs play in digital factories, Table 1 shows the potential attacks that can leave factories vulnerable. The threat scores listed in the third column leverage the first.org Common Vulnerability Scoring System Version 3.0 Calculator [2]. The higher the score, the greater the security risk, indicating the need to take proactive steps to enable countermeasures.

Table 1. Typical security threats for PLCs

Threat	Threat Description	Threat Score	CVSS
Denial-of-service attacks	Bringing the system or PLC network down through malicious attacks; overloading the data stream to overload the memory, for example	8.6	CVSS Calculation – 8.6
Spoofing	Intercepting communication to the host from the PLC and modifying it maliciously	8.5	CVSS Calculation – 8.5
Man-in-the-middle attacks	A rogue PLC or remote input/output (I/O) intercepts and modifies/changes messages from a valid source, and forwards attack messages to a targeted PLC in an attempt to take down the PLC or have it respond in unintended way, like shutting down a section of a factory	8.5	CVSS Calculation – 8.5
Rogue PLC joining network	A rogue PLC impersonating a legitimate PLC joins a factory network to create attack scenarios	8.5	CVSS Calculation – 8.5
PLC takeover	Changing the PLC program or boot image to alter intended operations and create attack scenarios or denial-of-service attacks	7.4	CVSS Calculation – 7.4
Remote device management serves exploits	Using remote device management services such as web managers, Telnet or Secure Shell running over a PLC for debugging or status reporting to gain control of a PLC or change its configuration	7.4	CVSS Calculation – 7.4

1. Inputs used in the CVSS 3.0 calculator are based on TI's assessment. You should review the threats and adjust based on your system design.

4 TI security frameworks

Texas Instruments (TI) has defined its security framework in *Building your application with security in mind* to provide an overview of why security matters, how to evaluate which security measures you need and how to implement these measures to protect against threats. The TI security framework also includes the main security enablers that TI offers to assist you in furthering your security objectives.

Table 2 maps the customer asset to TI security enablers.

Table 2. Customer asset to TI security enablers

Threat	Customer Asset	Counter Measures	Device Asset	Exposure Point	TI Security Enabler(s)	TI Security Enabler Usage
PLC takeover	Customer booting software images	• Trusted booting images and trusted over-the-air updates. • Closed debugging ports.	Code, identity and keys	Storage, run time	• Secure boot • Secure firmware updates • Debugging security	• Device validates the image digital signature every boot and rejects the image if the authentication fails. • Secure over-the-air update for images using device stored keys. • The device, before updating software, checks the authenticity via digital certificates attached to images using keys stored in the device. Only if the authentication is a success, the updated images are accepted.

Table 2. Customer asset to TI security enablers (continued)

Threat	Customer Asset	Counter Measures	Device Asset	Exposure Point	TI Security Enabler(s)	TI Security Enabler Usage
Spoofing	Data sent to host for further action	Encrypt and sign the messages to the host	Data, identity and keys	Run time, transfer	• Cryptographic acceleration • Secure storage • Networking security	• Use negotiated or pre-shared keys in secure storage to encrypt and sign messages meant for the host. • Offer cryptographic cores like Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA) and Public Key Algorithms (PKA) to encrypt/sign messages, thereby achieving the required performance.
Man-in-the-middle attacks	Data as received by the PLC	Check the authenticity of messages before acting on the message	Data, identity and keys	Run time, transfer	• Cryptographic acceleration • Secure storage • Networking security	• Use negotiated or pre-shared keys in secure storage to verify and decrypt messages meant for the host. • Offer cryptographic cores like AES/SHA/PKA to decrypt/verify messages, thereby achieving the required performance.
Rogue PLC joining the network	Device identity	Secure onboarding procedure to install new devices on factory networks	Device identity and keys	Storage	• Device identity/keys • Initial secure programming	• Device identity and keys to authenticate the device are part of factory floor onboarding procedures. • In this scenario, the PLC must prove its authenticity cryptographically to the host to be part of the factory network.

Table 2. Customer asset to TI security enablers (continued)

Threat	Customer Asset	Counter Measures	Device Asset	Exposure Point	TI Security Enabler(s)	TI Security Enabler Usage
Denial-of-service attacks	The PLC is unable to respond to legitimate requests. The PLC starts flooding the network targeting a victim (a remote I/O node or another PLC).	Software running on the PLC must be trusted. Attempts to override device through the debugging ports must be countered.	Code	Storage, run time	• Secure boot • Device identity • Debugging security	• Device forces authentication of software images during secure boot and also during secure over-the-air updates. • Debugging ports are closed by default and can be only opened by signed certificates/software.
Remote device management services exploits	PLC configuration change or illegal software update.	Remote device management allowed after authentication	Code	Run time	• Secure boot • Device identity • Keys • Debugging security • Secure storage	• Device uses secure boot to allow only trusted software that restricts use of the remote device management port to authorized users after checking credentials. • Device software uses keys from secure storage to authenticate requests for device management services.

5 TI devices with security enablers

Table 3 describes security enablers in TI Sitara™ processors targeting PLC applications.

Table 3. TI Sitara devices for PLC applications with security enablers

	TI Device			
Enabler	**AM335x**	**AM43x**	**AM574x**	**AM654x**
	Low end/nano, human machine interface PLC	**Low end, tamper PLC**	**Mid-high, motion control PLC**	**Mid-high, safety PLC**
Cryptography acceleration	√	√	√	√
Device identity and keys	√	√	√	√
Secure boot	√	√	√	√
Debugging security	√	√	√	√

Sitara processor differentiation:

- System-level security integrated with PLC communications, safety and Industry 4.0 services.
- Secure boot support across devices with features like key ring and anti-rollback.

6 Conclusion

As Industry 4.0 brings automation, connectivity (local and cloud) and real-time processing/control to prominence, the chance of more sophisticated and remote attack scenarios increases. These scenarios could range from impacting:

- Product quality (changing specifications)
- Safety (taking control of a robot arm remotely to cause damage)
- Throughput (denial-of-service attacks)
- Entire networks (introducing malware and viruses into the network and potential cloud compromise)

PLCs, remote I/Os and field bus controllers need to be at the forefront of the security defenses against these attacks; the processors driving these products need to be capable of addressing security requirements. TI processors and microcontrollers offer various security tools to protect against nefarious attacks without compromising the need for innovation in performance and features.

7 References

1. Reinventing the PLC for Industry 4.0 DesignSpark blog post, March 29, 2017.
2. Common Vulnerability Scoring System Version 3.0 Calculator
3. Texas Instruments: *Building your application with security in mind*

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265