PLC Device Security - Tailoring needs

Wen Chinn Yew

PLC Device Security – Tailoring needs

GIAC (GSEC) Gold Certification

Author: Wen Chinn Yew, wenchinn@outlook.com
Advisor: Rodney Caudle

Accepted: October 18th 2014

Abstract

Programmable Logic Controller (PLC) is widely used in many industries. With increasing concern and interest in the security of these controllers and their impact to the industries, there is a growing trend to integrate security directly into them. It is not realistic or wise to have a one size fit all solution. This paper presents focus areas and requirements suited for various classes of PLCs in the market. It looks at the threats and vulnerabilities faced by them and current security solutions adopted. The paper then recommends how PLC vendors should have different but extensible security solutions applied across various classes of controllers in their product portfolio.

1. Introduction

A programmable logic controller (PLC) is a piece of industrial computing equipment that can be programmed to perform different control functions for automation purposes. They are widely used in many industries, from Automotive to Food and Beverage, to Machinery and Water Treatment.

PLC was born in the 1960s (Segovia & Theorin, 2012) as a replacement for the traditional relays and wires used in a control room. Then, in the 1990s, it was expanded to control and communicate with end devices in a distributed system. Competing communication protocols flourished, but they were not designed with security in mind (NIST, 2013, p3-5), not to mention the equipment itself.

With ever-increasing cyber threats and increased scrutiny from governments, public and private bodies, as well as interested parties, there is a growing pressure among PLC vendors to begin to design security into their products. "A clear trend is to integrate cyber security directly into the PLC platform" (ARC Advisory Group, 2013). Industrial equipment, in contrast with consumer equipment, has relatively longer setup, commissioning and shelf life. Upgrades can be costly and it is highly desirable to design in security that is sustainable.

Standards from the International Society of Automation and the National Institute of Standards and Technology, such as ISA S99/IEC62443 and NIST 800, are available that advance the cause against security risks (ICS-CERT, 2014). They are broad-based and not specifically targeted to PLCs per se. Risk is the combination of Threat and Vulnerability. If there is a threat without any vulnerability or, there is vulnerability without threat, then the risk is very low (SANS SEC401, 2014).

Risk analysis can be used to identify focus areas and requirements that are suitable for implementation into various classes of PLCs. There should be a basic set of requirements and then based upon considerations of different threats and vulnerabilities, selected solutions will be applied.

Wen Chinn Yew, wenchinn@outlook.com

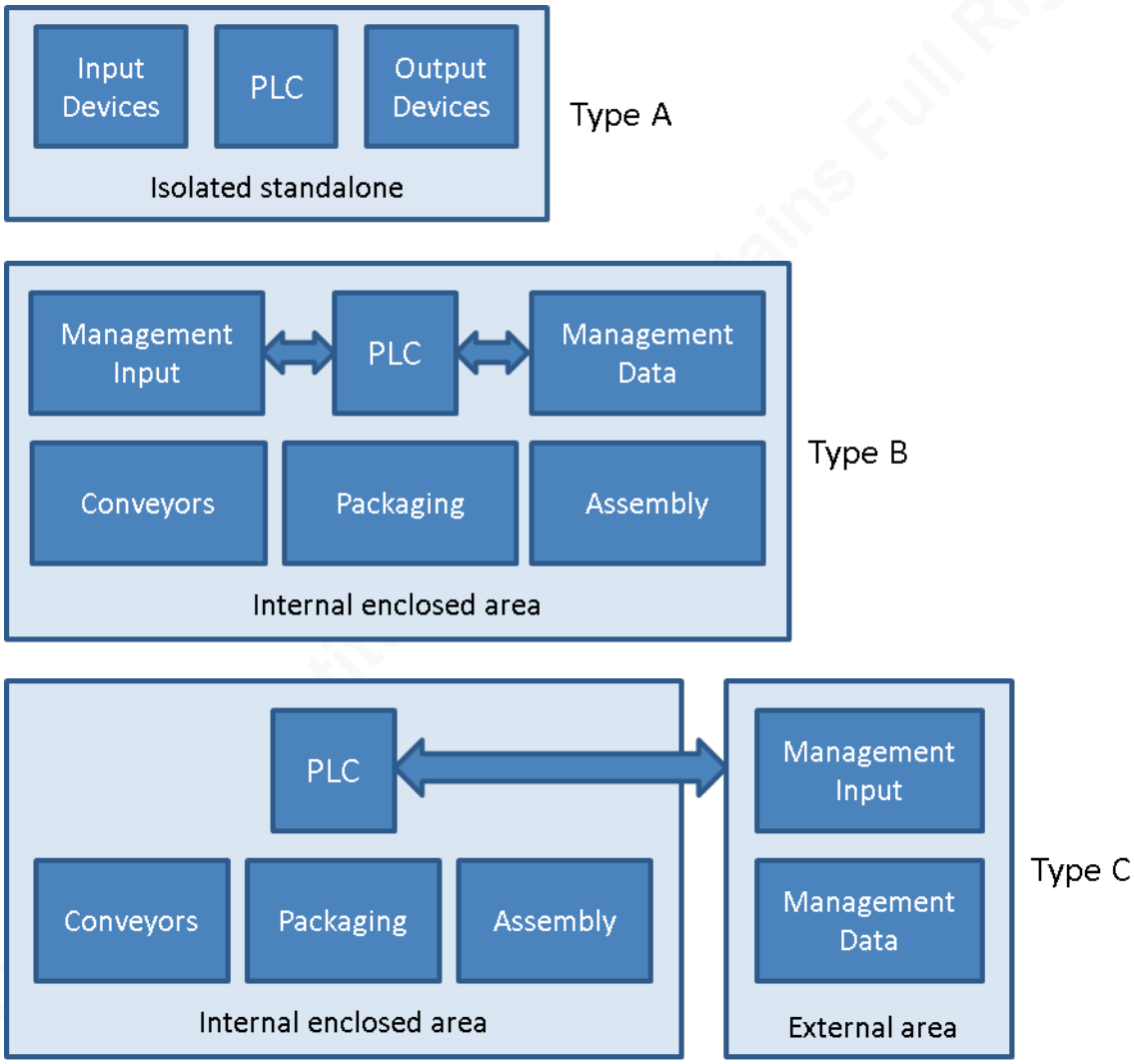
2. PLC Device Classification

PLCs are traditionally classified into Nano, Micro, Small and Large controller class. The criteria are based on the number of IO (Input/Output) points, performance and physical size. Nano and Micro class PLCs are also typically contained in a single housing with a fixed number of IOs, as opposed to a modular type in the Small and Large controller class where there is a backplane to insert modules that can expand the functionality of the PLC (Electrical Contractor Magazine, 2008; PLC dev, 2014).

Nano and Micro class PLCs have smaller physical size, lower performance and lesser functionality compared to Small and Large PLCs. They pack less functionality because of the lower cost pegged to the limited IO numbers. Their smaller hardware real estate is also a contributing factor to their inability to support more features. Before the cost of adoption of Ethernet was lowered considerably, Nano and Micro class PLCs had limited networking capabilities. They were used mainly in standalone applications or applications with limited distributed access. Small and Large class PLCs, being of modular types, are able to extend their functionality with specialized modules supported over a backplane. They are used in applications that require high performance and often in distributed control.

The line is now blurred in the networking capability of different classes of PLCs, with the drop in the cost of hardware (Liptak, 2006, p.909). Network capabilities and performance can still be distinct between classes of PLCs, typically because of vendor directed market positioning based on hardware price, performance, features and capabilities.

This paper broadly categorizes three different types of network where PLCs are used with increasing performance and cost. Type A is an isolated network in a standalone machine, Type B is an internal network confined to a closed area and Type C is a network accessible outside of a closed area as shown below.



An example of a Type A network is a standalone stretch wrapping machine. It is accessed via a HMI (Human Machine Interface) touch pad and some push buttons. A small packaging line, whose control and monitoring is confined to a closed area, is an example of Type B network. There can be avenues for access to the system via physical communication ports that may be exposed within the confines of the area. Type C networks can be a complete production and packaging line, with control and monitoring integrated into the enterprise network or remote facility. The avenues for system access are increased. Nano and Micro class PLCs are most frequently used in Type A network while Small and Large PLCs, in Type C network. For Type B network, Micro and Small are popular.

Wen Chinn Yew, wenchinn@outlook.com

3. Threats and vulnerabilities against PLC devices

Industrial control system (ICS) is a general term used to refer to three main types of control systems in automation. They are a supervisory control and data acquisition (SCADA) system, a distributed control systems (DCS) and other smaller control systems (NIST, 2013, p.2-1). PLCs are one of many components used in SCADA and DCS systems but are the main component in smaller control systems.

SCADA systems consist of a central control and monitoring center that controls geographically distributed field sites where PLCs are used. They operate distribution systems in the water, oil and gas, electrical and transportation industries. The control and monitoring of the remote field sites in these water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems, requires the use of large communication networks. The SCADA system is analogous to a Type C network mentioned earlier.

DCS also serve the same industries as SCADA systems, but in the control of the industrial processes such as water and wastewater treatment, oil refineries, electric power generation and automotive production. Controls and monitoring are in the same geographical location. DCS can be analogous mostly to a Type B network. In some cases where there are connections out to the enterprise/outside world, then possibly a Type C network. This is because SCADA and DCS systems can also be networked together.

Smaller control systems are used in many industries in a wide range of automation applications. They operate as a standalone machine in many cases such as in a skid mounted mixer or a commercial dryer. In some cases, control is confined to a closed area like in an automated car wash facility. Such a small control system is analogous to a Type A network for a standalone machine or Type B network in the case of an enclosed perimeter.

ICS operates both essential infrastructures and other less critical systems that affect our daily lives. The threats and vulnerabilities against PLCs used in ICS can be analyzed to assess the risk to different classes of PLC. Threats can be divided into Basic, Advanced and Advanced Persistent Threats (APT) (SANS SEC401, 2014). Basic threats can be like generic phishing scams or attacks against organizations with little or no

security. The attack techniques are available on the internet or open source. Advanced threats can be DDoS (Distributed Denial of Service), private data extraction or extortions using custom tools or techniques. APTs are sophisticated adversaries that bypass today's best practices.

Types of threats can be *Attackers*, *Bot-network operators*, *Criminal groups*, *Foreign intelligence services*, *Insiders*, *Phishers*, *Spammers*, *Spyware/malware authors*, *Terrorists* and *Industrial spies* (NIST, 2013, p.3-5). Let us look at the definition of each threat actor in more detail as described by NIST, and discuss the susceptibility of different controller class. *Attackers* compromise systems for individual satisfactions. They can be users of kiddie scripts and might not have the skills to target more secure critical infrastructures and services. Controllers used in Type A network has Low risk because they are isolated and standalone. *Attackers* usually will not have physical or network access to it. *Bot-network operators* are slightly more sophisticated than *Attackers* and use multiple systems and networks in their act. They would be categorized under Advanced Threat but still pose Low risk to controllers in Type A network for the same reason as *Attackers*.

Criminal groups operate in an orchestrated manner with the goal of monetary gain through theft or extortion. *Industrial spies* belong to the same category except that the goal is for intellectual properties and know-how, albeit indirectly still for monetary gains. The factor of monetary gain will place controllers used in Type A network under High risk. Even with limited connectivity, a threat vector can be made to reach the controller via physical access or other ingenious means. *Criminal groups* and *Industrial spies* would belong to the category of Advanced Threat. Another threat actor, the *Insiders*, include employees, contractors, or business partners. By virtue of possibly having less obstacles to target access, *Insiders* pose a High risk to controllers in Type A network. *Insiders* have the added advantage of intimate knowledge of the target and hence might be a formidable threat even with Basic skills.

Foreign intelligence services have the resources and capability support from Nation state/s to enact significant physical, social and economic impact onto others. They belong to the Advanced/ATP threat category. Controllers in Type A network might not

be of interest to them as they are not typically used in critical large scale infrastructures that require higher performance and connectivity. Similarly, *Terrorists* target Nation state/s and the risk of controllers in Type A network can be considered Low.

The last three types of threat are *Phishers*, *Spammers* and *Spyware/malware authors*. The first two can be individuals or organizations and they normally operate via networked electronic communication means, such as email and internet. They do not belong to the APT category as this requires great resources and skills. *Spyware/malware authors* are described as "Individuals or organizations with malicious intent (who) carry out attacks against users by producing and distributing spyware and malware" (NIST, 2013, p.3-6). The *authors* need certain level of skilled expertise and are categorized as Advanced/APT. All three types of threat discussed here pose Low risk to controllers in Type A network with limited connectivity.

In summary, controllers in Type A network are at High risk to *Criminal groups*, *Insiders* and *Industrial spies*. *Foreign intelligence services* and *Terrorists* do not normally target users of controllers in Type A network. The lack of connectivity in Type A network also reduce the risk of other types of threat to Low. Controllers used in Type B network face the same High risk threats as Type A network for the same reasons. A classification of Medium risk is assigned to controllers in Type B network, for threats that are of Low risk to controllers in Type A network. The increase in risk factor is attributed to the availability of more avenues of access to the controllers, both physical and remote. The amount of remote access however, is still confined to a controlled perimeter area. For controllers used in Type C network, where connectivity is wide, all types of threat should be classified as High risk.

Assimilating the above information, Table 1 lists the different categories each threat fall under, and its potential as a threat vector for controllers used in the 3 types of Network discussed in Section 2.

Table 1

Type of Threat	Category	Type A	Type B	Type C
Attackers	Basic	Low	Medium	High

Bot-network operators	Advanced	Low	Medium	High
Criminal groups	Advanced	High	High	High
Foreign intelligence services	Advanced / APT	Low	Medium	High
Insiders	Basic	High	High	High
Phishers	Basic / Advanced	Low	Medium	High
Spammers	Basic / Advanced	Low	Medium	High
Spyware/malware authors	Advanced / APT	Low	Medium	High
Terrorists	Advanced / APT	Low	Medium	High
Industrial spies	Advanced	High	High	High

Based on Table 1, the basic requirements when designing in security to a PLC must address *Criminal groups*, *Insiders* and *Industrial spies* with physical access considerations. On the other extreme, Large class PLC need to build in the capability to address the broad spectrum of threats. As for the middle ground, Micro and Small class PLCs should have the ability to add on security measures when required.

4. Current security solutions in PLC devices

Open literature from top PLC vendors (PLC vendors, 2014) show that they currently offer security solutions focusing on the following broad areas: Deactivation of unused features, Integrity protection, Authorization and Access Control, Communication protection, System protection and Physical.

4.1. Deactivation of unused features

One of the most basic security mechanism is to remove the attack vector. Some PLCs offer the ability to deactivate physical ports, network services and even individual commands. For automation applications that have no use for certain physical ports, there is an option to turn them off. Out of the box , vulnerable features such as embedded Webserver or less commonly used features like NTP client services are disabled as a default. All these help to reduce the attack surface. There are PLCs that provide finer deactivation granularity such as the option to turn off all write requests to data values on the PLCs.

4.2. Integrity protection

Integrity protection can be divided into three main areas. The first area is the static firmware image of an upgradable PLC. This image is used to operate the PLC, much like the BIOS and operating system (OS) of a PC. The second area is the user configuration and program downloaded into the PLC. This is designed by the user using a PLC software programming tool, and downloaded into the PLC to control his automation system. An analogy can be the application that will run on a PC. The third and final area is when the user program is operationally running, live data values are dynamically being read and written to, essentially changing to reflect the state of operation of the automation system.

The integrity of the upgradable firmware image has been addressed by PLCs with digital signature technology to provide non-repudiation. It provides confidence in the integrity and authenticity of the image.

Protection of the user configuration/program from being altered maliciously is more complex. If configuration/program download can be contained to authorized users, then a hashing algorithm is sufficient. However in some scenarios where a configuration can be dynamic and there is no good mechanism to ensure a user is authorized, some PLCs address this by providing a way to detect and report this change. This does not strictly ensure integrity protection, but rather detection.

The third area of dynamic data values cannot be easily addressed unless a secured communication mechanism is used to transmit these changes to the PLC.

4.3. Authorization and Access Control

PLCs offer different authorization and access control for different areas such as configuration/program and runtime data. These areas can be further segregated based on the access medium, such as the physical interface, communication protocol and command type.

For example, there can be access levels of None, Read or Read/Write for the Configuration/Program and for the External Network. More granular control could also be extended to the lower layer physical interfaces, of individual ports of the PLC, and up to the application layers, of FTP and SMTP applications. Some PLCs provide control access to individual commands sent to the controller if the protocol can support it.

Authorization and access control are typically realized with a password mechanism to grant access. It is well known that most of these mechanisms have limitations because of the protocol's inherent lack of security. In some cases, clear-text is used, while for others, there are no good ways to identify the authorized communication channel.

4.4. Communication protection

Communication protection offered by PLCs range from simple means such as whitelisting of IP addresses, to more involved technologies such as SSL/TLS. Some PLCs provide a simple built-in firewall in the form of allowing users to selectively allow traffic based on a predetermined list of IP addresses. This can be easily bypassed with spoofing tools. Embedded webservers support is common in PLCs. There are PLCs that

support HTTP Secure in place of HTTP to provide better security for users. It is of course not a panacea, with known weaknesses, of which sometimes is due to the unsuspecting user himself.

Vendors create modules external to the PLC to provide firewall and VPN capabilities that can be used seamlessly with the PLC to provide enhanced security. It is not common to see them integrated into the PLC for cost reasons. An external module also provides increased flexibility in deployment. It is possible to use similar off-the-shelf products but they incur more integration overheads.

4.5. System protection

PLC vendors are aware of the need to build in robustness in their product against DoS attacks. Some PLCs claim robustness in this area. There are also certification authorities such as ISASecure that certify tests in these areas, although there is no clear trend at the moment to suggest industry convergence on them, and the variety of protocols adds complexity. There are PLCs that monitor the frequency of abnormal activities and take appropriate actions. This is by no means as powerful or advanced as a standalone IDS/IPS used in the IT industries. Conscious efforts in the area of system protection suggests acknowledgement by the industry of possible opportunities in these technologies to enhance security.

4.6. Physical protection

Physical protection in the context of the PLC alone, can refer to the deterrence of users to manipulate, for example, controller mode switches or IP address switches. Some PLCs provide a small door cover that must be opened to access the physical switches. The door comes with a provision to use a tiny padlock. The effectiveness is debatable if the padlock can be easily compromised.

5. Security focus area for PLC devices

The classes of PLCs and network types have been discussed, together with the threats and vulnerabilities. Table 2 below classifies PLCs into three Built-in Security Levels and suggests their level of extensibility.

Table 2

PLC Class	Nano	Micro/Small	Large
Network Type	Type A	Type B	Type C
Threat	Attackers, Criminal groups, Insiders and Industrial spies with physical access considerations.	Same as Type A, with additional possible medium level threats from Bot-network operators, Foreign intelligence services, Phishers, Spammers, Spyware/malware authors and Terrorists.	Broad spectrum
Built-in Security Level	Basic	Intermediate	Advanced
Extensibility of Security Level	Low	Medium/High	High

5.1. Built-in Security Level - Basic

Device Hardening is one of the most basic protection required. It is imperative that a device be built with security in mind. There are standards, guidelines and best practices to adopt that can help developers create a secure embedded device (Department of Homeland Security, 2014).

Adopt a "Just Enough" concept for the PLC product and its application. In the product, it is to make sure that features or even artifacts of features that are not required for the product are removed. In the application, it is to provide the customers with the capability to remove unwanted threat entry points. Examples discussed are the deactivation of unused features like communication ports and network services.

Use technologies that can help ensure the integrity of the PLC's operating system/firmware and its application. Digital signature technology should be used to check the authenticity of firmware upgrade images. Authorization is required before any changes can be applied to a PLC's application and configuration.

PLC security should not rely on the absence of physical access. PLC vendors should introduce more barriers into the execution of a factory reset that can bring a PLC out of its "lock down" state.

5.2. Built-in Security Level - Intermediate

Enhancing the concept of a "Just Enough" design, PLC vendors can add higher value and security to their products by providing more options for their users to enable/disable features or services in the controller. An example is the ability to have a finer control over sub features of a feature.

Integrity protection of PLC application/configuration can be taken a further step to allow the application to detect that a change has occurred. A change could be intended or unintended. A PLC that allows the user to define what parameters can be altered, the valid range values of the parameters, and the ability to detect and prevent changes to the parameters, is an area that can help enhance security.

Basic Authorization and Access Control typically grants access to the PLC device as a whole. An extension is to be able to grant access to different sections or layers of the device. Access can be segregated based on physical interfaces, communication protocols, network services, features, sub features and others.

For communication protection, simple firewall techniques can be used to block access. Other areas that can enhance system protection include the capability to monitor

system attributes like communication traffic rate and CPU bandwidth usage and to issue a notification for abnormal behavior.

The sophistication of these intermediate-level security features depends on the hardware support in the PLC. Besides only depending on the embedded hardware in the device, another option is to provide add-on components to the PLC to enhance its hardware ability to support the features. Micro and Small controllers can be suitable candidates. This provides extensibility to the security level of the PLC. The users can decide what additional level of security is required for their application and add on components for enhancements.

5.3. Built-in Security Level - Advanced

Advanced-level security features can be supported more realistically by Large class PLCs. These are also known as Programmable Automation Controllers (PACs). They are the top of the range multi-disciple control platform and naturally pack more hardware capabilities to support more demanding features.

Providing integrity protection for dynamically changing data, as well as ways to control authorization and access can be a challenging area to look into. Robust and secure communication protocols might be one solution. Although designing and using secure communication protocols and technology should be part of basic device hardening, most legacy protocols cannot fulfill the requirement.

The industry is aware of this deficiency and has seen players work to enhance and incorporate security into protocols. The enhancement might require new hardware support and possibly new versions of protocols. Interoperability with other types of devices needs to be part of the equation. This can be turned into an advantage with the concept of Trusted Devices where Vendors can offer a total solution to bundle other devices such as HMIs and Drives that can interoperate securely with the PLC.

To add on to the system protection methods mentioned in the Intermediate-level, IDS/IPS capabilities can be introduced to target flagship communication protocols commonly used in the industry. Integrating IT industry types of IDS/IPS, firewall and

VPN capabilities into a PLC might be too costly, but providing ease of integration of such devices to work with a PLC can greatly promote adoption.

Physical protection, in the form of only allowing authorized physical access to effect any change to the PLC, can be controlled with contemporary Biometrics Identification technologies. This will help especially in preventing controller mode or IP address from being changed with a flick of a switch. Tamper proofing PLC is another important mechanism to prevent disclosure of information. Such information may aid reverse engineering that can compromise security.

Wen Chinn Yew, wenchinn@outlook.com

6. Conclusion

This paper presents the various classes of PLCs based on their hardware capabilities, performance and features. It also highlights the risk factor against threats, where risk increases with the class. It then recommends three levels of built-in security for these different classes of PLCs which takes into account the risks and hardware capabilities – Basic-level for Nano, Intermediate-level for Micro/Small and Advanced-level for Large.

The idea of an incrementing built-in security level applied across incrementing performance class of PLCs in a product portfolio, will enable the design of an extensible security solution. Large class PLCs will incorporate Basic-, Intermediate- and up to Advanced-levels of security while Nano class has at least a solid Basic-level.

This paper focuses on securing the PLC device. However it must be noted that security of an Industrial Control System (ICS), where a PLC is only one component, relies on a combination of many technical and non-technical elements. Technical are things like Device hardening, System-wide security controls (Defense in Depth) and Infrastructure, to name a few. Non-technical being people and process such as during the ICS lifecycle of Design, Install, Operate and Maintain. Securing the PLC as an individual component is a step towards preventing it from being the weakest link in the ICS.

Wen Chinn Yew, wenchinn@outlook.com

7. References

ARC Advisory Group (2013). Programmable Logic Controllers (PLCs) and PLC-based Programmable Automation Controllers. Retrieved Jul 29, 2014 from http://www.arcweb.com/market-studies/pages/plcs-programmable-logic-controllers.aspx

Department of Homeland Security (2014). Build Security In. Retrieved Jul 30, 2014 from https://buildsecurityin.us-cert.gov/

Electrical Contractor Magazine (2008). PLCs: Black Magic in a Box. Retrieved 19 Sep, 2014 from http://www.ecmag.com/section/systems/plcs-black-magic-box

ICS-Cert (2014). Standards and References. Retrieved Jul 29, 2014 from http://ics-cert.us-cert.gov/Standards-and-References

Liptak, B. G. (2006). Instrument Engineer's Handbook: Process Control and Optimization Volume 2, Fourth Edition. CRC Press

NIST 800-82r1 (2013). Guide to Industrial Control System (ICS) Security. Retrieved Jul 29, 2014 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf

PLC dev (2014). PLC Basics. Retrieved Jul 29, 2014 from www.plcdev.com/book/export/html/9

PLC vendors (2014). Retrieved Jul 29, 2014 from http://www.automation.siemens.com/mcms/programmable-logic-controller/en/pages/default.aspx
http://www.mitsubishielectric.com/fa/products/cnt/plc/

Wen Chinn Yew, wenchinn@outlook.com

http://ab.rockwellautomation.com/Programmable-Controllers

SANS SEC401 (2014)

Segovia, V.R. & Theorin, A. (2012). History of Control, History of PLC and DCS. Retrieved Jul 29, 2014 from http://www.control.lth.se/media/Education/DoctorateProgram/2012/HistoryOfControl/Vanessa_Alfred_report.pdf

Wen Chinn Yew, wenchinn@outlook.com