GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"ICS/SCADA Security Essentials (Industrial Control Systems 410)"
at http://www.giac.org/registration/gicsp

An Abbreviated History of Automation & Industrial Controls System and Cybersecurity

GIAC (GICSP) Gold Certification

Author: Ernie Hayden, enhayden1321@gmail.com
Advisor: Michael Assante
Accepted:

Date: 22 January 2015

Template Version September 2014

Abstract

Today's "new world" of cybersecurity is now invading the older, foundational industrial control systems (aka "old world") used in factories, power plants, and other critical infrastructure. The cyber security challenges are becoming increasingly serious each day and as such SANS has introduced the Global Industrial Cyber Security Professional (GICSP) certification. However, many of the IT security professionals do not understand what constitutes industrial control systems (ICS)and they do not have familiarity with the history of the ICS systems and controls. This paper is intended to offer the reader a brief history of industrial controls, what they are, where they came from, and an elementary look at control theory. Finally we discuss at a high level the cybersecurity issues ICS and other Operational Technologies (OT) face including a brief review of the Stuxnet attack that brought ICS security to the forefront in the world today.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Automation and industrial controls systems – often referred to as ICS – have an interesting and fairly long history. Today we are often discussing industrial controls issues and cyber/physical security; however, that has not always been the case. The underlying concepts for control and feedback had to start at some point, hence, this paper is prepared to provide a brief history of the development of today's control systems and an accounting of how cybersecurity emerged as a concern to reliability and predictability.

For the purposes of this paper we will be using ICS to refer to the myriad of automation and control system applications and descriptions to include:

Industrial Control Systems (ICS): A term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being 'a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.' The following table is just a few of the applications and labels we use to describe ICS.

Table 1 Types of Industrial Controls

Types of Industrial/facility Automation & Control	Uses & Applications	Examples
SCADA & EMS – Supervisory Control & Data Acquisition & Energy Management System	Control and data acquisition over large geographic areas	Electricity transmission & distribution, pipeline, water distribution
DCS - Distributed Control System	Systems which control, monitor, and manage industrial processes that are disbursed but operated as a coupled system	Oil refinery, chemical processing plant, Thermal plant auxiliary systems
PCS – Process Control System	Systems which control, monitor, and manage an industrial processes	Thermal power plant, Nuclear Power Plant Systems, Wind Farm, etc.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

Types of Industrial/facility Automation & Control	Uses & Applications	Examples
Building Automation, Building Management System	Control systems used to manage security, safety, fire, water, air handling in a building or facility	Data center's environmental systems, control centers, etc.
I&C - Instrumentation & Control	Electronic devices or assemblies used to monitor, measure, manage or operate equipment in many applications	Nuclear Power Production
SIS - Safety Instrumented System, safety systems, protection systems	System with the sole function to monitor specific conditions and act to maintain safety of the process	Refinery, Chemical Plant, Power Plant

Table 1 Types of Industrial Controls

* Some refer to the collection of technologies that supports operations as "Operational Technology (OT)" to distinguish it from "Information Technology (IT)"[1]

2. But First, Some Elementary Controls Theory

Control theory is an interdisciplinary branch of engineering and mathematics dealing with the behavior of dynamic systems with inputs. The objective of control theory is to calculate solutions for the proper corrective action from the controller that results in system stability, i.e., the system will hold the set point and not oscillate around it.

[1] **Operational Technology (OT)** is an umbrella term used for various technologies that support "operations", such as SCADA EMS. This term can be more inclusive than Industrial Control Systems (ICS) control systems and can include market systems that interface directly through technology with operational assets. Industrial control systems can be relatively simple, such as one that monitors environmental emissions on a stack, or incredibly complex, such as a system that monitors and controls activity in a thermal power plant and the state of large power transmission system.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

There are two major divisions in control theory: classical and modern. Classical control theory is limited to single-input and single-output (SISO) system design. Modern control theory can deal with multi-input and multi-output (MIMO) systems. Hence, modern control theory overcomes the limitations of classical control theory in more sophisticated design problems.

Control systems can be thought of as having four functions:

- Measure
- Compare
- Compute
- Correct

These four functions are completed by five elements:

- Sensor
- Transducer
- Transmitter
- Controller
- Final Control Element

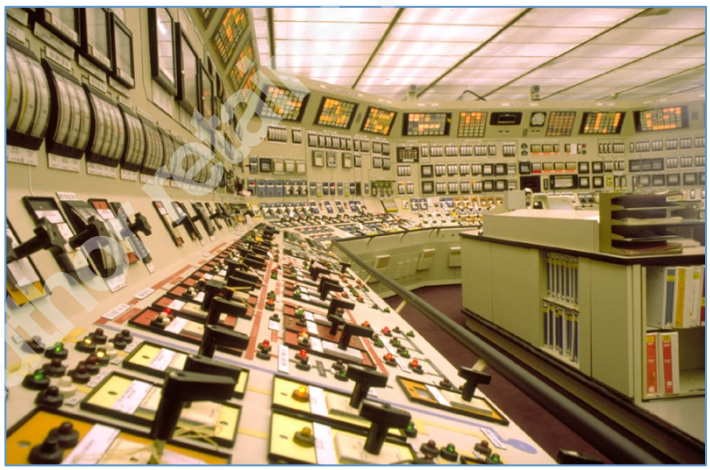


Figure 1 Typical Power Plant Control Room
http://powerplantmen.files.wordpress.com/2013/04/power-plant-control-room.jpg

Please keep these functions and elements in mind as we discuss key aspects of automation.

There are two common types of automation. One is called ***Feedback Control*** and the other is called ***Sequence Control.***

2.1. Feedback Control

Feedback control is usually a continuous process and includes taking measurements with a sensor and making calculated adjustments via the controller to an output device to keep the measured variable within a set range. For instance, in a water heater, the sensor is the thermometer which measures the temperature of the water. The output of the thermometer is sent to the controller which compares the current temperature to the set point (aka desired temperature). Then, based on the difference

© 2015 The SANS Institute Author retains full rights.

between the current temperature and the set point a signal will be sent to the heaters to go on or off depending upon whether or not the water is hot enough or not.

All the elements constituting the measurement and control of a single variable is called a ***Control Loop***[2].

A simple diagram showing this control loop is shown in the figure below:

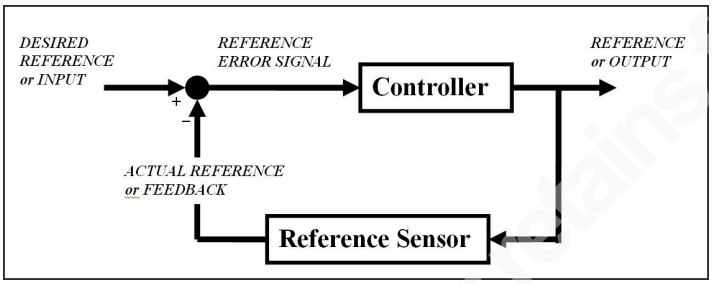


Figure 2 http://upload.wikimedia.org/wikipedia/en/4/40/Feedback_loop.JPG

It is also important to understand if your feedback controller is ***Open-Loop*** or ***Closed-Loop.***

An **Open-Loop** controller does not have any measurement of the system's output – e.g., the water temperature – used to alter the water heating element. As a result, the controller cannot compensate for changes acting on the system. Open Loop controls are usually managed by human intervention where an operator observes a key metric – such as system power, pressure, and level – and then makes manual adjustments to the controls to achieve the desired result. Imagine driving your car without cruise control turned on. You press or release the accelerator or brake pedal to manage the auto's speed. That is an Open-Loop control operation.

A **Closed-Loop** controller is basically that shown in Figure 2 above. A sensor monitors the system's condition (e.g., temperature, pressure, speed, etc.) and feeds the data to a controller which adjusts the output device (e.g., the water heater heating element) as necessary to maintain the desired system output such as temperature, speed, etc.

---

[2] Control loop theory is used for calculating and controlling an environment or process based on feedback.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

The design of this feedback process can also be referred to as a ***Control Loop*** since the system state is fed back to the controller and reference to provide and error signal to the controller to make the necessary changes to the output device. Again, using the car analogy, your cruise control system (when activated) is a Closed-Loop controller in operation.

2.2. Sequence Control

Sequence Control may be either to a fixed sequence or a logical one that will perform different actions based on various system states. An example is an elevator that uses logic based on the system states.

A sequence control diagram for an elevator is shown below:

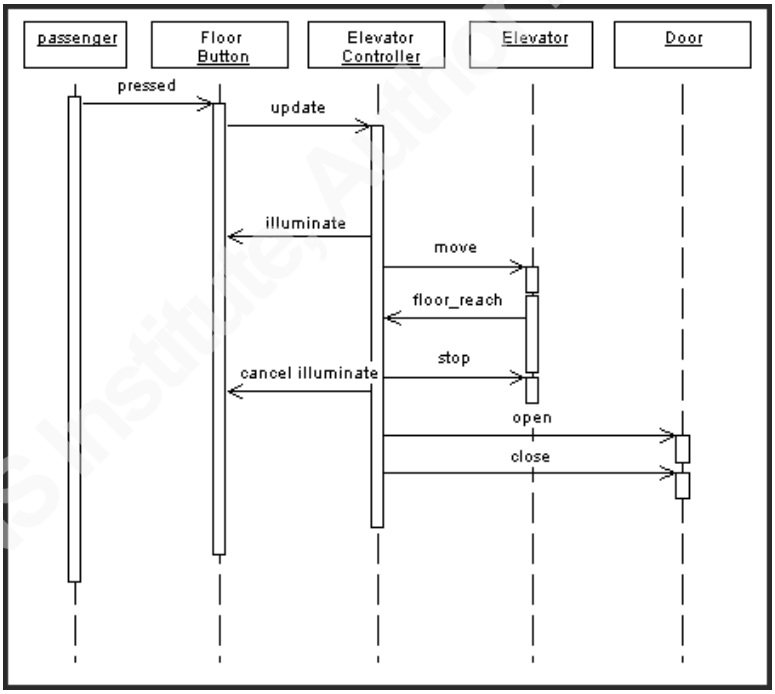


Figure 3 Sequence Control Example – Elevator
(http://www.web-feats.com/classes/dj/lessons/uml/elevator_files/flr_seq.gif)

As sequential controls were established and became more and more part of the industrial automation landscape we will see that these became included in ***Relay Logic***. Essentially this approach is where electrical relays engage electrical contacts which either start or interrupt power to a device. According to one source, electrical relays are referenced in industrial automation discussions from 1860.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

We will discuss relay logic and extensions of the relay controls later in the history section.

2.3. Control Circuits

Another concept you will hear in controls theory is the idea of a Control Circuit. A control circuit is a type of circuit that uses control devices to determine when loads are energized or de-energized by controlling current flow[3]. Control circuits usually carry lower voltages than power circuits.

A typical control circuit would be a hard-wired motor start and stop circuit (please see the top control circuit figure below). The motor is started by pushing a "Start" or "Run" button that activates a relay that then closes a "holding contact" thus keeping the relay energized and thus keeping the contact closed.

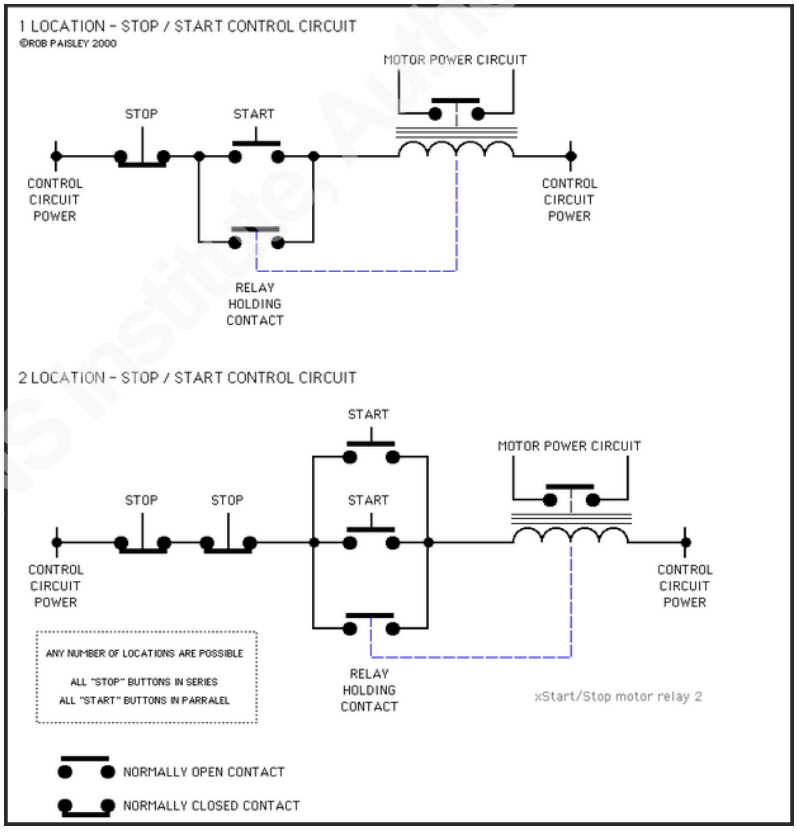


Figure 4 http://home.cogeco.ca/~rpaisley4/xStopStart1.GIF

[3] http://www.toolingu.com/definition-460310-34114-control-circuit.html

© 2015 The SANS Institute Author retains full rights.

Although we won't go into much detail on the control circuit concept, it is useful to understand the elementary concepts for later discussions on relay and ladder logic.

2.4. The Concept of Hysteresis[4]

Have you ever wondered why certain everyday controls you use do not "hunt"[5] for the right output to match the desired set point? The aspect of "hysteresis" is an important control system concept necessary for the efficient and stable operation of Closed-Loop systems.

The term "hysteresis" is derived from an ancient Greek word meaning "deficiency" or "lagging behind." Some early work on describing hysteresis in mechanical systems was performed by James Clerk Maxwell (1831-1879) as part of his work on governors.

Hysteresis is used to filter signals so that the output reacts more slowly than it ordinarily would. For example, a thermostat controlling a heating element may turn the heater on when the temperature falls below X degrees, but not turn off until the temperature rise reaches Y degrees (e.g., 72 degrees +/- 2 degrees operating band). This thermostat has hysteresis built into the control logic.

This concept can be used for pressure switches, electronic circuits, speed controls and aerodynamics.

3. History: Ancient Times and Industrial Controls

There is a rich historic record of events that constitute a timeline of what we would describe as automation or systems or mechanisms used for control that have

---

[4] For more detailed explanation of Hysteresis, please see the Wikipedia article on this subject at http://en.wikipedia.org/wiki/Hysteresis

[5] Hunting: a phenomenon that may occur in control systems in which the system first overcorrects itself in one direction and then overcorrects itself in the opposite direction trying to stabilize at the set point.

© 2015 The SANS Institute Author retains full rights.

evolved into modern day control systems. This is a history of the more general use of science and technology by man for the purpose of increasing the amount of work a human can accomplish or to achieve an outcome that relied upon specific conditions or amounts. The benefits of achieving automation is that it reduces the amount of labor, can save energy through efficiency gains, reduces the amount of materials needed, and improves quality, accuracy, predictability, and precision. Control systems also improve safety by removing humans from unsafe or dangerous conditions.

Control systems began by giving humans a way to apply general timing and now have evolved through technology and innovation to being able to sense and act within cycles of time so small (milliseconds) that a human cannot perceive it or react that quickly.

Although we consider industrial controls as part of the factory processes since the mid 1800's, the early Greek and Arabic societies actually had some float-valve regulators in devices such as water clocks, oil lamps, wine dispensers and water tanks. For an interesting and simple understanding of the water clock "automated controls" take a look at the YouTube video provided by Edison Tech Center (Link: http://www.youtube.com/watch?v=KlxYtk4Fiuw&noredirect=1).

One of the first feedback control devices on record is believed to be the ancient water clock of Ktesibios in Alexandria, Egypt around 250 B.C. The Ktesibios's water clock was an amazing design using water to fuel and regulate an accurate timekeeping mechanism. According to Jeremy Norman's *History of Information.com* article "The First Truly Automatic Self-regulatory Device (Circa 250 BCE) the clock kept more accurate time than any clock invented until the Dutch physicist Christiaan Huygens invented the pendulum clock of the 17th century.

Dancing "automata" have existed in various forms as inventors tried to capture the movement of living things in machines. The first recorded application and roots of "automata" go back to about 400 BCE. A Greek philosopher, mathematician, and strategist named Archytas was reputed to have designed a bird shaped machine that could fly suspended by a wire. It was referred to as "the

© 2015 The SANS Institute Author retains full rights.

Pigeon" or wooden dove automation[6]. Dancing "automata" began to take shape as mechanical devices that could accomplish a series of movements. The technology is an excellent example of an open loop control system.

In 1620, Cornelis Drebbel designed a feedback loop, or closed loop control system, to operate a furnace, effectively designing the first thermostat[7]. As cited by Stuart Bennett of the University of Sheffield in his paper *A Brief History of Automatic Control*, he notes that René-Antoine Ferchault de Réamur (1683-1757) proposed ideas for automatic devices to control the temperature of incubators. His idea was based on temperature being measured by the expansion of a liquid in a container connected to a U-tube containing mercury. A float in the mercury operated an arm which controlled the draft to a furnace via mechanical linkage. As the draft was opened or closed it affected the rate of combustion and heat output. This concept was also a closed-loop feedback system since the incubator temperature would provide feedback to the liquid and ultimately back to the furnace draft control.

One of the earliest feedback control mechanisms mentioned in recorded history was used to tent the sails of windmills in order to control the gap between the grain grinding stones being driven by the rotating sails. This mechanism was patented by Edmund Lee in 1745. The concept ultimately led to one of the most significant controls developments in the 18th century resulting in the steam engine governor.

The first steam governor was produced in November 1788 by James Watt (1736-1819). Although it was not a true, perfect control, it still provided proportionate control[8] and could not provide precise or exact speed control. (In fact because it was not a true "governor" it was referred to as a "moderator" in some circles.)

---

[6] Nocks, *The Robot*. The life story of a technology (2008)
[7] Franklin, Gene F., Powell, J. David & Emami-Naeini, Abass Feedback Control Dynamic Systems, 4th Edition.
[8] In a proportionate control algorithm, the controller output is proportional to the error signal, which is the difference between the set point and the process variable. In other words, the output of a proportional controller is the multiplication product of the error signal and the proportional gain. (Walker)

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

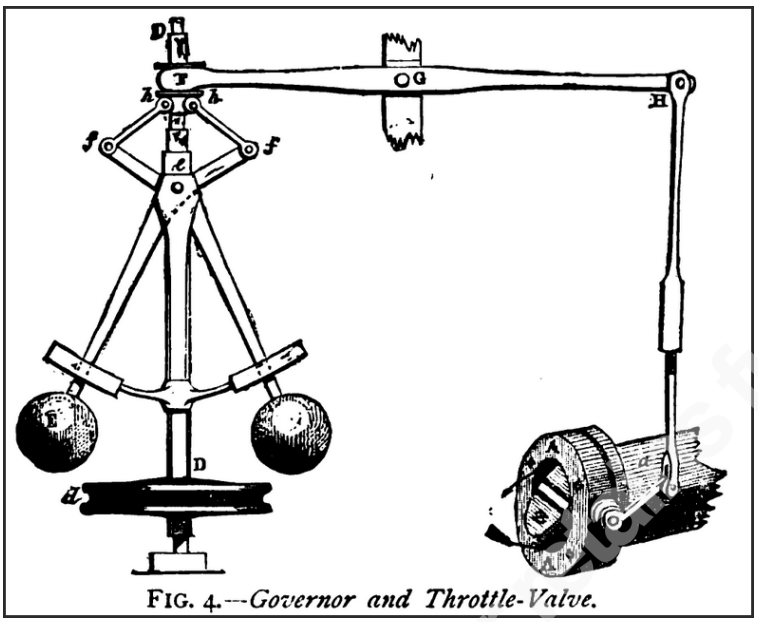


Figure 5 http://upload.wikimedia.org/wikipedia/commons/1/1e/Centrifugal_governor.png

Until the late 1860's there were many efforts to improve on the Watt governor. Thousands of patents were granted throughout the world. Many of the individuals focusing on this solution included now-famous individuals such as William Siemens (1823-1883). In 1868 James Clerk Maxwell (1831-1879) – famous for his electromagnetic theories and the Maxwell Equation – published a now-famous paper entitled *On Governors*. The paper is listed in the Bibliography below and is mathematically rigorous. Maxwell did show how to derive the linear differential equations for different governor mechanisms. Of note, Dr. Bennett noted in his paper *A Brief History of Automatic Control* that Maxwell's paper was "…little noticed at the time and it was not until the early years of the (20th) century that the work began to be assimilated as engineering knowledge."

From the late 1800's to early 1900's most of the control systems inventions were focused on the basic process activities of controlling temperatures, pressures, liquid levels and the speed of rotating machines. However, as the growth in the size of naval guns, ships and new weapons such as torpedoes, (invented in 1867) there was an increased need for industrial controls on hydraulic, pneumatic and steam systems.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

As ships got bigger the steering controls became more complex due to the larger hydrodynamic forces on the rudder and the larger gear ratios between the helm and the rudder resulted in slow response times to steering changes. In 1873 Jean Joseph Léon Farcot published a book on what he called "servo-motcur" or "moteur asservi" which we now call **servomechanisms** and **servomotors.**

Relay logic was introduced with factory electrification which underwent rapid adoption from 1900 through the 1920's. Essentially relay logic is a means to represent the manufacturing program or other logic (such as "On/Off" or "Yes/No") in a form normally used for relays. This relay logic concept was incorporated into future Programmable Logic Controllers (PLCs) in that PLCs simulate relay logic.

Significant Application of Relays and Relay Logic

The automatic telephone switchboard was introduced in 1892. By 1929 almost 32% of the Bell Telephone System was automatic. Automatic telephone switching originally used electro-mechanical switches – which consumed a large amount of electricity. Call volume eventually grew so fast that it was feared the telephone system would consume all electricity production, prompting Bell Labs to begin research on the transistor.

A Century of Innovation: Twenty Engineering Achievements that Transformed Our Lives by George Constable and Bob Somerville (1964)

The fledgling electric utility industry also began to demand industrial controls. For instance, arc lamps in use at the time required the gap in the electrodes be sustained and it was desired that the voltage or current of the power supply was kept constant. Hence, development of electrical system monitoring and controls were being invented and designed. Oh, yes, the utilities were also very interested in automatic control and improved economic operation of their steam-operated boilers thus requiring even more automatic controls.

In the 1920's central control rooms became common at power plants and major factories. Even through the late 1930's most process control was "On/Off." Operators monitored charts drawn by recorders and to make corrections to the processes, the operators opened or closed valves or turned switches on or off (e.g.,

© 2015 The SANS Institute Author retains full rights.

Open Loop). In his book *History of Control Engineering 1800-1930,* Dr. Stuart Bennett observed control rooms also used color-coded lights to send signals to workers in the plants to manually make certain changes.

Another area of growth for control systems was from 1907 to 1914 where gyroscopes were being used for ship stabilization and autopilots. Mr. Elmer Sperry (1860-1930) was the early inventor of the *active stabilizer*. By 1930 many airlines were using the Sperry autopilots for long-distance flights.

However, challenges in understanding true control theory were abundant. Engineers were confused when a controller worked fine in one environment but failed miserably in another. Also, analysis tools for the control systems and loops were mainly elementary differential equations and could not take into account operator actions that included anticipation, backing off the power as a set point was approached, and small adjustments when the error continued.

Fortunately by 1932 the concept of "negative feedback"[9] was understood and was incorporated into new control theory concepts and design of control systems. This new concept also became known as the "standard closed-loop" analysis.

This period closed with the advent of the "communications boom" as wired and wireless systems began to emerge and pass information over distances. These events would combine with control advancements to set the stage for modern control system applications.

4. The "Classical Period" – 1935 to 1950

In papers by Dr. Bennett and C.C. Bissell they both referred to this time period as the "Classical Period" of industrial controls. There were three groups in the US working on controls and control theory during this period. They included:

[9] Feedback is a correcting signal received from the output of a control processer. The correcting signal is fed to the controller for process correction and can either have an additive effect (positive) or subtracting effect (negative). Hence, "negative feedback" tends to lessen the control signal.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

- A**merican Telephone & Telegraph (AT&T)** – They were focused on ways of extending the bandwidth of its communications systems.
- **Process Engineers and Physicists Led by Ed Smith of the Builders Iron Foundry Company** – They began to systematically develop a thorough theoretical understanding of control systems they used. They sought a common terminology and persuaded the American Society of Mechanical Engineers (ASME) to form an Industrial Instruments and Regulators Committee in 1936.
- **Foxboro Company –** Designed the Stabilog controller which provided proportional plus integral action control.
- **Servomechanisms Laboratory – Massachusetts Institute of Technology** – This group devised the concept of "block diagrams" and simulated control systems.

The inter-war period and onset of World War II brought many controls experts together – such as the groups above – to solve the "so-called fire control problem." Basically, problems with platform stability, moving targets, target tracking, and gun aiming/prediction were the key areas requiring solutions from these experts.

Needless to say the war also brought together the advanced controls experts in the UK, Germany and USSR with similar focus on war-centric control systems and problems that had application to all aspects of day-to-day life.

The efforts of this period on control system design and implementation were finally beginning to surface in the open literature after the war ended. A few books on automatic control engineering and servomechanism theory were published. In 1946 the Institution of Electrical Engineers held a conference on radar with several papers related to servomechanisms. Even the MIT Radiation Laboratory – which focused on radar problems – issued a series of books including *Theory of Servomechanism."*

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

5. Modern Controls Emerge

By the early 1950s control engineers began to realize that control systems are non-linear, that real measurements contain errors and are contaminated by noise, and in real systems both the process and the environment are uncertain. The 50's led to new ways to model the process control systems and plants using physical-mathematical mass/energy balance, "black box" models, etc. Also, engineering schools began to teach courses on servomechanisms and control theory.

The history of modern day control systems is linked to communications and the invention of data processing machines, which laid the groundwork for computers, as we know them today. In 1950, the Sperry Rand Corporation built UNIVAC I, the first commercial data processing machine.

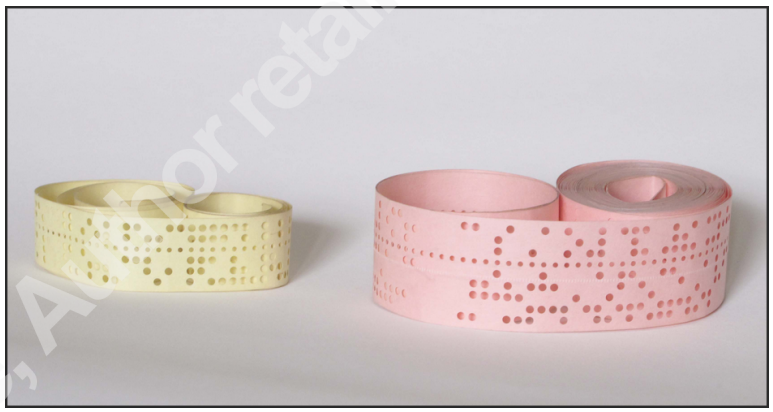


Figure 6 Numerical Control Punched Tape (Public Domain)
http://en.wikipedia.org/wiki/Punched_tape#mediaviewer/File:PaperTapes-

Machine tools were beginning to be automated in the 1950's with Numerical Control (NC) using punched paper tape (Figure 6). This evolved into Computerized Numerical Control (CNC).

Prior to the 1950's the predominant control systems were analog-based or were simply "on-off" controls due to switch or relay positions. The first reported use of **digital control systems** (DCS) began development in 1956 and was placed into operation in 1959 at the Port Arthur (Texas) refinery and in 1960 at the Monsanto ammonia plant in Luling, Louisiana. These systems were supervisory in nature and the individual loops were controlled by conventional electrical, pneumatic or hydraulic controllers but monitored by a computer. Work began in

© 2015 The SANS Institute Author retains full rights.

1959 to devise a digital computer that could fully control an industrial controls process[10].

In the later 1960's some specialized process control computers arrived on the scene offering **direct digital control** (DDC). In DDC the computer implements a discrete form of a control algorithm. Unfortunately these DDC systems were expensive and were superseded by the cheaper microcomputers of the early 1970's.

5.1. The Programmable Logic Controller (PLC)

In Jay Hooper's book, *Introduction to PLCs Second Edition*, he includes an "Origin Story" that paints the picture of the value of the PLC[11] in the modern factory. The story is included below due to its entertainment and historical perspective:

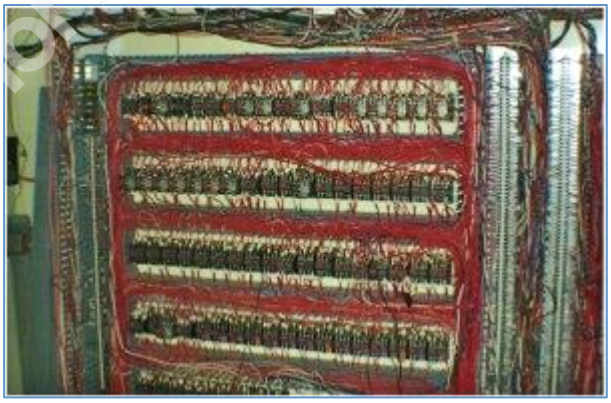


Figure 7 Picture of Factory Relay Rack (http://www.blog.beldensolutions.com/wp-content/uploads/Old-Relay-System-300x195.jpg)

So how did this control solution called a PLC come into such widespread use? Well, let me tell you an origin story to give you a sense of what happened.

At one point in the history of the car industry there were a lot of sheet metal changes every model year. This necessitated frequent changes in the configurations of the machines used in automobile manufacturing plants. The limit switches and sensors were hooked to banks and banks of control relays. These, in turn, had to be hand-wired every model year.

One year someone at a car company realized that there was "a whole lot of switchin' going on." That person thought that maybe the company could use a

[10] Bennett, S. (2004). Control and the digital computer: the early years. Measurement and Control, 37(10), 307-311

[11] PLC: programmable microprocessor-based device that is used to monitor and control instruments through a number of input and outputs with instruments, sensors, actuators, motors, etc.

© 2015 The SANS Institute Author retains full rights.

mini-computer to manage the interfaces from the switches and sensors to all of the solenoids and contactor coils. That way, the company would only need to wire up the sensors and the coils one time, and just change the logic program in the mini-computer each model year.

So, the company requested designs from various mini-computer manufacturers, who developed rudimentary PLCs and installed them in the factory. Well, after a period of time the company met with the mini-computer folks and said, "We have some good news and some bad news. The good news is that the units worked OK in our factory applications. The bad news is that we can't use any of them."

"What?" "You've got to be kidding," "What's the problem?"

It turned out that all of the units were using a high-level computer language such as FORTRAN or a low-level language such as Assembler to run the mini-computers. The problem was that in order for factory floor workers or troubleshooters to make a change or a modification in the program, they would have to know the programming language or they were stuck.

Someone in the company mused, "Well, you know, all of our electricians and control people know ladder logic. Now if the units could be programmed in ladder logic…"

"The rest is history," as they say.

So, even though we won't go into ladder logic in depth, you should know that ladder logic is an industry standard for representing relay logic control systems. The diagram resembles a ladder because the vertical supports of the ladder appear as power feed and return buses, and the horizontal rungs of the ladder appear as series and/or parallel circuits connected across the power lines.

Early relay stacks in use at that time also had their limitations. They were expensive, difficult to wire and configure, and once they were up and running they were very cumbersome to change. These shortcomings led to the development of the modern PLC. It is often noted in the history of PLCs that in extreme cases – such as in the auto industry – complete relay racks had to be removed/disposed of and

© 2015 The SANS Institute Author retains full rights.

replaced since it was not economically feasible to rewire the old panels with each production model changeover.

Mr. Dick Morley[12] is probably the "father" of the PLC. In his narrative called *The History of the PLC* he notes that the PLC was detailed on New Year's Day, 1968. Anyway, the initial machine – which was never delivered – only had 125 words of memory and there were no considerations for speed. However, when they tested the first PLC it immediately ran out of memory and it was too slow to perform any function near the relay response times required.

The first PLC to be delivered was called Modicon. The name Modicon stood for MOdular DIgital CONtroller. One of the first units was designed for the machine tool industry. The first location for the Modicon PLC was the Bryant Chuck and Grinder company in Springfield, Vermont. They brought up the model 084 (stood for Project 084). The machine was built to be rugged – it had no ON/OFF switch, had no fans, did not make any noise and had no parts to wear out.

According to Mr. Morley's narrative, however, the staff at Bryant "…liked the equipment so much that they never bought one. They in turn thought it was a good idea, and as many did at that time, tried to evolve their own."

The next major customer for the Modicon PLC was Landis in Landis, Pennsylvania. The Landis engineers were initially impressed with the Modicon PLC; however, they decided to do some of their own field testing. Mr. Morley reports that Landis wrapped welding wires around the Modicon to induce electro-magnetic noise to see if they could make it fail. But it passed

[12] http://en.wikipedia.org/wiki/Dick_Morley

© 2015 The SANS Institute Author retains full rights.



Figure 8 Modicon 084 with Modicon Team (http://gozarian.net/)

Of note, Morley also reported in his narrative that at one time the PLC mean-time-before-failure (MTBF) in the field was 50,000 hours. Pretty impressive!

Of course Modicon is not the only brand or type of PLC. In fact there are multiple brands of PLCs available on the market from Schneider, Siemens, General Electric, Mitsubishi, Yokagawa, Rockwell, etc. And, over time, PLCs are becoming more powerful due to the improved computing power and memory size.

For example, the Siemens SIMATIC N module in 1965 could perform 20 transistor functions and consequently 15 instructions per second. In the S5 model of 1988, the number had soared to about four million transistor functions and 32,000 instructions per second.

6. Energy and Utility Automation Systems

The need for improved controls systems at electric utilities and at a refinery were very briefly discussed previously. However, three of the largest users of industrial control systems – especially across large geographic areas – are electric and gas utilities and pipeline companies. In this section we will cover the automation systems energy and utility companies rely upon.

In the 1930's individual utilities and generators started to interconnect to interchange electricity for reliability and to reduce operating costs. With this new interconnection there was a greater need to control the generation more closely. Hence, analog computers were developed and installed to monitor and control generator output, tie-line power flows and line frequency. By the 1950's the analog

© 2015 The SANS Institute Author retains full rights.

computers were improved to schedule each generator as needed across the system to provide the lowest cost and continue with good reliability. These functions were called Economic Dispatch (ED) and Automatic Generation Control (AGC). These systems combined were labeled Energy Management Systems (EMS).

Supervisory control in electric utility systems also evolved from the need to operate equipment located in remote substations. In the past it was necessary to have personnel stationed at the remote site to open circuit breakers or close valves. Alternatively they sent a crew out to operate equipment. The first approach until the 1940's was to use a pair of wires or a multi-pair cable between the sites – also known as "pilot wires." Each pair of wires operated a unique piece of equipment. This was expensive but justified if the equipment needed to be operated often or in order to restore service rapidly.

In the late 1960's digital computers and associated software were developed to replace the analog EMS. These systems were initially unique and custom built for the individual customer; however, over time the new replacement EMSs are built to open standards that support real-time applications.

6.1. SCADA – Supervisory Control and Data Acquisition

The term SCADA is normally associated with those control systems that cover a large geographic area. SCADA systems have been installed as early as the 1920's where some high voltage substations adjacent to power plants could be monitored and controlled from the power plant's control room.

According to the National Institute of Standards and Technology (NIST), SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical power grids, and railway

© 2015 The SANS Institute Author retains full rights.

transportation systems. A SCADA[13] control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as **field devices**. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

6.2. Remote Terminal Units (RTUs)

The remote placement of the SCADA systems required development of devices called Remote Terminal Units (RTU's). The initial RTUs were deployed during the 1960's. RTU's were supplied primarily by the SCADA vendor; however a market for RTU's developed later from vendors other than primary SCADA vendors. RTU's used solid state components, mounted on printed circuit cards and typically housed in card racks installed in equipment cabinets, suitable for mounting in a remote power substations. They needed to operate -- even if the power was out at the station -- so they were connected to the substation battery, which was usually 129 volts DC.

The basic structure of a RTU consisted of the communication interface, central logic controller, and input/output system with analog inputs, digital inputs, control digital outputs and sometimes analog control outputs. They were typically supplied in steel cabinets with room for terminal blocks for field wiring to substation equipment. Large SCADA systems would have several hundred RTU's.

Since most RTU's operated on a continuous scan basis, and since it is important to have fast response to control operations in event of a system disturbance, the communication protocol needed to be both efficient and very

[13] The use of the term "SCADA" is often used by individuals to represent any type of industrial control system. This is misleading but common. To be more precise in your conversations the term Industrial Control Systems (ICS) is more appropriate and recognize that SCADA is a type of ICS.

© 2015 The SANS Institute Author retains full rights.

secure. Security was a primary factor, so sophisticated checksum security characters were transmitted with each message, and the select/before/operate scheme was used on control operations. The most common security check code used was BCH, which was a communication check code developed in the 60's. During the 60's and 70's most RTU communication protocols were unique to the RTU vendor i.e. proprietary.

Because of the need for both very high security and efficiency, common protocols such as ASCII were not used. In order to allow different brands of RTU's on a SCADA system there was an effort to standardize protocols led by the International Society of Electrical and Electronics Engineers (IEEE). The development of the microprocessor-based communication interface solved some of the compatibility problems.

By the way, as microprocessors began to be applied to protective relays, meters, various controllers and other devices at the utilities there was some concern raised about the appropriate name for these devices. So, the IEEE Power and Energy Society (PES) Substations Committee decided to call these devices – especially those power system components with a microprocessor and communications port – an **Intelligent Electronic Device (IED).**

6.3. Communications

Early utility control and monitoring systems were based on telephone technology using leased telephone lines operating at 300 bits/second (aka baud rate). Many utilities still use leased phone lines but they have increased the baud rate to 1200 bits/second and even to 9600 bits/second. Some utilities have decided to not rely on leased phone systems and instead have installed their own private telephone systems for increased reliability and control (in theory).

However, as we said earlier, these control systems need to communicate over large geographic distances and to remote locations. So, some utilities installed power-line carrier systems between large substations. The power-line carrier systems carried both voice and data. However, don't be surprised if most utilities

© 2015 The SANS Institute Author retains full rights.

have replaced these power-line carrier systems with microwave – either private or public systems.

Fiber optic networks are also being installed and used as Wide Area Networks (WAN) while energy and utility companies upgrade their systems.

Some utilities have implemented satellite communications for some of the more remote locations and there is some use of licensed and non-licensed 900 Megahertz point-to-point radio systems because they are cheaper than leased phone lines.

6.4. Protocols

With the advent of new PLCs, RTUs and IEDs the communications protocols for the signals are more than simple On/Off bits on the phone line. Instead they have blossomed with the number of different vendor offerings for their equipment. In the Wikipedia article on automation protocols there are about 37 different process automation protocols listed! There are also six power system automation protocols!

This situation was getting more complex over time. In the late 1980's the IEEE PES Substations Committee formed a working group to investigate the problem with the expanded number of proprietary, closed-source protocols and identify some reasonable solutions. The Working Group (WG) collected information on 120 potential protocols which were then screened against industry requirements. Upon review and ballot two protocols were selected for standardized use: Distributed Network Protocol version 3 (DNP3) and International Electrotechnical Commission (IEC) 60870-5-101.

DNP3 is now the most widely deployed and specific protocol in North America – not only for substation use but also for substation to master station communications. Of note the DNP3 ownership and maintenance is under control of the DNP Users Group (www.dnp.org) since 1996.

The IEC 61850 protocol has been deemed the substation communication protocol for smart grid implementation.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

Of note, in his article *A Brief History of Electric Utility Automation System,* Mr. H. Lee Smith observed that some North American utilities are using DNP3, Modbus and IEC 61850 GOOSE (Generic Object Oriented Substation Event) messages in the same substation local area network (LAN).

7. Cybersecurity and Control Systems

Computerized control systems have not been immune from cyber security threats. Although many of the initial cyber incidents impacting control systems were not directed at ICS, these recorded incidents were the result of wide spreading worms on the Internet that found their way into ICS networks through connections, remote access, or being carried in physically on portable media. However, there have been examples of insiders and some external actors who have specifically targeted ICS by exploiting vulnerabilities, or commanding unauthorized actions, or changing set points. One of the most touted ICS cyber incidents did involve the unauthorized release of sewage[14] as the result of malicious operation of the industrial control system. Cyber incidents that impact or take command of the control system have raised the specter of consequences that are not shared by Information Technology (IT).

Cyber threats have become more of a concern as cyber attacks can now easily rival the consequences of physical attacks[15]. In 2007, researchers at Idaho National Laboratory (INL) demonstrated the ability of using cyber to make unauthorized

---

[14] Maroochy Shire Sewage Spill: In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government but was not accepted for the position. Over a two-month time period, the disgruntled employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewage pumping stations and caused malfunctions in their operations ultimately releasing 264,000 gallons of raw sewage into nearby rivers and parks and a hotel campus.

[15] Michael Assante, *Infrastructure Protection in the Ancient World*, Proceedings of the 42nd Hawaii International Conference on System Sciences, 2009

© 2015 The SANS Institute Author retains full rights.

changes in ICS components which could result in physical damage to equipment[16]. In the late 2000s, along came the Stuxnet Worm, which took the hypothetical concept extrapolated from the Aurora research and proved not only that it had been done, but also that it was released and traveling through cyberspace undetected.

Stuxnet is a computer worm that was designed to attack ICS -- specifically Siemens Step7 software running on a Windows operating system and Siemens PLCs. Stuxnet was credited as a precision attack only causing physical damage to Iranian nuclear centrifuges by spinning them out of control while simultaneously replaying the recorded system values, which showed the normal functioning centrifuge during the attack.

The potential of cyber attacks impacting ICS and that can cause physical consequences was enough to raise policy issues and call for the development of standards and in some cases regulation in the late 1990's. Real world examples of ICS-focused attacks that have resulted in process effects and physical damage have galvanized cyber threats as a risk to system performance, reliability, and safety. The automation and control system industry has been working through a series of community efforts such as standard development and adoption of professional certifications like the Global Industrial Cybersecurity Professional (GICSP) offered by the SANS GIAC[17].

8. Evolution of Industrial Controls and New Pace of Change

The history of the ICS has evolved from a slowly engineered systems approach that rarely used Information Technology systems, protocols or components to the newer ICS deployments including TCP/IP protocols and current,

[16] Michael Assante, *Bad new world: Cyber risk and the future of our nation*, CSO Online, 2011

[17] The Global Industrial Cybersecurity Professional (GICSP) is the newest certification in the GIAC family and focuses on the foundational knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cyber security to achieve security for industrial control systems from design through retirement. http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

© 2015 The SANS Institute Author retains full rights.

open-source operating systems. The good news with these changes is that it is easier to integrate different brands of components onto the same ICS control network since they "speak the same language." Basically they are "interoperable." However, there is a challenge with this evolution to the more IT-centric implementations. For example, it has been historically noted that many ICS deployments used proprietary protocols and were difficult to attack by cyber means due to their "security by obscurity" either because of the older age of the device, its proprietary protocol, or difficulty in obtaining technical information on the device from the Internet or even technical vendors.[18] However, with new systems being based on publically available operating systems and communicating by TCP/IP, these devices and systems are vulnerable to cyber attacks that can affect IT systems, too.

As a recent example of this challenge, take a look at Microsoft's conclusion of support for the XP Operating System. Many ICS systems have been relying on XP for the past decade and with the long life-cycle for these systems – i.e., they are not changed out for years at a time – has minimized maintenance and operational impacts on these devices. However, with XP now out of support there are increased security concerns for these machines/devices and their security exposure – but, changing out these systems is not as easy as replacing a laptop or server due to the critical need for ICS system availability to run factories, generation plants, etc.

Essentially we have gone from an environment of "zero-decade" vulnerabilities and attacks to systems vulnerable to "zero-day" attacks. Therefore, there is an urgent need to be more aware and proactive of the cybersecurity aspects of these systems than ever before.

[18] "Security by Obscurity" is a term of art used in the security field to depict the approach of simply "hiding" a target to protect it rather than truly securing it. This approach is easily identified by even the less experienced attackers/hackers. This approach should not be considered a viable defense strategy.

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

9. Conclusion

This paper has been prepared to give the reader a brief history of automation and industrial control systems, along with the cybersecurity implications to modern computerized control systems. These systems are intended overall to operate equipment such as machinery, factory processes, boilers, heat-treating ovens, switching telephone networks, steering and stabilization of ships and aircraft, and other industrial applications. Automation and the associated control systems offer both advantages and disadvantages.

The main advantages of automation include:

- Increased output or productivity
- Improved quality
- Increased predictability of quality
- Improved consistency of processes or product
- Reduce direct human labor costs and expenses
- Improved safety environment for production and operations

The main disadvantages of automation include:

- Security vulnerabilities – an automated system may have limited level of intelligence and are therefore susceptible to injects that may "confuse" and overwhelm the processing capabilities
- The research and development cost of automating a process may exceed the cost saved by the automation itself
- High initial cost – the automation of a new product or plant typically requires large initial investment in comparison with the unit cost of the product
- Causing unemployment and poverty by replacing human labor

Overall automation and automatic controls have brought – and continue to bring -- benefits to society thus enabling modern production techniques, energy supply, water supply, environmental control, information and communications technologies, etc. These systems will be expanded in their complexity and sophistication, their significance will increase and they will be a larger impact on our society. Continued evolution of control

© 2015 The SANS Institute Author retains full rights.

systems with added emphasis on their cybersecurity is important and necessary as we move towards more automation.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

Automation. (2014, February 8). Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Automation

Bennett, S. (1996, June). *A Brief History of Automatic Control.* Retrieved February 12, 2014, from IEEE Control Systems Society: http://www.ieeecss.org/CSM/library/1996/june1996/02-HistoryofAutoCtrl.pdf

Bissell, C. C. (2009). History of Automatic Control. In S. Y. Nof, & S. Y. Nof (Ed.), *Springer Handbook of Automation* (pp. 1-15). Springer. Retrieved February 12, 2014, from http://siamun.weebly.com/uploads/4/1/7/3/4173241/history_of_automatic_control.pdf

Control Engineering. (2014, January 24). Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Control_engineering

Control Theory. (2014, February 11). Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Control_theory

Dunning, G. (2002). *Introduction to Programmable Logic Controllers (Second Edition)* (2nd ed.). Albany, NY, USA: Thomson Learning.

Edison Tech Center. (2013, March 20). *History of Automatic Control Engineering*. Retrieved February 12, 2014, from You Tube: http://www.youtube.com/watch?v=KlxYtk4Fiuw&noredirect=1

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

Hooper, J. F. (2006). *Introduction to PLCs (Second Edition)* (2nd ed.). Durahm, North Carolina, USA: Carolina Academic Press.

IEEE Control Systems Society. (n.d.). *Control and Control History.* Retrieved February 12, 2014, from IEEE Transactions on Automatic Control: http://www3.nd.edu/~ieeetac/history.html

List of Automation Protocols. (2013, August 5). Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/List_of_automation_protocols

Marschall, L. (2005). *History of Industrial Automation.* Retrieved February 11, 2014, from Siemens Global Website: http://www.siemens.com/innovation/en/publikationen/publications_pof/pof_spring_2005/history_of_industrial_automation.htm

Maxwell, J. C. (1868, March 5). On Governors. *Proceedings of the Royal Society of London*, 270-283. Retrieved February 12, 2014, from http://www.jstor.org/stable/112510?origin=JSTOR-pdf

Morley, R. L. (n.d.). *The History of the PLC - As Told to Howard Hendricks by Dick Morley.* Retrieved February 11, 2014, from R. Morley, Inc.: http://www.barn.org/FILES/historyofplc.html

Norman, Jeremy (2015, January 15). *The First Truly Automatic Self-Regulatory Device (Circa 250 BCE).* Retrieved January 15, 2015, from History of Information.com: http://www.historyofinformation.com/expanded.php?id=2306

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

Petruzella, F. D. (1998). *Programmable Logic Controllers (Second Edition)* (2nd ed.). New York, NY, USA: Glencoe McGraw-Hill.

Pinto, J. (2007, April 24). *Short History of Automation Growth.* Retrieved February 11, 2014, from Automation.com: http://www.automation.com/library/articles-white-papers/articles-by-jim-pinto/a-short-history-of-automation-growth

Ramebäck, C. (2003). Process Automation - History and Future. (p. 33). ABB. Retrieved February 11, 2014

Russell, J. (n.d.). *Brief History of SCADA/EMS.* Retrieved February 12, 2014, from http://scadahistory.com/

Smith, H. L. (2010, April). *A Brief History of Electric Utility Automation Systems.* Retrieved February 11, 2014, from Electric Energy Online.com: http://www.electricenergyonline.com/show_article.php?mag=63&article=491

Stuxnet. (2014, February 9). Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Stuxnet

ToolingU. (n.d.). *Motor Controls Training Reversing Motor Circuits 310*. Retrieved February 12, 2014, from ToolingU: http://www.toolingu.com/definition-460310-34114-control-circuit.html

Walker, J. (n.d.). *Bang Bang vs Proportional Control.* Retrieved December 9, 2014, from http://www.fourmilab.ch/hackdiet/www/subsection1_2_3_0_5.html

Ernie Hayden, enhayden1321@gmail.com

© 2015 The SANS Institute Author retains full rights.

Wikipedia. (2014, April 26). *Hysteresis*. Retrieved June 20, 2014, from Wikipedia - the Free Encyclopedia: http://en.wikipedia.org/wiki/Hysteresis

Wikipedia. (2014, February 11). *Relay.* Retrieved February 12, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Relay#History

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.