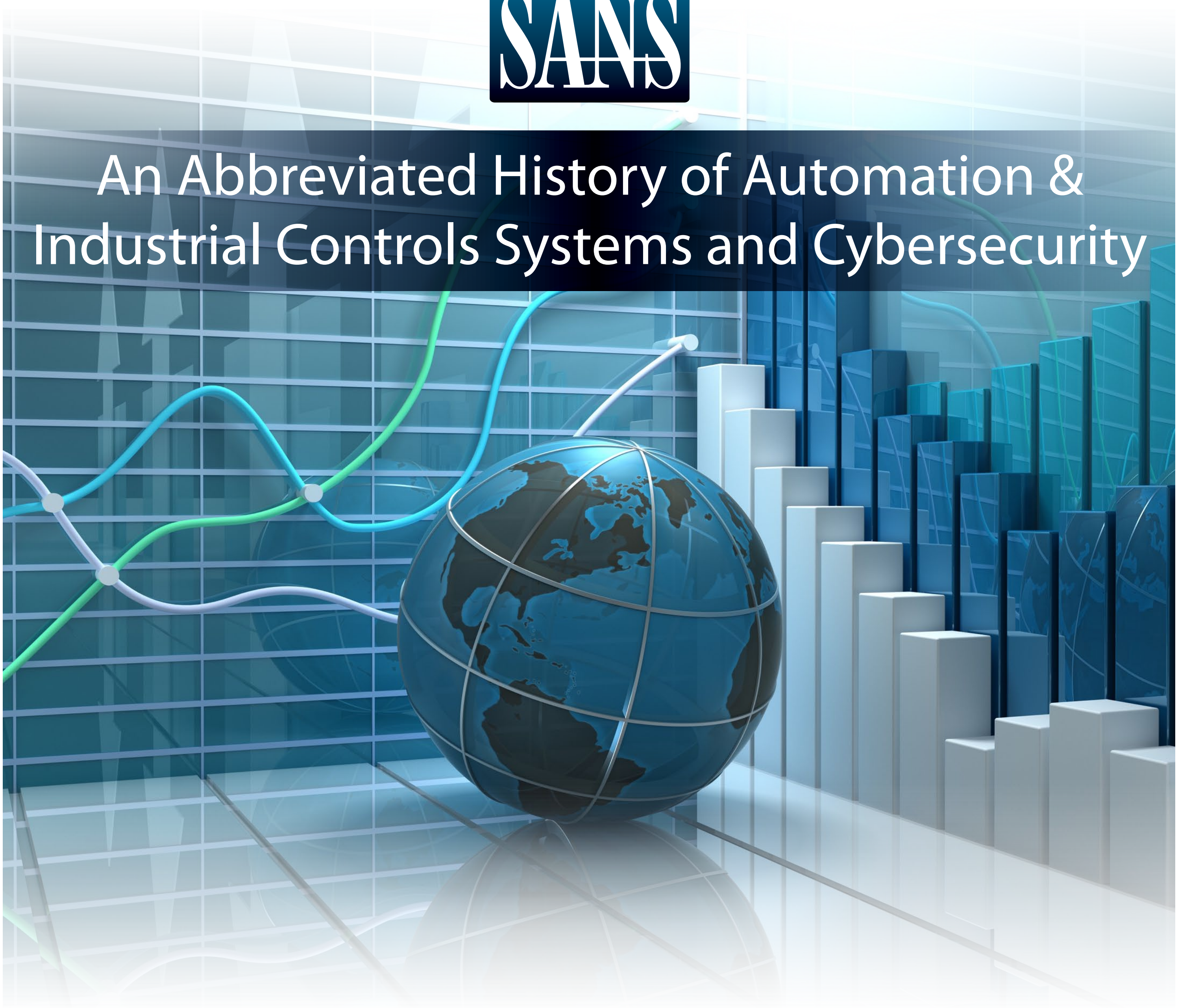

An Abbreviated History of Automation & Industrial Controls Systems and Cybersecurity

A SANS Analyst Whitepaper

Written by:

Ernie Hayden GICSP, CISSP, CEH | Michael Assante | Tim Conway

August 2014

About this Paper

Automation and Industrial Control Systems – often referred to as ICS – have an interesting and fairly long history. Today it's quite common to see discussions of industrial controls paired cyber/physical security; however, that's a relatively recent phenomenon. This paper will cover some of the history and evolution of today's control systems and provide an accounting of how cybersecurity emerged as a significant concern to their reliability and predictability.

For the purposes of this paper we will be using "ICS" to refer to the many types of automation and control system applications. This definition will get us off to a good start:

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 includes just a few of the ICS-related applications and labels we use.

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

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	SCADA & EMS – Supervisory Control & Data Acquisition & Energy Management System
DCS - Distributed Control System	Systems which control, monitor, and manage industrial processes that are disbursed but operated as a coupled system	DCS - Distributed Control System
PCS – Process Control System	Systems which control, monitor, and manage an industrial processes	PCS – Process Control System
Building Automation, BMS -Building Management System	Control systems used to manage security, safety, fire, water, air handling in a building or facility	Building Automation, BMS -Building Management System
I&C - Instrumentation & Control	Electronic devices or assemblies used to monitor, measure, manage or operate equipment in many applications	I&C - Instrumentation & Control
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	SIS - Safety Instrumented System, safety systems, protection systems

[1] Operation 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.

But First, Elementary Controls Theory in Brief

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.

Figure 1. Typical Power Plant Control Room[2]

There are two major schools of practice in control theory: classical and modern. Classical control theory is limited to single-input and single-output (SISO) system design. Modern control theory also includes with multi-input and multi-output (MIMO) systems. Hence, modern control theory overcomes the limitations of classical control theory in more sophisticated design problems such as fighter aircraft control.

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

Control systems can be thought of as having four functions:

- Measure (obtain values from sensors and read as input to process or provide as output)
- Compare (evaluate measured value to process design value)
- Compute (calculate current error, historic error, and future error)
- Correct (operator initiated actions or automated process adjustments)

These four functions are performed by five elements:

- Sensors (devices capable of measuring various physical properties)
- Transducers (converts non-electrical signal into an electrical value)
- Transmitters (device that converts measurements from a sensor and sends the signal)
- Controllers (provide the logic and I/O for the process)
- Final Control Elements (actuators that physically change a process)

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

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

[2] http://powerplantmen.files.wordpress.com/2013/04/power-plant-control-room.jpg

Feedback Control

Feedback Control is usually a continuous process and includes taking measurements with a sensor and making calculated adjustments via a 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 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.

The elements constituting the measurement and control of a single variable are called a ***Control Loop***[3].

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

A simple control loop[4] is shown in the figure below:

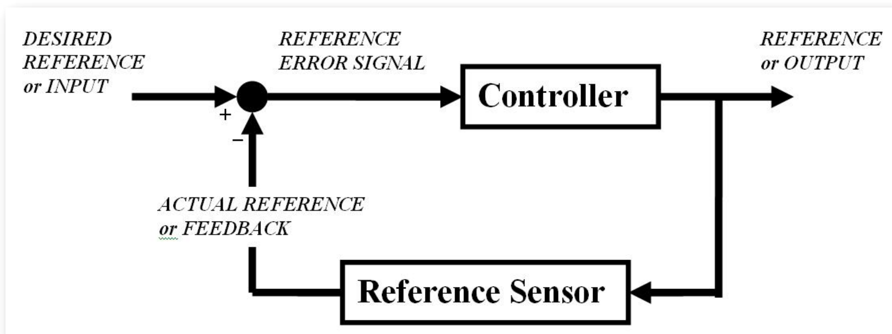

Figure 2. Diagram showing a control loop[4]

It is also important to understand if a 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, or level – and then makes manual adjustments to the controls to achieve the desired result. Imagine driving a car without cruise control turned on. The automobile's speed is managed by the driver pressing or releasing the accelerator or brake pedal That is an Open-Loop control operation.

[3] Control loop theory is used for calculating and controlling an environment or process based on feedback. Proportional, Integral, and Derivative (PID) controller theory is used to optimize tuning.

[4] http://powerplantmen.files.wordpress.com/2013/04/power-plant-control-room.jpg

In a **Closed-Loop** controller, as depicted inFigure 2 above, A 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.

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 referenced to provide an error signal to the controller to make the necessary changes to the output device.

Again, using the car analogy, a cruise control system (when activated) is a Closed-Loop controller in operation.

Sequence Control

Sequence Control may be either to a fixed sequence or a logical one that performs 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:

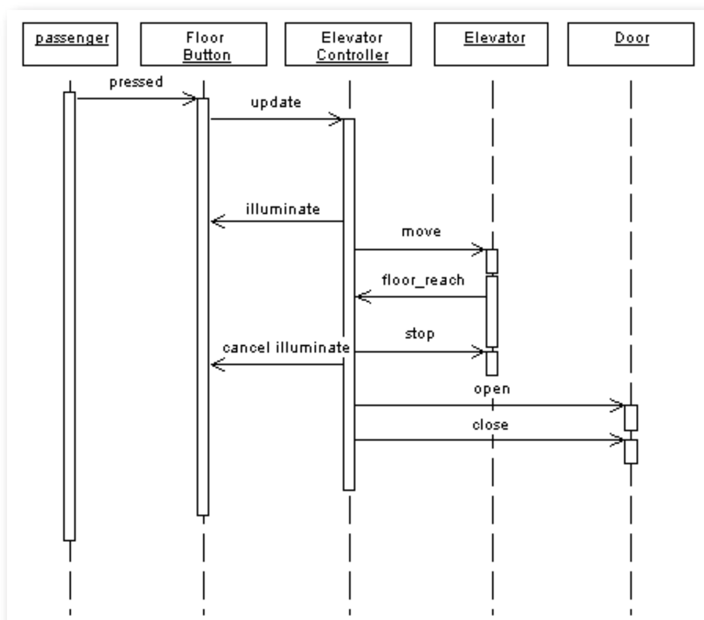

Figure 3. Sequence Control Example – Elevator [5]

As sequential controls were established and became more and more part of the industrial automation landscape they became included in **Relay Logic**. Essentially this 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 as early as 1860.

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

[5] http://www.web-feats.com/classes/dj/lessons/uml/elevator_files/flr_seq.gif

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[6]. 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.

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.

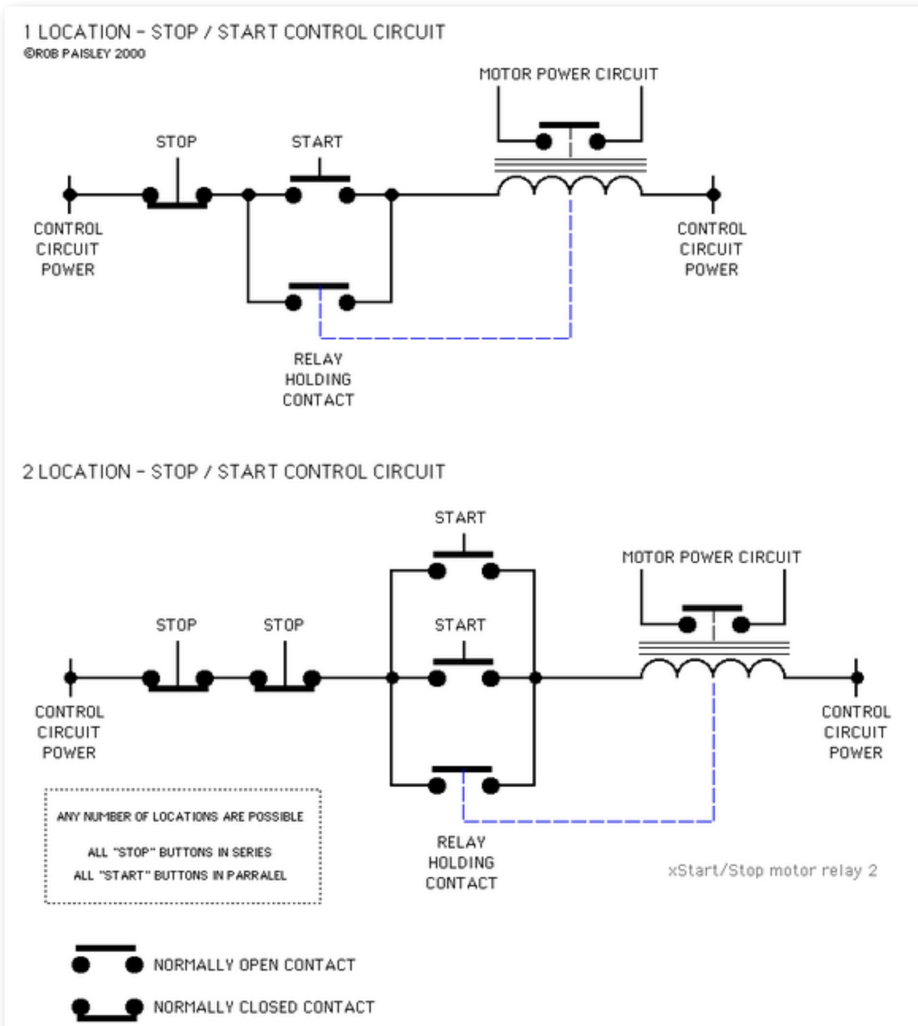

Figure 4. A Stop/Start Control Circuit [7]

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

[7] http://home.cogeco.ca/~rpaisley4/xStopStart1.GIF

The term "hysteresis" is derived from an ancient Greek word meaning "deficiency" or "lagging behind."

The Concept of Hysteresis[8]

Have you ever wondered why certain everyday controls do not "hunt" for the right output to match the desired setpoint? "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 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 it 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.

Again, this concept of hysteresis prevents rapid switching on and off – also known as "hunting" -- of the heating element as the temperature drifts around the setpoint.

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

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

History: Ancient Times and Industrial Controls

There is a rich historic record of what we would describe as automation or control systems that 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 could accomplish or to achieve an outcome that relied upon specific conditions. The benefits of automation are 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 have evolved through technology and innovation to being able to sense and act within cycles of time smaller (milliseconds) than human operators can perceive.

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.

Although we consider industrial controls as part of 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 water clocks' "automated controls" take a look at the YouTube video provided by Edison Tech Center.[9]

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. The clock kept more accurate time than any clock invented until 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 B.C. 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 Pigeon" or wooden dove automation[10]. Dancing "automata" began to take shape as mechanical devices that could accomplish a series of movements. This type of technology is an excellent example of open loop control systems.

[9] http://www.youtube.com/watch?v=KlxYtk4Fiuw&noredirect=1

[10] Nocks, The Robot. The life story of a technology (2008)

In 1620, Cornelis Drebbel designed a feedback loop, or closed loop control system, to operate a furnace, effectively designing the first thermostat[11]. Stuart Bennett of the University of Sheffield, in his paper *A Brief History of Automatic Control*, 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 as the incubator temperature would provide feedback to the liquid and ultimately back to the furnace draft control.

One of the earliest feedback control mechanisms 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 without providing precise or exact speed control. (In fact because it was not a true "governor" it was referred to as a "moderator" in some circles.)

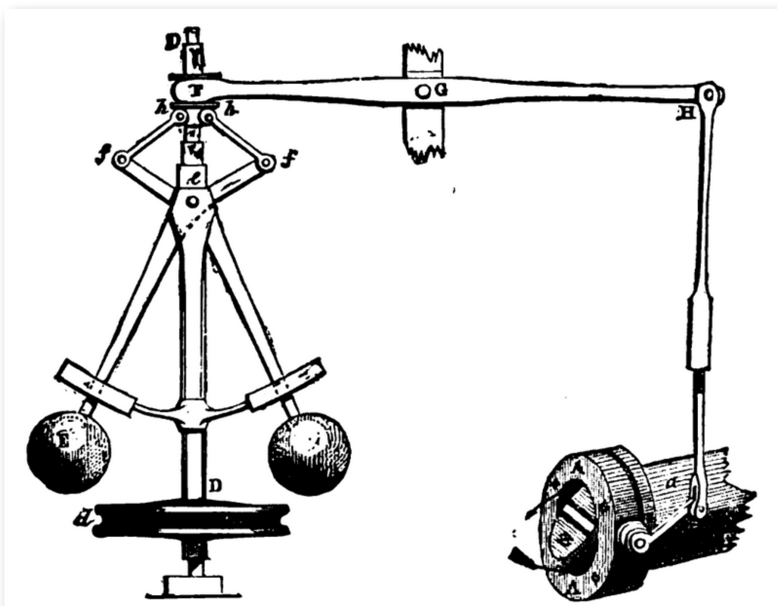

Figure 5. A Governor and Throttle Valve[12]

[11] Franklin, Gene F., Powell, J. David & Emami-Naeini, Abass Feedback Control Dynamic Systems, 4th Edition.

[12] 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 individuals such as William Siemens (1823-1883). In 1868 James Clerk Maxwell (1831-1879) – well known for his electromagnetic theories and the Maxwell Equation – published a now-famous paper entitled *On Governors*. The paper is mathematically rigorous. Maxwell showed how to derive linear differential equations for different governor mechanisms. 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."

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.[13]

From the late 1800's to the early 1900's most controls systems inventions were focused on the basic process activities of controlling temperatures, pressures, liquid levels and the speed of rotating machines. However, with 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.

Naval – 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**.

Manufacturing – Relay logic was introduced with factory electrification and 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) allowing PLCs simulate relay ladder logic.

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

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

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 (i.e., Open Loop). According to Dr. Steven Bennett control rooms also used color-coded lights to send signals to plant workers to manually make certain changes.

Transportation – 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.

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 often confused when a controller worked fine in one environment but failed miserably in another. Also, analysis tools for 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, or small adjustments when the error continued.

Fortunately by 1932 the concept of "negative feedback" 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 approach provided the much needed capability to impact the input to a process based on logic and the measured output of the same process.

This period closed with the advent of the "communications boom" as wired and wireless systems began to emerge and pass information over distances. Combined with additional control advancements, this set the stage for modern control system applications.

The "Classical Period" – 1935 to 1950

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

- **American Telephone & Telegraph (AT&T)** – 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** – 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 – includingthe 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 advanced controls experts in the UK, Germany and USSR with a similar focus on war-centric control systems and problems that had applications to many aspects of day-to-day life.

The fruits of this period on control system design and implementation began to surface in post-war literature. 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. And the MIT Radiation Laboratory – which focused on radar problems – issued a series of related books including *Theory of Servomechanism.*

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 saw the development of new ways to model 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.

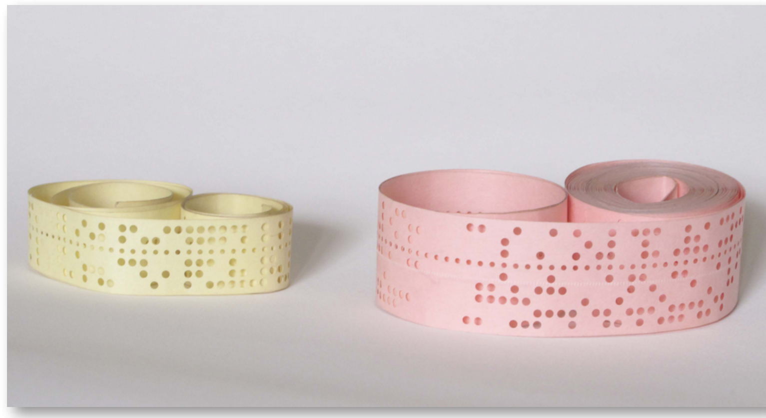

Figure 6. Numerical Control Punched Tape[14]

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).

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.

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 with analogue switch or relay positions. The first digital control systems (DCS) began development in 1956 and were placed into operation in 1959 at the Port Arthur (Texas) refinery and at the Monsanto ammonia plant in Luling, Louisiana the next year. 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 1959 to devise a digital computer that could fully control an industrial controls process[15].

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.

[14] http://upload.wikimedia.org/wikipedia/commons/0/00/PaperTapes-5and8Hole.jpg

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

The Programmable Logic Controller (PLC)

In Jay Hooper's book, *Introduction to PLCs Second Edition*, he describes the value of the PLC[16] to the modern factory:

> *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 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.*

[16] 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.

So while 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.

The first PLC delivered was called Modicon. The name Modicon stood for MOdular DIgital CONtroller.

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

Mr. Dick Morley[18] is probably the "father" of the PLC. In his narrative called "The History of the PLC" he notes that the modern PLC was born on New Year's Day, 1968. The initial machine – which was never delivered – only had 125 words of memory and there were no considerations for speed. When they tested the first PLC immediately ran out of memory and it was too slow to perform any function close to the relay response times required.

The first PLC 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 location for the first Modicon PLC was the Bryant Chuck and Grinder company in Springfield, Vermont, which used thethe model 084, whichstood 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.

[17] http://www.blog.beldensolutions.com/wp-content/uploads/Old-Relay-System-300x195.jpg

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

Figure 8. Bryant Chuck and Grinder, Springfield, VT[19]

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 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.

Figure 9. Modicon 084 with Modicon Team[20]

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

Of course Modicon is not the only type of PLC. In fact there are multiple brands of PLCs available 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.

[19] http://www.bryantgrinder.com/history_heritage.html#

[20] http://gozarian.net

Energy and Utility Automation Systems

The need for improved controls systems at electric utilities and at a refinery wasdiscussed 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 describe the automation systems upon which energy and utility companies rely.

In the 1930's individual utilities and generators started to interconnect to exchange electricity across regions for reliability and to reduce operating costs. Interconnection demanded more precise controlof generation operations. Hence, analog computers were developed and installed to monitor and control generator output, tie-line power flows and line frequency. By the 1950's these analog computers were improved to schedule each generator as needed across the system to provide the lowest cost and maintain high rates of reliability. These functions were called Economic Dispatch (ED) and Automatic Generation Control (AGC), and when combined came to be called 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 operate switches. Alternatively they dispatchedcrews on an as-needed basis. Until the 1940's a pair of wires or a multi-pair cable between sites, known as "pilot wires" helped crews perform these functions. 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 analog EMS systems. These systems were initially unique and custom built for the individual customer; however, over time the new replacement EMS's were built to open standards and came to support real-time applications.

SCADA – Supervisory Control and Data Acquisition

The term SCADA is normally associated with control systems that cover a large geographic area. SCADA systems wereinstalled 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 transportation systems. A SCADA 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.

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.

Remote Terminal Units (RTUs)

The remote placement of 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 use solid state components mounted on printed circuit cards and typically housed in card racks installed in equipment cabinets, suitable for mounting in remote power substations. They need to operate - even if the power is out at the station - so they are typically connected to a substation battery, which is usually 129 volts DC.

The basic structure of an RTU consists of the communication interface, a central logic controller, and an input/output system with analog inputs, digital inputs, control digital outputs and sometimes analog control outputs. They are typically supplied in steel cabinets with room for terminal blocks for field wiring to substation equipment. Large SCADA systems often 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 the event of a system disturbance, the communication protocol needed to be both efficient and very 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.

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).

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 or 9600 bits/second. Some utilities have decided to not rely on leased phone systems and instead have installed their own private communications systems seeking, but not always achieving, increased reliability and control.

However, as we said earlier, utility control systems need to communicate over large geographic distances and to remote locations. So, utilities installed power-line carrier systems between large substations. The power-line carrier systems carried both voice and data. However, many if not most utilities 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.

Protocols

With the advent of new PLCs, RTUs and IEDs, communications protocols for the signals are more than simple On/Off bits on the phone line. They number of offerings and options has proliferated. 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 diversity poses signficant challenges for utilities and suppliers attempting to deploy, operate and maintain these systems.

And the situation has been getting worse over time. In the late 1980's the IEEE PES Substations Committee formed a working group to investigate the problem of the expanding number of proprietary, closed-source protocols and identify some practical 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 protocol in North America – not only for substation use but also for substation-to-master station communications. DNP3 ownership and maintenance has been 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. Mr. H. Lee Smith, he noted 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).

Cybersecurity and Control Systems

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.

Computerized control systems have not been immune from cyber security threats. Although many of the initial cyber incidents impacting control systems were not targeting ICS systems, these incidents were the result of widespread Internet worms that found their way into ICS networks via network connections, remote access, and/or portable media. There have also been examples of insiders and external actors who have specifically targeted ICS by exploiting vulnerabilities, performing unauthorized actions, and/or changing setpoints. One of the most touted ICS cyber incidents involved the unauthorized release of sewage 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 to ICS rival or surpass the consequences of physical attacks[20]. In 2007, researchers at Idaho National Laboratory (INL) demonstrated the ability of using cyber techniques to make unauthorized changes in ICS components which could result in physical damage to utility equipment[21]. In the late 2000s, the Stuxnet Wormtook the hypothetical scenario demonstrated in the Aurora research and proved not only that a successful cyber attack on an operations environment could be executed , but also that it was released and traveled through cyberspace undetected.

The Stuxnet computer worm was designed specifically to attack ICS – specifically Siemens Step7 software running on a Windows operating system and Siemens PLCs. Stuxnet performed a precision attack causing physical damage to a specific Iranian nuclear operations environment. The centrifuges at the facility were impacted through modification of their control parameters, while simultaneously displaying expected system values to the operators. Their displaysshowed normal centrifuge functions throughout the course of the attack.

There has been an observed increase in cited ICS incidents to include evidence pointing to attacks that are targeted and include ICS-capable exploits. The Department of Homeland Security's ICS-CERT in the U.S. has been warning of increased risk of control system focused attacks (they cite an increase in Internet accessible configurations, the availability of control system specific exploitation tools, and increased interest by threat actors).

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

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

Cyber threats have become ICS-capable through malware designed for ICS applications. The addition of an OPC (OLE for Process Control) exploit module to the Havex Trojan and observed delivery tactic of watering-holes using ICS supply chain related websites exemplifies the newest chapter in the book of ICS cyber threats. The objective of the OPC exploit is two-fold - 1) targeting OPC gives the attackers a wide swath as it is a common solution designed to exchange data between diverse control systems, and 2) to gather the necessary information on connected ICS devices to select appropriate payloads and perform a successful follow-on attack. This form of directed attack requires ICS defenders to deploy improved defenses and gain the necessary knowledge and skills to respond effectively.

We can use a specific example to illustrate the growing number of ICS-capable security testing tools that can be used by someone to conduct a crafted attack. Critical Intelligence, an ICS security focused intelligence firm, has reported a shocking growth in electric smart meter attack tools after several researchers in 2009 discussed the security weaknesses in existing smart grid technology and how attacks could occur. They have catalogued the following tools that apply to smart meters: GoodFET, YARD Stick, RFCat, KillerBee, HackRF, Ettus B200, Ettus USRP x300, Nuand BladeRR, Sewio, ApiMote, Termineter, Optiguard.

Real-world ICS-focused attacks that have resulted in process effects and physical damage have galvanized the ICS supplier, user and regulator communities to develop responsive policies and standards. One good outcome of this heightened attention is the development and adoption of professional certifications like the Global Industrial Cybersecurity Professional (GICSP) offered by the SANS GIAC[22].

[22] 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

Integrated Abbreviated Timeline of Automation, Cybersecurity, and Policy/Governance

It is interesting to integrate and display automation and control system innovations alongside of cybersecurity incidents and developments in the area of policy, standards, and programs. The following table provides an abbreviated chronology of some of the noteworthy events:

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
1700-1900 1st Industrial Revolution – Mechanical production powered by steam	**1700s** René-Antoine Ferchault de Réamur proposed ideas for automatic devices to provide feedback for the purposes of control **1745** Edmund Lee's tenting of sails on windmills **1788** James Watt's steam governor provided proportional control of the throttle **1873** Jean Joseph Léon Farcot published a book on what he called "servo-motcur" **1900s** Use of relays and control cabinets in remote rooms to turn things on/off by use of switches and monitor recorders		
1900-1970 2nd Industrial Revolution – Mass production powered by electricity	**1932** The concept of "negative feedback" was understood and was incorporated into new control theory concepts and design of control systems **1950s** Machine tools were automated using Numerical Control (NC) using punched paper tape **1959** First use of distributed control throughout a large industrial plant **1968** First design concept of a Programmable Controller **1969** Modicon 084 the first Programmable Controller (PC) implemented. (Modicon stood for MOdular DIgital CONtroller)		

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
1970-2000 3rd Industrial Revolution – Automation of production by electronics	**1971** Allen-Bradley designed and named he Bulletin 1774 PLC and coined the term "Programmable Logic Controller" **1973** Modbus introduced to allow PLCs to talk with one another **1976** Introduces remote I/O **1986** PLCs are linked to PCs **1990s** Fieldbus protocols to include ControlNet, DeviceNet, Profibus, Fieldbus Foundation **1992** Ethernet and TCP/IP connectivity for PLCs	**1980s** Uncoraborated report of a Trojan program inserted into SCADA system software that caused a massive natural gas explosion along the Trans-Siberian pipeline in 1982. 'Farewell Dossier' **March 2000** Sewage-processing plant attacked by former contractor resulting in release of sewage. The electronic attacks on the Maroochy Shire sewage control system in Queensland in 2000, highlight the need to manage and promote the security and protection of critical infrastructure. **April 2000** Media reports about GAZPROM cyber incident impacting operatinal systems	**1997** The Report of The President's Commission on Critical Infrastructure Protection **1998** The White House acknowledged the work of the Commission and released an important policy document known as the Presidential Decision Directive 63 (PDD63). It recognized since 1998 through the PDD-63 and the PCCIP that allowing an adversary to control a critical infrastructure through SCADA could cause national problems. **1998** Sandia established its SCADA Security Development Laboratory (SSDL)

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
2001-2004	**2003** First controllers with embedded web server	**January 2003** Plant computers infected by Slammer worm. The "Slammer" worm disabled the computerized safety monitoring system at the Davis-Besse nuclear power plant in Ohio, which was shut down for repair at that time. The responsible managers considered the plant "secure," as its outside network connection was protected by a firewall. The worm entered the plant network via a contractor's infected computer connected via telephone dial-up directly to the plant network, thus bypassing the firewall. apparently migrated through the corporate networks until it finally reached the critical **January 2003** The SCADA control network used frame relay. The telecommunications frame relay utilized Asynchronous Transfer Mode (ATM) through the telecommunication network backbone for a variety of services. The ATM bandwidth became overwhelmed by the worm blocking SCADA traffic on the Frame Relay Service. **August 2003** The Blaster worm infected the communication system of the U.S. railway company. The dispatching and signaling systems were affected and all passenger and freight traffic, including morning commuter traffic in the Washington, DC, area, had to be stopped for about half a day **December 2003** Staff noticed that the Advanced Process Controls (APC) Servers were getting slower and slower. Investigators found Nachi (AKA Welchia) virus on 8 APCs (running Windows 2000) and, disconnected these servers from production network for 5 hours. **December 2003** Bulk Electric System Control Center servers and computers were infected by the Nachi virus. A new server was delivered from the supplier that was infected and placed on the network.	**2002** Homeland Security Act consolidates cybersecurityinto DHS, e.g., FEDCIRC from GSA, NIPC from FBI, NCS from DOD **2002** ISA-99 Committee formed **2003** The President released The National Strategy to Secure Cyberspace. This document was addressed to the American public with the intention of expanding the effort and broadening participation. **2003** Hacker interest was a presentation at the 2003 Brumcon meeting titled "Water Management Systems Using Packet Radio **2003** Created in 2003, the DOE National SCADA Test Bed (NSTB) **2004** DHS Control Systems Security Program managed by the Idaho National Laboratory, implements Cybersecurity test bed focused on Critical Infrastructure **April 2004** NIST published the System Protection Profile – Industrial Control Systems

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
2005-2010		**2005** SCADA workstations shipped to utility with infections **August 2005** Zotob worm infects 13 US auto plants causing shutdowns and delays **November 2006** Breach into PA water plant installation of spyware on plant's computer systems **August 2007** LA Traffic System cyber intrusion by insiders (labor strike) **January 2008** Commuter tram collision by glancing blow and derailment due to unauthorized switching. Polish teenager allegedly turned the tram system in the city of Lodz into his own personal train set, triggering chaos and derailing four vehicles in the process. Twelve people were injured in one of the incidents. Four trams were derailed, and others had to make emergency stops that left passengers hurt."He studied the trams and the tracks for a long time and then built a device that looked like a TV remote control and used it to manoeuvre the trams and the tracks," said Miroslaw Micor, a spokesman for Lodz police.	**2005** NERC has established cyber security standards that it holds it members to. "Urgent Action Standard 1200 – Cyber Security" lays out security requirements, measures for compliance, compliance monitoring through self-certification, levels of non-compliance and sanctions **2005** PCSF is still in its infancy having had its formational meeting in February 2005 and planning to have its first Forum meeting in May 2005 **December 2005** Qatar established the Qatar Computer Emergency Response Team (Q-CERT) **March 2006** AGA-12 Part 1 published **March 2006** First SANS SCADA Security Summit – now the annual SANS ICS Summit **2007** ISA-62443-1-1 formerly referred to as ISA-99 Part 1 was originally published as ISA standard ANSI/ISA-99.00.01-2007 and IEC/TS 62443-1-1 **February 2007** CPNI created in the UK followed by the development of a SCADA Program **March 2007** Aurora generator test is conducted **2008** DC Blackhat - "Breakage" presentation on what you can do to impact the process **2008** Joint National and Homeland Security Presidential Directives (NSPD-54/HSPD-23) for Cybersecurity Policyand creation of the Comprehensive National Cybersecurity Initiative

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
2005-2010 ***(Continued)***		**January 2008** U.S. Government Official discloses: "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyberattacks have been used to disrupt power equipment in several regions outside the United States.	**2008** Repository of Industrial Security Incidents (RISI) created
		February 2009 Conficker Worm gets into ICS along with 12 million general computers. Conficker recorded as infecting power generation plants ICS components in the US **2009** Off-shore oil platform hacks impact leak detection systems. Unauthorized access and control of off shore platform leak detection and monitoring system **September 2009** Utility smart meters are compromised in scale resulting in loss revenue **December 2009** Virus infection of OPC servers at Petro-checmical plant in South Africa	**2009** Shodan - It was launched in 2009 by computer programmer John Matherly, who, in 2003,[3] conceived the idea of searching devices linked to the Internet. ICS Map was released in May 2014 **2009** Release of the White House 60-Day Cyber Study **2009** European Commission adopted a Communication on Critical Information Infrastructure Protection CIIP **July 2009** In 2008 Eric Byres of Byres Research Inc. and Mark Fabro of Lofty Perch Inc. began collaboration on a project to develop the Repository of Industrial Security Incidents (RISI) with a goal of making RISI available to the entire industrial automation community. On March 31st, 2009 exida acquired Byres Research and in July 2009 created the Security Incidents Organization™, to operate RISI and fulfill the vision of Eric, Justin, David, and Mark that one day this important information would be available to the community. **2009** DHS ICS-CERT was formed
		2010 Stuxnet worm discovered. Stuxnet is a computer worm that was discovered in June 2010 but evidence suggests variations may have dated back to 2007/2005	**2010** They were renumbered to be the ANSI/ISA-62443 series. This change was intended to align the ISA and ANSI document numbering with the corresponding International Electrotechnical Commission (IEC) standards. **October 2010** ICSJWG held first meeting

EPOCH	Automation Event	ICS Security Event	ICS Policy, Standards, Program Event
2011-Today		**September 2011** Duqu computer Malware discovered **February 2011** Conficker still infecting ICS as a Metal Manufacturing plant in Rio de janeiro is impacted **2012** Houston water system compromise **2012** A series of Advanced Persistent Threat (APT) cases are noted that have ICS aspects **May 2012** Flame computer Malware discovered **September 2012** Telvent intrusion, company warns ICS customers (ICS supplier) **2012** Several ICS honeynet projects are published that demonstrate the speed and depth of cyber attacks **Today** A never ending series of ICS incidents are now being disclosed with varying level of detail and new ICS-specific attacks continue. The June 2014 discovery of an ICS-focused water-holing attack that utilized the Havex Trojan continues to receive attention due to the observer malware capability to locate OPC servers and attempt to exfiltrate data collected.	**December 2011** ENISA published a report 'Protecting Industrial Control Systems: Recommendations for Europe and Member States' **2012** SCADA lab established in Spain **March 2012** Japan's CSSC was established in March of 2012, and is emulating what they view as the successes in the US, UK and other countries. **February 2013** Executive Order - February 19, 2013, which directed the National Institute of Standards and Technology (NIST) to lead the development of a framework to reduce cyber risks to critical infrastructure.

Evolution of Industrial Controls and New Pace of Change

Essentially we have gone from an environment of "zero-decade" vulnerabilities and attacks to systems vulnerable to "zero-day" attacks.

The history of the ICS systems has evolved from a slowly developed system that rarely used Information Technology systems, protocols or components to the newer ICS deployments including TCP/IP protocols and current, open-source operating sytems. 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." 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." 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 – and an approach to patching and maintenance that 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.

Conclusions

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
- Creation of higher value jobs to support and maintain ICS environments

The main disadvantages of automation include:

- Security vulnerabilities – an automated system may have a 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, therefore, their significance will increase and they will be a larger impact on our society.

Bibliography

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

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)*. 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

Hooper, J. F. (2006). *Introduction to PLCs (Second Edition)*. Durham, 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: 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

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

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

Pinto, J. (2007, April 24). *Short History of Automation Growth*. Retrieved February 11, 2014, from Automation.com: 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

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: 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: www.toolingu.com/definition-460310-34114-control-circuit.html

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

About the Authors

Ernie Hayden – GICSP, CISSP, CEH, Executive Consultant, at Securicon, LLC providing Critical Infrastructure Protection and Industrial Controls Security Expertise. Ernie is a highly experienced and seasoned technical consultant, author, speaker, strategist and thought-leader with extensive experience in the power utility industry, critical infrastructure protection/information security domain, industrial controls security, cybercrime and cyberwarfare areas. His primary emphasis is on project and business development involving cyber and physical security of industrial controls, smart grid, energy supply, and oil/gas/electric systems and facilities with special expertise on industrial controls and NERC Critical Infrastructure Protection (NERC CIP) standards. Hayden has held roles as Global Managing Principal – Critical Infrastructure/Industrial Controls Security at Verizon, held information security officer/manager positions at the Port of Seattle, Group Health Cooperative (Seattle), ALSTOM ESCA and Seattle City Light. In 2012 Ernie was named a "Smart Grid Pioneer" by Smart Grid Today and published an article on Microgrid security in Jesse Berst's Smart Grid News Ernie is a frequent author of blogs, opinion pieces and white papers. He has been cited in the Financial Times, Boston Globe, Energy Biz Magazine, and Puget Sound Business Journal. Many of his articles have been posted to such forums as Energy Central, Public Utility Fortnightly "SPARK," and his own blog on Infrastructure Security.

Michael Assante – Michael Assante is currently the SANS project lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security. He served as Vice President and Chief Security Officer of the North American Electric Reliability (NERC) Corporation, where he oversaw industry-wide implementation of cyber security standards across the continent. Prior to joining NERC, Mr. Assante held a number of high-level positions at Idaho National Labs and served and as Vice President and Chief Security Officer for American Electric Power. Mr. Assante's work in ICS security has been widely recognized and was selected by his peers as the winner of Information Security Magazine's security leadership award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its outstanding achievement award in the practice of security within an organization.

Tim Conway – Technical Director ICS and SCADA programs at SANS. Responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Formerly, the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO). Responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Previously, an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. Former Chair of the RFC CIPC, current Chair of the NERC CIP Interpretation Drafting Team, member of the NESCO advisory board, current Chair of the NERC CIPC GridEx Working Group, and Chair of the NBISE Smart Grid Cyber Security panel.