SANDIA REPORT

SAND2010-5183
Unlimited Release
Printed August 2010

Control System Devices: Architectures and Supply Channels Overview

Moses D. Schwartz, John Mulder, Jason Trent, William D. Atkins

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multi-program laboratory managed and operated by Sandia Corporation,
a wholly owned subsidiary of Lockheed Martin Corporation, for the US Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@adonis.osti.gov
Online ordering:	http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.fedworld.gov
Online order:	http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2010-5183
Unlimited Release
Printed August 2010

Control System Devices: Architectures and Supply Channels Overview

Moses D. Schwartz, John Mulder, Jason Trent, William D. Atkins
Critical Infrastructure Systems Department 5628
Computer Sciences Department 5621
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0671

Abstract

This report describes a research project to examine the hardware used in automated control systems like those that control the electric grid. This report provides an overview of the vendors, architectures, and supply channels for a number of control system devices. The research itself represents an attempt to probe more deeply into the area of programmable logic controllers (PLCs)—the specialized digital computers that control individual processes within supervisory control and data acquisition (SCADA) systems. The report (1) provides an overview of control system networks and PLC architecture, (2) furnishes profiles for the top eight vendors in the PLC industry, (3) discusses the communications protocols used in different industries, and (4) analyzes the hardware used in several PLC devices. As part of the project, several PLCs were disassembled to identify constituent components. That information will direct the next step of the research, which will greatly increase our understanding of PLC security in both the hardware and software areas. Such an understanding is vital for discerning the potential national security impact of security flaws in these devices, as well as for developing proactive countermeasures.

Page intentionally blank

CONTENTS

FIGURES

FIGURES (CONCLUDED)

Page intentionally blank

1. INTRODUCTION

1.1 Background

The automated systems that control United States critical infrastructures (e.g., the electric distribution system) are vulnerable to physical and cyber attack, with potential negative consequences that range from significant interruption of utility services to loss of human life. Numerous efforts have been made to understand and mitigate the threats to critical infrastructure control systems, particularly supervisory control and data acquisition (SCADA) systems. Many of these threat-mitigation efforts have been conducted through the National SCADA Test Bed (NSTB) Program, which is directed by the Department of Energy (DOE). The DOE Office of Electricity Delivery and Energy Reliability (OE) is tasked with assisting industry and government in improving the security of energy sector control systems. The research in this report, although not directly supported by the NSTB, builds on research and experience acquired from NSTB projects.

This report describes an internally funded research project that addresses an area of research that has not been well explored—the specific hardware and communications protocols used in automated control systems across industries and regions. This report provides an overview of the vendors, architectures, and supply channels for a number of control system devices. The research itself represents an attempt to probe more deeply into the area of programmable logic controllers (PLCs)—the specialized digital computers that control individual processes within SCADA systems.

1.2 Purpose

This report is intended to convey an overview of the control systems markets, with a significant focus on the PLC sector. The overview includes information on major vendors, types of technologies used, larger trends in the industry, markets and locations served, and some supply chain analysis. This document also includes detailed results of dissections of several PLCs, showing each component.

Most attacks on critical infrastructure control systems have focused on PC-based parts of the control system network. Defense against these attacks has also focused on those parts. The focus here, on the PLC, is motivated by several factors: (1) their prevalence, (2) the fact that they are located close to the physical system being controlled, and (3) the fact that embedded devices have had comparatively little detection, protection, or forensics work conducted to characterize them. A detailed analysis of the hardware and low-level software of PLCs is necessary to develop effective defensive strategies and technologies. Such an analysis is also necessary to understand the potential threats to these systems.

This report is intended to improve understanding of the threats posed to critical infrastructures by sophisticated adversaries. The analyses provided in this report will extend our assessment capabilities to the hardware component level.

1.3 Scope and Methodology

The information in this report was compiled using primarily open source information, including corporate reports and industry news. The authors also collected information through interviews with subject matter experts. The research for this report included the disassembly of several PLC devices and subsequent examination of the internal hardware to gain an understanding of the components that are most common to PLCs. The components were then researched to determine their capabilities and origins. This report represents the first step in a project intended to improve our understanding of these devices. Future work will focus on a more detailed analysis of individual devices. The selection of those devices will be directed by the findings in this report.

2. CONTROL SYSTEMS OVERVIEW

2.1 Control System Components

Control system components can be broadly grouped into two categories: control center devices and remote site devices. Control center devices reside in system control centers. They include human-machine interfaces (HMI), engineering workstations, and data historians. Remote site devices reside in the field and directly connect to actuators and sensors to supervise and control physical processes. Although field devices are not typically directly interfaceable by humans, they present a larger attack surface because field locations are often in less secure perimeters than control centers.

2.1.1 Control Center Devices

The HMI, sometimes referred to as the SCADA system, is the system that allows a human operator to monitor and control a process. HMIs are typically pure-software applications run on commodity hardware, often in a Microsoft Windows operating environment. Some common HMIs in industry include Wonderware, Siemens WinCC, Rockwell RSView, and Areva's e-terra solution.

The Data Historian is a database that contains a history of the state of a process control system. In some cases, the interface for the Historian is sufficiently powerful that it serves as an HMI for the control system. The Historian typically runs on mainstream operating systems and commodity hardware, and is often mirrored on the corporate network.

2.1.2 Remote Site Devices

Remote site devices include PLCs, remote terminal units (RTUs), intelligent electronic devices (IEDs), and electrical relays. Although these devices are very different in capability and purpose, they may be roughly grouped together because their ultimate functions are similar.[1] Additionally, the hardware used in each of these devices is becoming quite similar. These devices provide analog and digital input/output (I/O) and control. Typically they either read directly from sensors and send changes directly to actuators or they are chained together with other field devices.

[1] This is a simplistic view of the devices and is intended to simplify this discussion. Each of these devices perform a subset of the functions in the control system object relational model (ORM) (see Appendix A). For example, an RTU normally only provides the SCADA Field Equipment functions of an I/O Controller doing sampling through Field I/O sensors. Some RTUs generate triggers to actuators, but this is not always true. On the other hand, a relay will always perform both the sampling and triggering function. An RTU will produce Status Data Field Points and sometimes process Command Data Field Points. A relay will produce Status Data Field Points but is unlikely to process Command Data Field Points. An RTU will have no local control function, but a relay will have that function. PLCs will have significant local control functionality in addition to communicating with sensors, actuators, and higher control functions. These functions appear similar, but are significantly different in the ORM.

2.2 Typical Control System Architecture

Figure 1. shows a typical control system architecture. In this example, a commodity PC running an HMI communicates over standard network protocols (such as Ethernet) to field devices such as PLCs. Engineering workstations and historians are also typically commodity PCs that communicate with field devices over standard network protocols. These field devices in turn connect to other local field devices using protocols such as Foundation Fieldbus (described in Section 5). The connections between field devices are often serial links that employ standards such as RS232 or RS485. Other local field devices connect directly to sensors, I/O devices, and equipment.

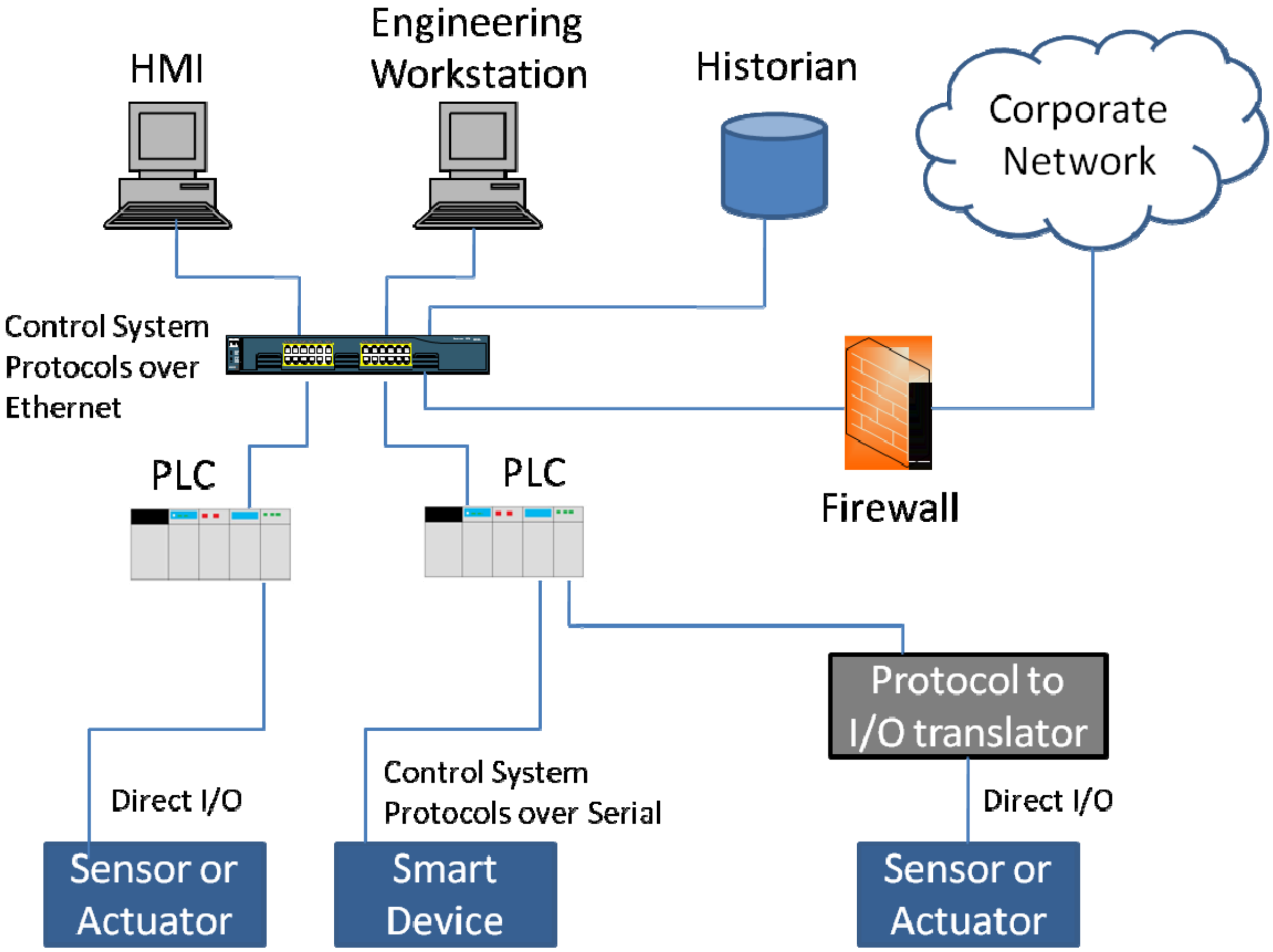


Figure 1. Typical distributed control system architecture.

2.3 Programmable Logic Controllers

As noted in Section 1, PLCs are the primary focus of the research project described in this report. A PLC is a field device that can be directly connected to sensors and actuators or to other field devices. PLCs have some local control in the form of a logic program (usually in an IEC 61131-3 defined format) and are generally capable of receiving control commands and queries from HMIs via a control system communications protocol. PLCs may be either modular or combined into compact fixed form factors, but both types use essentially the same underlying components.

2.3.2 PLC Programming

PLCs may be programmed using one of the languages listed in IEC 61131-3:

- Ladder diagram (LD), graphical
- Function block diagram (FBD), graphical
- Structured text (ST), textual
- Instruction list (IL), textual
- Sequential function chart (SFC), graphical

The PLC operates in a loop cycle called a "scan." The scan consists of input, logic execution, and output.

2.3.3 Generic Modular PLC Architecture

Figure 2 shows a generic modular PLC architecture. Modular PLCs are composed of discrete modules that are connected via a backplane. Non-modular PLCs share all the same components, but with those components integrated into one board.

2.3.4 PLC Module Interaction

In the generic PLC architecture shown in Figure 2, each module has a physical slot with a range of backplane addresses assigned to it. Interface registers and memory buffers are exposed within the backplane address range. To send and receive messages, modules read from and write to registers and buffers in other modules.

2.3.5 Processor Module

The processor module is the core of the PLC. It coordinates between modules, sometimes acting as the backplane arbiter. If the other modules do not store their own configurations, the processor module will configure them on power-up.

The processor module interprets and executes the ladder logic, reads values from the protocol and I/O modules, maintains state, runs through a scan of ladder logic, and writes values to the protocol and I/O modules.

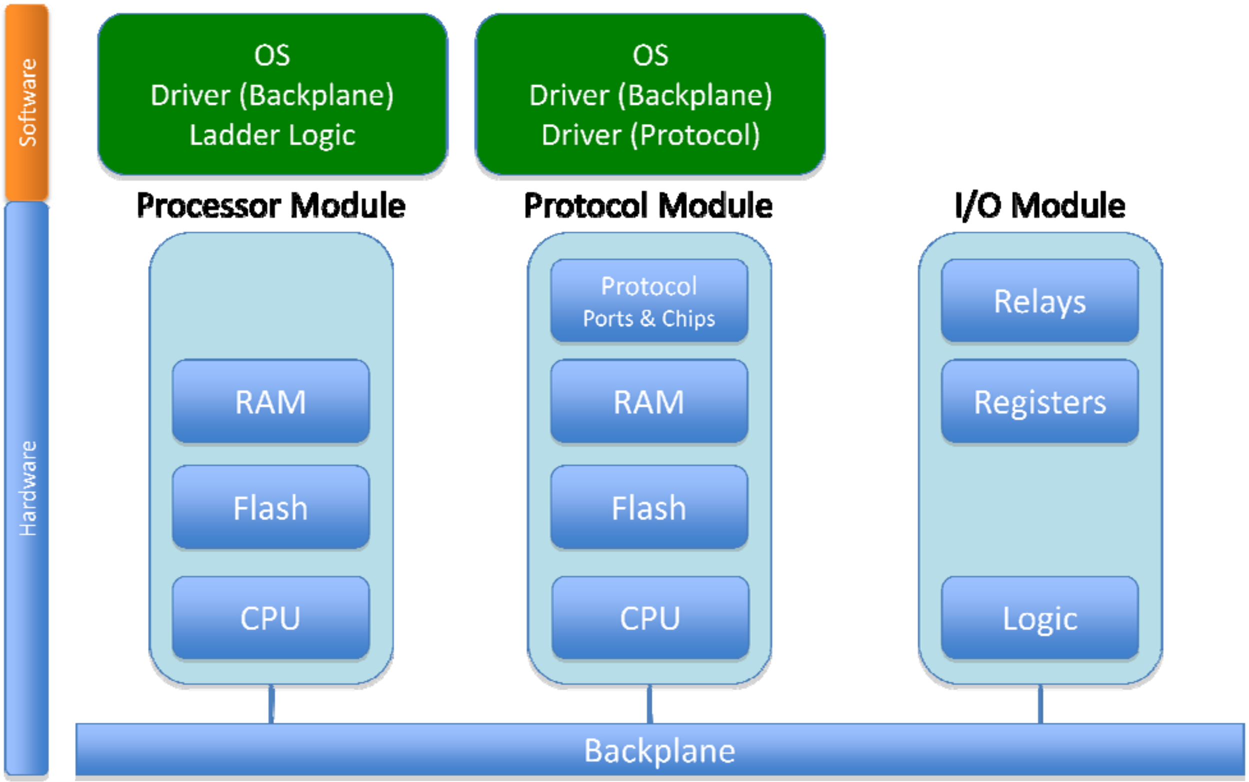


Figure 2. Generic modular PLC architecture.

2.3.6 Communications Modules

Communications modules remove complex, communications protocol-specific code from the processor module. They offload time-sensitive protocol interaction from the processor module, which is in its own time-sensitive control loop. Because some control system protocols are extremely complex, protocol modules may contain significant processing power and intelligence. These modules can be as sophisticated as the processor module.

2.3.7 I/O Modules

I/O modules convert signals between low voltage (3.3 volt or 5 volt), low current (milliamps) control logic and high voltage (24+volt), high current (amps) process control. Analog I/O modules contain analog to digital converters (ADC) and digital to analog converters (DAC). These are the simplest modules, and include very little intelligence. Their only task is to convert signals between analog and digital representations.

2.3.8 Common Processors

The processor architectures most commonly found in PLCs are of three types:

- ARM (family 7 or 9),
- Motorola/Freescale 68000 series, and
- Power architecture.

The ARM architecture is designed by a UK-based company, ARM Ltd., which employs more than 1700 people. ARM does not manufacture chips but rather designs and licenses intellectual property. (1) ARM architecture is widely used in embedded systems and devices; it has an especially large presence in consumer electronics such as mobile phones and personal digital assistants (PDAs), with a market share of over 90%. (2) An ARM processor may operate in either big-endian or little-endian mode, and may use ARM (32-bit) and Thumb (16-bit) instruction sets. ARM processors are usually part of a custom system on a chip (SOC).

The Motorola (now Freescale) 68000 series is a 32-bit complex instruction set computing (CISC) microprocessor. It is used extensively in embedded applications. As of the year 2000, it was the best selling 32-bit architecture in the world. (2) The 68000 series is big-endian.

The Power architecture, which includes the PowerPC, is a reduced instruction set computing (RISC) instruction set implemented by companies including IBM, Freescale, AMCC, Tundra, and P.A. Semi. The Power architecture is big-endian.

2.3.9 Memory Layout

PLCs generally use nonvolatile flash storage to store firmware for a module's processor and ladder logic (or other IEC 61131-3 language) programs. The flash storage is memory-mapped into the processor's address space, as are the control registers for other on-board devices. RAM is used for maintaining run-time state.

2.3.10 Embedded Operating Systems

Many embedded operating systems are considered real time operating systems (RTOS). To be considered an RTOS, an operating system must be "deterministic and have guaranteed worst-case interrupt latency and context-switch times."[2]

PLCs frequently use commercial RTOS implementations such as VxWorks, Windows CE, or QNX. They may also use custom "in-house" operating systems. Although uncommon, some manufacturers have starting using Linux-based operating systems on PLCs.

[2] http://www.netrino.com/Embedded-Systems/How-To/RTOS-Selection/

3. INDUSTRY OVERVIEW

PLCs and SCADA systems are used in a large number of industries, where they provide oversight and control of automated functions. Those industries include the following:

- Automotive
- Building (facility) Automation
- Cement and Glass
- Chemical, Electronics and Electrical
- Electric Power
- Food and Beverage
- Machinery
- Mining and Metals
- Oil and Gas
- Pharmaceutical and Biotech
- Pulp and Paper
- Refining
- Semiconductors
- Water and Wastewater. (3)

This paper is intended to be industry-agnostic; however, some sections may focus more heavily on the electric power and the oil and gas industries, reflecting areas in which the authors have the most experience.

4. PLC MARKET OVERVIEW

In 2007, the most recent year for which complete data are available, the global PLC market was approximately $8.9 billion. Siemens (31.3% market share) and Rockwell Automation (22.1%) are the dominant vendors in this market, with a combined market share of more than 50%. Other large vendors are Mitsubishi Electric (12.7%), Schneider Electric (8.0%), Omron (6.1%), B&R Industrial Automation (3.6%), GE Fanuc (3.5%), and ABB (2.1%). Assorted smaller vendors make up the remaining 10.6% of the market. (4) Figure 3 gives the breakdown.

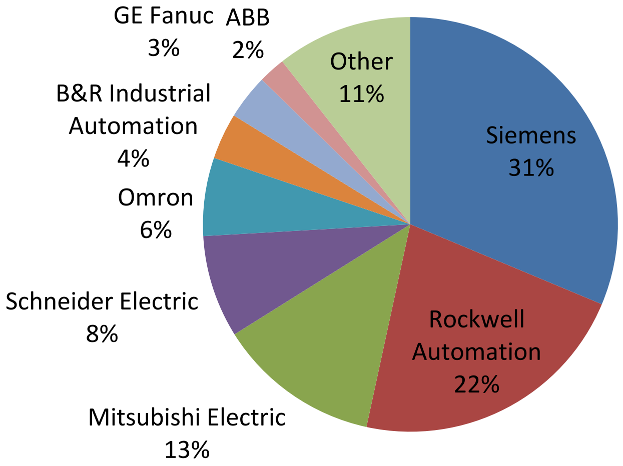


Figure 3. Chart showing 2007 PLC vendor share in the global market. (4)

Vendor market shares in different geographic regions vary considerably. For example, Siemens's industry division (including automation and SCADA systems) had more than half its 2009 revenues from European countries, while Rockwell Automation derived about half its sales from the United States alone.(5) (6)

Market share for vendors can vary considerably by industry as well as region. Figure 4 shows market share in the North American electric utilities market. In this market, Schneider Electric is the leading PLC vendor, with 45% market share, followed by Rockwell Automation (29%), Cutler Hammer (9%), and others (17%). (7)

Market share data are provided to show an overall view of the industry leaders. In the following overview of vendors, we consider only total revenue. This consideration reflects the fact that we are not concerned with profit margins but rather with the number of actual units being purchased and used.

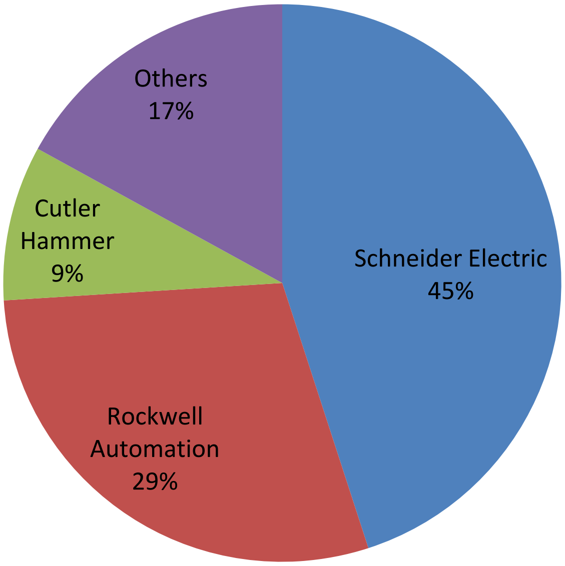


Figure 4. North American electric utilities PLC market share. (7)

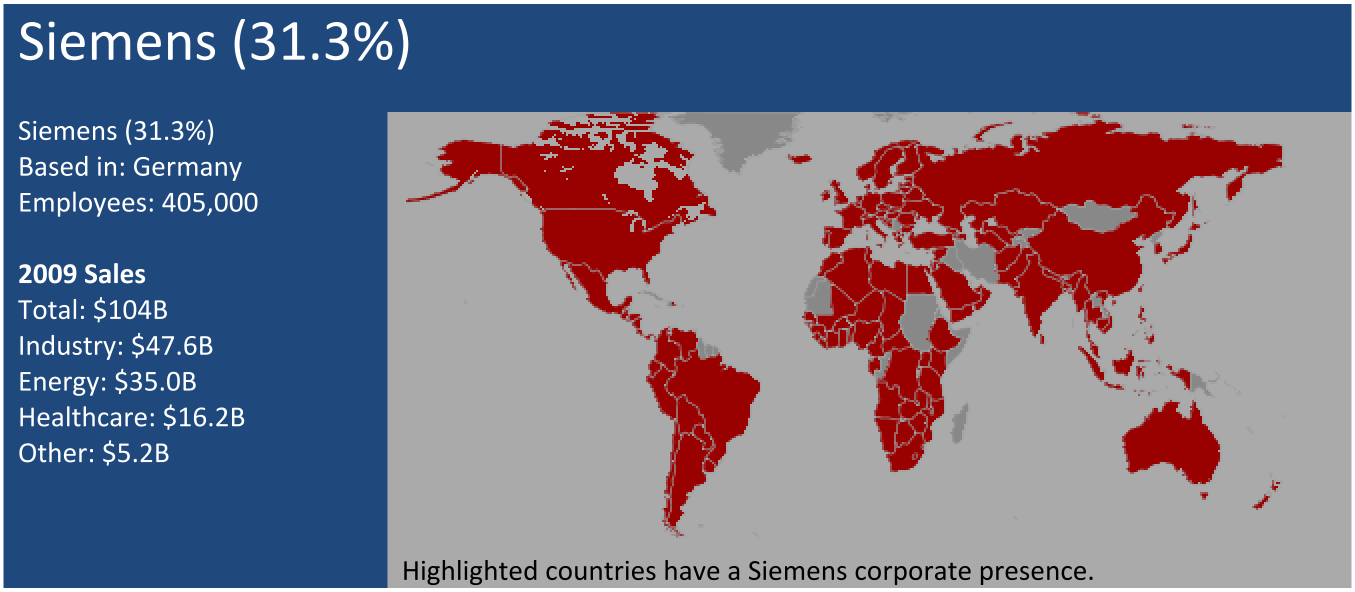
The following subsections present summaries of the primary vendors. Full surveys of these vendors—including information about products, revenue, workforce size, and industry sectors—are provided in Appendix B.

4.1 Siemens

Siemens is based in Germany and employs 405,000 people worldwide. Siemens is the leading vendor in the PLC market (4) and is among the larger vendors in the energy sector. Its operations largely focus on the European market, but it has a strong presence worldwide. (6) Siemens produces devices for three market sectors: industry, energy, and health care.

Siemens's 2009 revenues totaled $104 billion.[3] Of that, Siemens's industry sector accounted for $47.6 billion, its energy sector for $35.0 billion, its healthcare sector $16.2 billion, and other business areas accounted for $5.2 billion.(6) One of Siemens's industry sector's business areas is PLC production.

[3] Siemens provides sales figures in Euros. US dollar values shown were calculated with a 1.3575 US dollar per Euro exchange rate.



Siemens (31.3%)

Siemens (31.3%)
Based in: Germany
Employees: 405,000

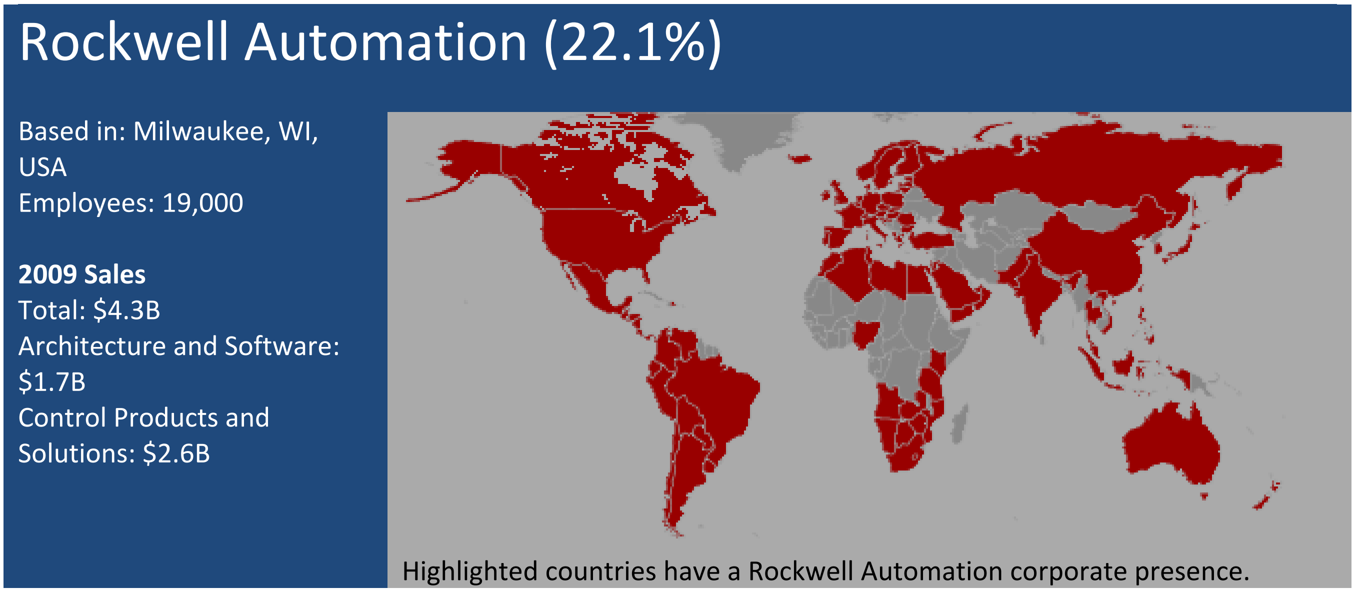
2009 Sales
Total: $104B
Industry: $47.6B
Energy: $35.0B
Healthcare: $16.2B
Other: $5.2B

Highlighted countries have a Siemens corporate presence.

Figure 5. Summary of Siemens 2009 corporate data.

4.2 Rockwell Automation

Rockwell Automation is based in Milwaukee, WI and employs 19,000 people worldwide. It sells control system components under the Allen-Bradley brand. Allen-Bradley products are represented in nearly every industry, although they are especially prevalent in manufacturing, building automation, (8)(9) and electrical utilities (2). The company is actively increasing its market penetration in the oil and gas industries. (5) Rockwell's 2009 revenues totaled $4.3 billion. (5)



Rockwell Automation (22.1%)

Based in: Milwaukee, WI, USA
Employees: 19,000

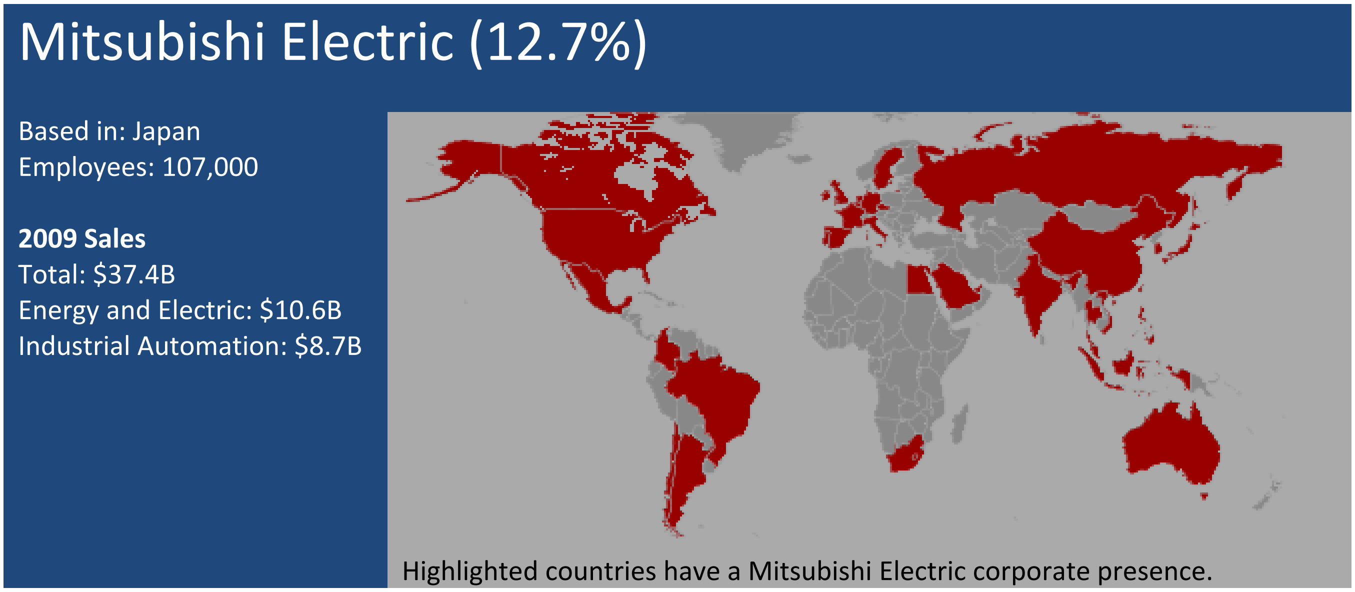
2009 Sales
Total: $4.3B
Architecture and Software: $1.7B
Control Products and Solutions: $2.6B

Highlighted countries have a Rockwell Automation corporate presence.

Figure 6. Summary of Rockwell Automation 2009 corporate data.

4.3 Mitsubishi Electric

Mitsubishi Electric Corporation is a Japan-based company that employs 107,000 people worldwide and manufactures electric and electronic equipment used in energy and electric systems, industrial automation, information and communication systems, electronic devices, and home appliances. (10) Mitsubishi Electric's 2009 revenues totaled $37.4 billion. Of particular interest are its energy and electric division ($10.6 billion in sales) and its industrial automation division ($8.7 billion in sales). (11)



Mitsubishi Electric (12.7%)

Based in: Japan
Employees: 107,000

2009 Sales
Total: $37.4B
Energy and Electric: $10.6B
Industrial Automation: $8.7B

Highlighted countries have a Mitsubishi Electric corporate presence.

Figure 7. Summary of Mitsubishi Electric 2009 corporate data.

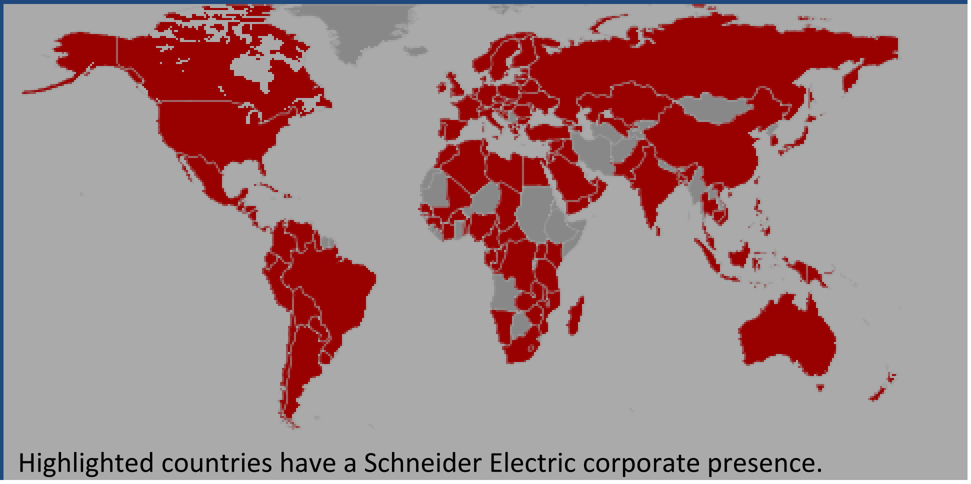
4.4 Schneider Electric

Schneider Electric is based in France and employs nearly 105,000 people worldwide. Schneider specializes in energy management, with operations in more than 100 countries. Schneider equipment is used in energy and infrastructure, industry, buildings, data centers and networks, and residential applications. (12) Schneider Electric's 2009 revenues totaled $21.4 billion. Its automation and control business accounted for $5.8 billion in sales, and its electrical distribution business accounted for $12.5 billion. (12)

Schneider Electric (8.0%)

Based in: France
Employees: 104,853

2009 Sales
Total: $21.4B
Electrical Distribution: $12.5B
Automation & Control: $5.8B
Critical Power & Cooling Systems: $3.2B



Highlighted countries have a Schneider Electric corporate presence.

Figure 8. Summary of Schneider Electric 2009 corporate data.

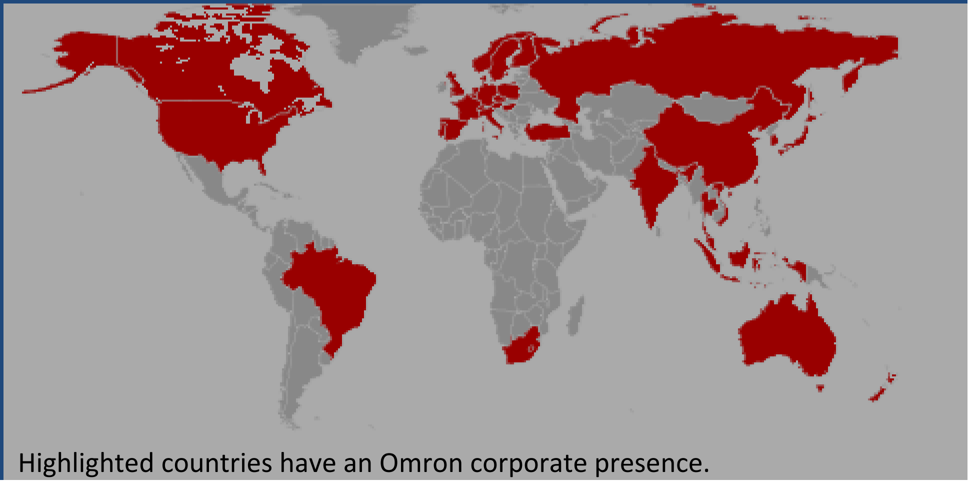
4.5 Omron

Omron is based in Japan and employs 32,500 people worldwide. The company primarily focuses on the manufacture and sale of automation systems, although it also produces medical equipment. More than half of Omron's sales are in Japan. Of the total, 70% are in Asia. Omron's 2008 revenues totaled $6.7 billion, with its industrial automation division accounting for $2.8 billion. (13)

Omron (6.1%)

Based in: Japan
Employees: 32,583

2008 Sales[4]
Total: $6.7B
Industrial Automation: $2.8B
Electronic Components: $1.3B
Automotive Electronic Components: $0.9B
Social Systems: $0.9B
Healthcare: $0.67B



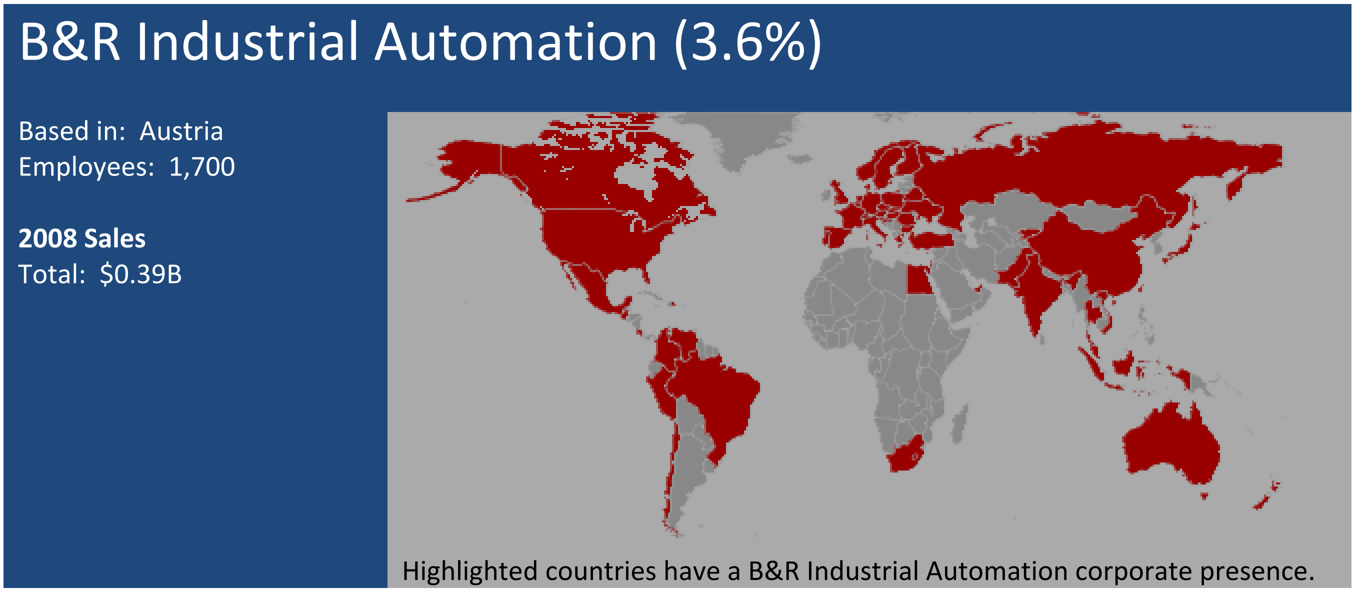
Highlighted countries have an Omron corporate presence.

Figure 9. Summary of Omron 2008 corporate data.

[4] Amounts converted from Japanese yen at a rate of 1 yen = 0.010629 US Dollars

4.6 B&R Industrial Automation

B&R Industrial Automation is a small company based in Eggelsberg, Austria. It employs 1700 people. It is one of the largest privately owned companies in the area of automation and process control. B&R's product range includes control, motion, operator interface, communication, and software products (14) Because B&R is privately owned, detailed sales figures are difficult to obtain.



B&R Industrial Automation (3.6%)

Based in: Austria
Employees: 1,700

2008 Sales
Total: $0.39B

Highlighted countries have a B&R Industrial Automation corporate presence.

Figure 10. Summary of available B&R Industrial Automation corporate data. Because B&R is a privately owned corporation, comparatively little data are available.

4.7 General Electric

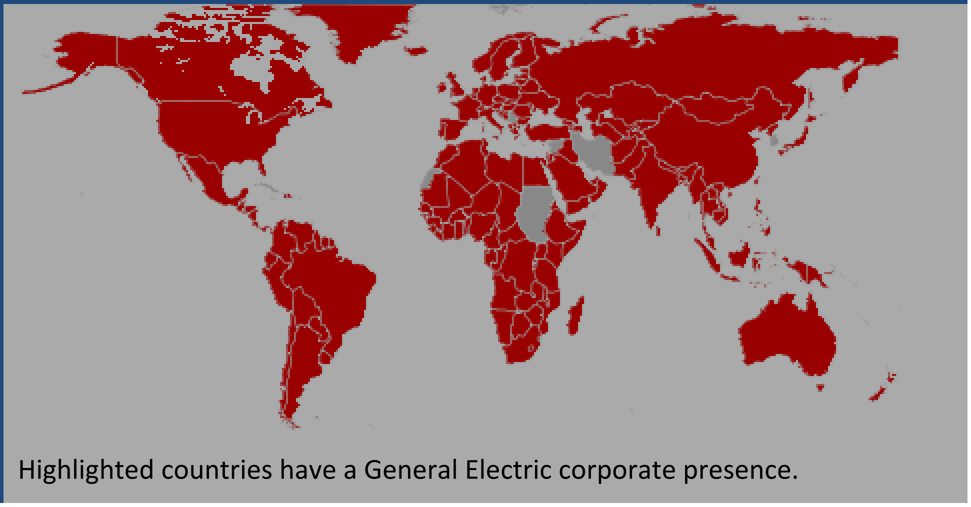
General Electric (GE) is a large, US-based company that employs 323,000 people worldwide. GE has a strong presence in energy and technology infrastructure. GE's Intelligent Platforms division sells PLCs, HMIs, and other process control devices for several sectors, including energy, technology, consumer, and industrial.

GE-FANUC Automation Corporation was a joint venture between FANUC Robotics America, Inc. and GE. However, in August 2009 the companies dissolved the joint venture. (15)

General Electric (3.5%)

Based in: United States
Employees: 323000

2008 Sales:
Total: $182B
Energy Infrastructure: $38.6B
Technology Infrastructure: $46.3B
Consumer & Industrial: $11.8B
Other: $8.4B



Highlighted countries have a General Electric corporate presence.

Figure 11. Summary of General Electric 2008 corporate data.

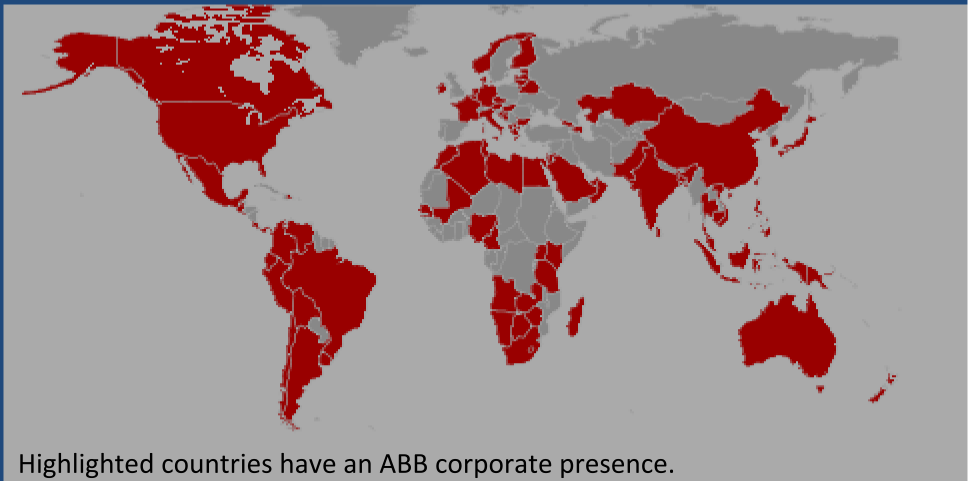
4.8 The ABB Group

ABB is based in Switzerland and employs 120,000 people. Its products are used for the automation of power systems, products and processes, robotics and manufacturing. The company develops automation technologies for use in the utility and industrial sectors. ABB's 2009 revenues totaled $34.9B, with its automation products division accounting for $10.3 billion and its process automation division accounting for $7.8 billion.

ABB (2.1%)

Based in: Switzerland
Employees: 120,000

2009 Sales
Total: $34.9B
Power Products: $11.9B
Power Systems: $6.9B
Automation Products: $10.3B
Process Automation: $7.8B
Robotics: $1.6B



Highlighted countries have an ABB corporate presence.

Figure 12. Summary of ABB 2009 corporate data.

5. CONTROL SYSTEM COMMUNICATIONS PROTOCOLS

The communications protocols used in control systems vary widely among industry sectors, the geographic regions where the systems are deployed, and the vendors who produce the systems.

5.2 Electric Sector

5.2.1 IEC 60870-5

IEC 60870-5 is likely the most popular electric substation automation protocol used internationally. In the United States, it is functionally equivalent to DNP3, which uses parts of IEC 60870-5 to provide the foundation for the data link layer. (16) Numerous companion standards have been developed, including the following:

- IEC 60870-5-101—Transmission protocols for power system monitoring, control, and associated communications for telecontrol, teleprotection, and associated telecommunications,
- IEC 60870-5-103—Transmission protocols enabling interoperability between protection equipment and devices of a control system in a substation, and
- IEC 60870-5-104—Extension of IEC 60870-5-101 with changes in transport, network, link, and physical layer services to suite interfacing with TCP/IP and other transports (ISDN, X.25 frame relay, etc.). (16)

Typical communication media include Ethernet and serial. Typical ports are 2404/UDP and 2404/TCP.

5.2.2 Distributed Network Protocol 3.0 (DNP3)

DNP3 is widely used in North America in place of IEC 60870-5. (16) It was developed in the early 1990s as a serial-line protocol, but UDP/IP and TCP/IP variants now also exist. Many similarities exist between DNP3 and IEC 60870-5, as several members of the IEC 60870-5 development committee split off early during the development effort to create what would become DNP3. As a result, the data link layers of both DNP3 and IEC 60870-5 are very similar, but the upper layers of the protocols have fewer commonalities.

The major industry adopter for DNP3 is the North American electric sector, but the protocol has also seen penetration into the water and wastewater industries. In 2008, more than half the North American electric utilities surveyed by Newton-Evans Research Company were using the UDP/IP or TCP/IP variant of DNP3. (7)

Development of security extensions for DNP3 is under way. These extensions are expected to provide link encryption and key management services. (8)

Typical communication media include Ethernet and serial connections. DNP3 typically uses ports 20000/UDP, 20000/TCP, 19999/UDP, and 19999/TCP.

5.2.3 FOUNDATION Fieldbus

FOUNDATION Fieldbus is a dominant fieldbus in several process industries. (3) It is primarily used in process/factory automation, but has been deployed in a variety of settings, including power plant/generator control and semiconductor manufacturing. (16)(8)

Typical communication media for FOUNDATION Fieldbus include twisted pair and fiber optic. Typical ports include 1089/UDP, 1089/TCP, 1090/UDP, 1090/TCP, 1091/UDP, and 1091/TCP.

A public list of FOUNDATION Fieldbus-enabled installations is provided on the Fieldbus Foundation website. The Fieldbus Foundation's membership includes over 350 leading control and instrumentation suppliers and end users.

5.2.4 Inter-Control Center Communications Protocol (ICCP)

ICCP (IEC 60870-6/TASE.2) is used for communications between control centers, primarily in the electric sector. In the United States, ICCP networks are frequently used to tie together groups of utility companies—typically a regional system operator with transmission utilities, distribution utilities, and generators. Regional operators may also be connected together to coordinate import and export of power between regions across major interties.(16)(8)

ICCP typically uses port 102/TCP.

5.2.5 Modbus

Given its simplicity, availability of free specification download, and royalty-free deployment, Modbus is likely the single most popular control protocol across all sectors.(8)

Intelligent devices like PLCs and relays often use Modbus variants to communicate with simpler devices like RTUs. Aside from the Modbus standard, Modbus+ is the most widespread proprietary variant.(8)(16)

A list of Modbus members (corporations and developers that are part of the Modbus developers group) is available at the Modbus website (17). This list includes domestic and international members along with a brief description of the products each member manufactures. A list of Modbus suppliers is also available (18), as is a list of Modbus devices (19) and a list of companies that supply Modbus integration services.(20)

Numerous Modbus variants exist. Modbus RTU, an open standard, allows for binary encoding over a serial connection. Modbus ASCII, also an open standard, supports ASCII encoding over a serial connection. Modbus/TCP, an open standard, encapsulates Modbus RTU payloads inside a TCP packet and places some limitations on function codes. Modbus/UDP varies by vendor, but is most commonly Modbus/TCP run over UDP. Modbus+ is an extended, high-speed (1Mbps) version that uses a token passing technique for media access control. Modbus+ is proprietary to Modicon. Enron (or Daniels) Modbus are standard Modbus protocols with vendor extensions that treat 32-bit values as one register rather than two. JBus is Modbus with minor addressing changes.(16)(8)

Typical communications media include Ethernet and serial (RS485 two-wire is very common). Modbus typically runs on port 502/TCP.

5.3 Oil and Gas Sector

The oil and gas sector does not have an immediately apparent dominant protocol. (8) The industry uses a mix of protocols such as DNP3, IEC 60870-5, and Modbus. These protocols were discussed in more depth in Section 5.2. Fieldbuses, such as FOUNDATION Fieldbus, are found in many oil and gas installations.(8)

Communications in the oil and gas sector are frequently over radio. RTUs and sensors provide flow and pressure data to PLCs, which run protection systems as well as tasks such as oil well control.(16)

5.3.1 DNP3 and IEC 60870-5

Discussions of DNP3 and IEC 60870-5 are provided in Section 5.2 Electric Sector. A list of oil and gas companies, both domestic and foreign, using DNP3 and IEC 60870-5 is given at the Triangle Microworks, Inc. site, where a white paper on the protocols can be found.(16) (21)

Typical communication media include Ethernet and serial connections. DNP3 typically uses ports 20000/UDP, 20000/TCP, 19999/UDP, and 19999/TCP, and IEC 60870-5 typically uses 2404/UDP and 2404/TCP.

5.3.2 Modbus

As noted in the description of Modbus in Section 5.2, Modbus is a popular control protocol in the oil and gas sector. FOUNDATION Fieldbus is particularly popular in the petrochemical industry.

Typical communications media include Ethernet and serial (RS485 two-wire is very common). Modbus typically runs on port 502/TCP.

5.4 Water Sector

5.4.1 DNP3

As noted in the description of DNP3 in Section 5.2, this protocol is also popular in the water sector.

Typical communication media include Ethernet and serial connections. DNP3 typically uses ports 20000/UDP, 20000/TCP, 19999/UDP, and 19999/TCP.

5.4.2 Modbus

As noted in the description of Modbus in the Electric Sector section, above, Modbus is a popular control protocol in the water sector.

Typical communications media include Ethernet and serial. Modbus typically runs on port 502/TCP.

5.1 Building Automation Sector

In the building automation sector, LonWorks (also LonTalk or ANSI/CEA 709.1B) is the dominant protocol, followed by DyNet and a number of residential/consumer protocols. (16) (8)

Typical communication media include powerline carrier, twisted pair/Ethernet, fiber optic, and RF. Common ports include 2540/UDP, 2540/TCP, 2541/UDP, and 2541/TCP.

5.1.1 LonWorks (or LonTalk, or ANSI/CEA 709.1-B)

LonWorks is a networking platform based on a protocol created by Echelon Corporation. The platform is widely used in many industries, including semiconductor manufacturing, lighting control systems, energy management systems, HVAC systems, security systems, home automation, consumer appliance controls, public street lighting/monitoring/control, and petroleum station control. A typical use of LonWorks is a thermostat that communicates via LonTalk to a PLC or PC that is coordinating a building's HVAC system.(16)(8)

ISO and IEC have granted the LonWorks platform compatibility standard numbers ISO/IEC 14908-1, -2, -3, and -4 (ANSI/CEA-852). LonWorks also forms the basis for IEEE 1473-L (locomotive networking), as well as several other application-specific platforms. China has ratified LonWorks as a national controls standard (GB/Z 20177.1-2006) and as a building and intelligent community standard (GB/T 20299.4-2006). The European Committee of Domestic Equipment Manufacturers has adopted LonWorks as part of its Household Appliances Control and Monitoring–Application Interworking Specification standards.(8)

5.1.2 DyNet

Typical communication media include RS-485 serial, RS-232 serial, Ethernet, and infrared.

DyNet is a proprietary protocol developed by Dynalite (now owned by Philips Electronics). DyNet devices include their own programmable controllers, and communicate in a peer-to-peer model.

5.1.3 Residential / consumer protocols

Numerous protocols are used for home automation systems. The most popular include INSTEON, X10, ZigBee, X-Wave, and KNX/Konnex.(8)

5.5 Process Automation (Manufacturing) Sector

Dominant protocols in the process automation sector are Fieldbus variants (PROFINET, FOUNDATION Fieldbus) and Common Industrial Protocol (CIP) derivatives. IEC 61158 and IEC 61784 contain profiles for each major Fieldbus variant.(16)

5.5.1 DF1

DF1 is a serial communications protocol defined in ANSI X3.28, subparagraphs D1 and F1. The protocol, originally developed by Allen-Bradley (now owned by Rockwell Automation), is often used as the mechanism to deliver programmable controller communications commands (PCCCs) to Allen-Bradley PLCs.(16)

5.5.2 FOUNDATION Fieldbus

FOUNDATION Fieldbus is suited for applications using basic and advanced regulatory control and for much of the discrete control associated with those functions. There are two implementations of FOUNDATION Fieldbus running at different speeds and over different physical media: H1, the most common implementation, generally connects field devices and runs at 31.25Kbps; HSE (high-speed Ethernet) connects hosts, I/O subsystems, gateways, and field devices, and runs at 100 Mbps. (16) FOUNDATION Fieldbus is included as a Fieldbus in IEC 61804.(16)

5.2.3 Profibus – Process Field Bus

Profibus was developed by BMBF, the German department of education and research. It has two variations. The more popular variation, Decentralized Peripherals (DP), is used for sensor/actuator operation via a centralized controller. The other variation, Process Automation (PA), monitors measuring equipment via a PCS. PA is designed for use in explosive and hazardous areas and uses a physical layer that conforms to IEC 61158-2. PA uses the same protocol as DP but runs at 31.25Kpbs. A coupler can be used to interface a DP network to a PA network, with the DP being used as a backbone.(16) Profibus is included as a Fieldbus in IEC 61158 and IEC 61784.(16)

5.2.4 PROFINET IO

The PROFINET concept features two perspectives—PROFINET CBA and PROFINET IO—both of which can communicate at the same time on the same bus system. They can be operated separately or combined so that a PROFINET IO subsystem can appear as a PROFINET CBA system from another perspective. PROFINET IO was developed for real-time (RT) and isochronous real-time (IRT) communication with the decentral periphery. RT has a 10 ms cycle time. IRT drives systems with cycle times of 1 ms or less. PROFINET CBA is suitable for component-based communication via TCP/IP and the real-time communication for real-time requirements in modular systems engineering. Both communication options can be used in parallel. PROFINET CBA has a reaction time in the range of 100 ms.(16)

PROFINET is included as a Fieldbus in IEC 61158 and IEC 61784.(16)

5.2.5 CC-Link

CC-Link was originally developed by Mitsubishi and has seen large adoption as a fieldbus by Japanese vendors.(16) There are more than 6 million CC-Link devices deployed, and more than 1000 different devices exist. (16) With CC-Link Industrial Ethernet, CC-Link can be integrated with typical IT networks.(16)

There are four CC-Link formats:

- CC-Link
- CC-Link LT (lightweight version for lower device communication)
- CC-Link Safety (high reliability, compliant w/IEC 61508 SIL3 and ISO13849-1 Cat 4)
- CC-Link IE (Industrial Ethernet).

Typical CC-Link communication media include twisted pair and fiber optic. The CC-Link Partner Association provides a list of domestic and international partners.(22)

5.2.6 Common Industrial Protocol (CIP)

Common Industrial Protocol (CIP) provides a unified communications architecture throughout the manufacturing sector. It can be seen as a common application layer to EtherNet/IP, DeviceNet, CompoNet, and ControlNet. CIP encompasses a comprehensive suite of messages and services for the collection of manufacturing automation applications—control, safety, synchronization, motion, configuration, and information. The protocol is managed by Open DeviceNet Vendors Association (ODVA).(16)

5.2.7 ControlNet

ControlNet is an implementation of CIP originally developed by Allen-Bradley. ControlNet has a built-in ability to support fully redundant link cables, and all communication is strictly scheduled and highly deterministic.(16)

The ControlNet physical layer is either RG-6 coaxial using BNC connectors or optical fiber. ControlNet uses Manchester encoding, and the bus speed is 5 Mbps. The link layer operates in cycles known as network update times (NUTs), with each NUT having two phases, the first of which is reserved for scheduled traffic transmission to guarantee a transmission opportunity, and the second of which is for unscheduled traffic transmission without any guarantee. The maximum frame size is 510 bytes.(16)

5.2.8 DeviceNet

DeviceNet is an implementation of CIP originally developed by Allen-Bradley. DeviceNet is layered on top of the Controller Area Network (CAN) physical layer and adapts ControlNet technology. It is low-cost and robust compared to traditional RS-485 based protocols.(16)

DeviceNet operates at baud rates of 125 Kbps, 250 Kbps, and 500 Kbps. Trunk length is inversely proportional to the speed of the bus—i.e., 500, 250, and 125 meters, respectively. The majority of installations use a master/slave configuration, but peer-to-peer is possible. Multiple masters can exist on a single logical network. DeviceNet is engineered to withstand noisy environments.(16)

5.2.9 EtherNet/IP

EtherNet/IP is an implementation of CIP originally developed by Rockwell Automation. The protocol's application layer is CIP. EtherNet/IP is an application layer protocol built on the standard TCP/IP stack that considers all devices on the network as a series of "objects." It makes use of existing Ethernet infrastructure (regardless of speed). An entire EtherNet/IP stack can be implemented in software on a microprocessor without the need for ASICs or field-programmable gate arrays (FPGAs). EtherNet/IP makes use of 44818/TCP for explicit messaging and 2222/UDP for implicit messaging.(16)

5.2.10 EtherCAT – Ethernet for Control Automation Technology

EtherCAT is an Ethernet-level protocol with Ethertype 0x88A4, with IP routing possible by insertion of frames into UDP datagrams. Rather than processing one frame per node per cycle (update time), EtherCAT uses "processing on the fly." Rather than an Ethernet frame being received, then interpreted and copied as process data at every node, EtherCAT slave devices read the data addressed to them while the datagram passes through the device. Similarly, input data are inserted while the datagram passes through. Many nodes can be addressed with one frame.(16)

Gateways are available to integrate EtherCAT networks with CANopen, DeviceNet, PROFIBUS, and other protocols. The EtherCAT Technology Group is the international user and vendor organization; it consists of over 1100 companies from 47 countries as of August 2009.(16) EtherCAT is included as a fieldbus in IEC 61158 and IEC 61784.(16)

EtherCAT uses ports 34980/UDP and 34980/TCP to route between Ethernet LANs.

5.2.11 EGD – Ethernet Global Data

Ethernet Global Data (EGD) is a mechanism that enables one CPU to share a portion of its internal reference memory with one or more other CPUs at a regularly scheduled periodic rate. EGD is used by some GE Fanuc PLCs.(16)

5.2.12 FINS

FINS is a protocol developed by Omron (a Japanese controls company) for use in many of its newer PLCs. It typically runs on IP-enabled systems using port 9600/UDP.(16)

5.2.13 Host Link

Host Link is a protocol developed by Omron for its older PLC line; however, many new Omron PLCs can still communicate using HostLink. It is an ASCII-based, RS-232 protocol.(16)

5.2.14 SERCOS Interface – Serial Real-Time Communication System

SERCOS has hard real-time requirements and is particularly useful in motion controls, e.g., metal cutting and forming, assembly machinery, packaging, robotics, printing, and materials handling. The protocol is governed by SERCOS International.[5] The current version is SERCOS-III. SERCOS is defined in IEC 61158 and IEC 61784.(16)

5.2.15 SRTP – Service Request Transfer Protocol

SRTP is a protocol used to communicate commands and data to/from PLCs from PCs. It is used by GE Fanuc PLCs as an application layer.

5.2.16 Sinec H1

Sinec H1 is a transport layer developed by Siemens. Different application layers may run on top of it. Its large bandwidth makes it ideal for large data volume transmission.(16)

[5] http://www.sercos.com/

6. PLC COMPONENT ANALYSIS

As part of this research project, the authors disassembled several PLCs to identify their constituent components. We identified some useful characteristics, such as the fact that all but one of the PLCs examined use ARM chips.

6.1 Methodology

We disassembled each PLC, noting all chip markings and photographing internal components. For each major component, we located, identified, characterized, and mapped the components found on each board. In some cases, our characterization of a component was based on an understanding of how the device is used in the field. We also identified buses and chip interconnect methods. We include chip markings for chips that could not be identified.

6.1.1 Supply Chain Analysis

To determine which countries were involved with the production of each PLC, we used chip markings, labels, and manufacturer information. This information is applicable to supply chain analysis.

6.1.2 Next-Step Analysis

This initial analysis of PLC devices will feed into the next step of this research project. We will choose a representative device and perform an in-depth analysis on both the hardware and software components.

Performing this next-step analysis requires significant capabilities in hardware and software reverse engineering. Because many of these devices use multiple processor architectures simultaneously (e.g., both ARM and PowerPC processors on a single board), a deep and wide-ranging understanding of processor architectures and embedded system design is necessary.

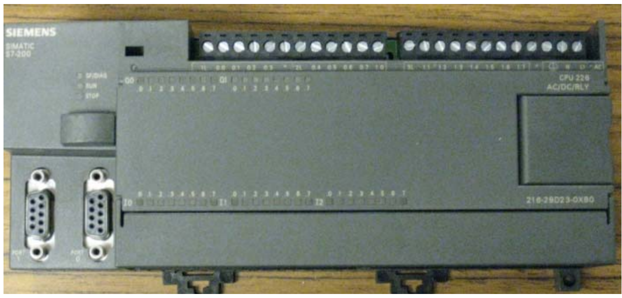
This analysis will greatly increase our understanding of PLC security in both the hardware and software areas. Such an understanding is vital for discerning the potential national security impact of security flaws in these devices, as well as for developing proactive countermeasures.

6.2 Siemens Simatic S7-200

The Siemens Simatic S7-200 is a modular PLC. The modules appear to be connected in series using small ribbon connectors. External markings indicate the device was made in Germany. The PLC consists of a main module, an Ethernet module, and an analog I/O module.

6.2.1 Main Module

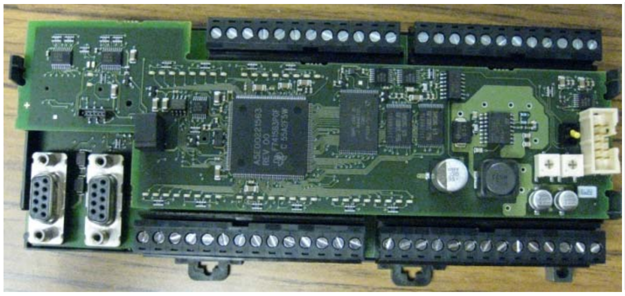
The module has two serial ports, several I/O ports, and a ribbon connector on one side for connecting external modules in series (Figure 13). Internally there are three boards, which appear to be for processing, I/O, and power.



```
External markings
6ES7 216-2BD23-0XB0
CPU 226
85-264VAC SUPPLY
SC-T7R22513
DI 24X24VDC 15-30V
DO 16 x RLY 30VDC/250VAC 2A
E-Stand:03
```

Figure 13. Siemens S7-200 CPU, CPU226 main module (left) and external markings (right).

On the processing board (Figure 14.) there are several Samsung memory chips, an AMD chip (flash memory), and a Texas Instruments processor.



```
TI processor markings
A5E00221563
REV 00
F741583PGF
C 55A2F5W
```

Figure 14. Siemens S7-200 Processing Board (left) and TI processor markings (right).

There are no processing or memory chips on the I/O board or the power supply (Figure 15.).

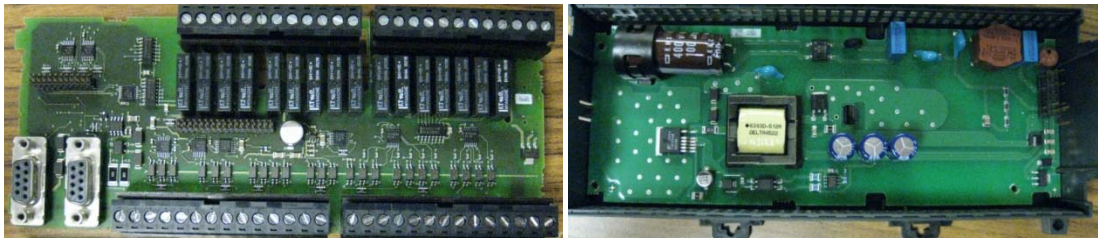


Figure 15. Siemens S7-200 I/O board (left) and power supply (right).

The module also contains an expansion module port (Figure 16.).

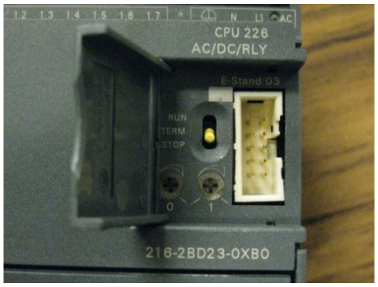
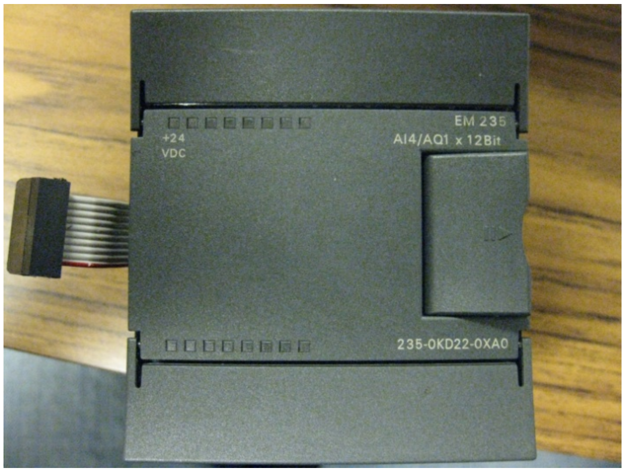


Figure 16. Siemens S7-200 expansion module port.

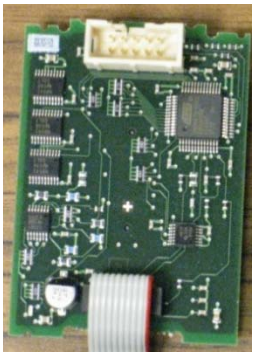
6.2.2 Analog I/O Module

The analog I/O module has a main board with I/O ports and an expansion board. The main board has three Maxim chips. The expansion board has an Atmel chip. Figure 17 shows the module in its closed state. Figure 18 shows the module's expansion board. Figure 19 shows the module's main board.



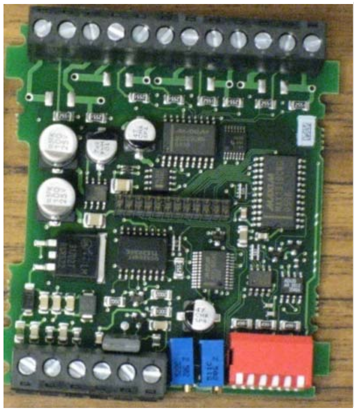
External markings
EM 235
A14/AQ1 x 12 Bit
235-0KD22-0XA0

Figure 17. Siemens S7-200 analog I/O module (left) and external markings (right).



Atmel chip markings
2808470-5001
82000778
4J4987
0522   PH

Figure 18. Siemens S7-200 I/O module expansion board (left) and chip markings (right).



Maxim chip markings

MAX191BCWG / 0508

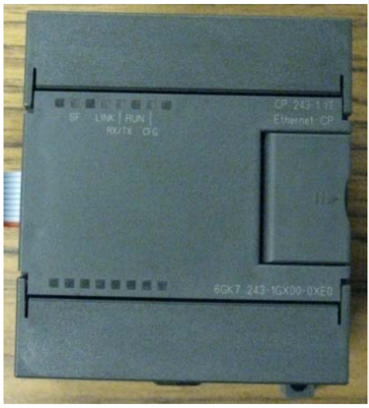
DG529CWN / 0439

MAX530BCAG / 0502

Figure 19. Siemens S7-200 I/O module main board (left) and chip markings (right).

6.2.3 Ethernet Module

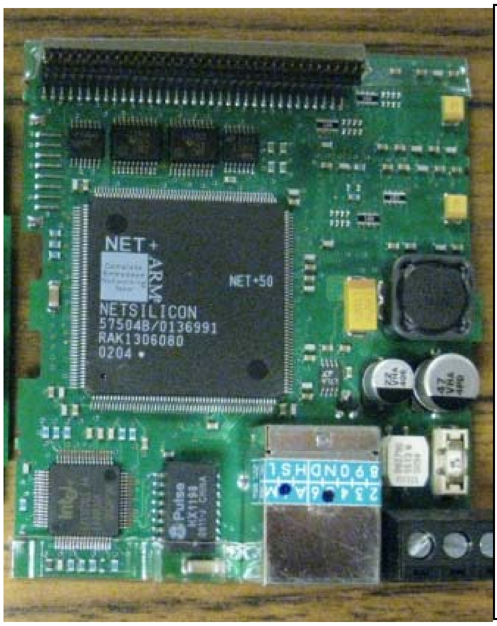
This module has external ports for Ethernet and power. The processing board has a Net+ARM 50, a 32-bit, 44MHz ARM7TDMI processor with Ethernet and 8kB of on-chip cache. Figure 20 shows the external module.



External markings
CP243-1 IT
6GK7 243-1GX00-0XE0

Figure 20. Siemens S7-200 Ethernet module exterior (left) and external markings (right).

Figure 21 shows the module's main board. Figure 22 shows the expansion board and chip markings.

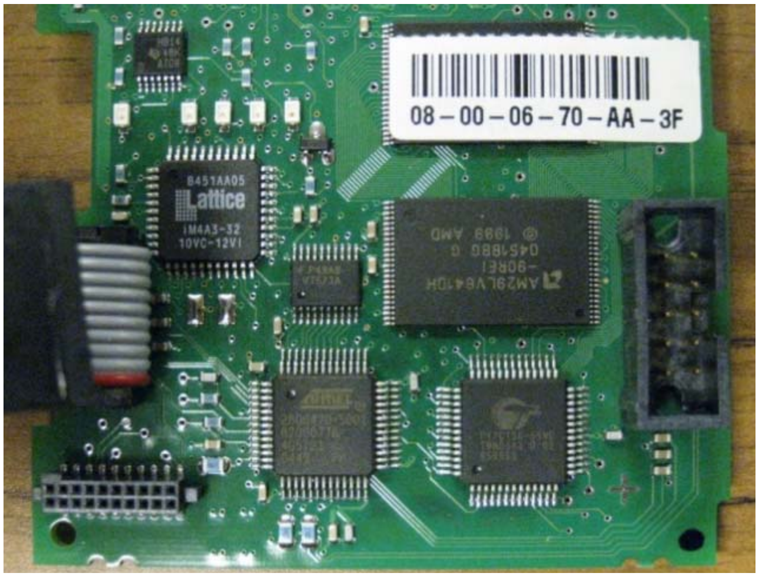


NET+ ARM chip markings
57504B/0136991
RAK1306080
0204

Intel chip markings
LXT971ALE A4
L448KA01

PULSE chip markings
HX1198
0511-J

Figure 21. Siemens S7-200 Ethernet module main board (left) and chip markings (right).



AMD chip markings
AM29LV6410H
-90REI
0451BBG G
1999 AMD

ATMEL chip markings
2808470-5001
82000778
4G5121
0449   PH

Lattice chip markings
B451AA05
LATTICE
iM4A3 - 32
10VC-12VI

Cypress chip markings
CY7C136-55NC
TWND443 G 02
656599

Figure 22. Siemens S7-200 Ethernet module expansion board (left) and chip markings (right).

6.3 Honeywell Experion C200 Process Controller

The Honeywell Experion C200 Process Controller is a modular PLC. It consists of a case, a separate power supply module, a control processor module, a network module, and several I/O modules. It is worth noting that this unit is essentially a rebranded Allen-Bradley PLC. Honeywell does not build its own PLCs and so is not ranked in our list of PLC vendors. The controller is shown in Figure 23.

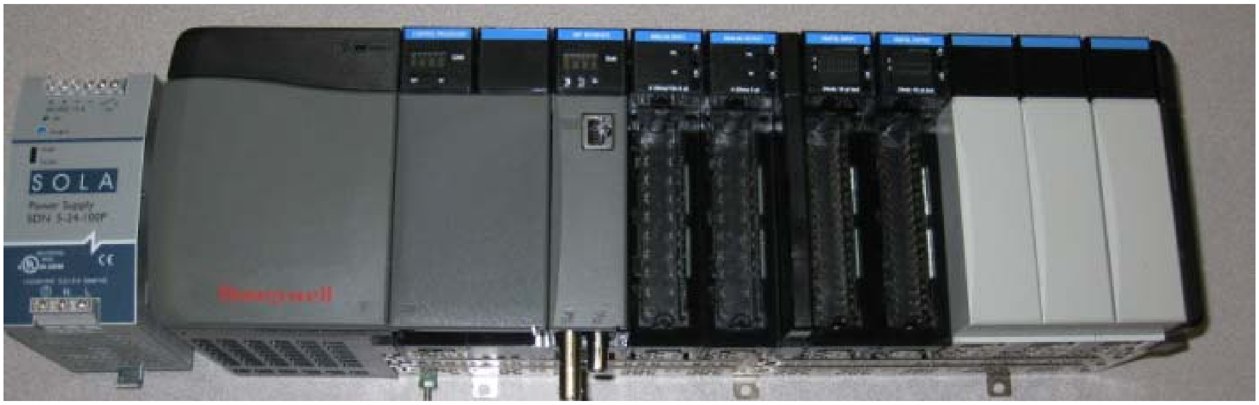
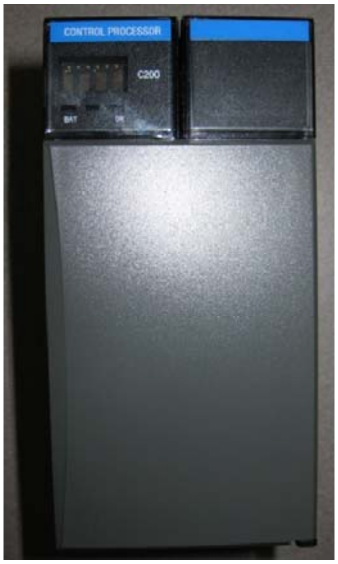


Figure 23. Honeywell Experion C200 Process Controller.

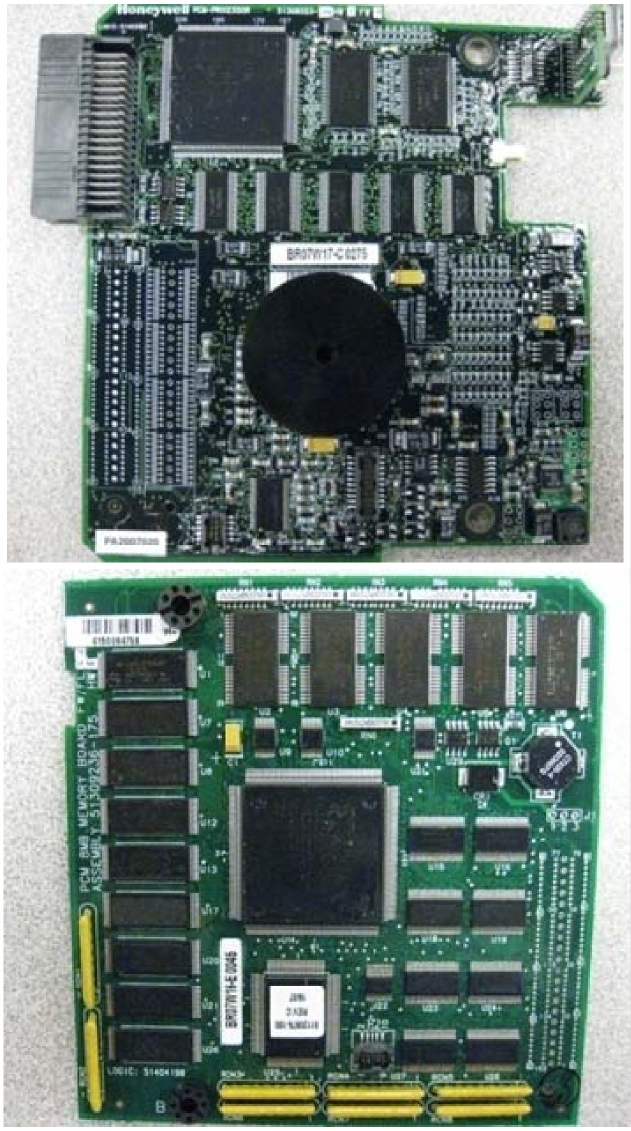
6.3.1 Control Processor C200 Rev J

The control processor module for the C200 Controller is shown in Figure 24. Figure 25 shows the control module's main and expansion boards. The subsections below describe the module's components.



External markings
Honeywell Control Processor C200
MODEL NO: TK-PRS021
REV: J
PART NO: 51404305-375

Figure 24. Honeywell Experion C200 control processor module.



Flash chip markings
AMD AM29F040B

FPGA chip markings
Xilinx XC4013E

SRAM chip markings
C106
0123 T88
HM5118165LTT6

Bus chips markings
TI 68CH5NK 64
LVTH162245

Lattice chip markings
Lattice
iM4A5-128/64
10YC-12YI
M707RR16

Backplane communication processor markings
Philips ARM
VY21422E
CSM2TRC09255
stG0647E
MIDRANGE P3E
943631-64

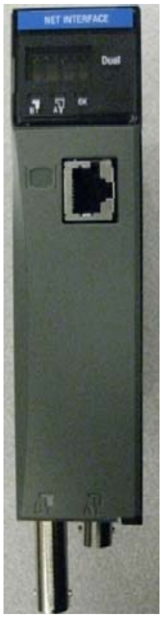
Main processor markings
MPC603R
RX200LC
30K20S
QCG0639H

Figure 25. Honeywell Experion C200 process control module main board (top left), process control module expansion board (bottom left), and chip markings (right).

6.3.2 Redundant Net Interface TC-CCR014, Model Rev. C01

The redundant network interface module (Figure 26) has one Ethernet and two BNC coaxial ports. Internally, it contains a single board with several microcontrollers, an FPGA, flash memory, and RAM. Near the backplane interface is an Atmel AT56 microcontroller. The AT56 is a customer-specific cell-based ASIC. This part went through quality assurance in Rousset, France and was manufactured in Korea.[6]

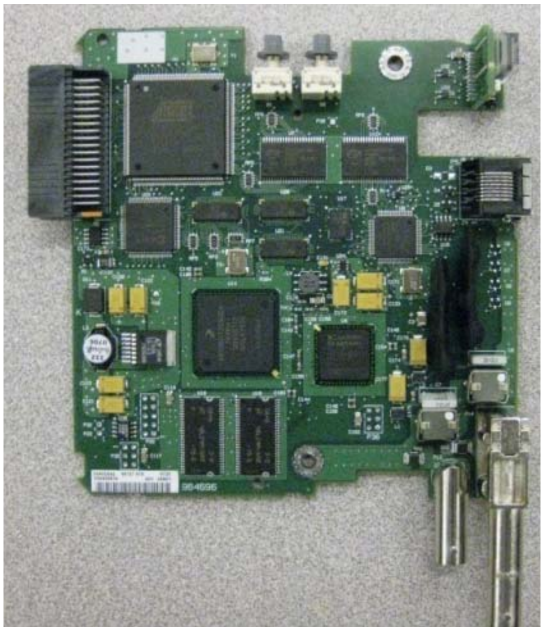
[6] http://www.atmel.com/quality/quality_locations.asp



External markings
Honeywell
REDUNDANT NET INTERFACE
NET INTERFACE-DUAL/RED.FW
MODEL: TC-CC4014
MODEL REV.: C01
PART NO.: 97321174 A01

Figure 26. Honeywell Experion C200 network interface module (left) and external markings (right).

The board also includes a Xilinx Spartan XC2S200, an FPGA with 200,000 reconfigurable gates. This part was manufactured in Taiwan. Located near the memory on the main board (Figure 27) is a Freescale Semiconductor MPC855T. This processor is a member of the MPC860 family and implements the Power architecture. This chip was manufactured in Malaysia. Near the Ethernet port there is an AMI 0642YMH chip, as well as a Broadcom chip.



Backplane communication processor markings
ami
0642ymh
smac4
s943407-73
19406-002

Cypress chip markings
Cypress SRAM
PHI
CY7C1041BN-15ZXI

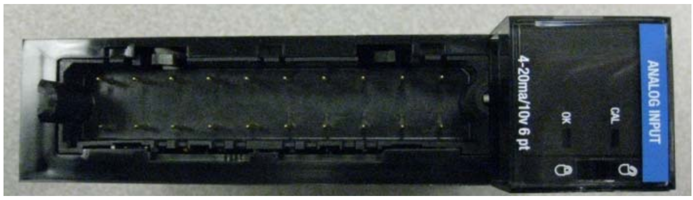
Micron chip markings
Micron SDRAM
48LC4M16A2

Flash Chip markings
MX Flash ROM

Figure 27. Honeywell Experion C200 network interface module mainboard (left) and chip markings (right).

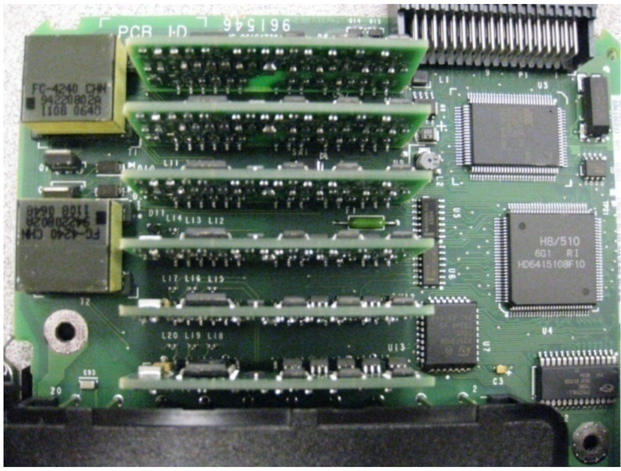
6.3.3 Analog Input Module TC-IAH061, REV K01, FW Rev 1.9

The analog input module supports currents of 4-20 mA at 10V. There is a single Atmel "CORELESS 2.4" microcontroller on board, as well as a Hitachi H8/510 microcontroller. Figure 28 shows the module. Figure 29 shows the internal board.



External markings
Honeywell
ANALOG INPUT
ANALOG INPUT 10V & 4-20Ma
MODEL: TC-IAH061
MODEL REV.: K01
PART NO.: 96978079 B01

Figure 28. Honeywell Experion C200 analog input module exterior (left) and markings (right).



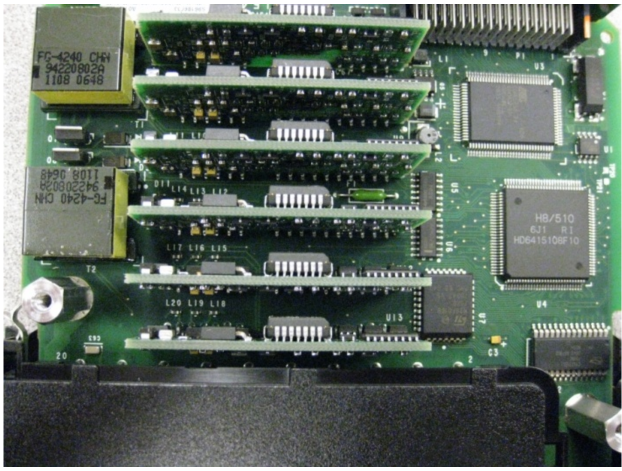
Microcontroller markings
H8/510
6G1 RI
HD6415108F10

Backplane communication processor markings
CORELESS 2.4
S943627-63
ROCKWELL
0635 5H0194

Figure 29. Honeywell Experion C200 analog input module internal board (left) and microcontroller markings (right).

6.3.4 Analog Output Module TC-OAH061, REV J01, FW Rev 1.9

The analog output module (Figure 30) supports 4-20 mA current. There is a single Atmel microcontroller on board.



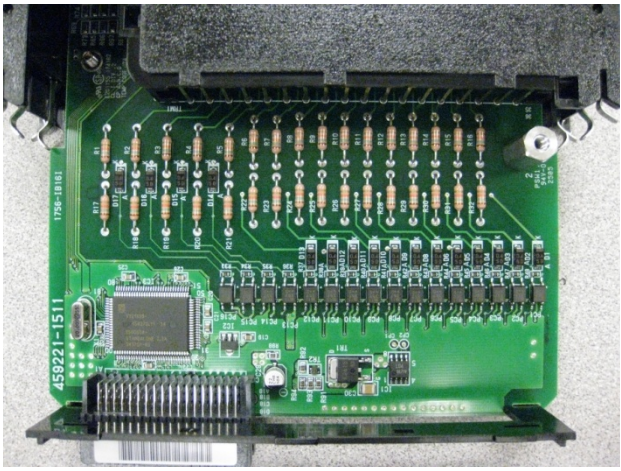
External markings
TC-OAH061
REV J01
Part #96978279 A01
Serial #00421BA8
FW Rev 1.9

Backplane communication processor markings
CORELESS 2.4
S943627-63
ROCKWELL
0635 5H0194

Figure 30. Honeywell Experion C200 analog output module internal board (left) and markings (right).

6.3.5 Digital Input Module, Model TC-IDJ161, Rev M01, FW Rev 2.1

The digital input module is shown in Figure 31. Markings on the case indicate that it can tolerate 10-30 VDC at 10 mA and/or 24 VDC isolated power.



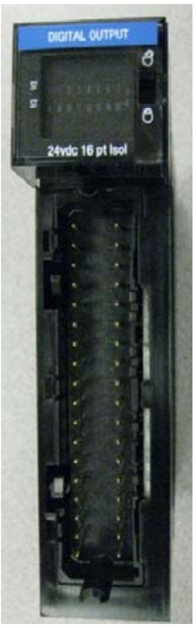
External Markings
Honeywell
MODEL: TC-IDJ161
MODEL REV. M01
PART NO. 97242671 A01
F/W REV. 2.1

Backplane communication processor markings
VY21699-
Y54270.Y1 14
KSG0504-
STANDALONE 2.2A
943701-65

Figure 31. Honeywell Experion C200 digital input module (left) and markings (right).

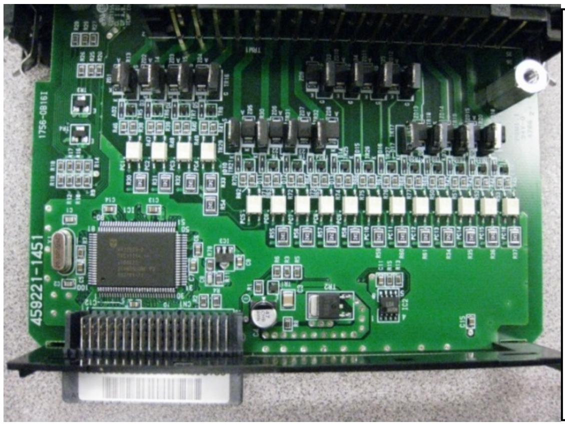
6.3.6 Digital Output Module, TC-ODJ161, Rev N01, FW Rev 3.2

The digital output module is shown in Figure 32. There is one unidentified AMI microprocessor, shown in Figure 33, in the digital output module.



External markings
Honeywell
DC OUTPUT 24VDC ISOLATED
2A Pilot Duty (DC-13/SQ)
MODEL: TC-ODJ161
MODEL REV. N01
PART NO. 97242771 A01
F/W REV. 3.2

Figure 32. Honeywell Experion C200 digital output module (left) and markings (right).



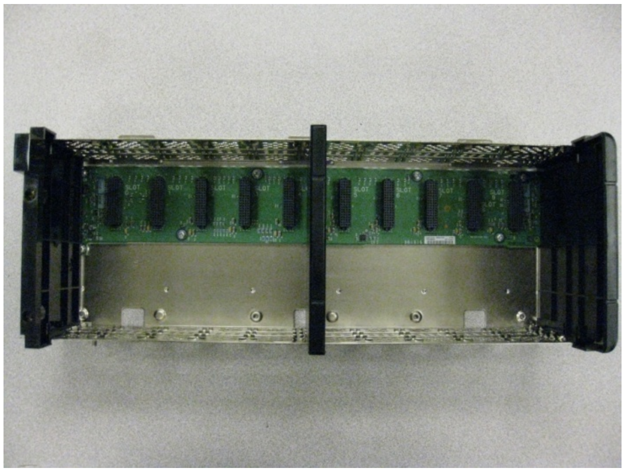
AMI backplane communication processor markings
VY22553-2
TRC11114
--stG0621-
STANDALONE P3
943701-71

Figure 33. Honeywell Experion C200 digital output module main board (left) and markings (right).

6.3.7 Ten-slot Rack, TC-FXX102, Rev K01

The ten-slot rack, shown in Figure 34, is what the other modules plug into. It is a simple steel cage and a backplane with no obvious chips or other circuitry. It supports up to 10 modules and a power supply. The power supply module used in this PLC is a SOLA Power Supply SDN 5-24-100P. It converts 110/220VAC to 24VDC/5A.

Each module plugs into a 18×4 pin connector on the backplane.

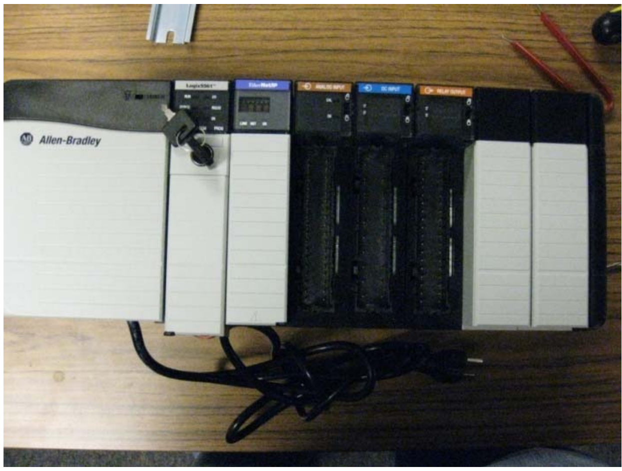


External markings
Honeywell
RACK 10 SLOT
MODEL: TC-FXX102
MODEL REV.: K01
PART NO.: 97126575
MADE IN U.S.A.

Figure 34. Honeywell Experion C200 ten-slot rack (left) and external markings (right).

6.4 Allen-Bradley Logix 5561

The Allen-Bradley Logix 5561 is a modular PLC. The Allen-Bradley unit shown in Figure 35 has a 7-slot rack and backplane piece, a power supply, a control module, an EtherNet/IP module, and some I/O modules. External markings indicate it was made in the United States.



Chassis markings
Allen-Bradley
CHASSIS 7 SLOT
CATALOG/SERIES: 1756-A7 B
CATALOG REV.: L01
PART NO.: 96345677
MADE IN USA

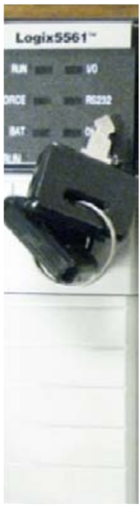
Power supply markings
Allen-Bradley
POWER SUPPLY AC
CATALOG/SERIES: 1756-PA75/B
CATALOG REV.: B01
PART NO. 96426272 A01
MADE IN USA

Figure 35. Allen-Bradley Logix 5561 chassis (left) and markings (right).

The main board on this PLC (Figure 36) has one ARM backplane communication and one other ARM processor.

6.4.1 Control Module

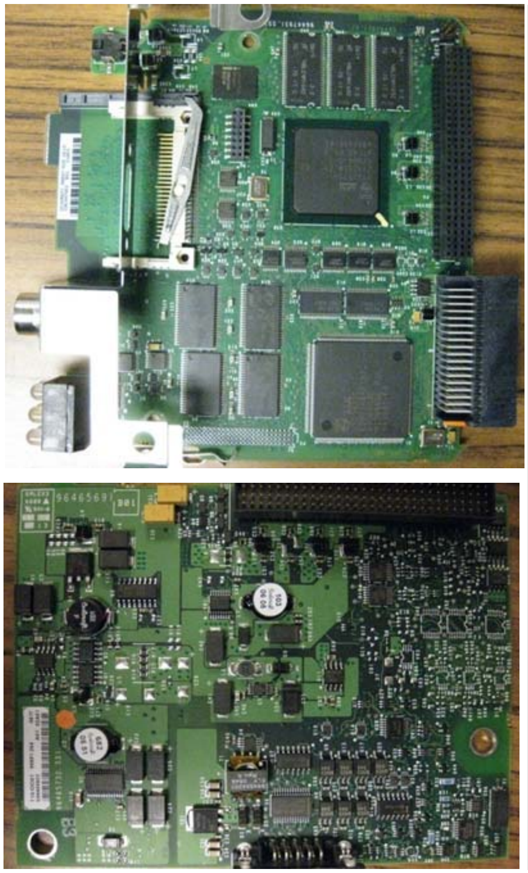
The control module (Figure 36) has an RS-232 port, a band of light-emitting diodes (LEDs), space for a flash card, and a key switch on the outside. Internally there are two Phillips ARM processors, as well as several memory chips made by Cypress, Micron Tech, and Samsung.



External markings
Allen-Bradley
LOGIX 5561 PROCESSOR
LOGIX PAC™
CATALOG/SERIES: 1756-L61 B
CAT.REV.: F01
PART NO.: 96479676 A01
F/W REV.: 1.9
SERIAL NO.: 0038BEFC
MADE IN U.S.A.

Figure 36. Allen-Bradley Logix 5561 control module (left) and external markings (right).

A close-up of the 5561 board is shown in Figure 37.



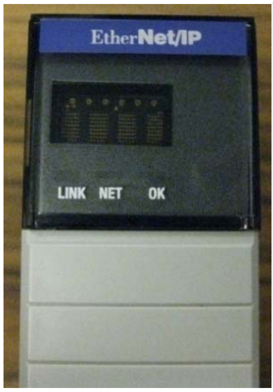
Main processor Markings
Philips ARM
VY22575-
ZYA26SW.71   02
TFN0610-Y
ATLAS R1.2
S944446-62

Backplane communication processor markings
Philips ARM
VY21422E
CSM2TRB48107
STG0604E
MIDRANGE P3E
943631-64

Figure 37. Allen-Bradley Logix 5561 main board (top left), expansion board (bottom left), and chip markings (right).

6.4.2 EtherNet/IP Module

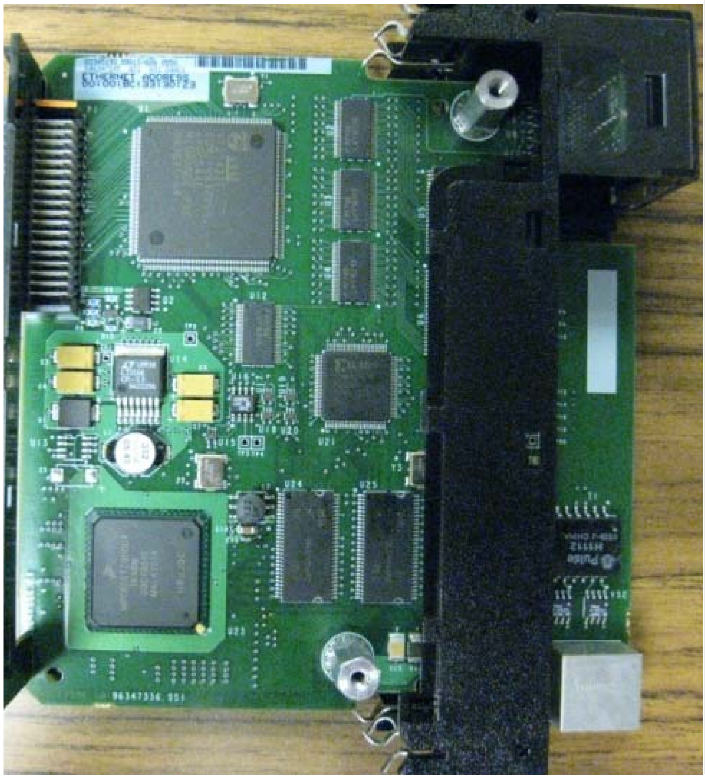
The processor on the EtherNet/IP module is PowerPC in this Allen-Bradley PLC (as well as in the Honeywell C200 Experion) but the PLCs use different processor models. They do, however, use the same ARM backplane communication processor. The EtherNet/IP module and its main processor markings are shown in Figure 38.



External markings
Allen-Bradley
Ethernet/IP 10/100 Mb/s
COMMUNICATIONS BRIDGE
CATALOG/SERIES: 1756-ENBT A
CATALOG REV.: P01
PART NO.: 96486474 A01
F/W REV.: 3.9
MADE IN USA

Figure 38. Allen-Bradley Logix 5561 EtherNet/IP module (left) and external markings (right).

The EtherNet/IP module's main board and chip markings are shown in Figure 39.



Main processor markings
VY21422E
CSM2TRB37059
stG0544E
MIDRANGE P3E
943631-64

Xilinx CLPD markings
XC9572XL
TQ100AWN0541
F1381115A
71

Freescale PowerPC markings
MPC855TZQ50D4
1K48M
QQGY0545
MALAYSIA
HRJJQC

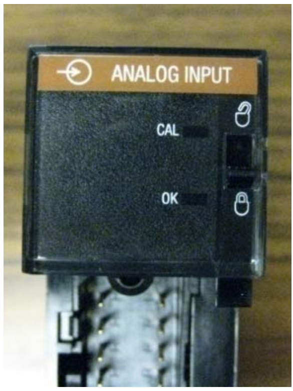
Broadcom chip markings
BCM5201KPT
CT0425B1 P
6531

PULSE chip markings
H1112
0539-J

Figure 39. Allen-Bradley Logix 5561 EtherNet/IP main board (left) and chip markings (right).

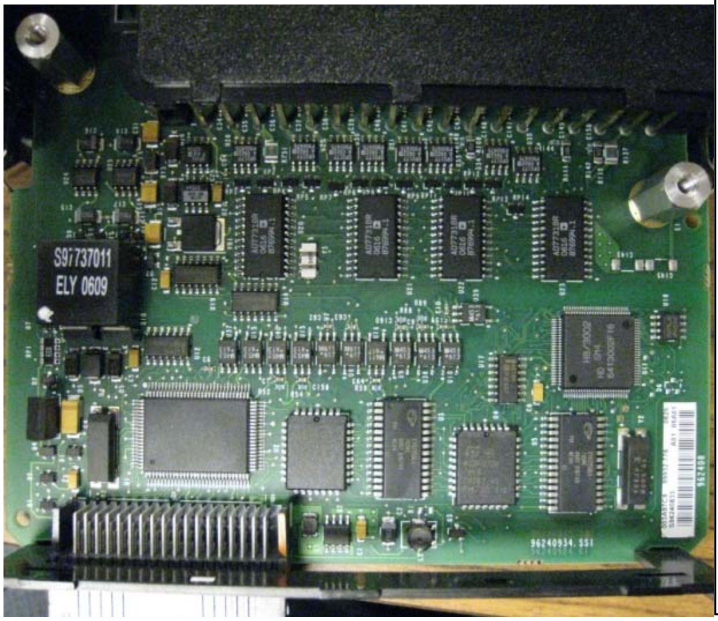
6.4.3 Analog Input Module

This module has a single board with several analog inputs, and quite a few chips on it. Figure 40 shows the module and external markings. Figure 41 shows the module board and its markings.



External markings
Allen-Bradley
ANALOG INPUT
10V & 4-20Ma 16 POINT INPUT
CATALOG/SERIES: 1756-IF16 A
CATALOG REV.: N01
PART NO.: 96240878 A01
F/W REV.: 1.5
MADE IN USA

Figure 40. Allen-Bradley Logix 5561 analog input module (left) and external markings (right).



Atmel Chip Markings
ATEMEL   AD0
CORELESS 2.4
S943627-63
ROCKWELL
0609 A05820

Memory Chip markings
ST
M29F010B
70K6
7B262 V5
PHL 88 618

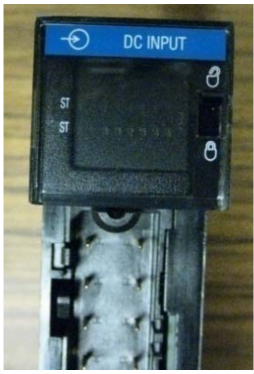
Static RAM Chip Markings
CY62256LL-
70SNC
0607 616749
PHI NE04

Hitachi Microcontroller Markings
H8 / 3002
HD 5M4
6413002F16

Figure 41. Allen-Bradley Logix 5561 analog input module board (left) and chip markings (right).

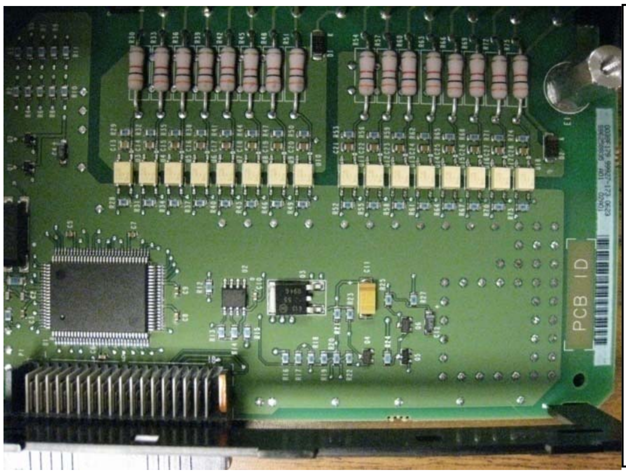
6.4.4 DC Input Module

The DC input module, shown in Figure 42, has a single medium-sized chip on the board. Figure 43 provides an internal view of the module.



External markings
Allen-Bradley
DC INPUT 16PT 24VDC
10-31.2VDC 10mA
CATALOG/SERIES: 1756-IB16/A
CATALOG REV.: H01
PART NO.: 96258876 A01
F/W REV.: 3.2
MADE IN USA

Figure 42. Allen-Bradley Logix 5561 DC input module (left) and external markings (right).



Chip markings
AMI
0550LZM
STANDALONE 3
S943701-71T
19405-001

Figure 43. Allen-Bradley Logix 5561 DC input module internals (left) and chip markings (right).

6.4.5 Relay Output Module

The relay output module and its external markings are shown in Figure 44. There are no processing or memory chips on the relay output module.

External Markings
Allen-Bradley
RELAY ISOL. OUTPUT 16PT. N.O.
AC C300/DC R150 PILOT DUTY
CATALOG/SERIES: 1756-0W16I/A
CATALOG REV.: L02
PART NO.: 96197677 A01
F/W Rev: 2.1
MADE IN MALAYSIA

Figure 44. Allen-Bradley Logix 5561 relay output module (left) and external markings (right).

Figure 45 shows the module's internal board.

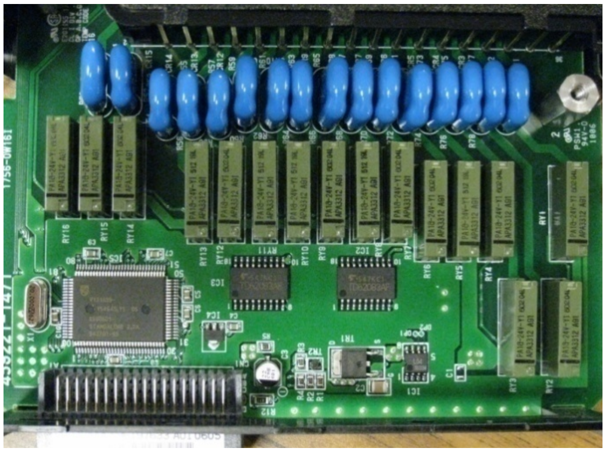
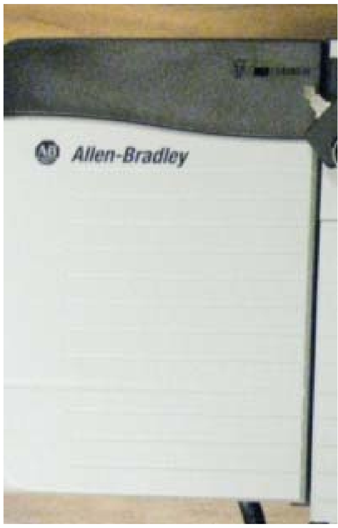


Figure 45. Allen-Bradley Logix 5561 Relay Output Module internal board.

6.4.6 Power Supply Module

The power supply module and markings are shown in Figure 46.



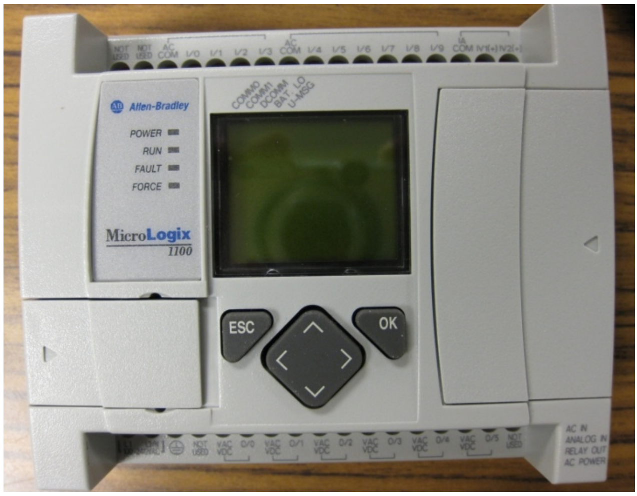
External markings
POWER SUPPLY AC
CAT / SERIES / REV
1756-PA75 / B / B01
Part No: 96426272 A01

Figure 46. Allen-Bradley Logix 5561 power supply module (left) and markings (right).

6.5 Allen-Bradley MicroLogix 1100

The Allen-Bradley MicroLogix 1100 is an all-in-one (i.e., not modular) PLC. The unit includes several analog inputs and outputs, an EtherNet/IP port, and an RS-232/485 port.

The PLC (shown in Figure 47) includes four boards: (1) processing and networking, (2) LCD display assembly, (3) analog input, and (4) power.

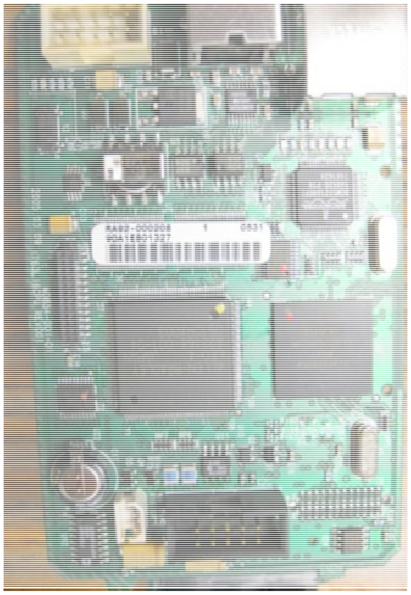


External Markings
Allen-Bradley
MicroLogix™ 1100
CAT.: 1763-L16AWA
SER.: A
REV.: A
OPERATING SYSTEM
INFORMATION: FRN1
MADE IN KOREA

Figure 47. Allen-Bradley MicroLogix 1110 exterior (left) and external markings (right).

6.5.1 Processing and Network Board

The main board of this PLC, shown in Figure 48, contains both the main processor and the communications processors. The board has two external ports (EtherNet/IP and RS-232/485).



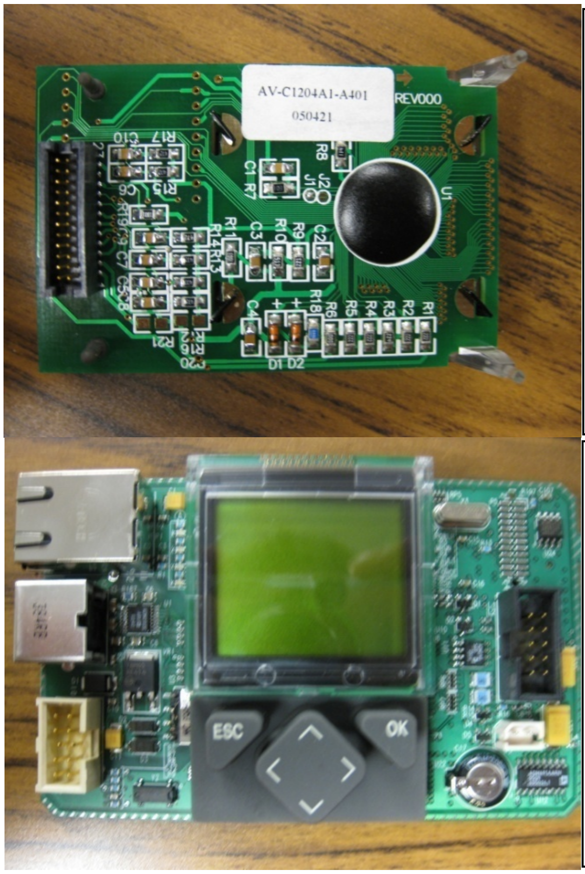
Board Markings
RA92-000208 1 0531
9DA1E801327
2005.03.09
1763L16CPU REV001
Chip Markings
ALLEN BRADLEY
LEO-4 JAPAN
A23168-001-04
0512PX003
Chip Markings
MOTOROLA
COLDFIRE
MCF5282CVF66
L95M
PSQAP0347C
T

Ethernet Transceiver Chip Markings
BROADCOM
BCM5221A4KPT
TA0520 P14
744162A
CMOS Static RAM Markings
SAMSUNG 504
K6X8016C3B-TF55
TLTH03CA

Figure 48. Allen-Bradley MicroLogix 1100 main board (left) and chip markings (right).

6.5.2 LCD Display Assembly

The display assembly has an LCD display and buttons (ESC, OK, and a four-directional button). There were no chips on the board.

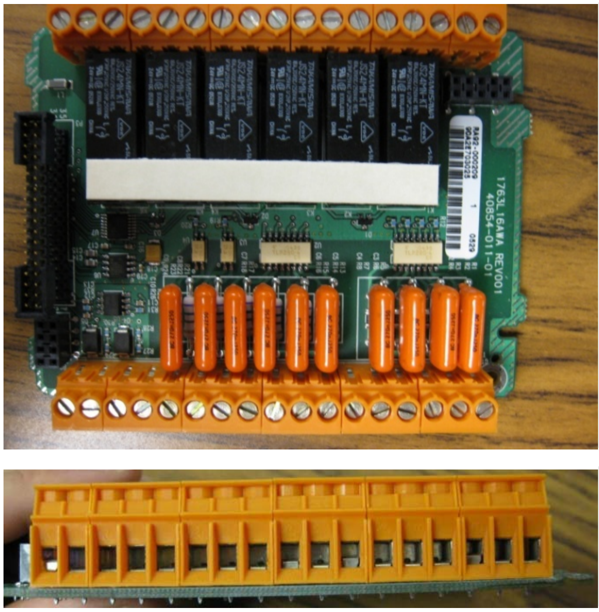


Board Markings
AV-C1204A1-A401
50421

Figure 49. Allen-Bradley MicroLogix 1100 LCD assembly (left) and board markings (right).

6.5.3 Analog I/O Board

The analog I/O board has all the input and output connectors. The board is shown in Figure 50. There are no processing or memory chips on the analog I/O board.

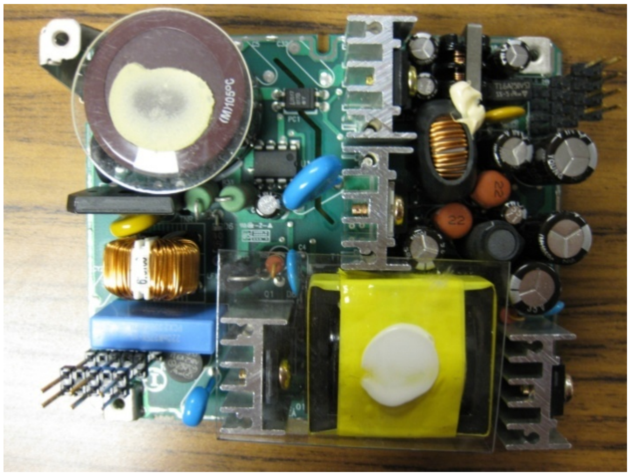


Board markings
1763L16AWA   REV001
40854-011-01
RA92-000209   1   0529
9DA2E703025

Figure 50. Allen-Bradley MicroLogix 1100 I/O board (left) and board markings (right).

6.5.4 Power Board

The power board consists of large capacitors, a transformer, and voltage regulators. The power board (shown in Figure 51) has no processing or memory chips.



Board Markings
ML1100 (AC-DC)
DONGYANG INSTRUMENT IND
CO, LTD
MODEL NO: 40854_050_01
REV 1.0 (05.04.01)

Figure 51. Allen-Bradley MicroLogix 1100 power board (left) and board markings (right).

7. SUMMARY

During the course of this project, the authors looked at the major vendors for PLCs, identified the communications protocols used in control systems in several industries, and disassembled and analyzed a number of PLCs.

The top PLC vendors in the global market are Siemens (31% market share), Rockwell Automation (22%), and Mitsubishi Electric (13%). It is worth noting that PLC market share varies significantly by country and industry; for example, in the North American electrical utilities market, the top vendors are Schneider Electric (45% market share), Rockwell Automation (29%), and Cutler Hammer (9%). Figure 52 shows these market share figures.

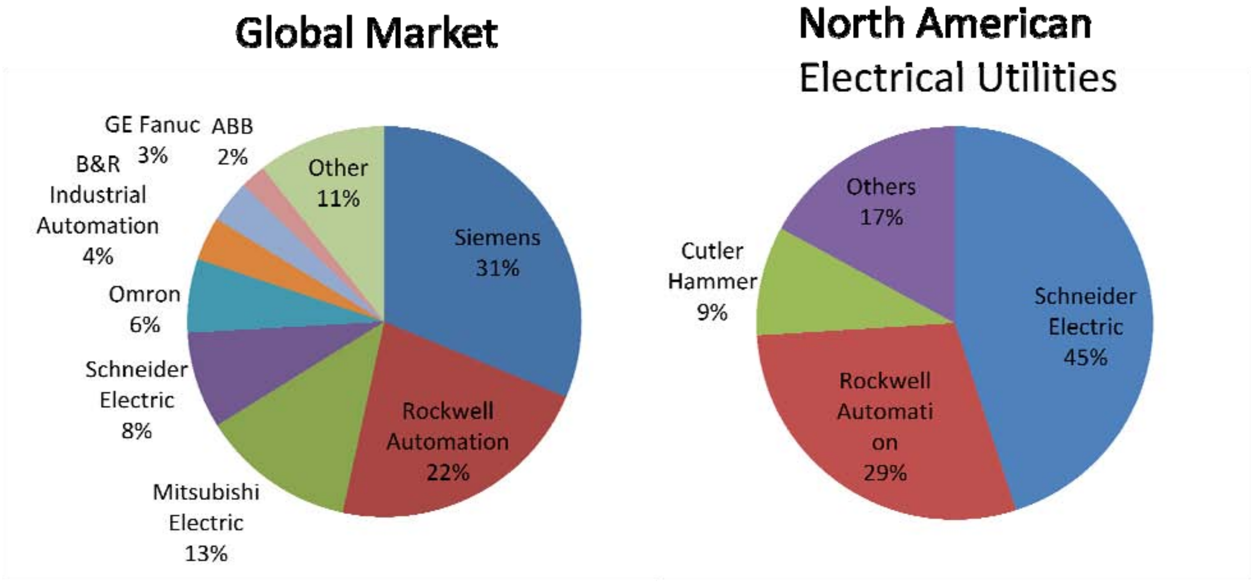


Figure 52. Market share for PLC vendors in the global market (left) and North American electrical utilities market (right).

The authors hypothesized that PLCs would be highly dependent on commodity components, with very few specialized parts. Our device teardowns and analysis confirmed that hypothesis. The devices used production chips from large manufacturers; only a few of the chips seemed to be variants produced for a particular vendor. The devices also use typical configurations of flash and RAM that are present in other embedded systems. PLCs typically use fairly simple (two- to four-layer) boards, whereas normal PC boards are often seven layers. Despite this simplicity, the interconnections used in PLCs can be difficult to understand because board layout is driven by efficiency.

Our findings in this project revealed that the most common processor architectures for these systems are ARM, PowerPC, and Motorola 68k. However, we note that it is common to have multiple processor architectures on a single board. Figure 53 shows an example of how processor architectures can be mixed on a single board: The Honeywell Experion C200 PLC

Control Processor main board has a Philips ARM backplane communication processor and a Freescale PowerPC main processor. This single board includes two processors with entirely different architectures.

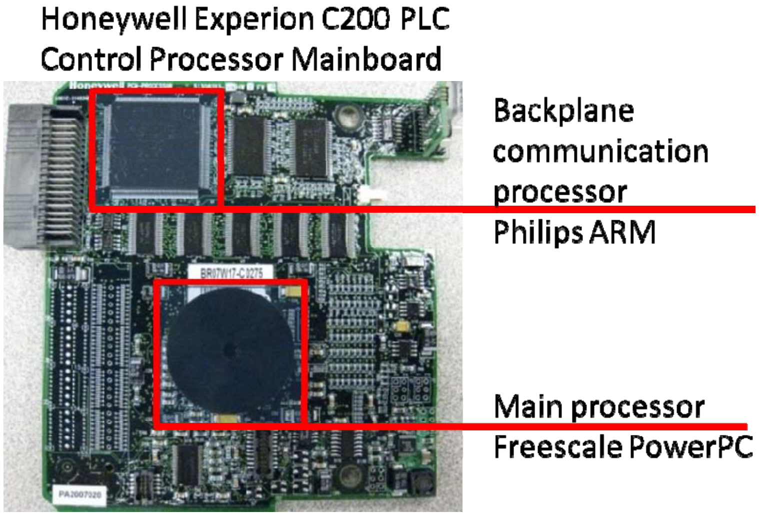

Honeywell Experion C200 PLC
Control Processor Mainboard
Backplane communication processor
Philips ARM
Main processor
Freescale PowerPC

Figure 53. Honeywell Experion C200 PLC Control Processor Mainboard.

Our findings also show that PLCs have very little hardware-level security. In some cases, production units have functional JTAG ports. The absence of security features may be because PLCs are typically installed in physically secure locations, so hardening against physical attacks is not considered a priority.[7]

Further research will focus on deeper analysis of individual PLCs, including analysis of the software on a device. This research will provide a basis on which to develop hardware-level security techniques (e.g., use of a technology such as a trusted platform module) to protect our critical infrastructure.

[7] The security of these remote sites often consists of a chain-link fence and a locked cabinet. Whether this security is sufficient depends on the sophistication of the adversary and the function of the PLC.

8. REFERENCES

1. **ARM.** ARM Company Profile. *ARM.* [Online] http://www.arm.com/about/company-profile/index.php.

2. **Data Respons.** Choosing a CPU: X86 VS ARM. *Data Respons Embedded Solutions.* [Online] February 23, 2010. http://www.datarespons.com/templates/interrupt.aspx?id=30531.

3. **ARC Advisory Group.** Programmable Logic Controllers (PLCs). *ARC Advirory Group.* [Online] June 30, 2009. http://www.arcweb.com/Research/Studies/Pages/PLCs.aspx.

4. **Zabel, Rick.** State of Manufacturing & Automation in the U.S. Looks Good. *Automation.com.* [Online] June 30, 2008. http://www.automation.com/content/state-of-manufacturing-and-automation?x=1&pagePath=00000000,00002687,00002765.

5. **Rockwell Automation.** *2009 Annual Report and Form 10-K.* 2009. www.rockwellautomation.com.

6. **Siemens.** *Annual Report 2009.* 2009. www.siemens.com.

7. **Idaho National Laboratory.** *National SCADA Test Bed Substation Automation Evaluation Report.* Idaho National Laboratory. Idaho Falls : INL, 2009. INL/EXT-09-15321.

8. **Atkins, William D.** *Interview Notes.* 2010.

9. **Berg, Michael.** *Interview Notes. 2010.*

10. **Mitsubishi Electric.** *Corporate Profile*. http://global.mitsubishielectric.com/company/corp/data

11. **Mitsubishi Electric.** *Annual Report 2009.* www.mitsubishielectric.com.

12. **Schneider Electric.** *Annual Report 2009.* 2009. http://www.schneider-electric.com.

13. **Omron.** *Annual Report 2009.* 2009. http://www.omron.com/ir/ir_annual.html.

14. **B&R Industrial Automation.** [Online] Bernecker + Rainer Industrie-Elektronik Ges.m.b.H. , 2004. http://www.br-automation.com.

15. **GE/FANUC.** GE and FANUC announce agreement to dissolve joint venture. Aug. 17, 2009. http://www.fanuc.co.jp/en/ir/irlibrary/pdf/osirase090818_e.pdf.

16. **Atkins, William D.** Open Source Survey of Control System Protocols. 2010.

17. **Modbus Organization.** Modbus Organization Members. http://www.modbus.com/about.php.

18. **Modbus Organization.** Modbus Supplier Directory. http://www.modbus.com/companies.php.

19. **Modbus Organization.** Modbus Device Directory. http://www.modbus.com/devices.php.

20. **Modbus Organization.** Modbus System Integrator Directory. http://www.modbus.com/si.php.

21. **Triangle MicroWorks, Inc.** Using DNP3 & IEC 60870-5 Communication Protocols In the Oil & Gas Industry. *Triangle MicroWorks, Inc.* March 26, 2001. http://www.trianglemicroworks.com.

22. **CC-Link Partner Association.** Partner Contact List. http://www.cc-link.org.

23. **Rockwell Automation.** www.rockwellautomation.com/locations.

APPENDIX A: CONTROL SYSTEM MODEL

The figure below shows the control system object relational model (ORM).

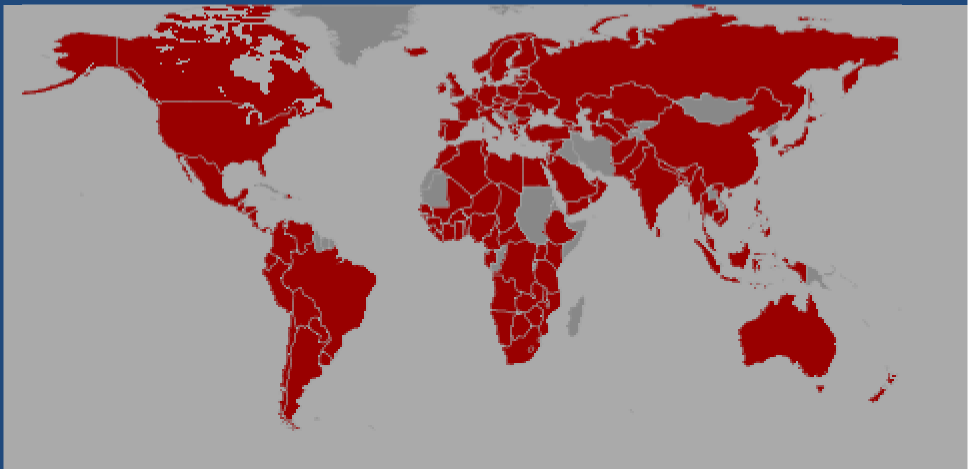
APPENDIX B: VENDOR SURVEYS

The information in this appendix supplements the vendor summary provided at the end of Section 4.

Siemens (31.3%)

Based in: Germany
Employees: 405,000

2009 Sales[8]
Total: $104B
Industry: $47.6B
Energy: $35.0B
Healthcare: $16.2B
Other: $5.2B



Siemens is the leading vendor in the PLC market (4) and is among the larger vendors in the energy sector. Its operations largely focus on the European market, but it has a strong presence worldwide. (6) Its three sectors and their 2009 revenues are presented in Table B-1.

Table B-1. Revenues by region for Siemens industry, energy, and health care sectors.

Revenue by Region	Industry Sector	Energy Sector	Healthcare Sector
Europe, Africa, & Middle East	$26.1B	$20.0B	$6.4B
Americas	$11.3B	$8.9B	$7.0B
Asia and Australia	$8.6B	$5.6B	$2.7B

Industry Sector

According to the Siemens *Annual Report*, the company's industry sector "offers a complete spectrum of products, services and solutions for the efficient use of resources and energy and

[8] Siemens provides sales figures in Euros. U.S. Dollar values shown were calculated with a 1.3575 U.S. Dollar per Euro exchange rate.

improvements of productivity in industry and infrastructure. Its integrated technologies and holistic solutions address primarily industrial customers, such as process and manufacturing industries, and infrastructure customers, especially in the areas of transport, buildings and utilities. The portfolio spans industry automation and drives products and services, building, lighting and mobility solutions and services, and system integration and solutions for plant businesses." (6) Relevant information from the *Annual Report* are presented in the text and tables that follow.

Table B-2. Breakdown of Siemens industry sector revenue.

Industry Sector Revenue	
Industry Automation	$9.6B
Drive Technologies	$10.2B
Building Technologies	$8.1B
OSRAM	$5.5B
Industry Solutions	$9.2B
Mobility	$8.7B

Description of Industry Sector Divisions

Industry Automation "Our comprehensive, integrated portfolio of automation systems, industrial switchgear, industrial software and complete industry solutions is making our customers in the manufacturing and process industries faster, more efficient and more flexible." (6)

Drive Technologies "Productivity, energy efficiency and reliability are our customers' key requirements. And as the world's No. 1 supplier of products, complete systems, applications and services for complete power trains and for all industry segments, we have the solutions they need." (6)

Building Technologies "We're the preferred partner when it comes to protecting people and infrastructures and maximizing energy efficiency in buildings. Our portfolio comprises products, solutions and services for building automation, fire safety, security and power distribution."(6)

OSRAM "We offer customers energy-saving lighting solutions for all areas of modern life. Our extensive portfolio includes not only lamps and optoelectronic semiconductor light sources such as light-emitting diodes (LEDs), LED systems and LED luminaires but also electronic control gear and light management systems."(6)

Industry Solutions "We provide comprehensive solutions and services for industrial plants and infrastructure systems. Our technologies are increasing our customers' productivity and competitiveness across entire lifecycles, from planning and construction to operation and services. We also offer a broad portfolio of ecofriendly solutions that are enabling customers to reduce their environmental footprint and conserve natural resources."(6)

Mobility "By networking transportation systems more effectively, our integrated solutions for intermodal transport, traffic management, postal automation and airport logistics are making the movement of people and goods more efficient and environmentally compatible."(6)

Energy Sector

The Siemens *Annual Report* states that the company's energy sector "offers a wide spectrum of products, services and solutions for the generation, transmission and distribution of power, and the extraction, conversion and transport of oil and gas. It primarily addresses the needs of energy providers, but also serves industrial companies, particularly in the oil and gas industry." (6)

Table B-3. Breakdown of energy sector revenues. Source: (6)

Energy Sector Revenue	
Fossil Power Generation	$13.3B
Renewable Energy	$3.2B
Oil and Gas	$5.8B
Power Transmission	$8.4B
Power Distribution	$4.5B

Description of Energy Sector Divisions

Fossil Power Generation "Our innovative technologies generate more electricity from less fuel. We boost the efficiency of coal- and gas-based power generation and supply technologies for low-carbon fossil power generation."(6)

Renewable Energy "We're steadily expanding our position in the dynamic renewables market – with innovative wind turbines that rank among the most reliable in the world, with major photovoltaic projects and with the most advanced technologies for solar-thermal power plants."(6)

Oil & Gas "The oil and gas industry, numerous process industries and electricity producers base their operations on our products, systems and solutions. We support our customers in tapping remote deposits and in producing and processing oil and gas. Our offerings include solutions for increasing pressure in oil and gas fields as well as applications for pipelines, floating production, storage and offloading (FPSO), and refineries."(6)

Energy Service "Our broad spectrum of innovative products and services ensures plant reliability, improved efficiency and optimal environmental performance for our customers' operating plant assets in the utility, oil and gas, industrial processing and power generation industries, enabling them to gain the maximum benefit from their investments."(6)

Power Transmission "Leveraging our innovative strengths in efficient power transmission, reliable switchgear, high-performance transformers and advanced power transmission systems, we enable customers to transport electricity safely and efficiently."(6)

Power Distribution "Our smart grid technologies increase energy system efficiency. We offer innovative medium-voltage components and systems, efficient solutions for energy automation, and services for electrical systems and networks."(6)

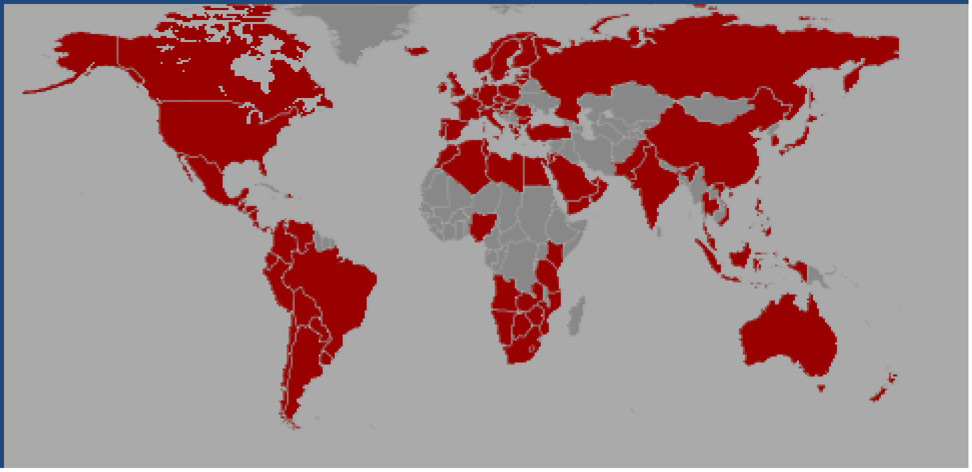
Health Care Sector

The *Annual Report* states that Siemens's health care sector "offers customers a comprehensive portfolio of medical solutions across the value-added chain – ranging from medical imaging to in-vitro diagnostics to interventional systems and clinical information technology systems – all from a single source. In addition, the Sector provides technical maintenance, professional and consulting services, and, together with Siemens Financial Services, financing to assist customers in purchasing the Sector's products."(6)

Rockwell Automation (22.1%)

Based in: Milwaukee, WI, USA
Employees: 19,000

2009 Sales
Total: $4.3B
Architecture and Software: $1.7B
Control Products and Solutions: $2.6B



Rockwell Automation sells control system components under the Allen-Bradley brand. Allen-Bradley products are represented in nearly every industry, although they are especially prevalent in manufacturing, building automation, (8)(9) and electrical utilities (2). The company is also actively increasing its market penetration in the oil and gas industries. (5)

In 2008, Rockwell Automation reported annual sales of $3.3B in control products and solutions. The company is actively working to diversify geographically and has seen strong revenue growth in the Asian Pacific, Latin America, and European markets. Rockwell's sales in China, a key emerging market, grew 37% in 2008. (5)

Products

Rockwell Automation produces a wide variety of control system-related products. Of particular interest is the Allen-Bradley line of Programmable Logic Controllers.

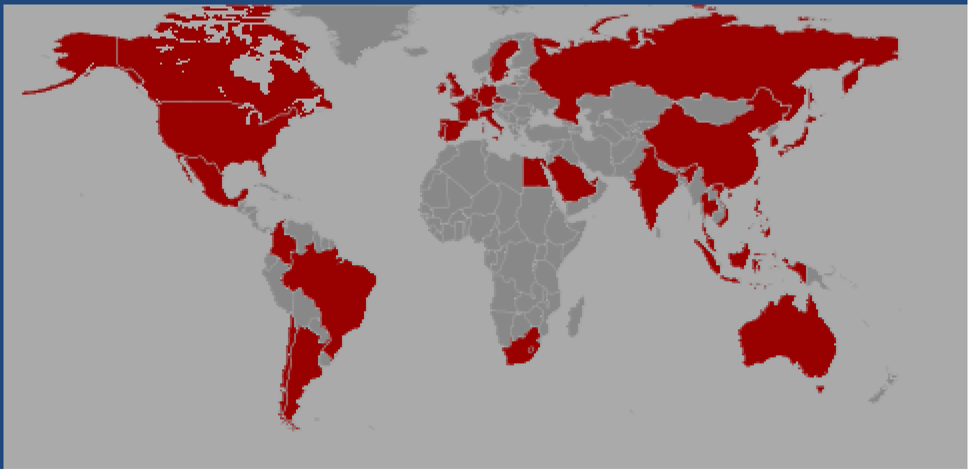
Locations

Rockwell Automation has a widely-distributed global presence. The company has 28 corporate locations in the Americas, 38 in Europe, 26 in the Middle East and Africa, and 15 in Asia and Oceania. Distributors for the company's products are also widely dispersed: 23 in the Americas, 33 in Europe, 22 in the Middle East and Africa, and 16 in Asia and Oceania. Third-party solution providers are primarily located in the Americas: 44 in North America and 40 in Latin America, but only 6 in Europe, the Middle East, and Africa. (23)

Mitsubishi Electric (12.7%)

Based in: Japan
Employees: 107,000

2009 Sales
Total: $37.4B
Energy and Electric: $10.6B
Industrial Automation: $8.7B



Mitsubishi Electric Corporation is a Japan-based company that manufactures electric and electronic equipment used in energy and electric systems, industrial automation, information and communication systems, electronic devices, and home appliances. (10) Table B-4 shows the percentage of total sales for each business segment.

Table B-4. Percentage of sales by business segment, 2009. (11)

Percentage of Sales by Business Segment	
Energy and Electric Systems:	25.1%
Industrial Automation Systems	20.5%
Information and Communications Systems	14.0%
Home Appliances	22.0%
Others	14.4%
Electronic Devices	4.0%

Energy and Electric Systems

The energy and electric systems division was responsible for $10.6B in revenues in 2009. (11) The division manufactures and sells a large number of devices. The company's online *Corporate Profile* lists them as "turbine generators, hydraulic turbine generators, nuclear power plant equipment, motors, transformers, power electronics equipment, circuit breakers, gas insulated switches, switch control devices, surveillance-system control and security systems, large display devices, electrical equipment for locomotives and rolling stock, elevators, escalators, building security systems, particle beam treatment systems, and others." (10)

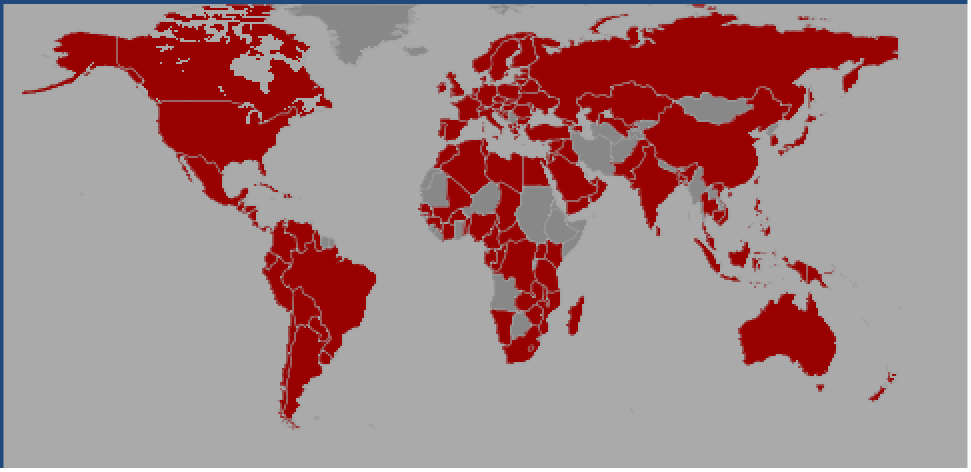
Industrial Automation Systems

The Mitsubishi industrial automation systems division was responsible for $8.7B in revenues in 2009. (11) The division manufactures and sells PLCs as well as "inverters, servomotors, human-machine interface, motors, hoists, magnetic switches, no-fuse circuit breakers, short-circuit breakers, transformers for electricity distribution, time and power meters, uninterruptible power supply, industrial sewing machines, computerized numerical controllers, electrical-discharge machines, laser processing machines, industrial robots, clutches, automotive electrical equipment, car electronics and car mechatronics, car multimedia, and others." (10)

Schneider Electric (8.0%)

Based in: France
Employees: 104,853

2009 Sales
Total: $21.4B
Electrical Distribution: $12.5B
Automation & Control: $5.8B
Critical Power & Cooling Systems: $3.2B



Schneider's annual report states: "As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments that make energy safe , reliable, efficient, productive and green. The Group enjoys leadership positions in energy and infrastructure, industry, buildings and data centres & networks, as well as a broad presence in residential applications." (12)

Table B-5. Schneider sales by segment.

Sales by Segment	
Electrical Distribution	$12.5B
Automation & Control	$5.8B
Critical Power	$3.2B

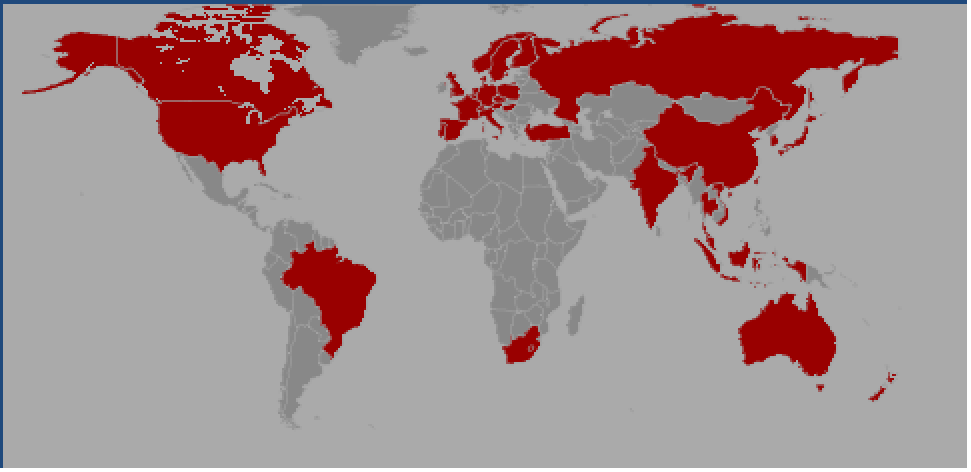
Table B-6. Schneider workforce by region.

Workforce by region	
Europe	43%
Asia-Pacific	25%
North America	24%
Other	8%

Omron (6.1%)

Based in: Japan
Employees: 32,583

2008 Sales[9]
Total: $6.7B
Industrial Automation: $2.8B
Electronic Components: $1.3B
Automotive Electronic Components: $0.9B
Social Systems: $0.9B
Healthcare: $0.67B



Omron primarily focuses on the manufacture and sale of automation systems, although the company also produces a variety of medical equipment. More than half of Omron's sales are in Japan. Of the total, 70% are in Asia.

Table B-7. Omron sales by segment.

Sales by Segment (13)	
Industrial Automation	42%
Electronic Components	20%
Automotive Electronic Components	13%
Social Systems	13%
Healthcare	10%

Table B-8. Omron sales by region.

Sales by Region (13)	
Japan (incl. direct exports)	52%
Other Asia	6%
Greater China	12%
Europe	16%
North America	13%

[9] Amounts converted from Japanese yen at a rate of 1 yen = 0.010629 U.S. Dollars

According to Omron's *Annual Report*, the company's industrial automation business (IAB) "provides a wide spectrum of equipment ranging from factory automation (FA) controllers to sensors, switches, relays, and safety equipment that meet some 100,000 specifications and support innovation in monozukuri (the art of product creation) and productivity improvement in all types of production operations. Commanding top domestic market share, IAB is the Japanese manufacturing industry's leading supplier of control equipment." (13)

The *Annual Report* also claims that "IAB is fortifying its customer service and support operations and expanding collaborative sales channel operations with the aim of raising sales. The segment is concentrating on fields where development investment is projected to continue while upgrading its solution proposal capabilities with a focus on issues pertaining to quality, safety, and the environment. IAB is also preparing to aggressively introduce products catered to markets in developing countries." (13)

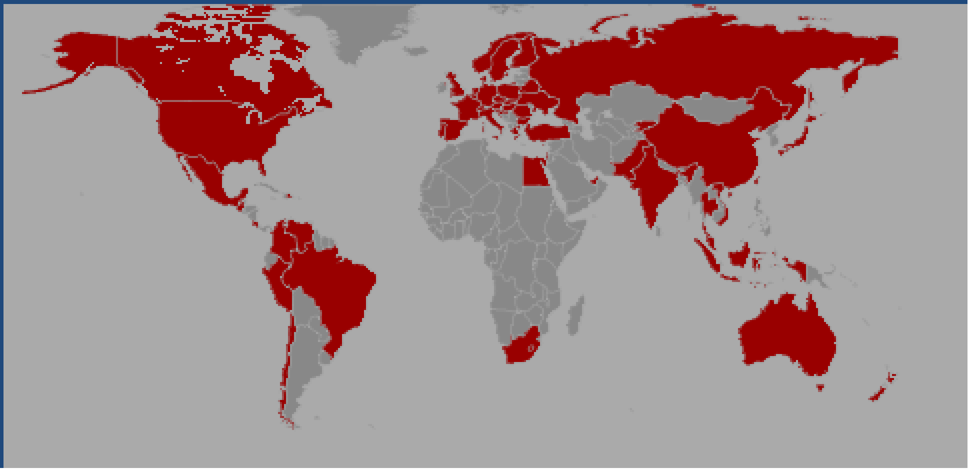
Table B-8. Omron industrial automation sales by region.

Industrial Automation	Sales by Region
Net sales	$2.8B
Japan	$1.2B
North America	$0.34B
Europe	$0.75B
Asia	$0.19B
China	$0.27B
Direct exports	$0.01B

B&R Industrial Automation (3.6%)

Based in: Austria
Employees: 1,700

2008 Sales
Total: $0.39B

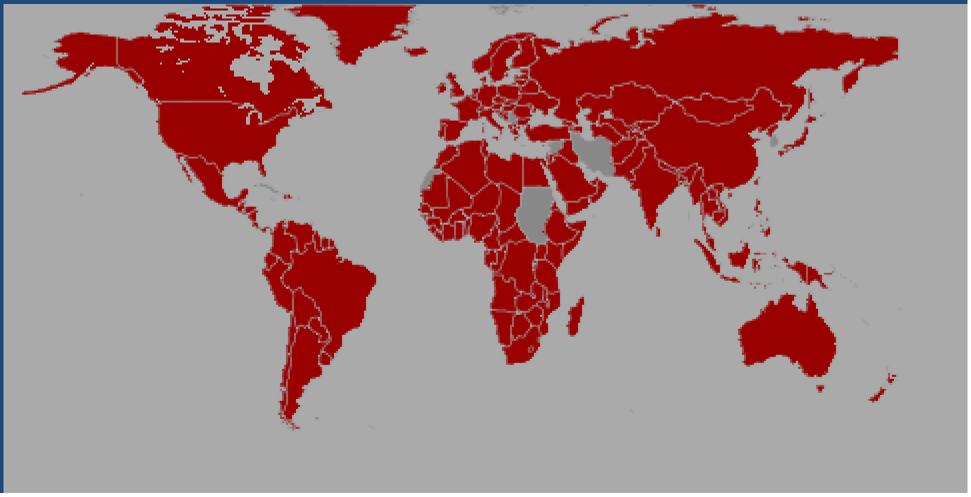


B&R Industrial Automation is one of the largest privately owned companies in the area of automation and process control. The company's web site lists its product range as "control, motion, operator interface, communication, and software products." (14) B&R has significantly fewer reporting requirements than other PLC vendors because it is a private company, making it difficult to obtain detailed sales figures.

General Electric (3.5%)

Based in: United States
Employees: 323,000

2008 Sales:
Total: $182B
Energy Infrastructure: $38.6B
Technology Infrastructure: $46.3B
Consumer and Industrial: $11.8B
Other: $8.4B



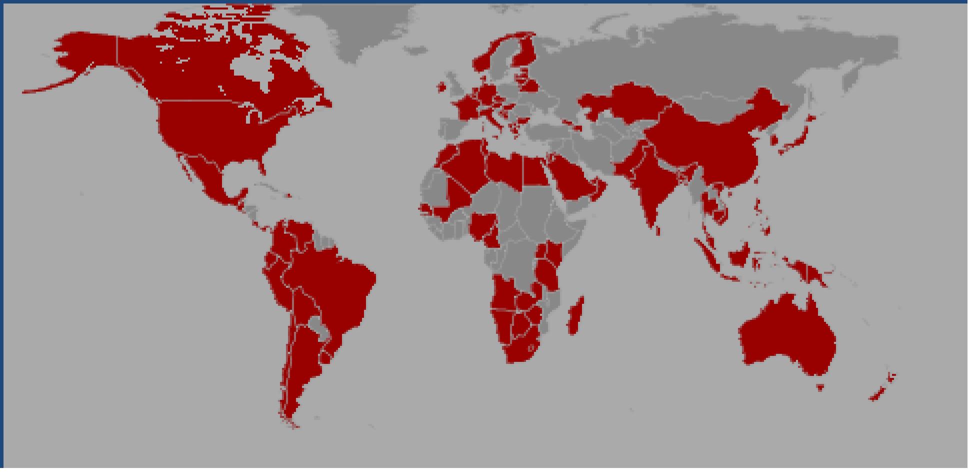
General Electric (GE) has a strong presence in energy and technology infrastructure. GE's 2008 revenues included $38.5 billion for energy infrastructure, $46.3 billion for technology infrastructure, and $11.7 billion for consumer and Industrial. GE Intelligent Platforms, a division of GE Enterprise Solutions, develops and sells PLCs, HMIs, and other process control devices.

GE-FANUC Automation Corporation was a joint venture between FANUC Robotics America, Inc. and GE. In August 2009, the companies dissolved the joint venture. (15)

ABB (2.1%)

Based in: Switzerland
Employees: 120,000

2009 Sales
Total: $34.9B
Power Products: $11.9B
Power Systems: $6.9B
Automation Products: $10.3B
Process Automation: $7.8B
Robotics: $1.6B



The ABB Group specializes in power and automation technologies for utilities and industry. The company stresses its efforts to reduce environmental impacts. ABB has offices in 87 countries.

Table B-9. ABB Industrial Statistics.

Segment	Revenue	Products
Power Products	$11890M	Transmission and distribution products and services. Serves electric, gas, and water utilities with products and services for power transmission and distribution.
Power Systems	$6912M	Engineering: grid systems, power generation, network management solutions, and substations. Deliverables include network management, utility communication, transmission and dist. substations, automation and electrical solutions for power plants. Automation, control, and protection systems for power transmission and distribution networks, power plants, and water pumping stations.
Automation Products	$10250M	Products and services including mechanical equipment such as motors and switches, and electronics systems, and some SCADA systems. 100 manufacturing sites in 50 countries.

Segment	Revenue	Products
Process Automation	$7815M	Process automation/SCADA systems in multiple industries. Markets: oil and gas, metals and minerals, pulp and paper, chemicals and pharmaceuticals.
Robotics	$1642M	Robots and manufacturing solutions. Auto industry, also foundry, metal fabrication, plastics, electronics, food and beverage, machine tools, solar, pharmaceuticals and chemicals, and wood.

Table B-10. ABB Revenues by Region.

Revenues by region	
Europe	$15815M
Asia	$8967M
Americas	$6428M
Middle East and Australia	$3702M

APPENDIX C: ACRONYMS

Term	**Meaning**
ADC	Analog to Digital Converters
ASIC	Application-specific Integrated Circuit
CIP	Common Industrial Protocol
CISC	Complex Instruction Set Computing
CLB	Configurable Logic Block
CPU	Central Processing Unit
DAC	Digital to Analog Converter
EDO	Extended Data Out
EGD	Ethernet Global Data
EtherCAT	Ethernet for Control Automation Technology
FINS	An Omron Corporation Ethernet protocol
FPGA	Field-programmable Gate Array
HSE	High-speed Ethernet
IOB	Input/Output Block
IP	Internet Protocol
LED	Light-emitting diode
PLC	Programmable Logic Controller
RISC	Reduced Instruction Set Computing
RTOS	Real Time Operating System
RTU	Remote Terminal Unit
SERCOS	Serial Real-time Communication System
SOC	System on a Chip
SRTP	Service Request Transfer Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

DISTRIBUTION

1	MS0671	Jennifer M. Depoy	5628
1	MS0620	Edward J. Nava	5620
1	MS0672	Jeffrey J. Danneels	5621
2	MS9018	Central Technical Files	8944
2	MS0899	Technical Library	9536
1	MS0123	D. Chavez, LDRD Office	1011

Sandia National Laboratories