Testimony by

Paul Skare

Product Manager

Siemens Power Transmission & Distribution, Inc.

Energy Management & Automation

to the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management, Government

Information, and International Security

July 19, 2005

Introduction

Good afternoon Chairman Coburn, ranking member Carper, and members of the Subcommittee on Federal Financial Management, Government Information, and International Security. I am Paul Skare, Product Manager at Siemens Power, Transmission and Distribution, Inc. I am representing one of the manufacturers of SCADA (Supervisory Control and Data Acquisition) systems. My role at Siemens includes managing products for SCADA systems as well as substation automation systems. I am also involved in standards groups related to SCADA.

Siemens is one of the largest electronics companies in the world, operating in over 190 countries. We're a diversified company, delivering a wide array of products, systems and services in six main industries. These include information and communications, automation and control, power, healthcare, transportation and lighting. Siemens has over 70,000 employees in the United States across all 50 states.

Siemens' Energy Management & Automation provides software and technologies in regulated and deregulated energy markets. A key product for these markets is SCADA. SCADA collects information from devices in the power system, identifies problems, and allows users to remotely control these devices. Adding additional applications to a SCADA allows a more focused and enhanced solution for transmission or distribution systems (referred to as an Energy Management System (EMS) for transmission or a Distribution Management System (DMS) for

distribution).

My testimony today focuses on identifying potential security vulnerabilities of SCADA systems, the state of activities related to this, and recommendations to better protect those systems from harmful intrusion.

While our customers primarily use our SCADA systems for the electric system, some also use the same SCADA system for gas, water, and transportation systems. Although our systems are not used as commonly in other settings such as industrial control systems, the concepts are the same across all SCADA systems. In the appendixes of the written testimony, I have provided background information on SCADA and security issues relevant to SCADA. I would like to take this opportunity to congratulate the industry and the government in the work that has been done in the last three years in this area – it has started moving this work from the realm of art to science, and is finally starting to not only spread awareness, but also to get various players to talk the same language.

SCADA Vulnerabilities

SCADA vulnerabilities that may be a problem often involve issues associated with the following:

Remote Access

Remote access to SCADA systems is available for a variety of reasons: user access

outside of the control room, user support, and vendor support. This is a problem if there are any accidental (configuration of) security holes. If any backdoors are in the system (either leftover from the vendor or in place for user support), access points are easier to exploit. Local access points must be physically secure or these issues will also apply to them.

Network configurations

Network (and firewall) configurations are a very important aspect for SCADA systems. SCADA systems depend on a network for operational needs. If a firewall is bypassed accidentally or is miss-configured, a severe security hole could exist.

Disgruntled employees

If an employee becomes disgruntled, either before or after action by a utility (current or former employees), if the security process has not yet closed all access for that individual, the case for doing damage is greatest, since all the security in place can still be used by an authorized individual.

Security holes, patches, viruses

Systems rely on standard IT solutions [Commercial Off The Shelf (COTS)] to create a SCADA solution. Some third party security holes in operating systems, commercial databases and other applications can directly translate into security issues for the SCADA.

Communication protocols not encrypted

Communications, being the largest cost driver in a SCADA solution, is an important area. Since many field devices can last 30 or more years, utilities are reluctant to upgrade them unless there are clear needs. This means many old low power (computationally) devices are in operation, for which there are not standard, interoperable, commercial encryption solutions available. More modern communications methods, which introduce greater security risks, can move toward modern PKI solutions. Older methods still need a technical solution.

Lack of incident reporting

Since utilities are reluctant to share any data on security violations due to the negative publicity that is possible and the potential for this to do damage to stock prices, no clear picture of existing threats based on reliable metrics is available. The North American Electric Reliability Council (NERC) is working on creating a way to do this, but it is unlikely many incidents will be reported due to the negative publicity this brings to the utility. Similarly utilities are reluctant to share this information even with their SCADA vendors. This means that the SCADA vendors' view of the security threats may be understated. If reporting occurred, vendors would also be even more motivated to provide secure solutions due to negative feedback possibilities of their products.

Challenges for SCADA installations

- Single user sign-on procedures to track/audit user activity.

- Security toolkits to secure older products and verify the security with reports.
- Secure operating systems, databases, and applications.
- Interoperable PKI solutions needed for LAN/WAN communications.
  - Interfaces to other systems must be secured.
- Secure device protocols for LAN/WAN communications.
- Secure device protocols for synchronous/asynchronous communications.
  - Low computing power devices still need a technical industry solution that is accepted by NERC and utilities and interoperable between vendors.

Recommendation: Business Process

To be successful, a utility needs corporate security policies in place. Even the best security built in to a SCADA product is insufficient to prevent hacking of a SCADA system if not complemented with a strong security policy and security enforcement program by the users of the SCADA system themselves. This requires:

- A Security Manager
- A Security Awareness Program
- Periodic changes of Username / Password with specials content requirements
  - No More Yellow Sticky Notes!
  - Audits

Internal utility organization models also can impact security solutions. Often, SCADA systems are run within Operations, while the rest of IT is in a separate organization. This is due to the different needs of SCADA systems. SCADA Systems must process

information every two seconds and on demand, so a computer or communication problem cannot be tolerated for any great length of time. IT organizations are not typically suited to respond at the speeds required for SCADA systems. This means dedicated support people are used to support SCADA systems, but this introduces the possibility of disjoint security implementations between operations and IT. Business process within such organizations must be aligned for security solutions.

Recommendation: Research

Support the development of commercial encryption for old low powered devices that are now in operation. The energy industry still needs research for effective and economic encryption for low powered devices, (both wired and wireless), so RTU and other small devices can have encrypted communications. This must then be taken out to become industry standards endorsed by groups such as NERC.

Recommendation: Reporting of both threats and incidents

Promote more widespread reporting of security incidents. Keep this reporting confidential so that a Utility does not fear leaks to the media. Also, a secure way to share threat information with vendors and utilities is needed that does not impact national security. This increases awareness and helps justify investment from the private sector.

Recommendation: Incentives for Utilities to secure their systems

A tax incentive for securing critical infrastructure would be a positive approach to

encourage culture change at electric utilities.

Recommendation: Federal and State cooperation

Electric Utilities can not simply invest in all needed cyber security improvements due to the cost. It is not only a few computer systems that need to be addressed, but their entire control system infrastructure, from the Control Center on out to every monitored substation and on out to each field device (IED). Utilities need to be able to bring these costs into their rate structures, and this can not happen with out the support of each state's Public Utilities Commission. Also, non-jurisdictional utilities need to secure their systems as well.

Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action

DHS and DOE have been cooperating, but as with any such large organizations there are still overlaps. This is evident at the National Labs. At Idaho National Laboratory, there is both the National SCADA Testbed (NSTB) (DOE), and the Control System Security and Test Center (CSSC) (DHS). These programs should be combined, and total funding increased for this valuable work. But also, the funding should be committed in advance for a five year period, so that the lab can also test the improvements made in the systems, until systems are judged to be secure. Competition between national labs such as INL, Sandia, PNNL and Oak Ridge for funding and programs should not create confusion in the eyes of the industry as it has in the past. Continued reorganizations and management changes combined with delays in

receiving funding have all contributed to overall delays in security enhancements over the last two years. Interestingly, the people I have met at DHS have been trying to go fast, efficient and cooperative in their work. To me this is a sign of a good culture at work in the organization.

Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds

As a vendor, I represent my customers and their wishes, as well as my company's interests. As a taxpayer, I want to see the security issues resolved as efficiently and effectively as possible, and a risk based approach is the most effective and efficient.

Conclusion

Siemens strongly supports securing the nation's critical infrastructure in many ways. Siemens believes that as a responsible corporate citizen, we have advanced the state of the art in SCADA systems by openly discussing security issues with our customers through our customer association, by creating add-on products for older versions of our products (a Security Toolkit to harden existing installations – a leading innovation in our industry), by participating strongly in standards groups on security of SCADA system (IEC TC57 WG15; NIST PCSRF; DHS PCSF), by having a strong corporate focus on security, and by implementing security programs and standards in our products.

As a SCADA vendor, we have and will continue to develop, implement and advise on

enhanced features and technology to prevent security loopholes. However, in addition to built-in security features for SCADA, it is necessary to merge/complement it with an enterprise wide IT security policy and company cultures that support this. I believe that a form of compliance to security standards is required to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

In conclusion, I appreciate the opportunity to express the views of a leading SCADA manufacturer. We applaud your leadership in examining potential security vulnerabilities to America's vital infrastructure. We believe security compliance is a matter of corporate culture and that this culture must be set and influenced from the very top of every corporation to be effective. By starting at the top of management, I know that the culture of Siemens is one that supports security. We look forward to working with you and the subcommittee in building support for a broader understanding of critical information security issues.

Appendixes to Testimony by

Paul Skare

Product Manager, Marketing

Siemens Power Transmission & Distribution, Inc.

Energy Management & Automation

to the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management, Government Information, and International Security

July 19, 2005

Summary or Abstract

- Industry provides the tools to secure SCADA systems even though not all utilities make use of these tools.
- Background on SCADA and SCADA security issues are explained.

Table of Contents:

1 Introduction 3
2 Potential Problems ..... **Error! Bookmark not defined.**
2.1 SCADA Vulnerabilities 4
2.1.1 Remote Access 4
2.1.2 Network configurations 4
2.1.3 Disgruntled employees 4
2.1.4 Security holes, patches, viruses 5
2.1.5 Communication protocols not encrypted 5
2.1.6 Lack of incident reporting 5
2.2 Challenges for SCADA installations 5
2.3 Recommendations 6
2.3.1 Recommendation: Business Process 6
2.3.2 Recommendation: Research 6
2.3.3 Recommendation: Reporting of both threats and incidents 6
2.3.4 Recommendation: Incentives for Utilities to secure their systems 7
2.3.5 Recommendation: Federal and State cooperation 7
2.3.6 Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action 7
2.3.7 Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds 7
3 SCADA Vulnerabilities ..... **Error! Bookmark not defined.**
3.1 Potential Problems ..... **Error! Bookmark not defined.**
3.1.1 Remote Access ..... **Error! Bookmark not defined.**
3.1.2 Network configurations ..... **Error! Bookmark not defined.**
3.1.3 Disgruntled employees ..... **Error! Bookmark not defined.**
3.1.4 Security holes, patches, viruses ..... **Error! Bookmark not defined.**
3.1.5 Communication protocols not encrypted ..... **Error! Bookmark not defined.**
3.1.6 Lack of incident reporting ..... **Error! Bookmark not defined.**
3.2 Challenges to overcome ..... **Error! Bookmark not defined.**
3.2.1 Impacts on SCADA Products ..... **Error! Bookmark not defined.**
3.2.2 Business Process Impacts ..... **Error! Bookmark not defined.**
4 What Siemens has done 7
5 Conclusion ..... **Error! Bookmark not defined.**
6 Conclusion 8

Appendix A – What is the SCADA Industry? 8
Appendix B – What is SCADA? 10
Appendix C – What are SCADA Applications? 15
Appendix D – What are SCADA Services? 18
Appendix E – SCADA Security Standards 19
Appendix F – The Use of Biometrics, Smart Cards 22
Appendix G – How do you secure SCADA? 23
Appendix H – Why aren't SCADA systems already fully secure? 25
Appendix I – SCADA Security Education 25

1 Introduction

Good afternoon Chairman Coburn, ranking member Carper, and members of the Subcommittee on Federal Financial Management, Government Information, and International Security. I am Paul Skare, Product Manager at Siemens Power, Transmission and Distribution, Inc. I am representing one of the manufacturers of SCADA (Supervisory Control and Data Acquisition) systems. My role at Siemens includes managing products for SCADA systems as well as substation automation systems. I am also involved in standards groups related to SCADA.

Siemens is one of the largest electronics companies in the world, operating in over 190 countries. We're a diversified company, delivering a wide array of products, systems and services in six main industries. These include information and communications, automation and control, power, healthcare, transportation and lighting. Siemens has over 70,000 employees in the United States across all 50 states.

Siemens' Energy Management and Automation provides software and technologies in regulated and deregulated markets for:

- Single energy suppliers
- Multiple energy suppliers (such as electricity and gas)
- Municipalities
- Generation companies, transmission providers, system operators, and distribution providers in deregulated energy markets
- New participants in the business such as energy traders, balance managers, risk assessors and energy suppliers

- Operators of traction power systems for railways
- Industrial power consumers

A key product for these markets is SCADA. SCADA collects information from devices in the power system, identifies problems, and allows users to remotely control these devices. Adding additional applications to a SCADA allows a more focused and enhanced solution for transmission or distribution systems (referred to as an Energy Management System (EMS) for transmission or a Distribution Management System (DMS) for distribution).

My testimony today focuses on identifying potential security vulnerabilities of SCADA systems, the state of activities related to this, and recommendations to better protect those systems from harmful intrusion.

While our customers primarily use our SCADA systems for the electric system, some also use the same SCADA system for gas, water, and transportation systems. Although our systems are not used as commonly in other settings such as industrial control systems, the concepts are the same across all SCADA systems. In the appendixes of the written testimony, I have provided background information on SCADA and security issues relevant to SCADA. I would like to take this opportunity to congratulate the industry and the government in the work that has been done in the last three years in this area – it has started moving this work from the realm of art to science, and is finally starting to not only spread awareness, but also to get various players to talk the same language.

2 SCADA Vulnerabilities

SCADA vulnerabilities that may be a problem often involve issues associated with the following:

2.1 Remote Access

Remote access to SCADA systems is available for a variety of reasons: user access outside of the control room, user support, and vendor support. This is a problem if there are any accidental (configuration of) security holes. If any backdoors are in the system (either leftover from the vendor or in place for user support), access points are easier to exploit. Local access points must be physically secure or these issues will also apply to them.

2.2 Network configurations

Network (and firewall) configurations are a very important aspect for SCADA systems. SCADA systems depend on a network for operational needs. If a firewall is bypassed accidentally or is miss-configured, a severe security hole could exist.

2.3 Disgruntled employees

If an employee becomes disgruntled, either before or after action by a utility (current or former employees), if the security process has not yet closed all access for that individual, the case for doing damage is greatest, since all the security in place can still be used by an authorized individual.

2.4 Security holes, patches, viruses

Systems rely on standard IT solutions [Commercial Off The Shelf (COTS)] to create a SCADA solution. Some third party security holes in operating systems, commercial databases and other applications can directly translate into security issues for the SCADA.

2.5 Communication protocols not encrypted

Communications, being the largest cost driver in a SCADA solution, is an important area. Since many field devices can last 30 or more years, utilities are reluctant to upgrade them unless there are clear needs. This means many old low power (computationally) devices are in operation, for which there are not standard, interoperable, commercial encryption solutions available. More modern communications methods, which introduce greater security risks, can move toward modern PKI solutions. Older methods still need a technical solution.

2.6 Lack of incident reporting

Since utilities are reluctant to share any data on security violations due to the negative publicity that is possible and the potential for this to do damage to stock prices, no clear picture of existing threats based on reliable metrics is available. The North American Electric Reliability Council (NERC) is working on creating a way to do this, but it is unlikely many incidents will be reported due to the negative publicity this brings to the utility. Similarly utilities are reluctant to share this information even with their SCADA vendors. This means that the SCADA vendors' view of the security threats may be understated. If reporting occurred, vendors would also be even more motivated to provide secure solutions due to negative feedback possibilities of their products.

2.7 Challenges for SCADA installations

- Single user sign-on procedures to track/audit user activity.
- Security toolkits to secure older products and verify the security with reports.
  - To secure operating systems, databases, and applications
- Interoperable PKI solutions needed for LAN/WAN communications.
  - Interfaces to other systems must be secured.
- Secure device protocols for LAN/WAN communications.
  - SCADA login access
  - RTU protocols – DNP over TCP/IP (DNPi)
  - Control Center data links – TASE.2 (ICCP) (Now Available)
  - Interfaces to other systems

Secure device protocols for synchronous/asynchronous communications.

- For synchronous/asynchronous communications - DNP 3.0 & Modbus serial

- Low computing power devices still need a technical industry solution that is accepted by NERC and utilities and interoperable between vendors.

3 Recommendations

3.1 Recommendation: Business Process

To be successful, a utility needs corporate security policies in place. Even the best security built in to a SCADA product is insufficient to prevent hacking of a SCADA system if not complemented with a strong security policy and security enforcement program by the users of the SCADA system themselves. This requires:

- A Security Manager
- A Security Awareness Program
- Periodic changes of Username / Password with specials content requirements
- No More Yellow Sticky Notes!
- Audits

Internal utility organization models also can impact security solutions. Often, SCADA systems are run within Operations, while the rest of IT is in a separate organization. This is due to the different needs of SCADA systems. SCADA Systems must process information every two seconds and on demand, so a computer or communication problem cannot be tolerated for any great length of time. IT organizations are not typically suited to respond at the speeds required for SCADA systems. This means dedicated support people are used to support SCADA systems, but this introduces the possibility of disjoint security implementations between operations and IT. Business process within such organizations must be aligned for security solutions.

3.2 Recommendation: Research

Support the development of commercial encryption for old low powered devices that are now in operation. The energy industry still needs research for effective and economic encryption for low powered devices, (both wired and wireless), so RTU and other small devices can have encrypted communications. This must then be taken out to become industry standards endorsed by groups such as NERC.

3.3 Recommendation: Reporting of both threats and incidents

Promote more widespread reporting of security incidents. Keep this reporting confidential so that a Utility does not fear leaks to the media. Also, a secure way to share threat information with vendors and utilities is needed that does not impact national security. This increases awareness and helps justify investment from the private sector.

3.4 Recommendation: Incentives for Utilities to secure their systems

A tax incentive for securing critical infrastructure would be a positive approach to encourage culture change at electric utilities.

3.5 Recommendation: Federal and State cooperation

Electric Utilities can not simply invest in all needed cyber security improvements due to the cost. It is not only a few computer systems that need to be addressed, but their entire control system infrastructure, from the Control Center on out to every monitored substation and on out to each field device (IED). Utilities need to be able to bring these costs into their rate structures, and this can not happen with out the support of each state's Public Utilities Commission. Also, non-jurisdictional utilities need to secure their systems as well.

3.6 Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action

DHS and DOE have been cooperating, but as with any such large organizations there are still overlaps. This is evident at the National Labs. At Idaho National Laboratory, there is both the National SCADA Testbed (NSTB) (DOE), and the Control System Security and Test Center (CSSC) (DHS). These programs should be combined, and total funding increased for this valuable work. But also, the funding should be committed in advance for a five year period, so that the lab can also test the improvements made in the systems, until systems are judged to be secure. Competition between national labs such as INL, Sandia, PNNL and Oak Ridge for funding and programs should not create confusion in the eyes of the industry as it has in the past. Continued reorganizations and management changes combined with delays in receiving funding have all contributed to overall delays in security enhancements over the last two years. Interestingly, the people I have met at DHS have been trying to go fast, efficient and cooperative in their work. To me this is a sign of a good culture at work in the organization.

3.7 Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds

As a vendor, I represent my customers and their wishes, as well as my company's interests. As a taxpayer, I want to see the security issues resolved as efficiently and effectively as possible, and a risk based approach is the most effective and efficient.

4 What Siemens has done

Siemens strongly supports securing the nations critical infrastructure in many ways. We have continued to add more security in our products, we are participating in standards groups to define interoperable security solutions, and we are working with the government and industry groups to promote security.

By starting at the top of management, the culture of Siemens supports security. This is exemplified in the way that Siemens is participating in standards groups and adding security features in our products.

5 Conclusion

Siemens strongly supports securing the nation's critical infrastructure in many ways.

Siemens believes that as a responsible corporate citizen, we have advanced the state of the art in SCADA systems by openly discussing security issues with our customers through our customer association, by creating add-on products for older versions of our products (a Security Toolkit to harden existing installations – a leading innovation in our industry), by participating strongly in standards groups on security of SCADA system (IEC TC57 WG15; NIST PCSRF; DHS PCSF), by having a strong corporate focus on security, and by implementing security programs and standards in our products.

As a SCADA vendor, we have and will continue to develop, implement and advise on enhanced features and technology to prevent security loopholes. However, in addition to built-in security features for SCADA, it is necessary to merge/complement it with an enterprise wide IT security policy and company cultures that support this. I believe that a form of compliance to security standards is required to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

The energy industry still needs research for effective and economic encryption for low powered devices, (like RTUs and even transmitters), so RTU and other small devices can have encrypted communications.

However, as a SCADA vendor, it is not possible to force our customers to buy all security offerings, nor to use the built-in security aspects of our products. Even the best security built-into a SCADA product is insufficient to prevent hacking of a SCADA system if it is not complemented with a strong security policy and security enforcement program by the users of the SCADA systems themselves.

Siemens input on the subject is that security compliance is a matter of corporate culture, and that this culture must be set and influenced from the very top of every corporation to be effective.

Siemens believes that a form of regulation/compliance to security standards is the only way to ensure that utilities will adopt sufficient security measures to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

In conclusion, I appreciate the opportunity to express the views of a leading SCADA manufacturer. We applaud your leadership in examining potential security vulnerabilities to America's vital infrastructure. We believe security compliance is a matter of corporate culture and that this culture must be set and influenced from the very top of every corporation to be effective. By starting at the top of management, I know that the culture of Siemens is one that supports security. We look forward to working with you and the subcommittee in building support for a broader understanding of critical information security issues.

Appendix A – What is the SCADA Industry?

Market

The SCADA and Energy Management System industry for high voltage electric transmission is a global market served by a very small number of large engineering firms and one dominant consulting organization. The important market forces that have shaped this industry include:

- A relatively small, and decreasing number of potential customers worldwide
- Very complex system requirements
- High R&D cost of market entry
- Low industry investment (perceived value) in systems upgrade / replacement
- High risks to technical and commercial success in systems delivery

Especially in recent years as investments in the transmission infrastructure in the U.S. have declined, there have been very few new system orders and technology previously delivered has in some cases not been well

maintained. Due to long project definition / delivery cycles and limited investments in maintenance and upgrades, the in-service SCADA infrastructure has significantly lagged the general information technology infrastructure.

Current business drivers within electric utilities are forcing integration of legacy (and in some cases obsolete) SCADA technology to other business systems and non-operational users at a rapid pace. This situation is creating new challenges for maintaining security on these proprietary systems originally designed to operate in isolation.

For Utilities to successfully cost justify the additional investments associated with security initiatives, a solid business case must be presented. Preparation of such a business case should include a security risk assessment including:

- Proving that threats are real and happening
- Using a common tool against your network and report on the attempt
- Assessing the impact an attack could have on your utility's reputation/profits
- Assessing the impact that a Denial of Service attack could have on your utility's reputation/profits
- Providing metrics to management on Internet attacks, companies affected, and damage caused
- Considering insider risks including all aspects of Internet usage
- Retaining a third party to perform a vulnerability assessment

Industry

While there are many niche vendors and small vendors of software in this business space, there are four major SCADA vendors: Siemens, Areva, ABB and GE (GE has been less and less engaged at the high end of the market). Some large SCADA systems require large bonds to be posted in order to bid on a order, and require a history of having delivered large systems due to the high importance of SCADA systems to everyone's infrastructure. All the big vendors have extensive presence internationally in this business, with business activities also spread out internationally. In the case of Siemens, development, delivery and support of the SCADA software is performed in Minneapolis (Minnetonka), Minnesota, USA as well as in Nuremberg, Germany.

When a utility determines it needs a new SCADA system, they will either write a specification (Request for Proposal – RFP) for the new SCADA system internally, or contract with a consultant to write one for them. These RFPs, along with the industry and IT standards, and NERC policies/standards greatly influence what vendors develop for their base products.

Vendors who are invited to bid on the order review the RFP, determine the aspects of the RFP that they can comply with, and propose a price based on the aspects of the RFP that they agree to meet.

The utility, typically together with the consultant, then evaluate the bids, and determine who has the best price for the needed requirements. An internally weighting is typically applied to the bids with unknown scales from the vendor's perspective.

Once a vendor is chosen, and a contract is signed, the project begins.

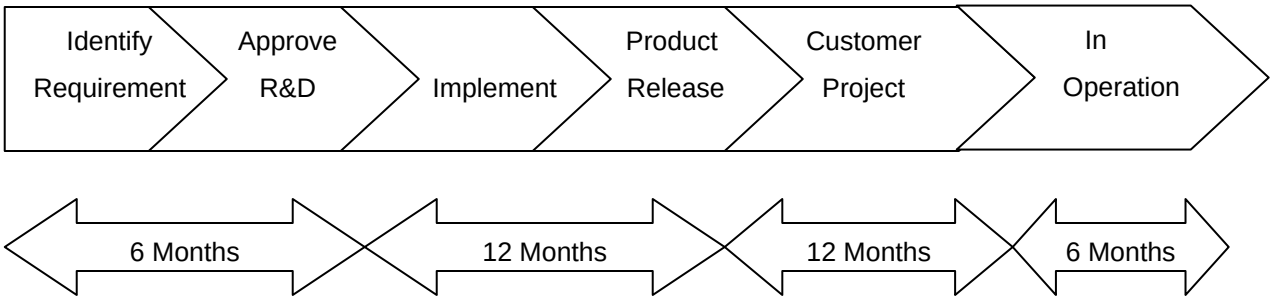
Dependence on mainstream IT

Due to the economic situation and the standards based requirements in the industry, we are dependant on the mainstream Information Technology (IT) world for security technology specifically, and for IT technology in general.

Product Delivery Influences

Delivery Timescales – Idea to R&D to project to field

Typical product delivery cycles include:

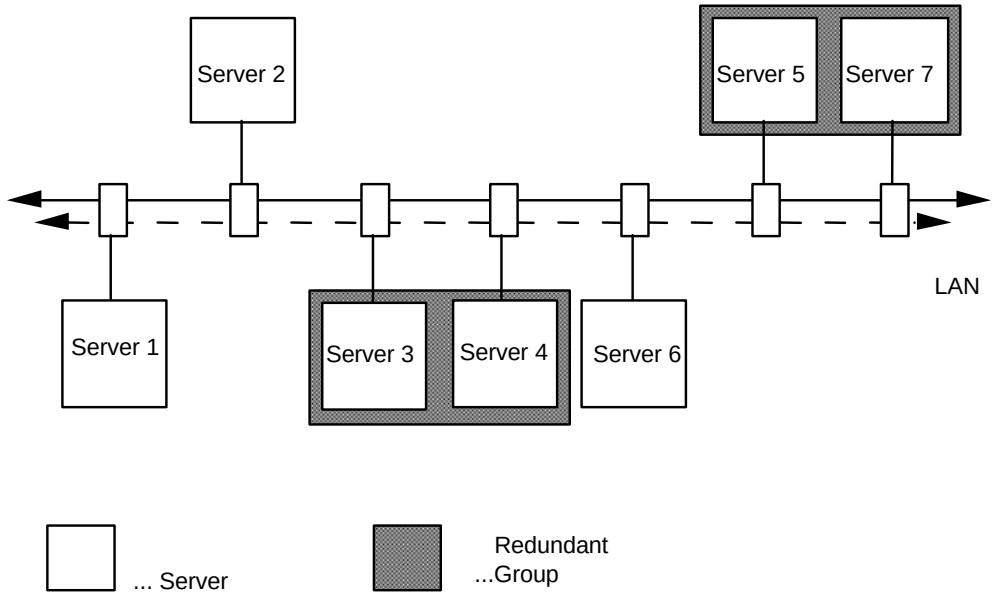


It is typical for some of these cycles to overlap, and all these numbers are samples that are typical, but vary widely. The sales cycle on these projects are commonly measured in years for new medium to large projects, in quarters for add-on, upgrade, and small projects.

The business cycle from the utility perspective can also be much longer, including rate cases with state PUCs, evaluating requirements, writing specifications, etc. Commercial projects have significant lag times between bookings and sales – from 3 to 48 months depending on the size of the project. The high end of the market is most prone to these effects, since there are few projects nationally each year, and each one has a higher degree of customization compared to lower level projects (at lower voltage levels) which rely more on base product approaches with lower levels of customization.

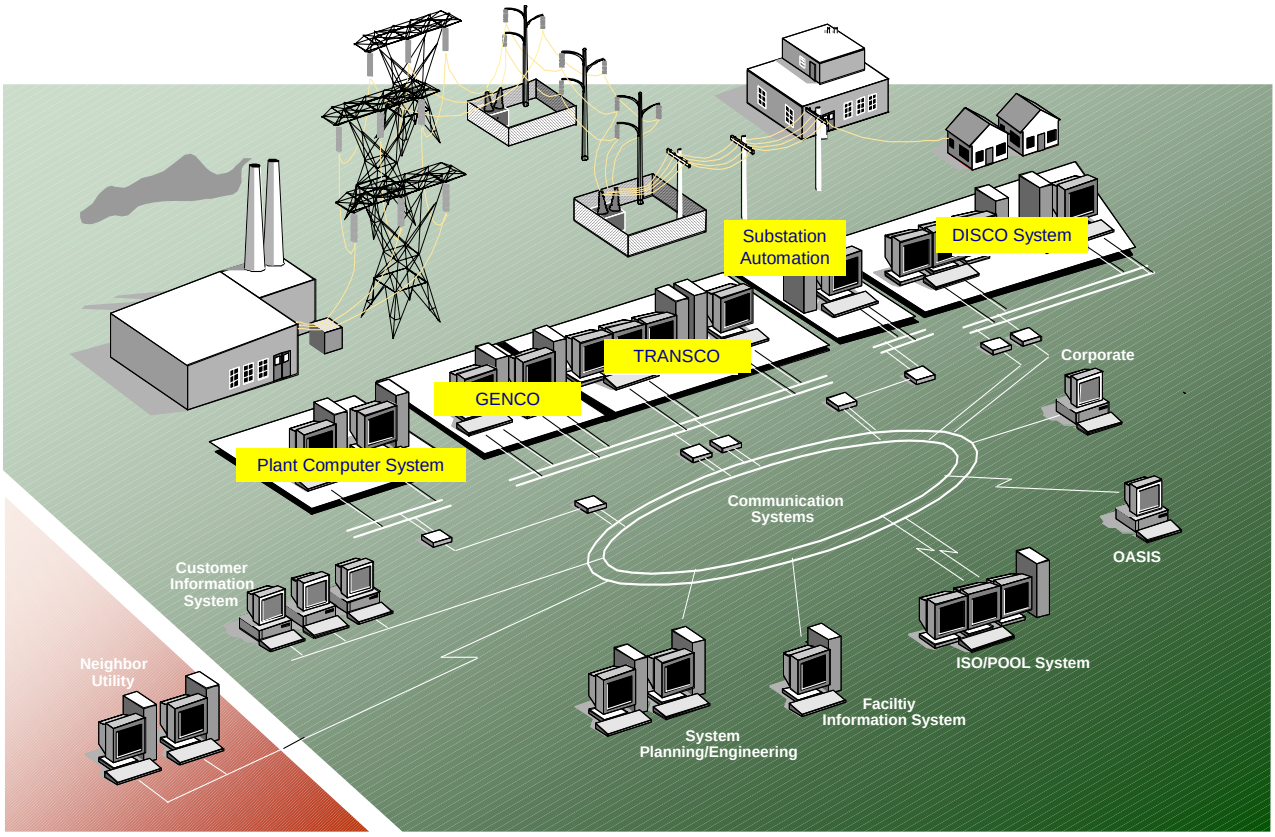
Appendix B – What is SCADA?

Supervisory Control And Data Acquisition (SCADA) systems collect data from substations, power plants, and other control centers. They then process the data, and allow for control actions to be sent back out. Other names of systems that can include SCADA include Energy Management Systems (EMS) and Distribution Management Systems (DMS). Typically these systems provide additional features on top of the basic SCADA, targeting either the transmission or distribution grids. SCADA systems are typically distributed on several servers connected via a redundant Local Area Network (LAN). A Utility's enterprise SCADA system might consist of anywhere from 2 to 150 computers. The SCADA itself does not include Remote Terminal Units (RTUs), devices, or computer networks and firewalls.



911B

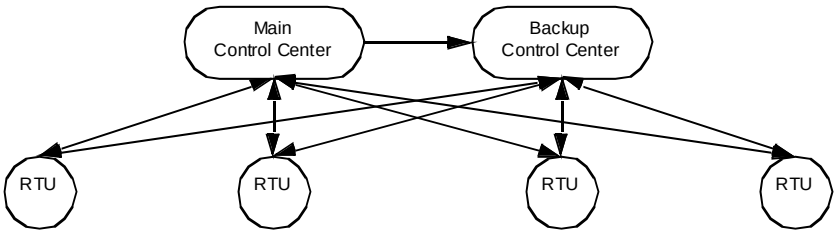
SCADA systems are typically run by an operations group in a central location for an electric utility. The following picture shows the systems a SCADA system usually communicates with. Deregulation has contributed to the entities who must communicate.



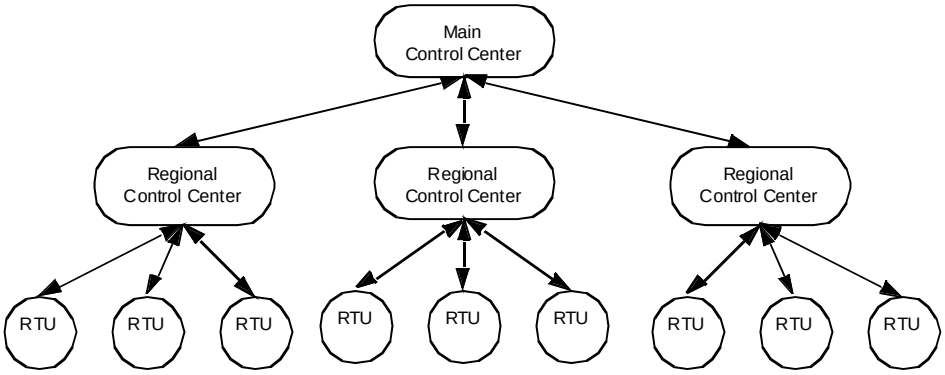
Below is a picture that shows how a SCADA control center appears much like NASA's Mission Control Center.

SCADA systems often have emergency back-up configurations.

A Typical Configuration (geographically separate backup location)



A Regional configuration



They communicate externally in a variety of ways. They use leased phone lines, dial-up phone lines, and LAN/WAN communications. These are usually provided by a local telecom. In addition, devices are commonly connected to the remote ends by additional communication methods, including hard wire contacts, radio, satellite, and microwave. Wireless technologies are being used more and more for connections to sensors.

These different methods of communication are used due to both economic and geographic reasons. All telemetry is expensive, but the more there is provides for a better understanding of the conditions of the electrical grid. Some places are quite remote and local telecom providers do not cover all areas needed. Further, some types of telemetry are of lower priority than others, so they can use less expensive, capable, or reliable means to get the data.

All decisions on communications methods are a business decision each Electric Utility makes. This includes not only the quantity and method of communication, but also the security involved with this communication.

Devices that SCADA systems communicate with typically are Remote Terminal Units (RTUs) that are in a substation or power plant, and hardwired to other devices to bring back meaningful information, such as current MW, MVAR, AMPS, volts, etc. More and more, Intelligent Electronic Devices (IEDs) are being used that can be connected directly to the SCADA systems or indirectly by means of a gateway computer (RTU).

The protocols that are used to communicate with RTUs have evolved over time as technology has progressed. Early protocols are Synchronous in nature (bit oriented – with a separate timing signal). They are very efficient, but do not have a lot of features, and require special hardware to operate. As PCs hit the market, Asynchronous (byte oriented – using standard serial ports) protocols became more popular. They used more computing power

and bandwidth, but supported faster speeds and more complex commands. Recently, TCP/IP based protocols have been growing in popularity, due to yet more complex command possibilities, and the proliferation of LAN/WAN communications and smarter devices. Telecoms have been spurring this on by raising prices on leased lines (used by synchronous/asynchronous communications), and lowering costs for frame relay connections (used by TCP/IP based communications). Technology has been spurring this on by providing more features and higher speeds by using TCP/IP based connections rather than serial communications.

Network connections in a SCADA system are connected via hubs, switches, routers and firewalls. A SCADA system is normally firewalled inside a utility's corporate firewalls, providing for a double level of firewall protection. Communication connections to the telecom for RTU communications typically bypass these firewalls. In the US, SCADA Vendors do not normally provide the network infrastructure or firewalls, but instead rely in the utility for these things, since most utilities have IT/MIS departments that provide these.

Interfaces to other systems

A SCADA system is increasingly connected to more and more systems in a Utility. Examples include:

- Asset Management (AM) / Facilities Management (FM) / Geographic Information System (GIS)
- Corporate Computer / Billing / CIS
- Trouble Call
- Load Management
- Corporate Dashboards

Each system that is connected to a SCADA system then becomes a security issue to make sure that all sides have adequate security in place. Most interfaces like those listed above are with other vendors' products. Enterprise Application Integration is an emerging trend used to connect these systems.

Control Center to Internet

Due to the proliferation of Internet based applications, such as e-tagging and OASIS, as well as e-mail and web site access, the Internet is connected more and more often to SCADA systems. This does not mean that a User Interface to the SCADA system is made available to the public Internet as is depicted in techno-thrillers made for TV, rather that there are multiple tiers of firewalls between the two. The risk is primarily of accidental connection or improperly configured firewalls and routers by the owners of the systems.

Control Center & Wireless

Some utilities have used wireless technologies, typically for remote crews working in the field and for monitoring of alarms in the SCADA system. Other uses include radio/satellite/wireless communication technologies to access remote locations where wired communication is either not possible or is economically disadvantageous. Any wireless communication can be a security threat if not encrypted, but encryption on small devices is often beyond the capabilities of small inexpensive field devices due to the computational requirements to encrypt communications. Wireless communications includes IEEE 802.11, Mobile phones (GSM/GPRS/SMS), and Bluetooth.

Telecom Dependencies

For most Electric Utilities, they are dependant on the local telecom provider for most communications between the control center and the external world. In particular, the control center to substation communication that typically either uses leased or dial-up phone lines and frame relay networks. Any security issue at the telecom provider becomes a security issue for the utility's SCADA system.

Third Party Security Solutions

SCADA vendors and their dependence on third party products create a security issue in their use of those third party products. Computer Hardware, Operating Systems, and Relational Databases are examples where SCADA vendors are dependant on third parties for major aspects of a SCADA solution. If the IT world and these

third party vendors have security issues, then the SCADA systems will have those same security issues. Some third party products offer an overview of security related issues.

Example: IBM Tivoli Netview

- Standardized security management over multiple platforms (AIX, NT, MVS)
- Produces audit trail
- Reports all events to a centralized source
- TACF (Tivoli Access Control Facility)
- Monitor/control access to selected system resources on a per-user basis
- Used to secure root and other common IDs.
- Logfile adapter monitors /var/adm/messages
- Plus modules for
    - ADSM backups
    - Oracle

Appendix C – What are SCADA Applications?

This section defines the security related functions within a SCADA system.

SCADA

Load Shed: manual and rotating: to drop load safely during emergencies – manually to select specific areas, rotating to spread the loss around.

Under Frequency Load Shed: To drop load safely based on under frequency conditions.

Alarm Processing: Notify users of problems in the system.

EMS Applications

Transmission Network Security

- Model Update: Update the data model of the network based on real-time inputs.
- State Estimator: Estimate values of non-telemetered points.
- Optimal Power Flow: Calculate power flows on transmission lines.
- Security Analysis: Study/Perform what-if scenarios based on loss of equipment in the grid.
- Voltage Stability Analysis: Study conditions in real-time that could lead to a voltage collapse.
- Dynamic Stability Analysis: Study conditions in real-time that could lead to dynamic instabilities.
- Operator Training Simulator: For training of users in normal operations, emergency operations, and system restoration activities.

Decision Support Tools in Systems Operation

Considering the events that led up to the recent and historic blackout of August 14, 2003, as well as the ramifications to the transmission system and the general population, it is clear that attention is being drawn to the reliability of the transmission system throughout the country. Although this particular event is not yet fully understood, it is true that many analysis tools exist today but are currently being underutilized as investments in the transmission infrastructure have stagnated. There are few systems indeed that fully utilize existing

capabilities in understanding the current real-time state of the network, its vulnerabilities to foreseeable events, its alternate and safer modes of operation, and its behavior during significantly degraded operations.

As the safety margins originally designed into the transmission system have all but disappeared through increasing loads, lagging investments, and new economic forces, it has become imperative that operations personnel have the clearest possible view of their transmission networks, be well trained for emergency operations, and be armed with effective decision support tools. The good news is that this technology not only exists today, but it can also be deployed in short order. Grid operators and utilities can take immediate advantage of System Analysis, Decision Support and Training tools from Siemens that can be quickly interfaced to an existing SCADA / EMS installations using industry standard technologies. There is no need to think in terms of wholesale system replacement in order to modernize your EMS.

What follows is a simple summary of the role and importance of existing network analysis tools, tools each of which have been deployed many times and on many different architectures throughout the energy industry. Through its Energy Management and Information Systems Division, Siemens has worldwide experience and expertise in getting these tools into production quickly and reliably. We believe that your goal of 100% reliability in the transmission system can only be achieved through proactive use of proven decision support tools, emergency procedure development, and comprehensive operator training. Siemens also has the integration tools, and the experience to incorporate these tools into your operation successfully.

State Estimation – As an adjunct to SCADA data processing, the State Estimator provides a simple and cohesive view of the real-time state of the entire transmission system, including a look into the health of neighboring networks as well as clearly representing the existence of "electrical islands". The State Estimator also identifies, and compensates for failures in the SCADA software subsystem, data telemetry, and local metering so that issues obscuring a proper view of the transmission system may be corrected proactively, not discovered during system emergencies or post-mortem analyses. New innovations in State Estimation now include the direct use of GPS provided Phase Angle measurements enabling more complete, and more robust solutions.

Intelligent Alarm Processing – In today's large systems high volumes of alarms are a fact of life. Coupled with old technology or poor user presentation, sometimes the most important system events are too easily overlooked or root causes impossible to determine. An intelligent alarm processor add-on not only ensures the operator sees the most important information, but also determines the root causes for cascading alarm situations immediately, and summarizes system problems involving hundreds of alarms simply. In times of seeming quiescence, the Intelligent Alarm Processor ensures that issues of low priority but significant duration, such as slow frequency oscillations, are not overlooked.

Security Analysis / Optimal Power Flow – You need to be aware, in advance, which potential system events will result in a degraded system operation that is simply unacceptable. Armed with real-time operational knowledge, the transmission system can be steered to a state which is not only secure during normal operations, but that will also remain secure in the event that any contingency becomes reality.

Dynamic Stability Analysis / Voltage Stability Analysis – These problems, usually well studied in the planning environment, are the most difficult to predict intuitively in the real-time operations environment. Although high loads and transmission stress can be an indicator of a potential problem, so can many other factors such as minimal loading, generation mix, load distribution, etc. Considering that the transmission grid is now often operated in an economic environment not planned for or well studied, on-line Dynamic Stability and Voltage Stability Analysis ensure that operators are alerted to conditions that could potentially lead to dynamic instabilities and voltage collapse.

Restoration Assistance – Should the worst happen and your system suffer a partial or complete shutdown, your Restoration Assistant becomes an invaluable tool for saving time and equipment during the extraordinarily complex task of system restoration. The Siemens Restoration Assistant can plan out an overall restoration strategy in minutes, or simply perform advance checks on switching operations such that generation, load, voltage and VAR supply all remain within critical balances. The Assistant also ensures that operations personnel understand the possible consequences of reconnecting your operational system with a neighboring system in order to support their restoration activities.

Simulation and Training – There can be no substitute for well-trained operational personnel. Their actions during critical situations equate directly to either the continued healthy operation of the system, or its being set on a course toward failure. Just like airline pilots that rely on well-planned emergency procedures and have trained exhaustively for failures in the sky, your operations staff needs to have developed and tested their emergency plans as well. Each and every operator needs the opportunity for emergency simulation training in order to safely carry their system through foreseeable emergency conditions. The Siemens Training Simulator is based on the open EPRI architecture model, resulting in a tool which can be plugged into your existing SCADA / EMS to provide simulation and training capabilities in an environment your operations personnel are already accustomed to.

Improved Data Modeling – Many transmission networks are modeled using outdated processes and tools, leading inherently to analysis errors in the operations environment. The Siemens Information Model manager (IMM), employs the latest in web-based deployment and visualization. All data is modeled within the industry standard Common Information Model (CIM), and is represented both within that structure as well as graphically – leading to efficient and accurate model checkout, and automatic one-line diagram generation. The standard formats used for data model and graphics exchange make interfacing this productivity tool to your system both simple and straightforward.

Historical Data Storage and Recovery – Having the ability to quickly, accurately, and efficiently store and recover historical data from your transmission system is critical to analyzing problems and developing effective operational solutions. Tools like the Siemens Historical Information System (HIS) are essential in today's environment. Accurate recording, archiving and quick recovery of essential operational data is necessary to ensure you operate your system within reliability standards, and to develop and test remedial action plans for those circumstances where reliability may have been compromised.

Operating your transmission system has always been a complex task. Thankfully, catastrophic failures have been rare, but also not rare enough. There is no question that the risks and consequences of failures are increasing. However, there are tools available today that can help to mitigate the challenges facing your system's grid operators. These tools and more are continually being developed and perfected by Siemens to help ensure the reliability, stability and security of one of the most important pieces of infrastructure in the world – the North American transmission grid.

DMS Applications

Distribution Network Applications

- Distribution System Power Flow: Determine power flows in the radial distribution network.
- Fault Location: Locate fault locations.
- Fault Isolation and Service Restoration: reroute distribution network to isolate faults and restore service.
- Volt/Var Control: Adjust volts/vars to more economically distribute power.

- Optimal Feeder Reconfiguration: Reconfigure the feeders based on system conditions.

Outage Analysis

- Outage Management System: Report and coordinate outages.
- Switching Procedure Management: Allow for collections of multiple control actions.

Energy Scheduling Applications

OASIS

This Internet based system allows market entities to buy transmission capacity on the grid.

E-Tagging

This Internet based system allows market entities to schedule the actual energy on the grid, previously arranged via OASIS.

RTUs/IEDs/other devices

These are the end devices that the SCADA system communicates with. Typically they are low non-powerful computing devices of various sorts, and do not have the computing strength for encryption. While newer devices are being developed with the necessary strength, older lower speed devices will continue to be in operation for decades to come. RTUs can have a lifetime of up to 50 years. Various studies estimate it costs a utility approximately $100,000 to put a new RTU in a substation. These costs are from the cost of the new RTU itself, the connection and installation of the new RTU, the configuration and tuning of the measurements of the RTU, the data maintenance needed in the SCADA system to properly define the new RTU and modify the SCADA displays that refer to the RTU. Repeated trips by field crews to the substation in coordination of personnel on the SCADA system are typically needed.

Substation Automation

As automation technology progresses to more quickly deal with protection, control, and metering issues in the substation, computers providing the solution also become security issues.

Appendix D – What are SCADA Services?

Maintenance Agreements

These are agreements between the SCADA vendor and the electric utility to provide experts to work on the SCADA system at predefined rates based on the amount of hours per year needed.

Software Subscription service

These are agreements between the SCADA vendor and the electric utility to provide new version of the base software when they are released based on a percentage of the intellectual property rights paid on a periodic basis.

Patch Management/Security service

A Subscription Based Security Information Service for Siemens SCADA

- Receive applicable Software Security Alerts for SPECTRUM and Third-Party Software – from Siemens
- Receive SPECTRUM Security Toolkit Upgrades – Harden your SPECTRUM System

Expected Future Additions

- Additional SCADA Products
- Industry Analysis
- Security Training Programs

Third Party Product Emergency Updates are used in the analysis

- Rollup of Third Party Product Updates
- CERT- Computer Emergency Response Team
    - SEI CERT- Software Engineering Institute
    - Siemens CERT- Siemens Corporate CERT
- ISAC- Information Sharing and Analysis Center Electricity Sector
- NIPC- National Infrastructure Protection Center

Optional Security Services

- Auditing Setup
- Run Penetration tests
- Implement Security Policy (e.g., SAS-70)
- Review Security Policy
- Incident Handling Procedures
- Certificate Authority

Application Service Providers (ASPs)

These applications are emerging as an economic alternative to ownership for utilities. They can access these applications over secure networks, and either pay on demand or pay monthly fees for access to the applications.

- Major offerings to date
    - Certificate Authority / Management
    - OASIS
    - E-Tag
    - Market Systems
- Requirements
    - Physically Secure Facility
    - Redundant Power Supply (computers, UPS, generation)
    - Redundant and Secure Communication Infrastructure

Appendix E – SCADA Security Standards

Existing Standards

While numerous standards bodies exist in the industry, the overall top level standards specific to electric utilities use of SCADA systems is the International Electrotechnical Commission (IEC) Technical Committee 57 - Power System Control and Associated Communications. In the US, the IEC operates in association with the American National Standards Institute (ANSI).

The IEC is one of the bodies recognized by the World Trade Organization (WTO) and entrusted by it to monitor the national and regional organizations agreeing to use the IEC's International Standards as the basis for national or regional standards as part of the WTO's Technical Barriers to Trade Agreement. [see http://www.iec.ch/about/partners/agreements/wto-e.htm for details],

The IEC works closely with its international standardization partners, the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), other regional standardization

organizations and international organizations, including the International Commission on Illumination (CIE), the International Council on Large Electric Systems (CIGRE), and the Union of the Electricity Industry (EURELECTRIC).

Security specific groups include:

Other groups with influence include the IEEE, IEE, NERC, FERC, NAESB, NRECA, EPRI, OMG, OAG, OPC Foundation, DOE, DHS, CIGRE, ITU-T, NIST, UCTE (former UCPTE), DNP User's Group, UCA International User's Group, the Whitehouse, National Labs.

EPRI: Enterprise Infrastructure Security (EIS)

IEC TC 57: WG 15

CERT- Computer Emergency Response Team (Carnegie Mellon University)

SEI CERT- Software Engineering Institute

Siemens CERT- Siemens Corporate CERT

ISAC- Information Sharing and Analysis Center (Electricity Sector)

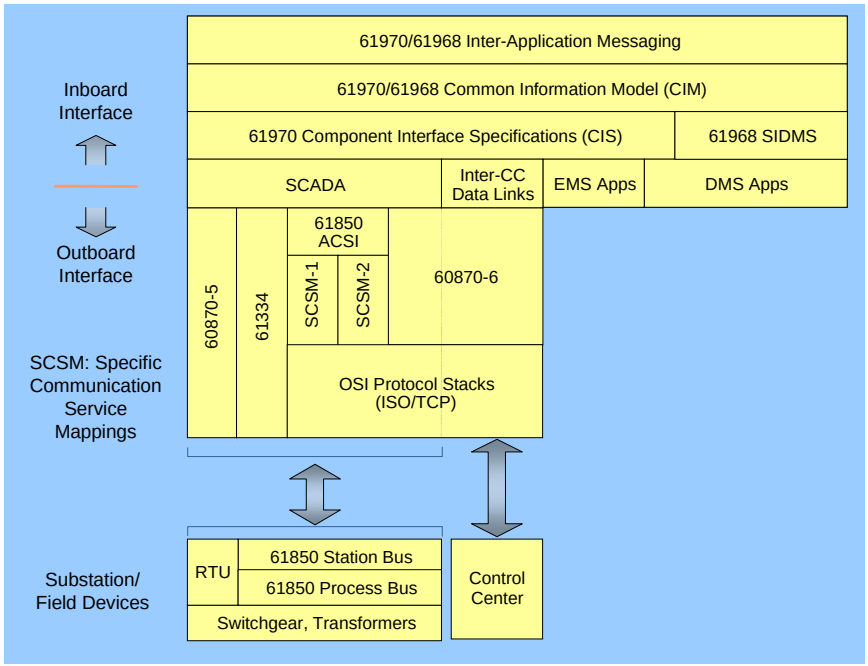
NIPC- National Infrastructure Protection Center

Working Groups

Following is a list of active working groups within the IEC TC57:

- WG 3: Telecontrol protocols
- WG 7: Telecontrol protocols compatible with ISO standards and ITU-T recommendations
- WG 9: Distribution automation using distribution line carrier systems
- WG 10, 11, 12: Communication standards for substations:
- WG 10: Functional architecture and general requirements
- WG 11: Communications within and between unit and station levels
- WG 12: Communication within and between process and unit level
- WG 13: Energy management system application program interface (EMS - API)
- WG 14: System interfaces for distribution management (SIDM)
- WG 15: Data and communication security
- WG 16: Framework for deregulated electricity market communications
- WG 19: Interoperability within TC 57 in the long term – responsible for the Reference Architecture

Graphical Overview of standards for SCADA

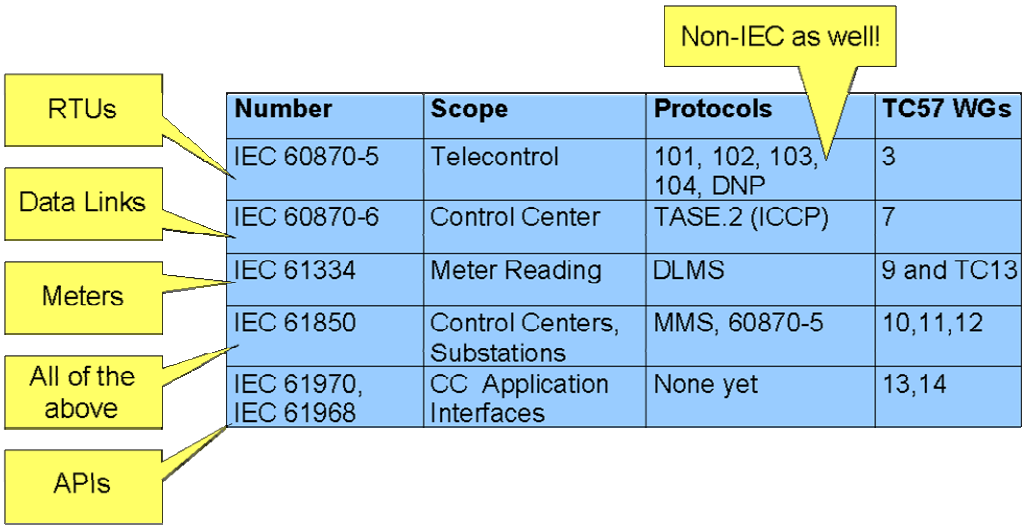


IEC TC57 WG15: Data and Communications Security

Mandate: Provide direction and assist other Working Groups Secure their protocols

Members of working group 15 come from consultants, vendors, utilities, and US national labs.

WG15 – Protocols and Groups Affected



Number	Scope	Protocols	TC57 WGs
IEC 60870-5	Telecontrol	101, 102, 103, 104, DNP	3
IEC 60870-6	Control Center	TASE.2 (ICCP)	7
IEC 61334	Meter Reading	DLMS	9 and TC13
IEC 61850	Control Centers, Substations	MMS, 60870-5	10,11,12
IEC 61970, IEC 61968	CC Application Interfaces	None yet	13,14

WG 15 Recommendations

- Use consequence-based analysis
- Provide multiple levels of security
- Focus on application layer
- Work together with other IEC TC 57 Working Groups
- Address key management
- Address the complete system
- Use ISO 15408 process (streamlined)

THREATS	***DUTIES***	***GOALS***
Denial of Service	**Be thorough**	**Confidentiality**
Replay	**Be clear and concise**	**Authentication of Data**
Access to strong points via weak points	**Consult all stakeholders**	**Authentication of Source**
Traffic Analysis	**Make it interoperable**	**Integrity of Data**
Impersonation	**Make it safe and secure!**	
Hijacking connections		
Disgruntled insiders		

Related Security Standards

IEEE Standard 1402-2000

IEEE Guide for Electric Power Substation Physical and Electronic Security

Provides definitions, parameters that influence threat of intrusions, and gives a criteria for substation security

Cyber methods considered:

- Passwords
- Dial-back verification
- Selective access
- Virus scans
- Encryption and encoding

NERC Security Policies

NERC Security Guidelines for the Electricity Sector: http://www.esisac.com/publicdocs/Guides

NERC Cyber Security Standards:
http://www.nerc.com/~filez/standards-cyber.html

SAS – 70 Security Standard

SAS-70 Audit

- Statement on Auditing Standards No. 70
- Audit procedure for Service Organizations that handle data and financial transactions
- Reports on the processing of Transactions by Service Organizations
- Audits company's ability to maintain systems so the data is secure and reports are secure and financially correct
- Many Companies accept SAS-70 results so they don't have to audit external companies individually.

Scope of SAS-70

- Documentation
- Data security
- Privacy of information
- Prevention of theft
- Availability of systems
- Authentication of sender and receiver
- Data integrity
- Controls
- Change Management Process
- Authorized access
- System backup and recovery procedures

Appendix F – The Use of Biometrics, Smart Cards

Advancing automation and the development of new technological systems, such as the internet and cellular phones, have led users to more frequent use of technical means rather than human beings in receiving

authorization. Personal identification has taken the form of secret passwords and PINs. Everyday examples requiring a password include the ATM, the cellular phone, or internet access on a personal computer. In order that a password cannot be guessed, it should be as long as possible, not appear in a dictionary, and include symbols such as +, -, %, or #. Moreover, for security purposes, a password should never be written down, never be given to another person, and should be changed at least every three months. When one considers that many people today need up to 30 passwords, most of which are rarely used, and that the expense and annoyance of a forgotten password is enormous, it is clear that users are forced to sacrifice security due to memory limitations. While the password is very machine friendly, it is far from user-friendly.

There is a solution that returns to the ways of nature. In order to identify an individual, humans differentiate between physical features such as facial structure or sound of the voice. Biometrics, as the science of measuring and compiling distinguishing physical features, now recognizes many further features as ideal for the definite identification of even an identical twin. Examples include a fingerprint, the iris, and vein structure. In order to perform recognition tasks at the level of the human brain (assuming that the brain would only use one single biometric trait), 100 million computations per second are required. Only recently have standard PCs reached this speed, and at the same time, the sensors required to measure traits are becoming cheaper and cheaper. Therefore, the time has come to replace the password with a more user-friendly solution -- biometric authorization.

Appendix G – How do you secure SCADA?

Actions Needed to Secure SCADA

- Secure Applications and Relational Database Access
    - Username/Password, roles, services, administrative authorities all must be set
- Operating System
    - Disable unused services and ports
    - Directory and file permission settings
    - Username/Password administration and auditing
    - User logon to domain
    - Authorization (restrict access to resources you have been assigned)
    - Resources assigned to individual or groups
    - Access Control Lists
    - Authentication (verify who you are)
        - Biometrics Options
            - Siemens ID Mouse with a capacitive sensor for fingerprint biometrics for logon.
            - Smart cards are an alternative to biometrics that relies on a possession for authentication.
- Network Communications
    - Deploy appropriate routers, firewalls, intrusion detection systems, Identify Security Administrator to manage security. Includes intrusion detection, intrusion prevention systems.

Physical Security

Guards and associated physical security are not part of a vendor's SCADA solution. They are specific to each Electric Utility.

Physical Security Monitoring

Monitoring of Physical Security issues can be done through the use of a SCADA system. Contacts can be wired for door access in substations as well as control rooms, and fed back into the SCADA system as a digital value. An Alarm category can be set up specifically for physical security violations, and this alarm category would be logged. A SCADA Display can be created to graphically display any security violations on a system basis. This type of capability is available via off the shelf software in most SCADA systems. This would typically be used as an operational back up of primary security systems.

Functional Security

Functional security is the area where SCADA applications must implement specific security technologies in order for the function to work. For example the Inter Control-Center Communication Protocol (ICCP) known as TASE.2 in the IEC has recently added a PKI solution to the international standard of ICCP. This required changes to the ICCP function itself in order to be possible.

Example: Siemens SCADA Security Toolkit

In order to provide for a secure Siemens SCADA solution on current and older version of the SCADA product, we have created a Security Toolkit. This evolving toolkit consists of a collection of utilities that allow the SCADA owner to tighten and monitor the security of the SCADA system. These utilities can be run once, or periodically automatically, and consider:

- Access policy (Host/LAN/VPN)
- Router/firewall configuration
- OS root/user username access
- UNIX services/programs
- Remote command usage
- FTP Usage by Applications
- Directory/file access rights
- RDBMS security
- Application passwords/authorities
- Integrity Scan (verify that SCADA program binaries have not been altered without authorization)

Other Solutions

The use of a Public/Private Key Infrastructure (PKI) solution addresses the following issues:

- **Privacy:** No one other than the parties or systems involved knows the details of the electronic messages. This is accomplished through the use of Encryption using Cryptographic Protocols;
- **Authentication:** All parties to a transaction or electronic message exchange know whom they are dealing with at the outset. This provides proof of identity through the use of UN/PW logins with Digital Certificates, Smart Cards, Biometrics.
- **Integrity:** Messages cannot be changed while in transit between parties or systems; and
- **Non-Repudiation:** A party cannot deny having engaged in a transaction or having sent an electronic message.

The following issues must be met via other solutions:

- **Protection (of Resources):** Firewall, DoS Protection, Content Filtering, Virus Scanning, and Intrusion Detection are all areas that traditional IT solutions usually are applied.
- **Authorization:** A party is set up to provide the Certificate Authority and User Name and Password administration, as well as any setup of biometrics. This can be an internal or external group but is dependant on the policies and organizational structure at a utility.
- **Physical Security:** The normal 'guards and guns' type security, along with monitoring and surveillance capabilities is either in house or contracted out depending on the utility. Badge or smart card accesses to SCADA areas within buildings are normally coordinated through here.

Appendix H – Why aren't SCADA systems already fully secure?

SCADA systems have only recently (in the last 10 years) been connected to other IT technologies in a significant fashion. Previously SCADA systems were very isolated. Now that SCADA systems are increasingly connected to the outside IT world, and Cyber security solutions have begun to find mainstream adoption, it is time to make sure SCADA systems are secure. There are numerous negative side effects that have been mentioned in the past that have slowed implementation of a strong security environment for SCADA users.

- One is that it is more difficult to use the system. Every user must individually login and logoff when using the system.
- Maintenance support is more time consuming due to the restrictions of putting quick fixes into the system must now go through more rigorous security measures to verify the legitimacy of the fix.
- A security policy is only good if it has a manager and periodic audits: This adds a lot of cost to the environment, as well as inconvenience by having periodic audits.
- Periodically being forced to change passwords is tedious and irritating, but it is something that users can grow accustomed to.
- Acquiring and changing Digital Certificates as needed is an additional cost and time consuming affair. Since Digital Certificates have limited life spans, this is an ongoing, recurring effort and expense.
- All security features of a SCADA system cost the vendor R&D and maintenance costs.

While none of the above effects should be showstoppers, they are frequently referred to and complained about. A successful security initiative must address these issues from the point of view of showing the overall benefits to the company.

Appendix I – SCADA Security Education

Siemens SCADA Customers

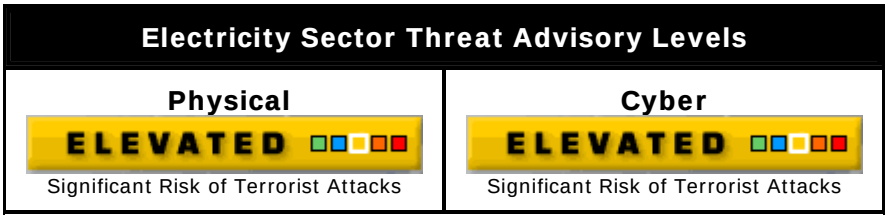
Siemens customers have a customer association that meets twice a year. It is named SECA (Siemens EMIS Customer Association). This meeting has a session/presentation about security at each meeting. Discussions about security features in the Siemens products, and feedback on security issues to Siemens are all features of these meetings. Panel sessions discussing real-world issues faced by SCADA users allow members to exchange information between each other as well as with Siemens. Bringing in industry experts (such as Jeff Dagle, Pacific Northwest National Laboratory in Richland, Washington) to discuss SCADA Security issues to the membership are also an example of the types of security discussions held at SECA meetings.

NERC Security Workshops

NERC is holding security workshops to heighten awareness of security issues for Electric Utilities. Other consulting groups are also holding security workshops, however there is a feeling that some are trying to take advantage of the situation.

NERC Security Status

NERC is also providing the industry with the current status of security threats at the national level. Below is an example of this.



Security Policy

An example of a good starting point for a security policy is through the use of the SAS-70 standard. This standard is already in use by some of the larger Utilities. The new NERC security guidelines are also a good description of what is needed for the control room.

More Security Information

See SANS (http://www.sans.org) for generic IT security information and information like this:

1. Key Elements of successful security awareness Program:
    - provide training on regular basis and include as part of new employee orientation program
    - Keep users informed about current trends in computer incidents
    - View security awareness as an on-going requirement
2. Key Elements of good security infrastructure:
    - Establish roadmap for security infrastructure improvements
    - Strong commitment from senior management to support security improvement roadmap
    - Metrics to measure security vulnerabilities and report to senior management
    - Understand risks to your environment
    - Justify the security infrastructure environment (potential impact to company's reputation/revenue)
3. Common Security Problems:
    - Administrators not properly trained in the area of information/network security
    - Administrators do not have upper management support to deploy appropriate security measures
    - Sites do not install security patches in a timely manner
    - Sites do not filter incoming mail for possible hostile attacks
    - Sites do update anti-virus software signature files on regular basis (should be automated procedure)
4. Common management errors:
    - Focus on reactive, short-term fixes resulting in problems re-emerging at later date
    - Rely only on a firewall for security perimeter protection

Fail to realize the value of their information and data

Fail to understand relationship of information security to the business (understand physical security but not consequence of poor information security)

SANS has a list of recommended steps to follow when responding to an incident. They are:

- Follow your policies and procedures
- Contact appropriate agencies
- Use 'out-of band' communications (like phone calls) to avoid intruders being notified of response
- Document your actions with good notes in chronological order
- Make a complete system backup and keep safe with a positive chain of custody
- If you are unsure of what actions to take, seek help before removing files or halting system processes
- Contact local law enforcement (police or FBI) for advice and assistance as soon as possible

The new NERC policies also cover this via the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) at http://www.esisac.com

http://www.incidents.org (by SANS institute)

http://icat.nist.gov (NIST security computer division)

http://cve.mitre.org (Common Vulnerabilities and Exposure)

http://xforce.iss.net (Internet Security Systems)

http://seclab.cs.ucdavis.edu/projects/vulnerabilities/#database/ (Univ of Calf Vulnerabilities Project)

http://www.cs.purdue.edu/coast/projects/vdb.htm (Univ of Purdue Cooperative Vulnerabilities Database)

http://www.siemens.com/biometrics (Siemens Biometrics)