

# Tackling Critical Energy Infrastructure Network Interdependencies



TUESDAY, 23 MARCH 2010 00:00 FRANCOIS GASPARD AND ALAIN HUBRECHT

Over the past decade, the energy sector, and more particularly the energy security sector, has received considerable attention from the public and governments around the world. Physical security is of course one of the main focus areas in energy security, however, another emerging area is cyber security.

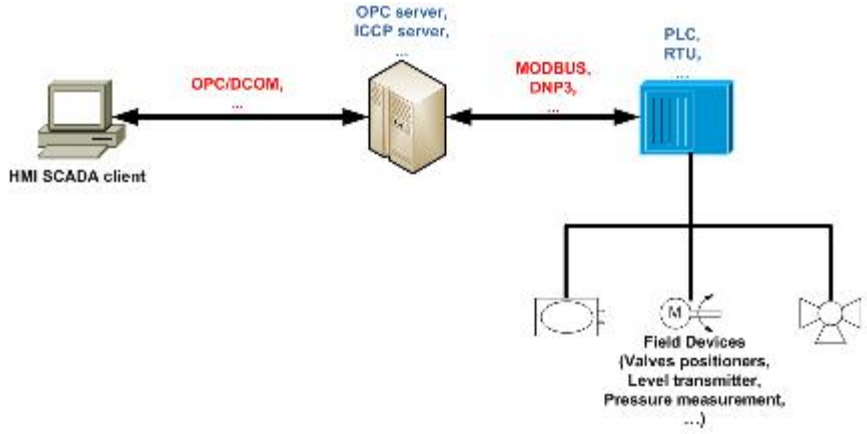
Since the widespread distribution of Information Technologies (IT) and IP (internet Protocol) technologies, more and more critical infrastructures, such as electric grids or gas utilities, use these technologies. However, improving and simplifying use and interoperability bring new security threats. An analogy to this development might be the introduction of just-in-time supply chains that deliver fresh food to supermarket distribution chains. While these systems are optimal in rendering greater efficiencies by avoiding the over-supply of perishable goods, given unforeseen natural disasters, truckers' strikes, or a breakdown in fuel distribution used for the transport of these goods, the system quickly breaks down, leaving consumers vulnerable to the lack of food availability.

The IT and IP sectors also use technologies such as SCADA networks for which security was not envisioned as part of the design phase. SCADA stands for supervisory control and data acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure-related or facility-based. Infrastructure systems include, for example, Infrastructure processes such as water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, civil defense siren systems, and large communication systems.

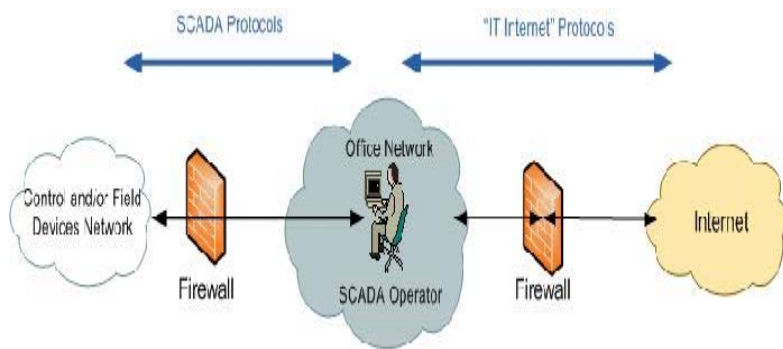
SCADA systems rely on multiple technologies, protocols and standards, for example Modbus—a protocol used to communicate data between a computer and a PLC (Programmable Logic Controller) or an RTU (Remote Terminal Unit). Other common protocols and standards include the Distributed Network Protocol (DNP3) which is a set of communications protocols used between components in process automation systems. Another is Inter-Control Center Communications Protocol (ICCP) or OLE for Process control (OPC). It is with the help of a SCADA network that an operator can monitor and control industrial systems

The multiple systems used in SCADA networks results in operational efficiency, but a lack in suitable security measures. This allows an attacker, state-sponsored agent or cyber-terrorist to access and take down these networks from virtually anywhere. These new threats are poorly understood by the energy sectors, as they generally consist of highly technical attack schemes. The well established IT security industry is also very distant from these threats, as it focuses primarily on IT systems and not Control Systems. A small but efficient Control Systems' security industry does exist. However, different critical resources (banking, energy, telecom, transport etc.) are not always handled holistically, resulting in one area treated on an independent basis, which by nature neglects the inter-connections between often interdependent systems. Moreover, a big gap exists between the people who actually make decisions (government officials, decisions makers etc.) and technical specialists (SCADA security expert, IT security etc.). As a consequence, the damage of a joint attack on all the critical infrastructures of a country is not well understood.

Because of these interdependencies, but also because of how critical they are to the infrastructures they support, SCADA networks are highly attractive targets for an attacker. A simplistic example of a SCADA network is shown on the diagram below, with OPC (OLE for Process Control) being a software interface technology used to communicate real-time plant data between control devices from different manufacturers, and Modbus being a protocol used to communicate data between a computer and a PLC (Programmable Logic Controller) or an RTU (Remote Terminal Unit). The data can be for example temperature and humidity measurements:



In theory, SCADA networks must be isolated from other networks such as office networks or external networks like the internet. However, with the proliferation of information and communications technologies (ICT) and a tendency to minimize cost, SCADA networks are often connected to other networks which bring new security threats and open these networks up to the possibility of cyber-attacks. It is not unusual for configurations in which the Human-Machine Interface (HMI), the application allowing an operator to control and monitor equipment, to be installed in an office network. In the following example, an operator can access the field device network from his desktop. This means he has an application installed on his desktop allowing him to control the SCADA network:



This example is of course very simplistic, and generally there are more layers such as supervisory, site manufacturing or control networks. But this example is enough to understand how a critical network can be accessed from an external network like the internet. The same station (the operator's computer) which has access to the internet can also access a very critical network. This is an ideal target for an attacker.

On top of this, many critical infrastructures depend on equipment located at multiple sites spread out all over the world, connected together by private lines, radio or Virtual Private Networks (VPN) over the internet. Unfortunately, there is the commonly held belief that SCADA networks are not connected to external networks such as the internet. However, in reality many SCADA networks have a connection, directly or indirectly, to the internet. Sometimes it is even possible to access a SCADA network via telephone lines. Often much of the critical equipment in SCADA networks have modems connected to them allowing third party access or vendor access to the equipment. In this case, firewall or network segregation is completely useless, as an attacker has simply to dial in to the modem to access the SCADA network. A strong authentication mechanism (or good password) is then necessary to prevent an attacker to access the SCADA network via dial in. However, many modems connected to critical systems still have default passwords which make them an easy and perfect target for an attacker.

The practice of accessing networks via telephone lines is called wardialing and was very popular in the 1980's despite being expensive to run. However, wardialing has seemed to have regained a second life recently, as hackers are now using wardialing with Voice over IP (VOIP). Security presentations about wardialing (a war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem) with VOIP to access SCADA networks have been seen at security conferences such as Kiwicon in New Zealand. During one presentation a security researcher simulated an attack on a power station accessed via war-dialing. The targeted computer was brought down through the internet via the modem connected to it. This resulted in the setting off of an alarm and the actual reprogramming of the device, which under real world conditions would have had significant impact on the power station's operations.

The most common way of accessing a SCADA network is by company employees. Indeed, statistics show us that a majority of

security incidents in the SCADA and process industries emerge from inside a company itself. Angry or annoyed employees are the first source of attacks to a SCADA network. For example, in 2000, a former contractor took control of the SCADA system controlling the sewage and water treatment system at Queensland's Maroochy Shire in Australia using a wireless connection and a stolen computer. This resulted in the release of millions of liters of raw sewage and sludge into creeks, parks and a nearby hotel.

This incident was not unique. A few other examples are cited below.

- \*1998 Gazprom: foreign hackers seized control of the main EU gas pipelines using trojan horse attacks
- \*2003 Davis-Besse nuclear plant: plant safety monitoring system was shut down for over five hours
- \*2005 International energy company: a malware-infected HMI system disabled the emergency stop of equipment under heavy weather conditions
- \*2009 Texas: an attacker takes control of the heating, ventilation and cooling control systems at a medical clinic
- \*2009 Integral Energy: a virus outbreak wreaked havoc with Integral Energy's computer network, forcing it to rebuild all 1000 of its desktop computers before the bug spread to the machines controlling the power grid

A more detailed explanation of SCADA system vulnerabilities is not necessary here. It is simply important to remember that there are three obvious different ways to access a SCADA network: access via the internet, access via telephone lines hooked up to a modem, and access granted to those working inside a company.

There are other entry points into control systems, but it is not always easy to understand how hackers or cyber-terrorists gain entry. We can reasonably assume that the majority of people working in the control system industry, and especially the energy industry, understand that a cyber-attack can affect their infrastructure, but few really know how this can be achieved. As previously mentioned, there is a control system security community that finds vulnerabilities, patches bugs, performs security assessment etc., however live penetration-testing against live production systems is often risky. Taking a website down for a couple of hours is not as damaging as taking down a nuclear centers' production network. Obviously the latter can have huge consequences not only for the facility itself but through the cascading effects of power disruption on other interconnected critical infrastructures. Indeed, as already explained in the article "European Energy Infrastructure Protection: Addressing the Cyber Warfare Threat" from Frank Umbach and Uwe Nerlich in the October issue of the *Journal of Energy Security*, critical national infrastructures are highly interdependent and depend upon the core elements of telecommunications, energy and transportation for their successful operations.

Some of the critical infrastructures and their dependencies are represented on the diagram below. Please note that not all critical infrastructures are represented here (such as emergency services, public health, food sector etc.), but highly important are the red squares on the left side which represent the critical infrastructures that are highly interdependent:

Interdependencies	Energy - Oil and Gas, Electricity	Telecommunication and Information	Banking and Finance	Water	Transportation
Energy - Oil and Gas, Electricity	Highly connected and interdependent Infrastructure for business and economic security				
Telecommunication and Information		Highly connected and interdependent Infrastructure for business and economic security			
Banking and Finance			Highly connected and interdependent Infrastructure for business and economic security		
Water				Essential and highly dependent Infrastructure for health and safety	
Transportation					Highly connected and interdependent Infrastructure for business and economic security

The telecommunication and energy sectors are probably the most interdependent sectors of all. Without public electricity, telecom services such as voice (telephones, mobiles phones) or data (internet, private networks between offices) are heavily impacted. Communications would still be possible between two entities (for example with radio communication) but most services would fail to run. All the switches, routers and firewalls needed by the telecom's industry would have no power at all. On the other hand, without telecommunication, the energy sector would lose a big part of its monitoring and system control capabilities. SCADA systems would be highly impacted. We could further extend these interdependencies: power generation

requires natural gas for its turbines, transportation and pipelines to supply fuel, water for cooling etc. The list goes on and on.

The financial sector is also vulnerable. Indeed, even if the connection between the energy sector and the financial sector is not as strong as the one between the energy and telecom sectors, the two sectors are still very inter-dependent. Banks need electric power for their day to day operations, but the energy sector also needs banking and financing for operations such as material procurement, fuel purchases and all sorts of financial transactions. As for the control system and telecom sectors, the financial sector has its own standards, technologies and networks. These special kinds of networks are sometimes called Electronic Funds Transfer systems (EFT). Some notable examples of these systems are SWIFTNet (Society for Worldwide Interbank Financial Telecommunication Network) for international transfers, Fedwire in the United States or TRANSFER (Trans-European Automated Real-time Gross Settlement Express Transfer System) in Europe. Again, these systems and networks are critical, not only for the energy sector, but also for national and international stability. Attacks against the financial sector have been seen in the news recently. It is important to note no major attack on core financial infrastructure has been reported to date, but financial companies, like companies in other sectors, tend not to report security incidents for fear of damaging their corporate reputation.

### **Understanding Cyber-Attacks**

It is necessary for all actors involved in the protection of critical infrastructures, and more precisely the energy security sector, to understand and address the question of cyber-attacks. However, as previously mentioned, the security of the energy sector infrastructure cannot be guaranteed without taking into consideration the security of other critical infrastructures such as telecom and finance infrastructures. The obvious way to understand the cascading and overall damage of a joint attack on all the critical infrastructures in a given country is to combine these different, but interconnected, critical infrastructure sectors. When an attacker launches a combined cyber-attack on the energy sector, telecommunication's sector, financial sector and other critical sectors such as transportation, water or public health systems, then the depth and gravity of the effects is nearly impossible to calculate. Fortunately nothing like this on such a scale has thus far been seen. The recent, but significantly overestimated, cyber-attacks in Georgia and Estonia received much media attention, but were in reality very basic attacks on internet web servers that avoided impacting other critical infrastructures. It should be clear, however, that an attack on all the critical infrastructures in a given country is technically feasible and could be carried out at a cost considerably less than that of sending a ground force into battle. Unfortunately, anticipating such an attack and how to respond to it is not that easy. As with traditional war, it is difficult to counter an enemy without knowing what he is capable of or, more importantly, how he plans to realize his objectives.

### **European Center for the Protection of Critical Resources**

For all of these reasons a new European Center for the Protection of Critical Resources (ECCRP) has been established in Brussels, Belgium. The ECCRP will offer to high-level decision makers and specialists next generation training and demonstrations for critical resource protection for sectors ranging from energy to banking and water distribution. The center will offer two types of training. The first training mode is Security Enforcement Training. This will be provided by high profile international experts in the field of critical resource protection. Most interesting is that the ECCRP will employ proprietary technology for Security Awareness Training in the form of the VisioSpace simulator. This simulator will allow easy navigation for participants into very large scale 3D worlds where critical infrastructure will be represented and integrated. The simulator can model, through three dimensional imaging, an entire city or even a country. Running through this virtual world, critical infrastructure networks are presented as realistically as possible. This technology can simulate all of the important protocols and information flows used in the management of energy and power resources such as electrical networks, water systems, oil and gas pipelines, telecommunications systems and financial systems, along with their underlying technologies. SCADA, TDM, VOIP, MPLS, SwiftNet or X.25 will be simulated with this simulator. Through this simulation, the energy sector will be able to merge with other critical infrastructure actors, understand its dependences and interconnections, and analyse how it can be attacked and defended. The center will be a central hub for all actors and a stand-alone institution for those responsible for preventing and responding to cyber-attacks and cyber-terrorism.

The VisioSpace simulator's key value added is not only in its unique combination of virtual reality and virtual networks, but also its ability to abstract assets. Computer programs creating virtual networks, such as a SCADA network, already exists on the market, however the majority of them are static and don't have a powerful 3D virtual visual interface, making them hard to understand and use for non experts.

On the other hand, virtual reality engines modeling an electricity network or a city do exist, but the simulated virtual networks are generally empty and lack interface and connection to the underlying networks supporting them. By way of example, an object in VisioSpace won't simply represent a power plant, but will also be associated with a complete simulated network supporting the plant: SCADA production networks (with simulated Windows/UNIX/real time system, PLC/RTU devices, OPC servers etc), office network (desktops, printers, applications), management networks, VPN connections, firewalls, Intrusion Detection System etc. In short, any system can be integrated into this high-level virtual network for the protection of critical infrastructure.

### **On Training**

How is training envisioned at the ECCRP? As an example, a SCADA engineer and the Chief Financial Officer (CFO) of a

company will be involved in VisioSpace training. VisioSpace can model the actual space and the networks integrating the cross-functions of these individuals where both actually work. The creation of an accurate network space requires input from the participants for networks utilized in daily practice so this data can be input into the simulator. The SCADA engineer will interact only with the common networks shared between himself and the CFO; he won't be able to access any other critical infrastructure network such as telecoms, finance, etc. ECCRP instructors explain how the network can be attacked, and then the SCADA engineer will act out in real time his response to network disruptions through the training exercise. He therefore will interact with the simulated computers and network devices of his/her company. In a sense the SCADA engineer will control the simulated network and will attempt to disrupt or protect it, depending on the scenario. Concurrently the CFO will be able to monitor events via his/her own virtual reality interface. The CFO does not know how to attack or protect the SCADA network and thus won't interact directly with the simulated network. However, what the CFO can do is to monitor the effects of network disruption in virtual reality. If the SCADA engineer successfully manages to take down the network by shutting down a critical system, the CFO will see the virtual consequences of the event not only on his activities but also on the continuity of the larger telecom and financial network feeding his activities.

Finally, the exercise teaches one how to react. In this case, the CFO can team up with the engineer defending the network and give him suggestions on how to minimize the consequence of the attack. It becomes here a policy exercise. Ultimately, the scenario could include people from the energy sector, telecom sector, finance sector and transportation sector. They all participate together in the same scenario. VisioSpace is so modular that it does not even need technical people attacking the critical infrastructures. This can be automated by VisioSpace, a feature which is particularly helpful for management and upper-level decision makers outside of technical IT domains.

Government representatives, i.e. Homeland security professionals, can also participate in VisioSpace training with a level of unprecedented detail. Training then becomes policy oriented. After each training exercise, the simulator renders a detailed report on the session's activities, reviewing what happened during the training exercise itself.

The ECCRP has lodged its first center in an old World War II bunker in the heart of Brussels, but the impact of its training will hopefully have global value. One of the goals of ECCRP is to open other similar centers in other countries once the Brussels center is well established. Other centers will then benefit from ECCRP trainers and the VisioSpace engine. Other countries will be able to offer advanced trainings similar to the Brussels one and modelize their own city or country.

*Francois Gaspard and Alain Hubrecht are co-founders of the European Center for Critical Infrastructure Protection. Additional information on the ECCRP can be obtained by email: [contact@eccrp.com](mailto:contact@eccrp.com)*