Global Information Assurance Certification Paper

PHYSICALLY SECURITY CONSIDERATIONS FOR HIGHLY DISTRIBUTED AUTOMATION NETWORKS

30 JULY 2004

TABLE OF CONTENTS

ABSTRACT

This paper aims to address the physical security requirements of highly distributed automation networks. Given the number of networks that span hundreds of small sites and nodes, remarkably little information is available to provide security administrators and planners with the tools they need to secure these resources. In an effort to provide this information, this paper will avoid focusing on specific brands of technology and will discuss the additional factors that need to be considered when large numbers of remote sites are being secured. This will help security personnel who have experience securing smaller sites to successfully apply their knowledge to highly distributed networks.

The specific areas that will be addressed include power, intrusion deterrence and detection, fire, flood, and temperature variances. As well, time will be spent examining different means of monitoring and logging information from these resources.

1. INTRODUCTION

In a perfect world, all networks would exist within neatly defined perimeters that could be easily checked by a security professional. In many cases today, this is the case. Most networks are limited to a single site, or perhaps two or three sites. Most importantly, the sites are commonly staffed, providing a security specialist with individuals that he can rely on to provide information about the status of a site. Even untrained, having someone available to be the 'eyes and ears' of a security team can be invaluable.

As noted though, not all networks are easily defined, nor are they limited to staffed facilities. In the case of distributed automation networks, a security designer may be presented with dozens or hundreds of small, independent facilities. Each of these network nodes could contain equipment that is critical to the safe operation of the network.

This paper will leave aside the challenges of securing the equipment at these field sites at an IT level and will focus on physically securing them. Following the security maxim that the best way to gain control of an asset is to simply possess it, we will look at the various means available to keep your technology out of the hands of someone else. This is a relatively simple task in a traditional networking scenario. If the equipment is locked in a secure server room with limited points of entry and exit, and the building itself is secure, then it should remain safe. With distributed networks spread over hundreds of kilometers, even simple physical security becomes a difficult task. Assume each field site has one entrance and exit. Then assume two hundred field sites, many of which are not regularly visible to your personnel and the challenge becomes apparent.

Before beginning though, it is important to note that physical security does not stop at simply preventing the theft or destruction of equipment by a human attacker. Security is built on the C-I-A triangle: Confidentiality, Integrity, and Availability. At the physical level, threats can include theft and manual destruction, but also extend to fire, flood, lack of power, and other natural and unnatural occurrences. Any of these could result in a failure to maintain C-I-A, and thus a security failure.

2. WHAT IS SCADA?

Highly distributed and unattended networks are not uncommon. Most of us rely on them every day without thinking about them. Examples include Point-Of-Sale systems (Interac), ATM machines, and similar. With each of these networks however, the failure of a single node is not necessarily critical. It may be inconvenient, but it would not result in a catastrophic outcome. As well, these devices are normally considered to be attended devices. Most ATMs are not located somewhere out of sight. In the rare cases when they are, some of the security measures we'll discuss become appropriate.

Instead of looking at these networks, this paper will focus on more critical infrastructure networks. These highly distributed, unstaffed networks are depended upon for reliable, secure service more than almost any other, and yet operate in conditions that make security difficult. Supervisory Control And Data Acquisition systems, also known as SCADA systems, are responsible for the operation of major gas, liquids, water, and electrical systems across the world. Unlike the loss of a single ATM, the violation of a remote SCADA monitoring site could result in the disruption of resource distribution, or possibly in an ecological disaster. For this reason, SCADA will be used as our primary model for this paper. Given the consequences of a security failure, this example will allow us to fully explore every aspect of physically securing an unmanned, distributed network. Should you encounter a situation where a failure is less significant, you will be aware of the tools that are available and can pick and choose from among those we discuss here.

Before we can analyze SCADA security, it's important to first have an understanding of the nature of SCADA. From there, we can begin to derive the vulnerabilities and threats involved.

A traditional SCADA network is intended to allow for the centralized command and control of a large range of devices scattered over a wide area. Those devices can be of any type. In gas pipelines, it's common to control pumps, valves, and to receive data from different types of meters. In an electrical grid, transformers, breakers, and generators might be your devices. While their specific nature is generally irrelevant, there are a number of things that they have in common.

Firstly, the devices are relied upon to operate when commanded remotely. This is critical when you consider what is at stake if they do not. Furthermore, every device on a SCADA network is expected to communicate accurately with the central operations center. If a device does not register an error, then the values that are reported to operations are assumed to be valid. Decisions will be made based on this information and the presence of invalid information is potentially even more damaging than the lack of it. For this reason, security is paramount in a SCADA network.

Each network node may take a different form. A meter may simple be a small remote terminal in a weatherproof housing located along a pipeline. Communications can range from radio and dial-up over the PSTN (Public Switched Telephone Network) to dedicated lines or WAN connectivity. At the other extreme, some SCADA nodes will consist of remote servers gathering information and relaying it to the operations center after processing. These sites may be located in an outbuilding with greater facilities available to a security professional. Conversely, the hardware present may be more valuable, more difficult to replace, and more significant if it is violated by an attacker.
An additional consideration is that many of these devices will be located far away from any communities. While this could be considered positive as it makes casual tampering less likely, it also makes it much easier for the facilities to be reconnoitered, and then exploited.

Finally, the scale of a SCADA network can never be forgotten. Any of these challenges could be considered relatively manageable for only a few facilities. That's something that security staffs cope with regularly. When the number of remote devices enters the hundreds, or thousands, it becomes a potential nightmare. The security design that is put in place must not only protect the assets, but it must not be harder to manage than the network itself. It must be far simpler and run with even greater autonomy.

3. HOW VULNERABLE IS SCADA TO PHYSICAL ATTACKS?

In assessing the vulnerabilities and threats that we have to deal with, it is important to confine our work solely to physical security. With highly distributed networks, it is very easy for task creep to take place. If security measures depend to an extent on communications, it's possible to quickly find a security team attempting to secure those communications as well as the physical structures. While it is important to secure the apparatus responsible for communications physically, any planning beyond that is outside the scope of our initial task. Physically securing a highly distributed network is complex enough without adding to that complexity.

When examining remote devices, there are three potential negative states. Our positive state is a fully functional device. The first negative state assumes the total loss of the device, requiring replacement or reconstruction. The second

state is loss of operational control with the potential to reacquire control remotely, or with limited local intervention. The third state assumes loss of control of that device while it is capable of operating.

The first two states are the result of a wide range of threats, but can generally be determined quickly. If a device drops out of communication, the physical security sensors should be capable of determining the cause in short order. If the sensors drop offline as well, then it narrows the number of options considerably. Based on an analysis of the communications link, a skilled operator can determine if there has been a communications failure, or if the device itself is offline. From that point, security logs should allow you to determine the cause of the failure. The third state is more challenging to determine. If executed properly, an attack that intends to leave the device operating should not result in any operational errors on the SCADA network. This means that any alarms at all will have to come from the physical security apparatus. Assuming that the attacker does not commit any acts that would result in device errors, they could conceivably remain in control of the device for an extended period without detection unless physical security prevents them.

Now that we have established the potential outcomes, it's necessary to look at some of the physical threats. Given that we're dealing with complex electronic devices, they may seem quite logical. Nevertheless, based on the distances involved and potentially slow response times, even something that would be an irritant in a traditional network can be a serious threat.

The first threat is a loss of power. The further away from populated areas the device is, the more likely that this will occur. While lack of power can prevent the operation of the equipment at a remote site, it also has the potential to render advanced security technologies equally worthless. It is important to consider the likelihood of a power outage when assessing the type of physical security to be deployed at a site. The components at the site must also be considered in this assessment. While some smaller sites can run off of solar cells, some are of limited value and will only have primary power. This significantly limits the security measures that can be put in place. In cases like these a security professional is generally prevented from using technologically advanced methods to secure a device. Fortunately, smaller sites of this type will also be of limited value and will likely not be your highest priority. Furthermore, if a high-value asset is close to several lower value sites, it is possible to take advantage of security tools at the more advanced site.

After looking at the power situation of a given site, the next issue to be addressed is physical intrusion. This applies no matter what the size or type of site and is perhaps the broadest category in terms of countermeasures. It's also one of the most significant challenges in terms of deciding on just how much to invest in security.

The remaining major vulnerabilities relate to natural forces. The first and potentially most destructive threat is fire, both natural and man-made. In a traditional environment, it's likely that a staff member would be close enough to recognize the signs of fire and sound an alarm. As well, it's likely that some form of fire suppression system would be in place to protect your assets. In a remote site, none of these can be safely assumed unless they're deliberately setup as physical security elements.

Closely related to fire is the possibility of temperature shifts. While some remote hardware is deliberately hardened against the elements, remote servers and sensing devices may have limited operating ranges. In these cases, temperature monitoring may allow for problems to be recognized in advance and then appropriate measures taken.

The final physical threat that will be addressed is that of flooding. Again, while this is not something that commonly occurs in a corporate environment, it is not unreasonable in a remote area. In many cases, outbuildings are not designed with the same integrity as offices and you will not be able to rely on someone else's planning to protect network assets.

4. POWER

Technology almost always relies upon power in order to function successfully. While this seems to be a simple statement, the further technology is moved from inhabited areas the more challenging this becomes. In an urban environment high power uptimes combined with rapid responses to failures are common. In these cases, the power company can usually be relied upon provide consumers with any level of redundancy they require.[1] In outlying areas you may find that your company must power your remote sites, or in the best conditions, have tenuous lines to the existing power grid.

From a security perspective, this can be both beneficial and problematic. If the power that's been run out to a specific site is reliable and robust then you have a fair bit of flexibility in choosing what equipment is deployed their to combat some of the threats that we'll discuss later. Unfortunately, many remote sites will be powered by limited systems that may only provide enough energy to run the existing equipment. This power may also be in a format that's not entirely compatible with commonly available security devices.

Based on this information, you may already face limitations on what you can do to guarantee uptime on these devices. For small devices that are kept outdoors or are located in a secured housing but have outside access, solar power may provide a degree of fault tolerance. It's questionable as to whether or not this will provide sufficient power to both run the device and any advanced security technologies.

[1] Siemens, p. 15

In larger remote sites where more advanced systems may be running, power may be more readily available. If servers are deployed then the uptime requirements are likely higher as is the value of the asset. In addition to warranting more advanced power backups, this also means that there will be sufficient energy available to run appropriate security devices.

Redundant power at a mid-sized remote site will likely take the form of UPS (Uninterruptible Power Supply) backups. Designed to provide backup power for standard AC equipment, UPS' are rated on the features they offer as well as on the amount of power they can generate in response to a failure. Before installing them though, it's important to determine the power requirements for the equipment in question as well as any additional tools that may need to run.[2] If you're installing the backup power as part of the security system, or as part of an initial build, this is a straightforward task. If you're upgrading the security though, it's important to consult with the individuals responsible for the existing systems. Every device you add to the facility that requires redundant power will reduce the duration of the UPS backups, possibly impacting operational capabilities. In this case, the costing for the security upgrades would have to include additional backup power.

When planning backup power through UPS, there are several factors to assess. The first is how long you need to power the equipment. This will be different for each facility and largely depends upon the equipment housed there. Once you know how long the equipment should be able to last without external power, you can determine how much power each device will draw. This will help you decide on what sort of systems to put in place.

Before deciding to put your security devices on the same backup systems as the rest of the equipment, make sure that their uptime meets your requirements. If the networked sensors and servers are only expected to run for 20 minutes and you anticipate that there could be outages that last longer, you may want to provide independent power for the security systems. While this may be expensive, it's important to consider that even if the distributed network can run without the SCADA sensors on the odd chance they have a prolonged outage, you may not want that equipment to be at risk. This will become more apparent in the following sections. Always keep in mind that any electronic security measures will cease to function as soon as they lose power and any security logging mechanisms will no longer run. A full outage of several hours may place thousands of dollars in equipment at risk. A good benchmark is to take the time that the entire site can run on backup power, add any additional uptime for the security devices, and make sure that the total is greater than the time you will require to get a repair or guard crew out to that site. Remember to include any time required for managerial approvals or any other procedures to be followed as well. Once you have personnel onsite, your security risk drops dramatically as you now have 'eyes-on.'

[2] UPS Selector Express

(PROBLEM DETERMINATION TIME)
+(PROCEDURAL TIME)
+(TRAVEL TIME TO SITE)
=TOTAL BACKUP POWER ESTIMATE

In larger remote sites, there may be sufficient power needs to justify a diesel generator.[3] This is the optimal case for security. Not only does the generator likely generate the power needed for any security systems over an extended period, it also requires regular maintenance visits. This guarantees a minimum frequency of staff visits to the facility. If those personnel are trained to look for signs of security risks or intrusions they can be a powerful asset.

Once provisions have been made to provide backup power, maintaining the availability of a remote asset, it is time to look at making sure that power is supplied to all key systems. If the facility is on a WAN link, it is highly likely that communications will remain functional along with the remote hardware, allowing you to not only track the status of the backup power but also to monitor security systems through the outage. If the communications are handled through a dial-out modem or radio, it is important to ensure that those systems will allow for communication with security devices as well. As most companies don't want to run multiple communications links out to a single site, it is likely that security sensors will send data back along the same link that is used for the SCADA distributed sensors. Since the site backups will power this link, it may lose power as soon as the main backups expire. If you have found it necessary to provide separate power to the security sensors, do not ignore this critical piece of infrastructure. If it is impossible or economically not viable to power the communications system independently, you may still benefit through the maintenance of local security measures, but you may find that you're blind to events at the remote site until after they have occurred. If communications is critical and you feel that the existing communications infrastructure is unreliable, then consider a cellular or satellite-based communications system with its own battery.

The key points to remember when assessing the power needs of a particular site can be summarized as follows. If the site is small enough and has minimal value security may need to be limited by the available power in an outage. For larger sites, determine the uptime requirements and then the overall power needs of the existing hardware. If the uptime requirements are not sufficient to maintain adequate power for security systems, consider running security off of a separate power backup system. Finally, make sure to consider the power requirements of any equipment that is required for the security apparatus to function during a power outage.

[3] StandBy Generator Systems

5. INTRUSION:

Now that we have established that a remote site will have power available both during normal operation and in the case of a power outage, it is time to determine the different types of security equipment that should be installed. In keeping with the general nature of this paper, specific brands will be avoided, focusing on different technologies that are available through multiple suppliers. The first type of threat to be examined is that of physical intrusion, or physical destruction. Our focus will be on preventing intrusion and providing warning of attempts to otherwise violate the integrity of the site. Extreme situations such as the use of explosives to destroy a remote site will be touched on only briefly as there is little chance of it happening to most facilities and even less that can generally be done about it. Instead, emphasis will be placed on preventing deliberate intrusions with the intention to violate the confidentiality, integrity, or availability of the equipment at that site. Given that in a highly distributed automation network, most sites contain sensors that provide critical information to the operations center, loss of any aspect of C-I-A could be significant.

The first area that needs to be examined is perimeter security. While the size of the perimeter changes with the size and type of site, the goal is the same. Prevent an unauthorized individual from entering and if this fails, notify security staff of the failure.

The most common and by far the simplest mechanism for keeping unauthorized personnel out of a remote facility or device is a lock. If the device is in a small housing, it may be a lock on the case itself, and in the case of a larger outbuilding or higher value asset it may also include a fence with a locked gate. While this sounds quite simple it does form a significant deterrent to a casual attacker. Presented with a challenge, they may seek a softer target. This will not stop a determined attacker however. Additionally, one of the most notable failings of locks is that it's hard to remotely determine if they've been cut, jimmied, or otherwise opened. In the case of a remote sensing site, it is important for security staff as well as operational staff to know when the integrity of a particular device has been violated. Once perimeter has been breached, the potential for loss of control of that device increases dramatically. Data also becomes questionable as access to the physical device sending it is one of the best ways to successfully undermine many communication security measures. For this reason, any locks employed should have a means by which to inform the operations center that they have been opened. Many field sensors or remote terminal units (RTUs) are equipped with locks in their housings that will send out an alarm if they are opened. This makes them fairly easy to monitor. If an alarm goes off, the data coming from that device can be flagged as questionable and a team can be dispatched to investigate. As these devices are of limited value and complexity, this may be the only form of security on the device itself. Fencing, cabinets, or other safeguards may be put in place but due to power limitations and cost effectiveness these additional protective measures are usually not intelligent and

simply serve as deterrents. [4] The use of barbed wire or electrification should also be considered for high-value sites, as they offer both psychological and physical deterrence should an attacker consider attempting to bypass a fence or wall. More complex remote sites require more complex physical intrusion protection. When costly devices are deployed to remote sites, whether they are remote servers, pumps, generators, or simply expensive sensor platforms, outbuildings are often constructed. These offer more protection that a simple RTU housing does and serve to prevent the elements from damaging equipment that does not normally have a housing. Buildings of this sort can range from small shacks designed to protect a field information gathering device or data concentrator up to multi-room pump houses that can also provide working areas for staff when they are in the field as well as workshops and sheltered server-space. Protecting the equipment at these locations is often a high priority not only due to its higher value but also due to the role that it plays in the operation of the network. The challenges facing a security professional are greater than they would be for an equivalently sized office space. These facilities may be left unattended for weeks or months and could provide many opportunities for the theft or alteration of data if they are successfully attacked. As an example, were attackers able to access a server located in a field station (or even a networked workstation reserved for field technicians) they could potentially have days or weeks to crack the password for that device. Provided that they didn't disrupt the operation of the facility itself, their attempts could go unnoticed. To a great extent, network and communications security work has a role in preventing this from happening. Log analysis and Network and Host Intrusion Detection are intended to prevent just this sort of unauthorized access. Nevertheless, the attacker gains a dramatic advantage when they can sit down at the console of a networked device, and they have automatically circumvented significant elements in a defense-in-depth strategy (Firewalls, proxies, some elements of Network Intrusion Detection Systems [NIDS], and many aspects of Host-based Intrusion Detection Systems [HIDS]).

In securing these structures, the first steps remain the same. Put physical barriers, such as fencing, doors, and locks in place. Establishing electronic alarming on gates and doors to notify a central location if these perimeters are violated.[5] This can be as complex as using a passcard-style access control system that is linked to the entry control mechanism at the corporate offices, or as simple as an infrared beam that is broken when the door is opened, sending out an alert.[6] Provided that power is available as was discussed above, this should be sufficient to warrant an investigation by a live staff member. If communications are lost with a field site without a reasonable explanation (or for an extended period) then human intervention is necessary in any case, limiting the effects of cutting communications to circumvent entry alarms. Whenever possible all entry alarms should be logged both locally and remotely. In the event

[4] Qinetiq, p.2
[5] Public Works And Government Services Canada, p. 1
[6] Chubb, p.2

of a communications failure, the system should remain in an alarm state until it is commanded to stand down by an authorized individual. These logs, like network activity logs or the access logs for a corporate headquarters, should be protected and stored in accordance with the regional legal requirements.[7]

At this point, we've discussed basic measures to prevent an intruder from gaining access to your remote facility. We've also highlighted one system (passcards) that allows the logging of legitimate entries as well. For smaller sites however, this is not a viable option both due to technical complexity and cost. In these cases, it is advisable to maintain written access logs. As well, when a legitimate entry alarm is generated on a smaller site such as an RTU the security or operations employee who acknowledges that alarm should be responsible for noting the individual accessing that site or hardware and their purpose.
A major consideration with an unstaffed site is that if it is physically violated, security response times are high and the potential for an attacker to do considerable damage increases the longer they have access. This makes internal security a priority as well. In sites with one room in an outbuilding, or a small housing, this security comes almost entirely from the IT security on the devices housed there and is beyond the scope of this document. In larger sites this does become a concern.

The simplest way to frustrate an attacker who has bypassed your perimeter security is to apply defense-in-depth. Add more locks, whether they are cardlocks, keylocks, or padlocks. Given that your staff will not be using the site frequently, the inconvenience is minimal to them but can provide you with valuable time to respond to a breach. If the site is large enough and valuable enough, interior cardlocks may be feasible but in most cases this will not be an option. Always remember that your primary goal once the perimeter has been broken is to prevent or minimize damage until staff or enforcement officials can respond.

The problem of long response times makes it possible for an attacker to penetrate your site, do what they intend to, and then escape before you can intervene. Depending on the type of site, you can approach this threat in different ways. Small sites can be examined by technicians for signs of tampering or replaced as a precaution and Intrusion Detection staff can investigate electronic attacks. The physical breach will give them the evidence they need to commence an inquiry. Unfortunately, if the attacker takes all evidence with them (or takes the object of the attack) or simply examines information that is in plain view, you have little to go on. Unlike a staffed site where investigators can rely on witnesses to provide information, a remote site will often require technology to minimize this vulnerability. The value of the site will determine if this is applied or not.

[7] Department of Energy, Office of Energy Assurance, p.5

Traditionally, video is used to record persons entering and leaving a facility. With recorders often stored in a secure room elsewhere on-site this is not a major challenge or an impossible cost outlay and can lower guard costs.[8] Remote sites make video deployment difficult. While cost is a concern due to the number of sites that may be involved, video surveillance faces obstacles even at high-priority sites. Local storage of recorded data is a risk as an attacker could simply remove the recording equipment to cover their tracks. Due to generally limited bandwidth, many sites cannot sustain a video feed to a central monitoring office. As well, traditional SCADA systems have many remote resources contacted only when information is required or when a command is to be issued, in a configuration known as host-poll. These factors combine to make any sort of internal monitoring near impossible. Fortunately for security personnel, broadband TCP/IP access to remote facilities is slowly becoming more prevalent, providing more options. Bandwidth is still an issue though, and may require advanced intelligent video technologies for this to be feasible.[9]

In cases where the bandwidth is available and connectivity is present, security cameras can be deployed. These can provide excellent evidence for authorities performing investigations. With recent advances in wireless video technology as well as increased miniaturization, cameras can also be placed more discretely than ever for lower costs.[10] With unstaffed sites, using motion-activated cameras can save communications time.[11] As well, it may not be necessary to continuously monitor feeds. Given that the sites involved are not expected to have anyone in them, simply storing video data on a server may be sufficient. When an intrusion alarm does sound, a security team member can then log into the feed and review any older footage. While this will not allow you to prevent the intrusion, it can provide information for your staff when they do reach the site. This information can also be provided to any law enforcement or local security personnel who are asked to investigate. This may enhance their ability to safely apprehend the individual responsible for the breach. The primary purpose of this data is to provide legal evidence of a criminal act, so always consult legal counsel both for your home region and for the area that each remote site is located in to ensure that video surveillance is legal, that all signs and warnings are properly posted, and that the information that you receive from the site is stored so as to preserve the integrity of the data in the eyes of the law. While it seems like a great deal of work initially, it is worth it in the long term.
If you are putting video monitoring in place, maximize your utility through careful placement. Minimize any terrain features (landscaping, garbage bins, or even vehicle parking) that could allow an attacker to approach your facility unseen or otherwise provide even temporary cover.[12] Even though a single point of entry seems simple enough to cover with video, consider consulting a professional

[8] Chubb, p.2
[9] miniMax, p.2
[10] Linksys, p.1
[11] miniMax, p.2
[12] Qinetiq, p.2

installer as they can suggest ways to prevent blind spots and to minimize shadows and glare. When you are deploying video surveillance, it is important to make sure that you provide adequate lighting for the video feed.

In extreme situations, far more advanced security measures can be put in place, beyond locks and video. While these technologies are attractive and powerful, for the vast majority of remote distributed computing sites they are not appropriate. You will be far more likely to see advanced systems used in protecting staffed facilities containing extremely sensitive information. Much as you may be tempted to over-secure your remote facilities, always review what you will be able to do with any information you receive from the site and what affect it would have on minimizing a vulnerability. Locks will deter or slow an attacker. Video can provide evidence of an attack that may not affect technology in a way that shows up in network intrusion logs. Advanced internal intrusion detection systems based on a network of infrared beams will tell you what you already know, especially in a site that consists of one or two rooms. This may seem simple, but proper employment of basic technology is more crucial in this case than expensive, more complex technologies.

6. FIRE

Much like intrusion detection, fire detection becomes both more complex at a remote site and a little bit simpler. The advantage to an unstaffed facility is that you do not normally have to concern yourself with evacuation issues. Escape routes must be planned if personnel do ever work there and the structures must meet fire codes, but it is not as complex in that regard. Further, small sites that consist of a single RTU or device do not normally need fire protection. If a fire approaches and is sufficiently hot to destroy the housing, then the unit must be replaced. Security staff will likely find out about a wildfire approaching their site through media as well as local fire departments and should be able to act accordingly, either protecting small devices or moving them out of the area. This leaves larger, more valuable sites that are usually housed in outbuildings. In case of wildfire, the structure itself may be more survivable and security personnel would be notified along with operations staff in advance of an actual threat. The greater concern is a fire within the structure. With no staff present to recognize any indicators, an alarm system is the only reliable way to detect a problem early enough to prevent major damage.

Alarming can take multiple forms when it comes to remote sites. At the most basic level, the alarm should sound to warn anyone in the facility (authorized or otherwise) to evacuate. It should also contact the local fire department so that they can respond to the fire appropriately if at all possible. Both of these apply equally to staffed facilities. Remote sites must perform beyond this level. A fire alarm in at a remote site should alert security personnel and operations staff. Operationally, this will make managers aware of the potential loss of that resource as well as the possibility of inaccurate information as temperatures

affect instrument or device performance. From a security perspective, an alarm has different requirements.

- Security staff need to be aware of a fire when emergency crews trip intrusion alarms
- If emergency crews do not have building access, it should be opened remotely if possible to prevent damage to the structure and locks
- Security personnel should be dispatched to the site to:
    - Maintain site integrity once locks and sensors are disabled
    - Make sure that emergency crews do as little damage as possible to equipment – this role may be shared with field operations staff
    - If appropriate, examine the site (when declared safe) to determine if any secure materials or equipment have been removed, suggesting arson. This allows the company to react as quickly as possible to any information that may no longer be confidential
- Security staff should be prepared to provide whatever information (security logs, video) to the investigating authorities in keeping with regional laws and corporate policy

The nature of the fire suppression equipment employed in a remote site is also different from that used in a staffed facility. While basic electrical fire, or in the case of industrial hardware, chemical fire suppression systems are appropriate, some may be dangerous. For many staffed server rooms, Halon extinguishers may be employed. While normally fatal to anyone in the room after they are set off, these extinguishers will often be triggered via a manual button. This allows employees to verify that a room has been vacated before using the extinguishers. Remote sites make it very difficult to guarantee that a building is not occupied. Depending on local laws, a company may be held responsible for the death of someone whether or not they were actually legally allowed to be in the site at that time. For this reason, if you cannot be certain that a facility is empty, less dangerous fire-suppression equipment may be better suited. Even if video is in place at the site, it may be obscured by smoke it an emergency. If you do choose to install Halon or CO2 extinguishers, consider making sure an alternative is available. Also, except in very rare cases fire suppression system should not be triggered remotely. Operations personnel may not be fully aware of the situation at a remote site and could put the lives of emergency personnel in danger if they make use of potential lethal suppression systems from offsite. As an alternative, consider installing a local control at the site to allow fire crews to manually trigger a suppression system after they've investigated the site. If this is done, a less harmful fire suppression system can be used automatically.

7. FLOODING

The counterpart to fire in physical security is flooding. Fortunately, unlike a fire flooding is normally a slower process. This can provide you with the warning you need to dispatch crews to the site to investigate and work to resolve the problem.

When most electrical or equipment rooms are built, they are designed to withstand an intake of water. Equipment is usually racked and outlets are positioned higher on the walls. While this is sufficient for a staffed site, additional precautions must be taken for unattended installations.

First of all, examine the terrain around your facility to determine the likelihood of flooding and try to find an approximate maximum depth. Use this figure as a guide for the positioning of interior equipment and if flooding is likely then consider mounting any electronics on walls or higher in racks. Adding an additional rack may be cheaper in the long run than replacing equipment damaged because it was mounted below the floodline. As well, if a site has been built with the potential for water to rise to a high level, consider altering the ground outside the facility to channel water away. This may prove to be more cost-effective than trying to redesign the structure or to relocate internal equipment.

Any security sensors that are in use for either fire detection or intrusion detection should also be mounted above the likely maximum height for water. If those devices are submerged it will certainly affect their ability to protect the site and may prevent you from monitoring that site.

In order to make sure that security staff are aware of flooding in sites, it is important to place hydro sensors in remote structures and on any freestanding RTUs that are of sufficient value. These sensors are designed to operate under water and can signal an operations center when flooding does occur. The use of multiple sensors at different heights will allow staff to gauge the depth of the water and determine how much time may be available at a site before critical equipment is submerged.

Most sensors of this type will communicate over TCP/IP to a central monitoring station. This means that you will need to provide them with some means of communication for them to function. As most remote sites will have some connectivity this is not normally an issue, but it’s important to make sure that any communications equipment is stored in a location that will remain dry. The same applies to power systems. If the facility is run off of grid power then work to ensure that UPS are stored near the tops of racks. Once communications is lost all security devices become local only.

It is important to consider that flooding may not only result in water damage. Even a relatively small flood can bring about loss of power or electrical fires that can put other equipment at risk. Staff monitoring remote physical security sensors should always watch all aspects of a sites’ status as it is very easy for one form of physical threat to transition to another quickly.

For minor floods, humidity sensors should also be investigated. Often easy to combine with water sensors, they may alert you to a level of water intake that is not sufficient to register as a flood but is still endangering your equipment.

8. TEMPERATURE

Last among the key threats to be examined is that of temperature. While this is largely a moot point when it comes to standalone field devices such as RTUs and PLCs it can be critical in more advanced field sites. In order to cut costs, forward-deployed servers or data-concentrators may be placed inside existing outbuildings. These structures may not have adequate ventilation or cooling depending on exterior weather conditions. Further, if other equipment is also in use in those sites it may contribute to problem temperatures.

For the most part physical security concerns will be focused on higher than normal temperatures. Even given limited insulation it is difficult to reach temperatures that will adversely affect electronic equipment provided that they are adequately sheltered. However, specific regions will require temperature maintenance beyond cooling and this should not be immediately discounted. In addition to concerns regarding ambient heat from external sources penetrating a sealed building, devices within the structure also contribute to the internal conditions. Modern workstations and servers can produce high amounts of heat and without adequate ventilation this can build up over extended periods. Further, the use of heavy equipment such as pumps can cause temperatures to skyrocket. A building that has been designed around a turbine pump is a good example. While the machinery housed in the building initially is manufactured to withstand the temperatures they cause for long enough to allow them to cool down, other devices may not be able to handle extremes. More than simply threatening the equipment itself, information integrity and availability are both threatened by high heat. Many IT professionals are familiar with the potential for errors to be generated by devices operating outside of their limits…in the case of SCADA unless the temperature variation is recognized that data could be considered valid by operations staff. This potential for loss of integrity easily has as much potential for long-term damage as the actual loss of the equipment, if not more.

Most servers are designed with internal temperature sensors that can notify an administrator of any problems. These should be monitored at all times just as in a production server housed at the corporate server farm. Unfortunately, these sensors can be affected by temperature changes and they may also be less reliable over a SCADA link. Many of them are designed to be monitored over high bandwidth links as part of a broader administrative connection.

The installation of temperature sensors with associated alarms can provide an additional level of redundancy to prevent the loss of availability or integrity. Designed to communicate over low-bandwidth connections and more

importantly, designed to operate in the temperature ranges where traditional IT equipment becomes unreliable, these sensors can form a warning system that allows operations personnel to treat data as questionable until a site can be investigated.

The first step in preventing temperature spikes from affecting IT equipment is to avoid putting sensitive devices in areas that are prone to extreme temperatures. To borrow from the previous example, do not put a data concentrator in with a turbine system. If it is unavoidable, store the more sensitive equipment in a separate room and employ climate control systems to moderate the temperature changes. Even if air conditioning systems are in place, temperature sensors do not become redundant. Older climate control systems may not be equipped to communicate with a monitoring station on their own so temperature alarms may be your first indication that there is a problem with a field HVAC system.
Like the other sensors described in this paper, temperature sensors rely on communications to notify a monitoring center of problems. In the case of high temperatures though, it may be feasible to shut down local systems to prevent damage. In the case of fire, flood, or power failures this is not a particularly useful option but in the presence of high or extremely low temperatures these measures may be able to preserve your hardware investment.

9. BRINGING IT TOGETHER:

Each of the above vulnerability assessments has discussed the use and placement of specific sensors within sites. While each section has briefly touched on some of the tools necessary to monitor them, this is important enough to warrant a section of its own.

While SCADA systems and other distributed networks are slowly migrating to TCP/IP based communications, many still remain linked by dial-up or radio-based connections. From a security perspective this means that communications is not 'always-on.' Security devices must then be managed very differently. They must either be able to communicate on their own or to initiate communications when necessary.

The first option is the simplest but also the most expensive in many cases. Installing dedicated communications equipment is not a cost-effective approach to installing security systems. Nonetheless it may be necessary if the communications media used by the existing equipment at the site is not readily adaptable to the physical security systems installed.

The second possibility is that you can take advantage of pre-existing infrastructure. This is fairly straightforward with phone-line access, which is quite common. Many security sensor systems contain modems that can be tied in alongside the field systems. While the line would be busy in the event of a security alert, the SCADA system will retry in a few seconds and the security

alert is likely of greater importance. Radio and microwave-based transmissions are far more challenging to adapt for security systems. With smaller RTUs the sensors can sometimes be tied into the device itself but otherwise the transmission protocols are usually proprietary and do not handle additional data easily.

In those cases, the introduction of a cellular modem may be a cost effective opportunity. In the case of extremely remote sites, satellite modems are also a reasonable option. The usage is extremely low due to the infrequent nature of alarms (or so it would be hoped) and deployment costs are decreasing rapidly. In terms of sensor management there are a number of different options available. Many sensor systems have a concentrator unit that takes the information provided from the input devices, process it, determine if alarms should be triggered, and then send that information out. These alerts can be as simple as a phone call to a specified number reading a pre-recorded message ("There is a fire alarm at site 17B")[13] or as complex as sending a signal to a central monitoring station and posting a status update on the web using an internal webserver.[14] Different approaches will suit your specific needs. In the case of a smaller network it might be sufficient to have emails sent out to an on-duty staff member or a phone message called to a company cellular phone. This allows an on-call employee to get immediate notification of a security issue wherever they might be. This is particularly good for companies that can't afford to keep a 24-hour security station staffed.

For larger companies that can keep an employee at a central monitoring station at all times, it is usually more informative to have a distributed security monitoring system that will report problems to a central location. This may be a hardware unit equipped with both dial-in and Ethernet connections that tracks data and then displays it to a graphic front-end or it could be as simple as a software package installed on a pc that takes incoming data and logs it. Both offer significant advantages over the simpler call-out system in that they log data, can easily perform trending, and can accept input from multiple sources simultaneously. They are also usually capable of presenting more detailed information to the user rapidly. As well, many of the more complex monitoring systems will perform call-outs or send email messages or pages to an on-duty number based on specific events.[15]

Selecting the monitoring system to be used for your distributed security sensors is likely going to be the first task you must accomplish. This will determine the type of local concentrators you install at your sites as well as any communications infrastructure that must be installed along with it. Carefully consider your future needs as well. As more and more systems move towards an 'always-on' TCP/IP-based communications model your security apparatus should

[13] Sensaphone 2000
[14] SHPro
[15] Siemens

evolve with it. Purchasing limited equipment will not be cost effective in the long term. As well, look at the maintenance procedures for the security equipment before purchasing. Some systems can be remotely adjusted and programmed while others require local updates and upgrades.[16] This limits your ability to adjust equipment to reflect changes in the remote site. The installation of a new server should not necessarily require a technician to drive out simply to adjust temperature sensors to accept a higher ambient heat level.

It is also very important to look at the rate at which a particular sensor system will bring updates into the control center. While many are configurable, it pays to make sure that their communications and update frequencies fit your needs and can be adjusted on a per-site or per-sensor basis. While door security alarms generally only need to communicate when they enter an alarm state, you may want to have temperature alarms providing regular updates to allow for monitoring. In order to keep communication costs low, you may choose to have updates every 10 minutes from a large site that has a broadband connection while hourly updates may suffice for a site using dial-up or satellite. As well, make sure that the system you choose has the ability to query the remote sensors from time to time, even when they have not alarmed. If a door alarm did enter an alarm state but failed to communicate that fact, a periodic check would detect the open state and trigger an alarm. While it would be late, it would still provide your operations staff with good information.

As can be seen from the above discussion, different sensors require different kinds of monitoring, and even different sites will need different configurations. The same applies to power systems. While they're often a separate part of the security system and may not be built to interface with your monitoring system, they cannot be forgotten. Any fluctuations in the power may affect your equipment and need to be reviewed regularly. If persistent under- or over-voltages occur, it indicates potential long-term problems both for the backup power system and for the equipment attached to it.[17] Unfortunately, many of the major backup power systems aren't designed to interface with most of the additional sensors you would deploy. In particular, the smaller units that would commonly be used for small sites generally only report information to a local PC. This is useful if you have one present but otherwise does not provide you with much information. For any site of significant value, make sure that the power system you have in place is capable of sending your operations center the information that you need. In smaller sites, investigate sensors that will detect power problems but will still connect to your management console.

10. CONCLUSION

Properly securing a highly distributed SCADA or automation network is an exceedingly complex task requiring the input of specialists with a range of skill

[16] Sensaphone Express II
[17] APC – Silcon Product Information

sets. While the information presented in this article isn't a substitute for the services of professional installers, it is intended to present a security specialist with some of additional factors that must be considered. While network security is effectively without borders, the physical security dynamic changes with the distance between the sites involved. As well, the lack of staff presence makes maintaining a secure environment difficult. While by no means exhaustive, the topics discussed above and the concerns relating to them form a checklist that can be used to formulate questions for specialists or to review systems that have already been put in place. When security gaps are found, specific technologies can be investigated to close the gaps and minimize the threats facing your distributed resources.

RESOURCES

APC (American Power Conversion Corporation) “Physical Security In Mission Critical Facilities, White Paper #82“ 2004. 1URL: ftp://www.apcmedia.com/salestools/SADE-5TNRPL_R1_EN.pdf (15 June 2004)

APC (American Power Conversion Corporation) “Management Strategy for Network Critical Physical Infrastructure, White Paper #100“ 2003. URL: ftp://www.apcmedia.com/salestools/KBRN-5TMSE9_R0_EN.pdf> (15 June 2004)

APC (American Power Conversion Corporation) “APC – Silcon – Product Information” URL: http://www.apc.com/products/family/index.cfm?id=158&tab=features#anchor1 (30 July 2004)

Beeferman, Steven J. “Economics of Tower Monitoring” *Private Wireless* December 2003. URL: http://www.ita-relay.com/magazine/PW2003/December_2003/TowerSiteMonitoring.pdf (12 June 2004)

Chubb Electronic Security “Integrated Security Management in the UK” 2004 URL: http://www.chubb.co.uk/pdfs/IMS_White_Paper.pdf (20 June 2004)

DeFusco, David “Remote Monitoring Systems: How they can help you save money” URL: http://www.sensaphone.com/press-releases/PR033-RE.PDF (10 July 2004)

Department of Energy, Office Of Energy Assurance. “21 Steps To Improve Security of SCADA Networks” URL: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf (21 June 2004)

Honeywell Security Products and Services URL: http://www.honeywell.com/homelandsecurity/products_security.html (14 July 2004)

“Linksys WVC11B Wireless-B Internet Video Camera” URL: http://www.linksys.com/products/product.asp?grid=33&scid=38&prid=566 (18 July 2004)

“miniMax SCADACAM” URL: http://www.minimax.net/documents/ScadaCamSlickupdate8-5-03.pdf (16 July 2004)

Square D/Schneider Electric “Power Logic Insider” 7 January 2003 URL: http://www.powerlogic.com/pdf/1.pdf (30 July 2004)

Public Works And Government Services Canada. “Industrial Security Manual (ISM) Chapter 4: Facility Protection” URL: http://www.ciisd.gc.ca/ism/Misc/ShowChapters.asp (28 June 2004)

“Sensaphone 2000” URL: http://www.sensaphone.com/sensaphone-2000.html (13 July 2004)

“Sensaphone Express II” URL: http://www.sensaphone.com/express-twod.html (13 July 2004)

“SHPro” URL: http://www.uptimedevices.com/new/specsheets/shpro.pdf (23 July 2004)

Smith, Paul E. “Physical Security: A bridesmaid to technology?” November 2003 URL: http://www.qinetiq.com/home_enterprise_security/white_paper_index.Par.0007.File.pdf (21 June 2004)

Stackhouse, Colin. Kantor, Mandy. Davis, Paula “Siemens Security and Safety White Paper April 2003” April 2003 URL: http://www.siemensenterprise.com/attachments/services/Security_White_Paper_Siemens_Corp_USA.pdf (10 June 2004)

Standby Generator Systems “Standby Generator Systems – Why Choose Standby Power?” URL: http://www.standbygeneratorsystems.com/difference/index.cfm (30 July 2004)

Tennefoss, Michael R. “Echelon White Paper: Implementing Open, Interoperable Building Control Systems” URL: http://www.echelon.com/solutions/building/papers/BacNetComp.pdf (15 June 2004)

“UPS Selector Express” URL: http://www.apc.com/template/size/express/index.cfm (25 July 2004)

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive