June 2012, issue 1-1

SCADA communications

A 360 degree approach to security

Aprisa SR

Contents

1 The need for 360 degree security

Would Edison recognise today's electricity distribution grid? With ever increasing automation and communication, more and more devices connected to the now two way network, and the use of IP and open standards, the electricity and information technology worlds are merging. There are now more network entry points and the grid is increasingly vulnerable to attacks, the types and sources of which continue to evolve. The long term approach that utilities take with regard to asset management means that upgradeability is essential, which creates further vulnerabilities.

Figure 1: Considerations in a 360 approach to security

For the communications connecting SCADA systems, simply bolting on security measures as an afterthought is not acceptable. A comprehensive and in depth approach to cyber security is the only way to protect the network, what we at 4RF call 360 degree security. This means taking into account four key factors:

- Security fundamentals: the key pillars of security best practice
- Sources and types of attack, whether accidental or malicious
- Types of interfaces: management and data, for all types of traffic
- Security standards and recommendations: the best in class

A changing world

Security used to mean network resilence and security of electricity supply. With the changing grid, cyber security is dominating the headlines.

Pike Research estimates that worldwide smart grid cyber security spending will reach over $1.7 billion in 2013. [1]

2 Considerations in a 360 degree approach

2.1 Security fundamentals

There are four key pillars to the security of industrial control systems:

- Integrity: preventing the unauthorised modification of information
- Availability: preventing the denial of a service
- Confidentiality: preventing the unauthorised access to information
- Non-repudiation: preventing the denial of an action

For critical infrastructure, reliability is one of the most important properties of such networks, due to the severity of the consequences of its neglect.

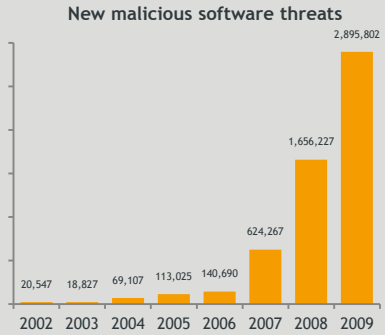
It is therefore not enough to address just the most commonly addressed issues of confidentiality and non-repudiation, which can be addressed through the use of publicly recognised encryption and authentication standards and algorithms. Reliability is achieved through maintaining integrity and availability and these are the two most important aspects of security to consider for the monitoring and control of critical infrastructure, as documented in the NIST SP 800 82 standard [4].

With regard to integrity, the communications network must ensure that a control message received by a remote asset is the same message that was originally sent to that asset. Catastrophic consequences could result if the system was compromised and a 'halt' message changed to a 'run' message, for example.

With regard to availability, there needs to be an assurance that messages sent to a remote asset actually arrive at their destination. Again, catastrophic consequences could result if an important control message instructing a remote asset to halt never arrives.

Today's cyber security issues

The Stuxnet worm, delivered as part of an industrial control system, is only one of the more recent cyber attacks to have been widely publicised. By September 2010, there were approximately 100,000 infected hosts.[2] More than half of the malicious software threats that have ever been identified were identified in 2009. [3]



2.2 Sources and types of attack

Today, cyber security is rarely out of the headlines. In the past, attacks were typically initiated from inside the communications network, with the disgruntled employee being the classic example. However, more recently, attacks have been initiated primarily from external sources. Even as far back as mid-2006, before the 'smart grid' term was widely adopted, the majority of attacks were external. The source of these attacks varies from 'script-kiddie' hackers through to state-sponsored attacks or terrorism.

The rise in such external attacks is due in part to the extensive use of standards-based technology such as IP, WiFi, USB and the Internet, and the fact that critical infrastructure networks are growing in response to drivers for greater control and monitoring.

There are numerous types of attack on industrial control systems. Some of the most important types of attack are defined in the table below:

Type of attack	Examples
Initial compromise / management	Eavesdropping: attacker monitors data travelling over a network for message content such as authentication credentials or passwords Cracking: attacker gains unauthorised access to a network or element of a network Traffic analysis: attacker monitors data travelling over a network for message patterns that enable protocol identification
Availability / denial of service	Flooding: attacker creates illegitimate signals whose presence means legitimate data signals are denied access to a network Jamming: attacker creates a significant illegitimate signal, the presence of which means that legitimate data signals on a network are masked
Integrity / man in the middle	Message modification: attacker intercepts legitimate messages and then alters and transmits these messages, such as to alter the intended operation of a remote asset via a modified control message Message replay: attacker intercepts legitimate messages and then retransmits these messages, for example transmitting legitimate messages to party one in order to attack party two without party two's knowledge

Changing sources of cyber attack

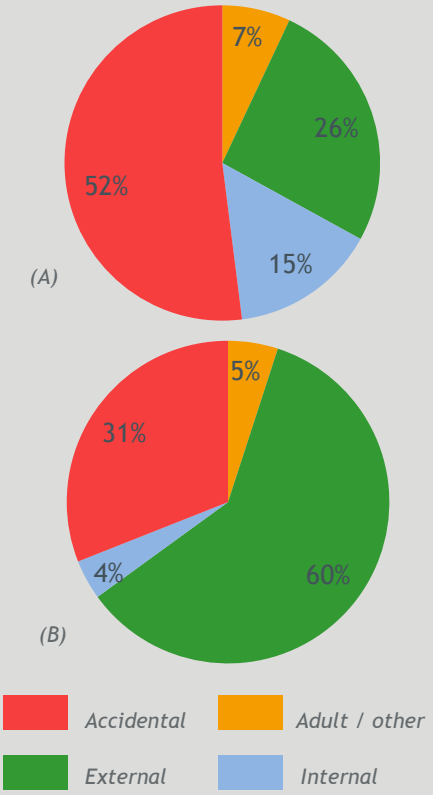


Figure 2: Changing sources of cyber attack: (A) 1982-2001 and (B) 2002-June 2006 [5]

2.3 Types of interfaces

When developing a secure communications product, another of the key considerations for a 360 degree approach to security is the interfaces between the product and the 'outside world'.

There are two main types of interface to the system:

- Data path, representing all the interfaces used for the transport of external data over the network
- Management path, representing all interfaces used to maintain the communications network itself

Considering the specifics of a radio communications network, the primary data interfaces are the wireless interface and the various wired interfaces, which may include serial and Ethernet connections. Management interfaces include the wireless interface for remote management as well as wired interfaces such as Ethernet and USB for local element management.

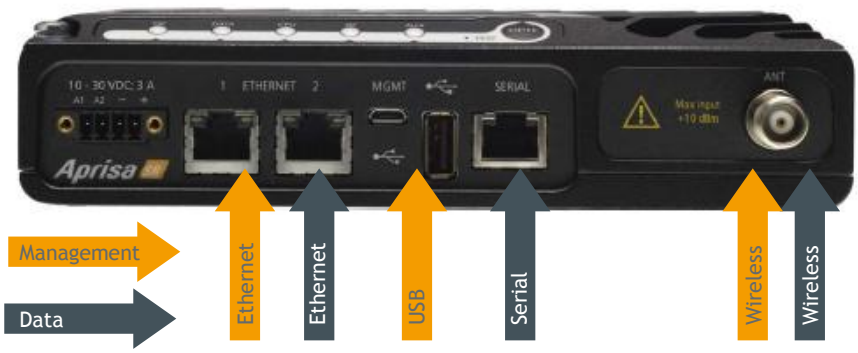


Figure 3: Multiple management and data interfaces

All interfaces in such a product need to be considered as any of them could be used to compromise the product and hence the network as a whole. Management interfaces are as important as data interfaces and identifying and protecting all of the interfaces is key to a 360 degree approach to security.

2.4 Security standards and recommendations

While continuing to evolve, security standards and recommendations are many and varied, including reference designs for industrial control systems, publicly available cyber security standards and advice and guidelines from government groups for critical infrastructure protection. Mandatory standards will become the norm, with standards becoming more stringent. With a 360 degree approach to security, two key issues must be considered:

- Such standards, recommendations and guidelines must be taken into account at the time of system design, to ensure they are embodied throughout the product, rather than 'added in' later
- Security measures within the product need to be able to be upgraded as cyber security threats evolve and best practice and standards evolve, both for new production and for products already in the field

Some relevant standards and recommendations are listed below:

IEC / TR 62443 (TC65)	Industrial Communications Networks – Network and System Security
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
FIPS PUB 197	Advanced Encryption Standard
NIST FP 800-38C	Recommendation for Block Cipher Modes of Operation. The CCM Mode for Authentication and Confidentiality
CPNI	Centre for the Protection of National Infrastructure

General guidelines for industrial security are provided in the IEC/TR 62443 [7] and NIST SP 800-82 [8] documents, with the NIST guidelines introducing integrity and availability as the two most important security pillars out of the four fundamentals that also include confidentiality and non-repudiation.

Public domain cyber security standards are provided in FIPS-197 [9] and NIST SP 800-38C [10], focusing on encryption and authentication. These address the security fundamental of confidentiality, which, while not a main design criteria for critical infrastructure communications design, is a necessary component of many authentication schemes required for network integrity. The use of public standards is crucial, since algorithmic flaws in closed systems are quickly revealed with public domain scrutiny. The AES and CCM algorithms have withstood such scrutiny and are the recommended algorithms for securing the types of data present in industrial communications networks.

In addition to these standards and recommendations, government groups that provide advice specifically for critical infrastructure protection, such as the CPNI in the UK, which regularly publishes information that is particularly relevant when designing communications equipment and networks.

Hacking and disruption incidents [6]

The Stuxnet worm is only one of the recent widely reported incidents.

- *February 2009: highly evasive Conficker/Downadup worm inlects 12 million computers, stealing information (BBC)*
- *June 2008: "Security Hole Exposes Utilities to Internet Attack" (Associated Press)*
- *May 2008: SCADA vulnerability… control software used by one-third of industrial plants (SC Magazine)*
- *March 2008: emergency 2-day shutdown of Hatch nuclear plant from software update on one business computer*
- *Feruary 2008: retail Chinese digital picture frame virus steals passwords and financial info (SF Chronicle)*
- *January 2008: hackers turn out the lights in multiple cities and demand extortion payments (Associated Press)*

3 Implementing a 360 degree approach

A 360 degree approach to security can be implemented through incorporating the four key considerations outlined in Section 1 and described in more detail in Section 2, taken into account from the outset. The Aprisa SR point-to-multipoint SCADA radio embodies a vast range of security features that combine to do just this:

- AES encryption, configurable as 128, 192 or 256 bit encryption, applied to all management and user data carried across the network
- CCM authentication to ensure that all data is from an authorised source
- Proprietary modulation / coding: based on the IEEE 802.15.4 standard
- Licensed frequency bands, which offers protection from RF interference from unauthorised users
- Direct conversion receiver architecture: the use of a high performance synthesiser and direct conversion architecture greatly improves interference performance
- Multiple user authorisation levels: applying authorisation levels and privileges limits the radio parameters that can be accessed by end-users
- Limiting the number of personnel who can change functional settings reduces the potential of inadvertent change or malicious tampering: view-only, technician, engineer and admin, with differing privileges
- Basic authentication with user name and password, ensuring that the end user must be approved by the system administrator before gaining access to the radio
- Session cookie over HTTPS on web interface, providing a secure connection to the SuperVisor web browser management application
- The use of session cookies, which expire when the end-user's browser is closed, provides increased user authentication
- Automatic logout: in the event of a user failing to end their management session, SuperVisor will automatically terminate the session, after a pre-determined time, and prevent unauthorised access to the radio
- No displayed output during boot sequence: limiting output data, and closing ports, during system start-up prevents the ability to interrupt the start-up sequence and compromise the operation of the radio
- No user access to terminal's file system: the core operating system of the radio is not accessible to, or programmable by, the end-user thus ensuring the core functionality of the radio cannot be compromised
- Telnet port block: restricting Telnet access prevents unauthorised access to the management functions of the radio

- ICMP block: blocking ICMP data protects the network should it become subject to a denial of service attack
- FTP block: limiting access to file transfer functionality prevents unauthorised users transferring and uploading malicious files over the communications network
- Encrypted USB data for software upgrades: all software upgrades are encrypted and are checked for authenticity before the upgrade process commences so if an unauthorised USB is inserted into the radio it is ignored
- Integrity check on software upgrades: during the software upgrade process the new software is checked for authentication and integrity before it becomes active on the radio. If invalid files are discovered during the upgrade process, the process is terminated
- Secure over the air updates of the radio network's encryption key: changing the encryption key at regular intervals greatly improves network security. Key Encryption Key (KEK) functionality is used to securely transfer the encryption key over the air and is managed using the secure connection to SuperVisor

4 Aprisa SR security feature summary

The features described above combine to create a powerful platform that not only takes into account security fundamentals, attack sources and types, interface types and security recommendations and guidelines, but is also upgradeable over the air as standards change. The following table summarises how each security feature contributes to the security fundamentals, attack types and interface types:

Feature	Fund.		Attack type							Interface type					
	Availability	Integrity	Eavesdropping	Cracking	Traffic analysis	Flooding	Jamming	Message modification	Message replay	Wireless data	Wireless management	Serial data	USB management	Ethernet data	Ethernet management
AES encryption		✔	✔	✔						✔	✔				
CCM authentication		✔						✔	✔	✔	✔				
Prop modulation/coding	✔				✔		✔			✔	✔				
Licensed freq.	✔									✔	✔				
Direction conversion	✔						✔			✔	✔				
User levels	✔					✔	✔				✔		✔		✔
Basic authentication	✔					✔	✔				✔		✔		✔
Cookie over HTTPS	✔		✔												✔
Automatic logout	✔			✔							✔		✔		✔
No boot output display				✔									✔		✔
Term. file sys no access		✔											✔		✔
Telnet port block						✔					✔		✔		✔
ICMP block					✔	✔									✔
FTP block						✔									✔
S/W upgrade USB enc.													✔		
S/W upgrade integrity													✔		

5 Conclusions

As monitoring, control and automation become more widespread in electricity networks, their communications networks become more open and are more vulnerable, to both accidental disruption and malicious threats or cyber terrorism.

A 360 degree approach to security takes into account security fundamentals, types and sources of attack, the data and management interfaces of the system and the best in class security recommendations. It also extends to system upgradeability to take into account the increasingly stringent requirements that governments and regulatory bodies will impose over the life of assets in the field.

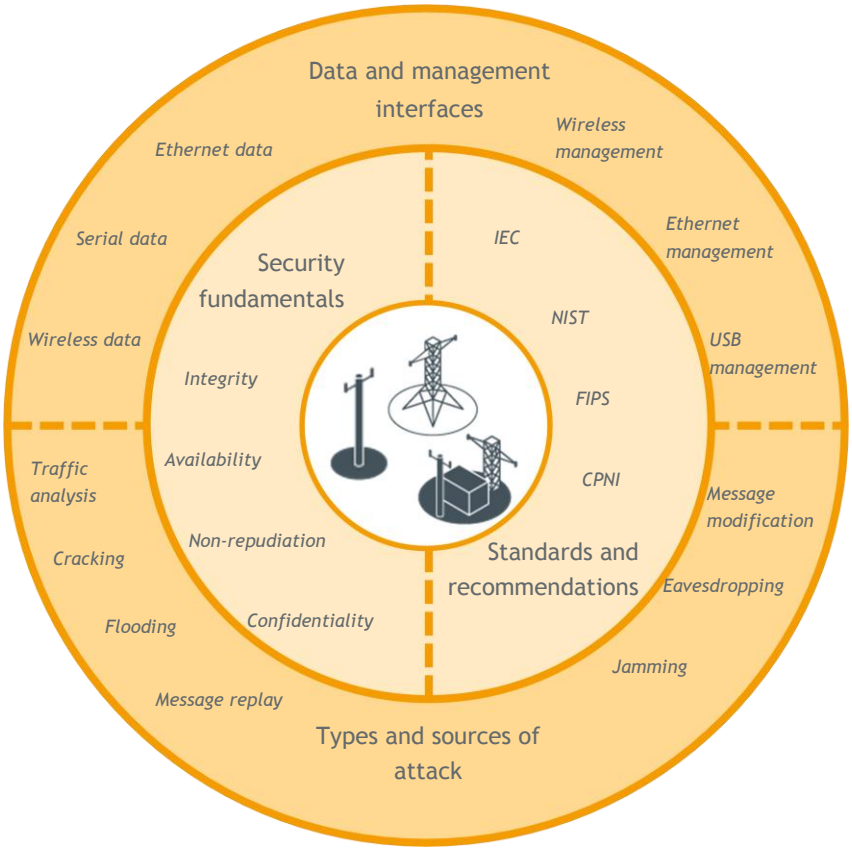


Figure 4: Summary of a 360 degree approach to security

When it comes to your critical infrastructure, a 360 degree approach to security is not just smart, it is essential.

6 References

1. Pike Research: '*Smart Grid: Ten Trends to watch in 2011 and Beyond*', www.pikeresearch.com
2. Symantec Security Response: '*W32.Stuxnet Dossier, Version 1.1 (October 2010)*', www.symantec.com
3. HM Government: '*Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*', October 2010, www.direct.gov.uk/sdsr
4. NIST SP 800 82: Guide to Industrial Control Systems (ICS) Security; Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)
5. The Industrial Ethernet Book: '*Security incidents and trends in SCADA and process industries*', May 2007
6. Pipeline & Gas Journal: *'Hacking the Industrial SCADA Network'*, Frank Dickman, November 2009
7. IEC/TR 62443 Industrial communication networks – Network and system security – Part 3 1: Security technologies for industrial automation and control systems
8. Federal Information Processing Standards (FIPS) Publication 197: Announcing the Advanced Encryption Standard
9. NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality

About 4RF

Operating in more than 130 countries, 4RF solutions are deployed by utilities, oil and gas companies, international aid organisations, public safety, military and security organisations, transport companies, broadcasters, enterprises and telecommunications operators.

The Aprisa SR is a smart, secure, point-to-multipoint radio for SCADA and monitoring and control communications.

4RF

26 Glover Street
Ngauranga
Wellington 6035
NEW ZEALAND

Telephone +64 4 499 6000
Facsimile +64 4 473 4447
Email sales@4rf.com
www.4rf.com