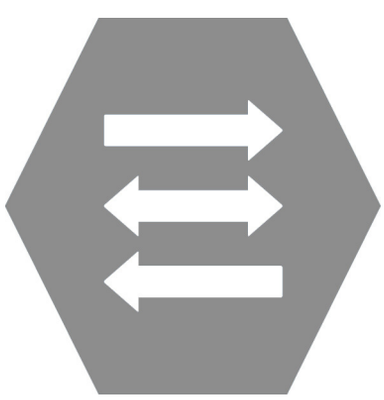
NEXOR

AIR-GAPS, FIREWALLS AND DATA DIODES IN INDUSTRIAL CONTROL SYSTEMS

MAY 2017

A NEXOR WHITE PAPER



CONTENTS

Version 1.0 published July 2013
Version 1.1 published February 2016
Version 1.2 published May 2017

INTRODUCTION

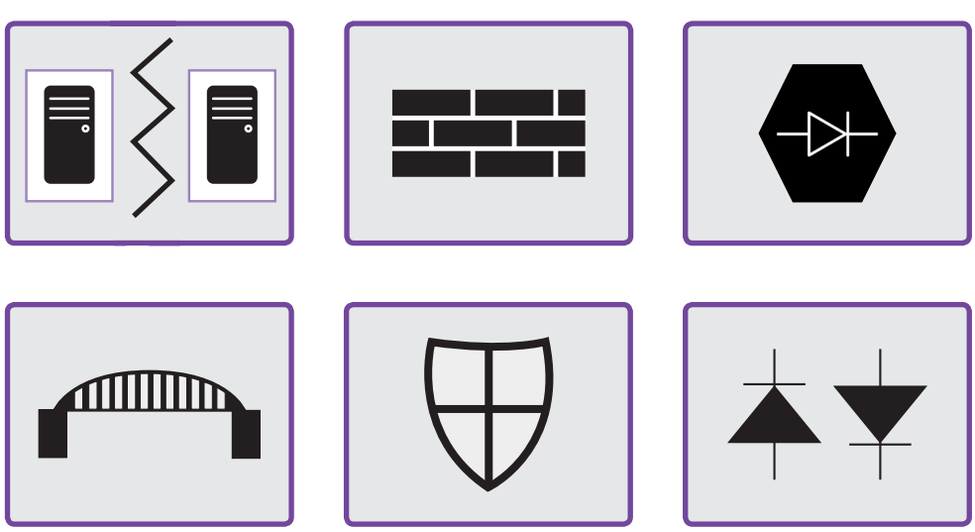
Due to recent security incidents, there is now a significant debate with regard to what is the best way to protect Industrial Control Systems (ICS).

Generally, the debate focuses on whether networks should be isolated via an Air-Gap, or joined by well-configured Firewall(s) but the debate often misses a third option – Data Diodes.

The purpose of this briefing is to provide the relevant information to help you to make the right decision for your business.

Our aim is to make it clear that:

- Data Diodes should become an integral part of any Air-Gap/Firewall debate;
- In the right circumstances, Data Diodes can provide a credible third option;
- Data Diodes are not always the answer;
- The relative merits of all the different alternatives need to be closely examined.



THE BACKGROUND

Businesses have a real, and ongoing, requirement to extract business information from Industrial Control Systems for crucially important management purposes.

For example:

- Where are our trains?
- How much electricity are we generating?
- How has the plant performed over the last day/week/month?

Traditionally, these systems have been separated, with no network connections – **Air-Gaps**.

As we'll demonstrate later, all but the most robust Air-Gaps are breached in some unexpected way.

More recently, we've seen network level connections with traditional network Firewalls.

We'll explore why such an approach introduces unexpected risk later in this briefing paper.

When dealing with a network security environment that isn't a traditional enterprise network, the threat and risk concerns need to be looked at with a different perspective. The business needs to exchange data via connecting networks but the Information Assurance (IA) World and the ICS World have different concerns.

The IA World is more worried about data loss while the ICS World is more worried about the risk to their process.

(Stuxnet has shown this to be a real risk, even on Air-Gapped systems – See Detail 1)

So, there's an obvious and profound dilemma here. There's a need to share information, but all of the current sharing mechanisms patently introduce differing levels of unmanaged risk to the ICS business processes.

DETAIL 1: STUXNET

Stuxnet is a highly sophisticated computer worm that targets SCADA systems and penetrates the Air-Gaps used to provide protection.

The worm initially spreads using infected removable drives such as USB flash drives, and then uses other techniques to infect and update other computers inside private networks that are not directly connected to the Internet.

Once inside the private network it includes a highly specialised malware payload to target SCADA systems that control and monitor specific industrial processes.

Different variants of Stuxnet targeted Iranian organisations with the probable target widely suspected to be uranium enrichment infrastructure in Iran.

Further reading:
https://en.wikipedia.org/wiki/Stuxnet

THE PROBLEM

The temptation to dive in with a purely technical solution should always be firmly resisted!

The first key step that an organisation needs to undertake is to ensure that the business problems are fully understood. This can be achieved by asking, and answering, a number of crucially important questions as indicated below.

WHAT ARE THE INFORMATION EXCHANGE REQUIREMENTS?

Look at who needs what information, the form they need it in and why they need it; where the information source is and where it needs to go; how often and in what time frame... and whether the information is sensitive.

WHAT ARE THE RISKS?

Examine the risks of loss of information, process failure, safety and discover the level of 'risk appetite'.

WHAT ARE THE THREATS?

Investigate whether there's a possibility of something being done, beyond the anticipated business process, either accidentally or deliberately, by an employee or a contractor or a third party engineer. Look at Network-Based Malware and Removable Media mis-use... non-specific and targeted.

WHAT ARE THE IMPACTS?

Look at what happens if the risk manifests itself in three key areas:

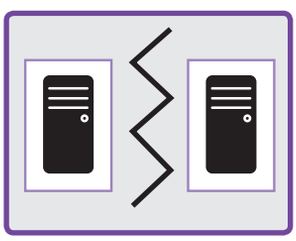
- as a minor inconvenience;
- as a business-ending scenario or;
- in a criminal context, as in corporate manslaughter.

This is critically important... the result will help to determine the level of control, and there's no point in making a £1m lock to protect a £5 note!

Once again, in this area impact needs to be examined with differing perspectives in order to satisfy both sides of the house. For example: With Information Assurance the drivers are usually confidentiality, integrity then availability. With Industrial Control Systems, the drivers are more likely to be availability, then integrity and confidentiality.

In the next section we look at multiple approaches to enable the sharing of information and examine them from a **'threat and trust'** perspective.

THE APPROACHES - AIR GAP



In theory, Air-Gaps seem to be a perfect solution because, as there's no network connection, there would appear to be no way that the data or information could leak out, or more crucially malware gain entry.

However, listen to the views of independent experts:

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network.

"On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment."

MR. SEAN MCGURK, THE DIRECTOR, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC) AT THE US DEPARTMENT OF HOMELAND SECURITY

In practice, as this identifies, there's always a need for a data exchange. For example – a maintenance engineer, recovering system diagnostic messages from a control system, may use a remote dial up line from a laptop connected wirelessly to the Internet, or re-use a USB memory device that has been connected to an Internet connected PC.

In both cases, an indirect route to the Internet exists, enabling a determined attacker to extract data or affect system behaviour. Consequently, the security of the system is compromised... not by bad technology but by bad business processes or user behaviour.

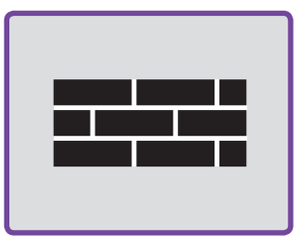
(See Detail 1 on page 4 about how a rogue USB stick is purported to have enabled Stuxnet to infect Iranian nuclear power stations.)

SUMMARY

The key benefit is that there is no direct network connection but the main issue is that Air-Gaps don't enable a real time flow of business information needs to have good human process to control it.

What's more, there are considerable, hidden risks involved. These include a potential for indirect network connections; poor process/ understanding; a false sense of security and weak internal controls.

THE APPROACHES - FIREWALL



To try and avoid out-of-band sharing it seems sensible to join the networks and to use a Firewall to manage the connection.

This approach seems to mitigate a people and process failure with technology, however, **there's a big but**! Down at the protocol level, a Firewall is inherently designed to enable two-way data flows and, no matter how well configured it may be, the technology fails to build robust network separation.

Domain Name System (DNS) is a very good example of a technology that can easily break a seemingly secure Firewall, with a technique called tunnelling (see Detail 2). Sadly, techniques such as DNS tunnelling mean that a Firewall is now pretty much useless as a tool to control the network traffic that enters or leaves a business or control network. Quite simply, attackers can use the DNS to set up a communications tunnel to get data in or out, or more malware in, once they have managed to get software to execute on the inside of the Firewall.

In ICS a common business tool is OSIsoft PI, used to migrate management data from an ICS to an enterprise – a fundamentally one way information flow. This is typically implemented via a pair of Firewalls and a DMZ2 , running over TCP/IP – a fundamentally two way protocol, wide open to tunnelling.

In short, if there's a network with a two-way connection, then data can be shared over it!

Technical failures are not the only Firewall issue. There is a cost factor too. They require regular patching and maintenance to ensure the security assurance persists, which is costly to a business. Also, initial configuration is complex to get right as most Firewall products are defacto "allow all traffic" as shipped, rather than a more secure default of deny communication.

SUMMARY

The benefits are that a Firewall enables business exchange of information; constitutes a simple, technical control to manage 'compliant' users and reduces risk of indirect communication channels. However, a Firewall increases risk of cross-contamination, needs careful maintenance and, as a physical two-way connection exists, it follows that it can be exploited.

There are two serious risks. There's no barrier to a sophisticated attacker and a Firewall implicitly enables two-way data flows, even if a high level protocol is only moving the information in one direction.

DETAIL 2: DNS TUNNELLING

The DNS is a vital, underlying service on the Internet that converts (for example) web site names into the IP addresses that computers need to access the web site. For example, the domain name www.example.com translates to the IP addresses 192.0.43.10.

If a computer on the inside of a network wants to talk to a computer on the outside (Internet), invariably a DNS lookup is needed to get the relevant IP address. Even if this is the only communication your Firewall is prepared to allow, an attacker can use this to pass information (and establish two-way communication).

For example, the following DNS query:

secret_data_sent_via_dns.infoleak.nexor.com

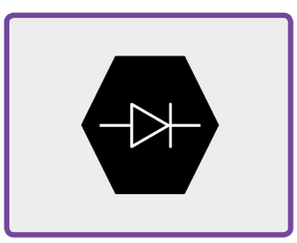
Will pass the message 'secret_data_sent_via_dns' to the server infoleak.nexor.com (data leaving network). The server might respond:

Response.infoleak.nexor.com. 0 IN TXT 'Message received – thanks'

Thus two-way data communication has occurred.

In sophisticated instances of tunnelling, rather than human textual messages being passed, base64 encoded data is used to effectively set up an IP communication channel.

THE APPROACHES - DATA DIODE



A Firewall allows two-way data flows **by design**. If the business information flow is a one-way requirement (ICS to Enterprise), why use a two-way network technology?

Data Diodes only allow one-way information flow at the physical layer. It is simply not possible for data to pass back, unless you can change the laws of physics.

But, there's a challenge here in that many network protocols fundamentally require a two-way connection – seemingly an issue when Data Diodes are used. This problem is easily overcome with the use of network proxies.

The important point is that trust is placed in the Data Diode itself (See Detail 3) – and not the proxies. If the proxies fail, or are compromised by the attacker, the data flow is still guaranteed to be one-way only.

By implementing a Data Diode to facilitate the required business information flows, the need for data transfers via USB memory device or for engineers to connect laptops to extract data can be eliminated. This reduces the risk of user or process failure.

Summary

The benefits of a Data Diode are that it enables the controlled exchange of business information and is 100% secure in one direction (in that data cannot be sent back via the Data Diode). It also reduces the risk of indirect communication channels; offers physical protection and is easier to maintain than a Firewall.

It can, however, be more complex to deploy than a Firewall due to the need to proxy data and the technology not being as well understood by mass-market Firewall consultants. Also a sophisticated attacker can still do harm (see Guard Technology on page 10).

DETAIL 3: TRUST

Knowing which elements of the system you can trust, and which elements an attacker can conceivably take control of is vital in building a defence-in-depth solution. In short what assurance can be provided that the product works?

Some vendors exhibit assurance, based on their brand reputation – "we are good guys".

Others (such as Nexor) choose to use third-party organisations to validate the claims made about products, using a scheme such as Common Criteria.

Common Criteria is an internationally agreed standard by which a third party validates the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous manner.

Further reading: https://en.wikipedia.org/wiki/Common_Criteria

THE APPROACHES - UNIDIRECTIONAL NETWORK BRIDGE

Some products that are marketed as Data Diodes are simply unidirectional network bridges (bridges/routers with cables removed) so that network connectivity only flows one-way. They can even be just two network cards partially joined by a cable.

In principle, it behaves exactly like a Data Diode. However, there are fundamental differences. For example, the hardware on the servers running the proxies, and thus the proxies, need to be inherently trusted – as they mediate access to the network cards.

If these proxies or servers are compromised, the attacker could achieve two-way data flows, using back channels.

Some unidirectional network systems operate purely as a network bridge, without proxies at all. While conceptually simple, they are complex to configure and maintain (see Detail 4 – ARP).

Summary

A Unidirectional Network Bridge is certainly a cheap solution but it's hard to configure and maintain and offers little inherent assurance.

DETAIL 4: ARP

One issue a network bridge has to address is the Address Resolution Protocol (ARP). ARP is an fundamental Internet protocol (RFC 826) used for resolution of layer-3 IP addresses (127.0.0.1 etc) into layer-2 MAC addresses.

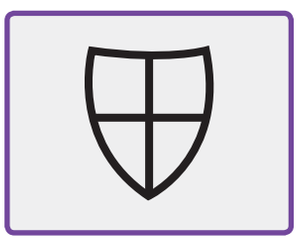
ARP is a request and reply protocol that uses a series of messages and announcements to build a cache of IP to MAC address mappings. Without this a LAN based network communication cannot be established.

Once a one-way connection is in place this process breaks as the ARP messages are not seen by both sides.

Thus, for a network bridge to work, you either need to establish proxies (as in a full Data Diode solution), or find manual mechanisms to populate the ARP caches and keep them up to date.

Further reading: https://en.wikipedia.org/wiki/Address_Resolution_Protocol

THE APPROACHES - GUARD TECHNOLOGY



Allowing a one-way data flow solves part of the issue in that data cannot flow in both directions. However, a Data Diode doesn't provide any control on what data can flow in the allowed direction – thus signalling, as described in Detail 5, is possible.

This is an issue for Firewalls too, due to the DNS tunnelling issue described in Detail 2.

Guard technology can be utilised in conjunction with a Firewall or Data Diode to prevent this kind of signalling.

Fundamentally, a guard works at the application's layer to restrict the type of data that can be exchanged. It only allows data conformant to the defined business processes to pass.

Summary

A guard can complement a Data Diode or a Firewall to reduce the risk of hidden content, signalling or malware by enforcing strict conformance at the application level.

The downside is that this is protocol specific, often leading to bespoke needs for specific business processes.

DETAIL 5: SIGNALLING USING A DATA DIODE

A Data Diode only allows data to flow one-way.

Attackers can still push information from one network to the other, but they cannot get any direct feedback.

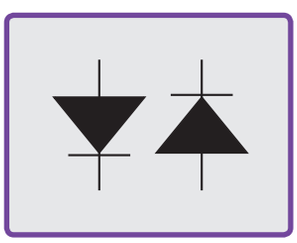
Consequently, there isn't any feedback on their actions (they have no way of knowing if they have logged in for example) thus a command and control mechanism cannot be set up – it all becomes guess work.

This prevents them from having any viable form of remote control.

Indirect feedback is still a potential – for example if I can get the computer screen on the secure network side of the Data Diode to flash on/off, while I get no direct network based feedback, I may still be able to observe the screen flashing on/off.

If the attacker can control this flashing, they can establish (binary-based) communication.

THE APPROACHES - BILATERAL DATA DIODE SOLUTIONS



Data Diodes are fundamentally one-way, so the concept of a Data Diode solution allowing information to flow both ways may seem an oxymoron at first sight.

There are situations where you not only want to monitor an industrial process or sensor, but also want to control it – but from a different network.

A simple example is surveillance CCTV cameras, when the cameras are on a potentially insecure network, but the control room on a secure network. You need to be able to get the video images from the insecure to secure network, but also control the cameras (move left... zoom in...) which required a data flow the other direction.

Firewalls could be used, but will allow all traffic, giving ample opportunity for attack.

The solution is to use a pair of Data Diodes to allow two-way information flows, but crucially each Data Diode needs to be paired with a guard to ensure only data related to the defined business process passes.

Summary

Bilateral Data Diode Solutions are an advanced concept, for use where the business process requires information to flow in both directions, but the risks associated with a generalist Firewall are simply not acceptable.

SUMMARY

As we've seen, there are differing solutions offering a variety of benefits, issues and risks. In order to implement a complete solution, the business problem needs to be fully understood at the outset.

What asset needs to be protected? What information needs to be communicated? Both the IA and ICS sides of the house need to be fully engaged because the perception of business requirements, and risks, is different. A system then needs to be designed, based on business information flows, **NOT** on underlying protocols.

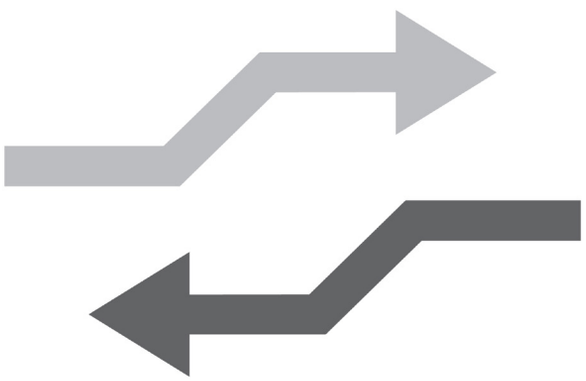
Of course, any solution involves a heady combination of people, product and process. History has shown us that people are invariably the weak link in the chain – a factor all too often overlooked in the design of a so called 'secure system'. It's important to understand that the use of a Data Diode greatly reduces the risk of human or procedural error.

It is crucially important to identify the business process that needs to happen and to identify threats. Then solution architecture needs to be designed to enable business process, mitigating the threats that have been identified.

So... what do **YOU** need to do? We would propose that you work, in an ongoing security partnership, with Nexor.

ABOUT NEXOR

Nexor has a rich history of deploying Secure Information Exchange solutions that support mission critical systems. With our heritage in research we continue to innovate and apply this approach to creating solutions to meet our customers' specific requirements.



Our innovative Secure Information Exchange solutions have created competitive advantage for our customers and on several occasions Nexor has created a solution that proves to be a technological first.

Our solutions are based on our industry-leading SIXA® technology portfolio, which has a modular architectural design that offers both security and flexibility. Combined with our technology integration and software engineering capabilities, this ensures that we can provide solutions to an extensive set of Secure Information Exchange scenarios.

Underlying our creativity is a value set that encompasses our commitment to customer service, communication and continuous improvement. We believe in 'doing things properly', which is why our customers have such high levels of confidence in our trustworthy Secure Information Exchange solutions.

CONTACT DETAILS

Nexor Limited, 8 The Triangle, Enterprise Way
ng2 Business Park, Nottingham, NG2 1AE, UK

+44 (0)115 952 0500
info@nexor.com
www.nexor.com