Session Number: 13

Industrial Control System (ICS) Cyber Security Protection – Threats and Best Practices

Presenter JHJ Pool
Principal Engineer (Cyber Security / ISITE) – Proconics (PTY) Ltd

Abstract

The landscape for industrial cyber security has been changing along with the general cyber security landscape. New threats have emerged to challenge the shock created by Stuxnet. At the same time South Africa is still lagging behind in terms of industrial protection. This paper will summarise the international and local state of affairs, investigate the threat landscape and international best practices. The paper also provides a description and summary of a honeynet set up to gauge the targeting of industrial control systems in South Africa.

Keywords: Cyber Security, Industrial Control Systems (ICS), Cyber Threats, Protection Practices

Introduction

Automation and control systems have become an everyday part of life and are being interconnected at unprecedented levels. This integrated and open nature brings with it vulnerabilities and exposure not found in proprietary legacy systems. Commonly employed ICT security is not suitable for ICS security as the requirements for the systems, the protocols used and the application is very different. These generally results in very little or even no security being employed.

International Trends

Europe, North America and recently Oceania, have very well developed reporting and tracking systems for cyber security incidents in place. The US Department of Homeland Security (DHS) established the Computer emergency response Team (CERT – later changed to Cyber Emergency Response Team) during the 1980’s and started reporting on incidents in 1988. Figure 1 shows the increasing trend in incidents from 1988 to 2003.

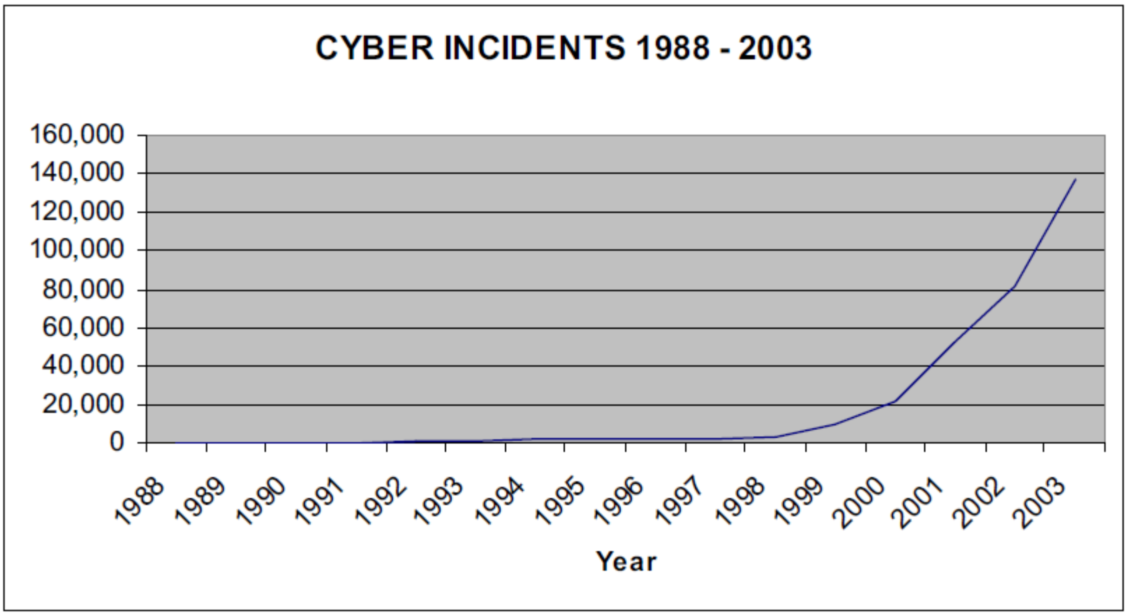


Figure 1 - Rise in Cyber incidents (Source: CERT)[1]

In 1988 six incidents were recorded and this rose to 137 529 in 2003. While still monitored and recorded, it is no longer being reported on. Only a small number of these incidents were related to control systems. At the same time the amount of reported system vulnerabilities also increased dramatically with 13 000 (mostly business system related) reported in 2003. The analysis of the data showed that approximately 120 incidents related to Industrial Control Systems (ICS) were reported in the fifteen year period.

If this is compared to the period October 2011 to September 2012, this single year had more, at 198, than the total fifteen year period. Figure 2 shows the incident distribution by sector.

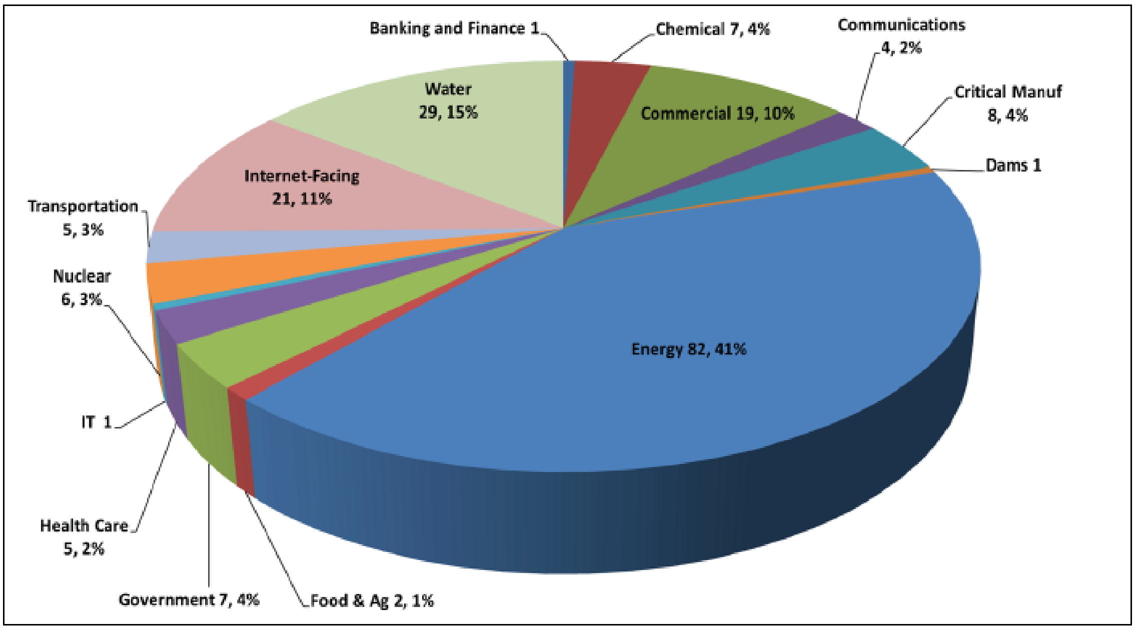
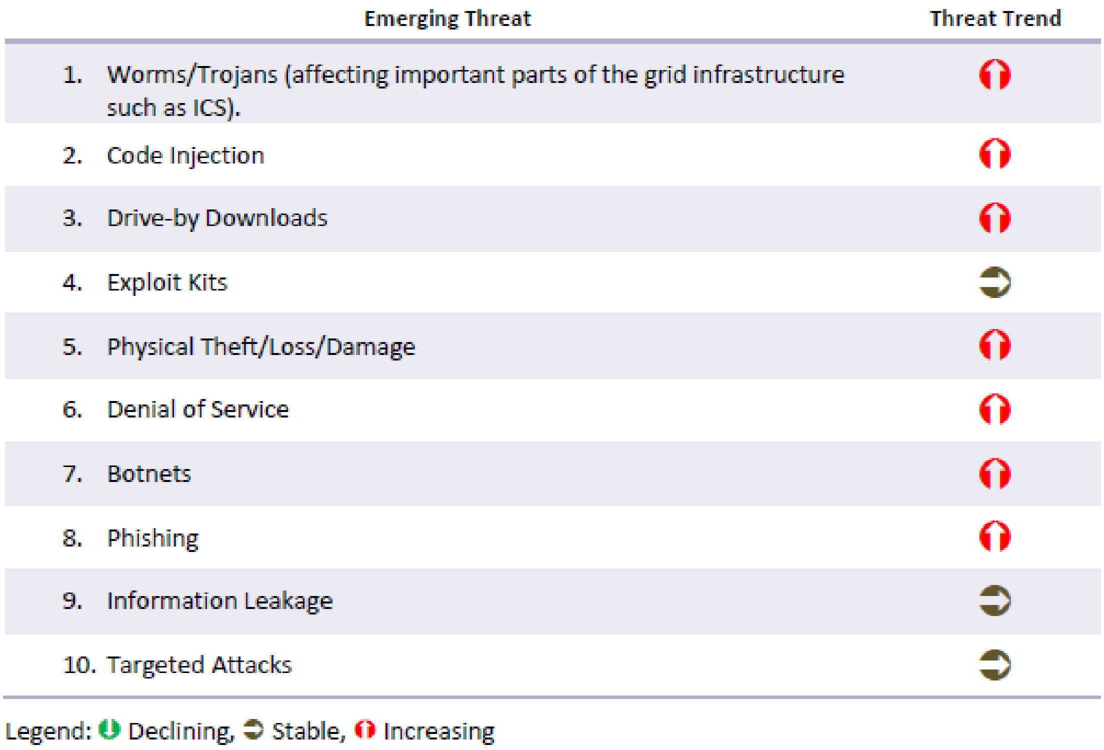


Figure 2 - ICS-CERT incidents FY2012 (Source: CERT)[2]

As can be expected the main utilities (energy and water) are priority targets. This is likely not only due to infrastructure targeting, but also because these sectors have a large footprint in the number of deployed systems.

The trend in Europe is not directly comparable since the European Union Agency for Network and Information Security (ENISA) has a much broader scope of reporting and analysis. In the recently published report on the threat landscape, it was found that none of the threats to critical infrastructure, and specifically the energy sector in the form of smart grid operations, have decreased during 2013 although some threats have remained stable. This is shown in figure 3 below.



Emerging Threat	Threat Trend
1. Worms/Trojans (affecting important parts of the grid infrastructure such as ICS).	↑
2. Code Injection	↑
3. Drive-by Downloads	↑
4. Exploit Kits	→
5. Physical Theft/Loss/Damage	↑
6. Denial of Service	↑
7. Botnets	↑
8. Phishing	↑
9. Information Leakage	→
10. Targeted Attacks	→

Legend: ↓ Declining, → Stable, ↑ Increasing

Figure 3 - Threats and trends in critical infrastructure (Source: ENISA) [3]

One encouraging aspect is that the targeted attacks, of which Stuxnet, Duqu and Night Dragon will form part, is at least stable with no large increase in incidents.

Local Trends

Depending on which report is given credence, South Africa is either the country with the sixth [4] or the third [5] highest incidence of cybercrime in the world. Independent corroboration seems to indicate that the latter is the more likely scenario. Irrespective of what the actual case is the economy lost in excess of R3,4 billion through reported cybercrime. The lack of consistent reporting means that this is most likely much higher.

South Africa is far behind on establishing official structures for both the reporting and investigation of cybercrime incidents. The draft policy for cyber security was published in the government gazette in 2010. [6] To date very little progress has been made in putting this into practice with the exception of the establishment of the National Cybersecurity Advisory Council (NCAC) in October 2013. [7] Looking at the reports generated by CSIRT (http://www.ssa.gov.za/CSIRT.aspx) investigating threats and incidents in South Africa it is very apparent that emphasis is being placed on business and general ICT related incidents. ICS systems are not referenced except where the same type of issues impact it.

This general lag is also found to a large extent in the control and automation environment. The following are some of the typical problems seen in the South African automation industry:

- Use of default credentials – especially passwords
- Sharing of business and industrial IT on the same network
- Dual homed machines where a separate network is installed for ICS's
- Lack of dedicated policies and procedures
- Lack of update management
- No intrusion detection
- No disaster recovery plans
- Lack of awareness and training

The concerns mentioned are not unique to South Africa, but the severe lack of awareness makes the situation all the more critical.

Best practices

There are a number of "best practice" methodologies available. This includes the Tofino / Exida model [8] and the widely accepted DHS DiD guidelines [9]. There are several aspects that most of these methodologies have in common. These include:

- System assessment
- Development and implementation of ICS specific policies and procedures
- System segmentation, by using ICS firewalls, resulting in Defence In Depth (DiD)
- Access control, both physical and logical
- System hardening
- Monitor and maintain

One aspect that is not always included, but would be very useful in the South African context, is that of training and as part of that awareness creation. Some of these are self-explanatory; others need a bit more discussion.

System Assessment

In the same way that there are different variations of "best practices", there are no absolutes in doing system assessments. One of the best tools available for system assessments is published by the US DHS. This is known as CSET and it is actually a comprehensive toolset for doing system evaluations as well as providing guidance when compiling the policies and procedures for protecting ICS's from cyber threats.

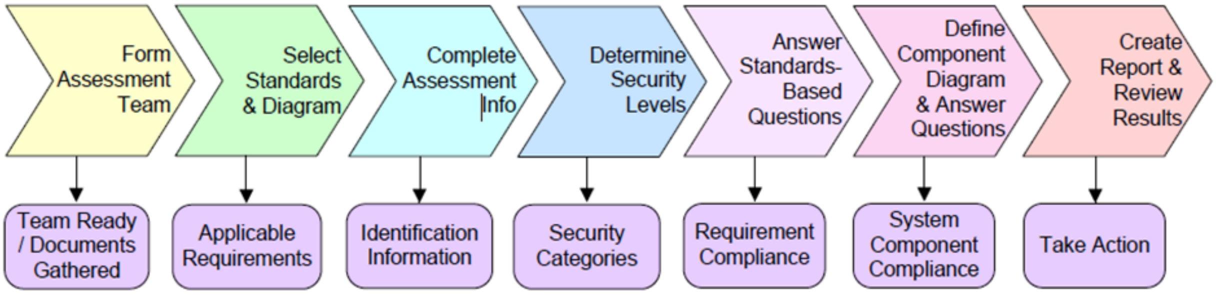

Form Assessment Team
Select Standards & Diagram
Complete Assessment Info
Determine Security Levels
Answer Standards-Based Questions
Define Component Diagram & Answer Questions
Create Report & Review Results
Team Ready / Documents Gathered
Applicable Requirements
Identification Information
Security Categories
Requirement Compliance
System Component Compliance
Take Action

Figure 4 - CSET assessment process [10]

As can be seen in figure 4, the process is very detailed and comprehensive. It is not always strictly required to follow the full process, but for critical infrastructure and plants, the time spent on this is well worth the reduction in risk.

System segmentation

The biggest mistake made by many companies is to only think about vertical segmentation and isolation when applying DiD strategies. This is well illustrated in figure 5 below.

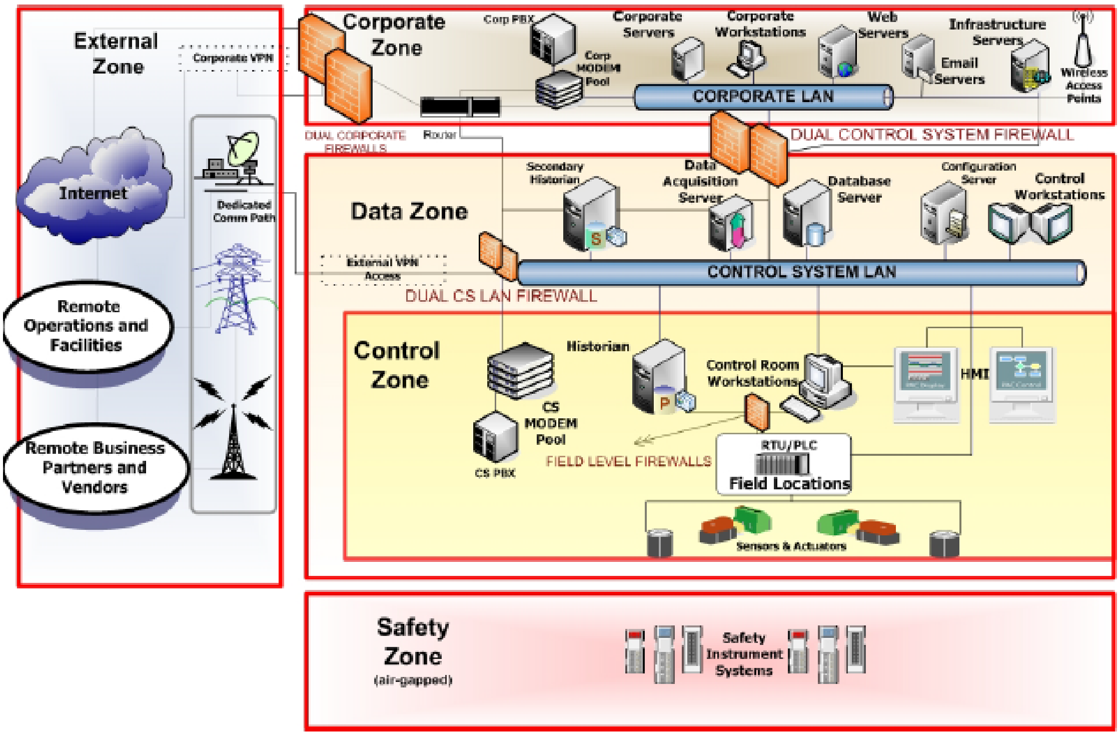


Figure 5 - Typical vertical segmentation (Source: US-DHS[9])

This is generally not sufficient as segmentation should be implemented between plant / units areas to limit or prevent cross infection in case of malware or horizontal targeted attack vectors.

As part of the segmentation a sadly neglected aspect is that of Intrusion Detection (IDS). When considering the amount of undirected attacks being performed continuously one must consider the possibility that if your system has not been attacked, it is very likely because you do not know about it. An IDS is absolutely critical in not only determining whether your system has been targeted, but also what kind of attacks are involved. SANS states that many unexplained malfunctions in control systems can be caused by directed and undirected attacks, which have simply not been identified as such: "*Abnormal activity or unexplained errors deserve a closer security look*" [11].

System hardening

Hardening can take many forms, but in general there are a few actions that should be performed. These are:

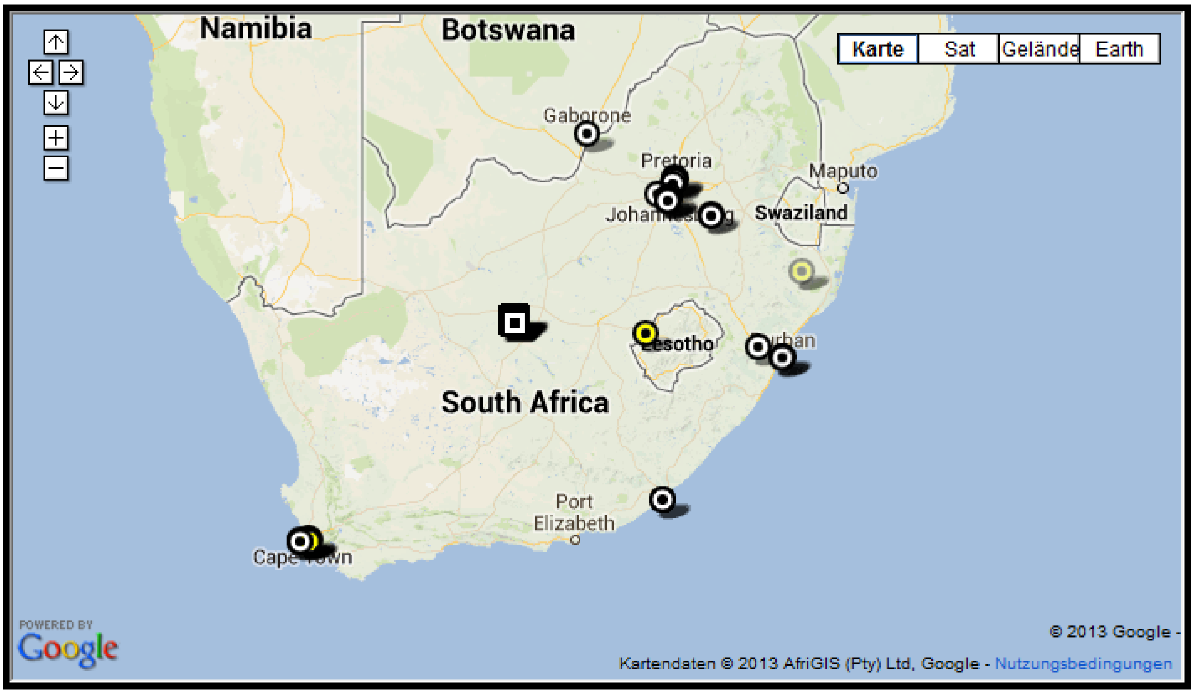
- Patching
  - OS
  - Antivirus
  - Firmware
- Component disabling
  - Web servers

  - Background services
- Port access
  - Disable ports not required especially ports for Modbus TCP
- Application whitelisting
  - Only allow the required applications to run
  - Only allow the required communication to take place
- Scanning – Check and fix vulnerabilities frequently

Threat Landscape

As shown in figure 3, many of the threats faced by ICS's are the same as those found in the ICT world. While many lament the rise of banner based search engines like Shodan (www.shodanhq.com) [12], the fact is that the information was always obtainable, albeit in a more difficult way. All systems and this includes every control system from building automation, substation control and protection and the more traditional process control systems, are made more vulnerable when exposed to public networks and the internet. To a certain extent this can be mitigated through the use of industrial firewalls, with IDS and VPN included, and strong security features.

A filtered and anonymised representation of "open" systems can be found at www.scadacs.org as shown below.



Größere Kartenansicht

🟨 BMS 🟪 ERP 🟧 HMI 🟫 PDU 🟥 PLC 🟩 PLCND 🟪 SCADA 🟦 UPS □ unknown Squares represent accuracy on a "city level".

Figure 6 - "Open" control systems in SA (Source: ScadaCS)

Each indication represents roughly 100 systems. The classic vertical and horizontal DiD strategy does provide a reasonable degree of protection against external threats as shown in figure 7. Insider threats, which form a substantial part of breaches, are not controlled by this. This is because trusted and authorised people are using their credentials to perform unauthorised actions. The most damaging actions are not always intentional, but this does not limit the damage.

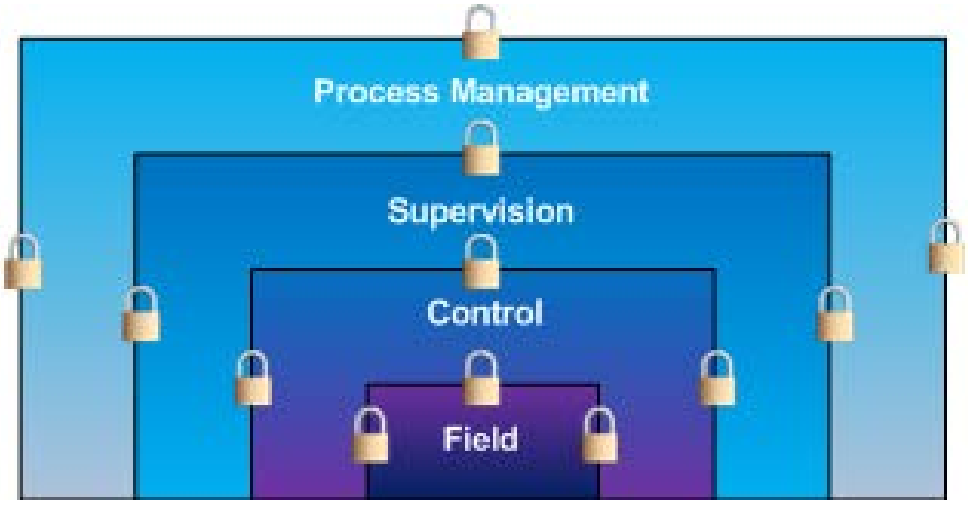


Figure 7 - DiD in process control

DiD strategies are designed to keep out intrusion from external sources, it is not effective against internal sources. One of the most concerning trends that are now emerging is the subversion of the traditional (seen as secure) field buses. Specifically the HART protocol that has been widely deployed on 4-20mA analogue systems has been shown to be vulnerable to code injection and spoofing of the transmitter values [13]. The proof of concept was demonstrated by Alexander Bolshev at the recent Digital Bond SX14 conference [14]. While it is true that a high level of technical competence is required to exploit this, the software and associated hardware schematics is freely available on the internet.

There is currently, and it is unlikely to be soon, no available protection against this type of combined insider and field entry attack. Periodic system audits, vulnerability assessment and intrusion detection (combined with traffic analysis) systems provide some possibility of locating and correcting these types of attacks. Prevention is unlikely.

Determining the level of activity in South Africa using a Honeynet

Honeynets and honeypots have been around for quite some time and have been used to evaluate the vulnerability of specific systems. There are numerous configurations available, but for this test it was decided to make use of the framework provided by Digital Bond. In general there are two types of honeynets, the first is a high interaction honeynet that is connected to a physical system (PLC, RTU etc.), and the second is a low interaction system that simulates the hardware connectivity, but with no actual hardware connected.

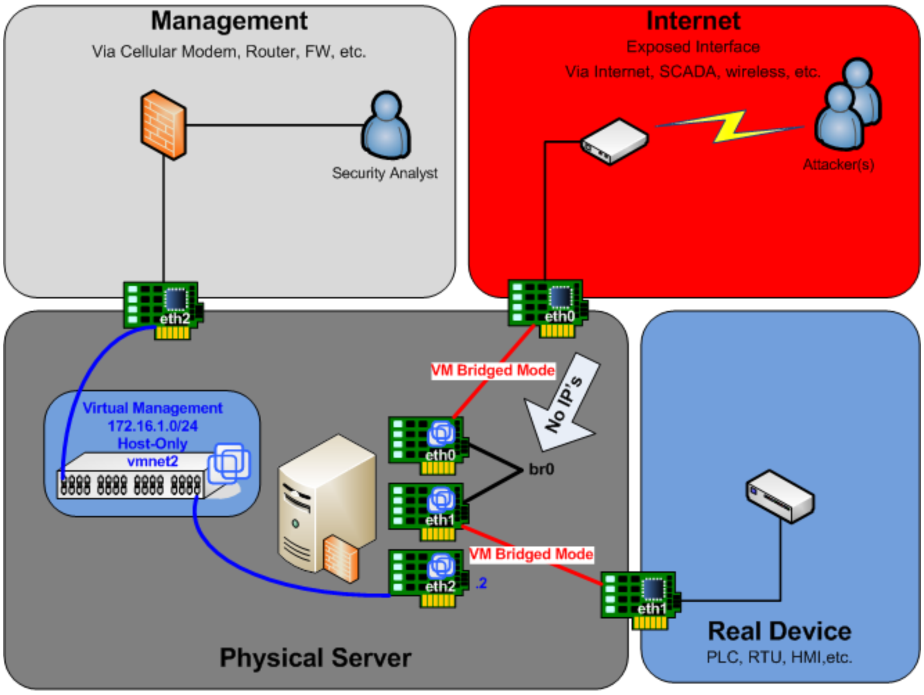
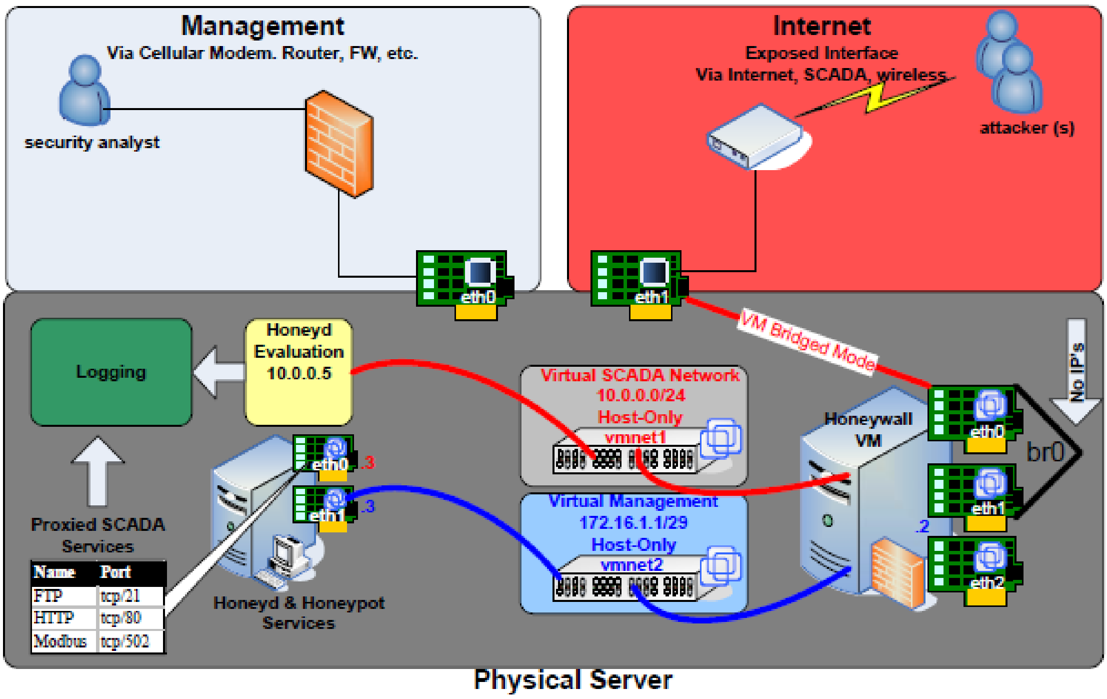


Figure 8 - High interaction honeynet (Source: Digital Bond)



Name	Port
FTP	tcp/21
HTTP	tcp/80
Modbus	tcp/502

Figure 9 - Low interaction honeynet (Source: Digital Bond)

For the test the low interaction configuration was chosen. This simulates a Schneider Quantum PLC with the following protocols exposed:

- Modbus TCP (port 502)
- HTTP (port 80)
- FTP (port 21)

- SNMP
- Telnet

The system has been running since June 2013 and is powered for 8 hours per day only. This limits the exposure, but ensures enough disconnected time to separately evaluate all attacks. Intrusion detection is handled by SNORT and the attack analysis through a combination of the Honeyd and Digital Bond tools provided. Active backtracking and tracing is not allowed for.

The results (as at the end of 2013) were split up according to target. Untargeted attacks were either reconnaissance being performed or malware attacks. The following figure is a summary of the attacks detected.

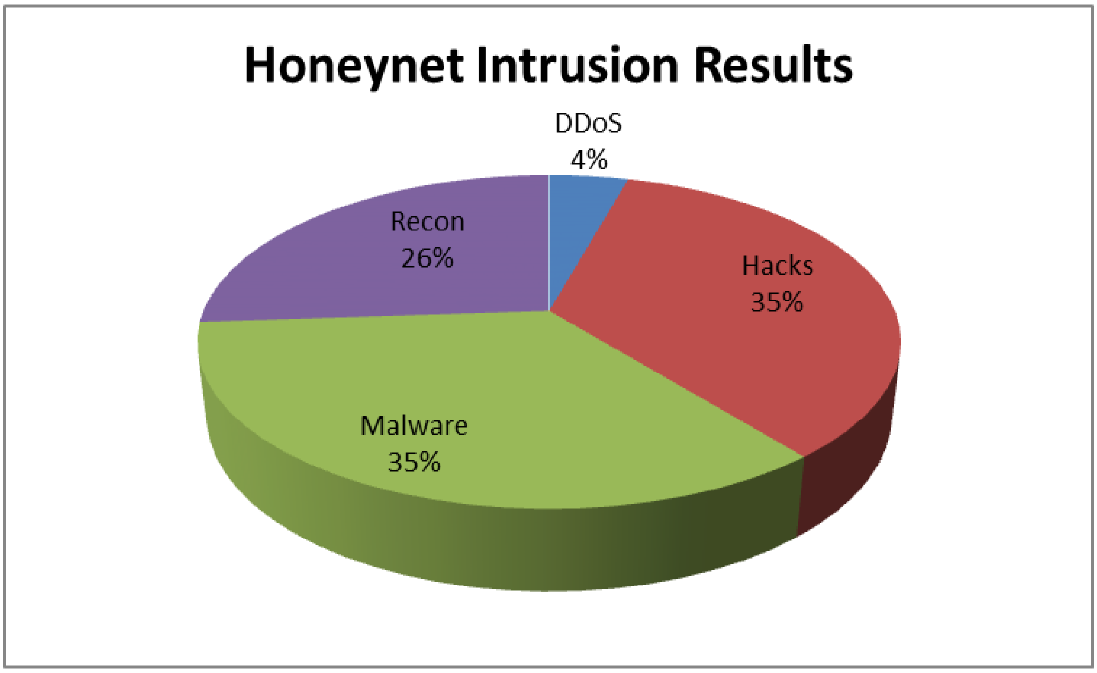


Figure 10 - Low interaction Honeynet Intrusions

While in terms of sheer numbers it does not seem that high (about one attack per week), if one considers the small exposure of the system it is worrying that so many attacks could be picked up, through a fairly unsophisticated monitoring system. The targeted hacks (2 against the Telnet service and the rest against Modbus) are very concerning as it requires quite a high level of sophistication and is in the case of Modbus, not something generally found in the ICT environment.

The reconnaissance attempts fell into two categories:

- Port scans
- Access attempts through the use of default passwords

While by no means definitive, these attempts indicate that South Africa is by no means exempt from being targeted for ICS

Conclusion

The threat against ICS systems is not decreasing and protection, god practices and monitoring is becoming ever more important. While measures are being put in place by government to ensure better protection through a legislative framework, we are still far behind and much still needs to be done especially in protection of production systems. Cybercrime is a global problem and South Africa is not exempt from this. The first step is to create awareness that there is a problem. DiD will not protect against all threats, and especially not against the insider threat, but together with good intrusion monitoring and vulnerability scanning and patching your systems will be much better protected.

References

1. Turk, RJ, "Cyber Incidents Involving Control Systems", October 2005, Idaho National Laboratories, INL/EXT-05-00671
2. "ICS-CERT Monitor", October – December 2012, US DHS ICS-CERT
3. ENISA Threat Landscape 2013, "Overview of current and emerging cyber threats", ENISA, December 2013
4. Skade, T, "Beware of the Trojan Horse on your stoep", November 2013, http://www.destinyconnect.com/2013/11/21/beware-of-the-trojan-horse-on-your-stoep/, from a report of the FBI
5. "Cybercrime: South Africa third most hard hit country", November 2013, http://www.flarenetwork.org/learn/africa/article/cybercrime_south_africa_third_most_hard_hit_country.htm, from Symantec report
6. "Draft Cybersecurity Policy of South Africa", February 2010, Government Gazette no: 32963 Vol. 536
7. Strydom, J, "Meet the National Cyber Security Advisory Council", October 2013, http://www.bandwidthblog.com/2013/10/16/meet-the-national-cyber-security-advisory-council/
8. Byres, E, Cusimano, J, "7 Steps to ICS and SCADA Security", February 2012, Version 1, Tofino Security | exida Consulting LLC
9. "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defence in Depth Strategies", October 2009, DHS, National Cyber Security Division
10. "CSET 4.1 User manual", July 2012, US Department of Homeland Security
11. "Control systems are a target", June 2013, SANS – Securing the human, www.sans.org/ics
12. "What you should know about SHODAN and SCADA", November 2010, http://www.digitalbond.com/blog/2010/11/02/what-you-should-know-about-shodan-and-scada/

13. Weiss, J, “An ICS vulnerability beyond Stuxnet”, January 2014, ControlGlobal, http://www.controlglobal.com/blogs/unfettered/an-ics-cyber-vulnerability-beyond-stuxnet/

14. “SX14 conference”, February 2014, Digital Bond, http://www.digitalbond.com/page/2/