The importance of field devices in industrial cybersecurity

JHJ Pool Pr. Eng, M. (Eng)

Cobus.pool@proconics.co.za

Introduction

There is little doubt that industrial systems are playing an increasingly important role in keeping the modern world working. The Covid19 pandemic again highlighted the importance of automation and maybe more critical the increased remote connectivity required by personnel. This, along with the growth in Industrial Internet of Things (IIoT) devices are pushing plant owners towards implementing more protection measures on their industrial plants. One aspect that is rarely (if ever) considered however, is the field device as either the cause of or a threat vector for a cyber incident. This article analysis some incidents to try and unravel the importance of these primary devices.

What is a cyber incident?

To understand the context of the data presented here, one must first have a common understanding of the terminology.

"Cyber" is derived from cybernetics which is the study of **control systems** and the interaction between man and machine.[1] Cybernetics is derived from the Greek word kubernētēs meaning pilot. This word should also be familiar to people involved in IT systems.

"Incident" is defined in the IEC62443-1-1 (SATS62443-1-1) standard as:

"adverse event in a system or network, or the threat of the occurrence of such an event"

In broader IT/ICT context a security incident can then be defined as anything that has an impact on the Confidentiality, Integrity or Availability of the system.

Field devices

Despite many criticisms, the Purdue model is still being widely used to define the functional levels in Industrial Control Systems (ICSs). Devices are grouped into functional levels as shown below.

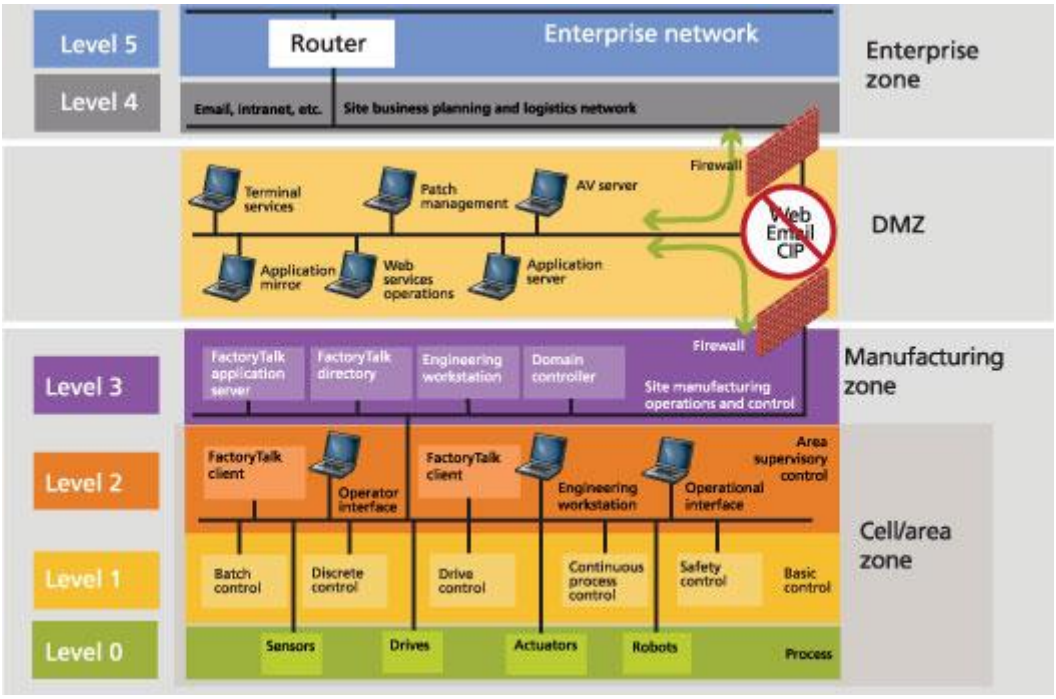

Figure 1 - Purdue Model levels - Source ISA[2]

Communication for system or components from levels 2 to 5 are normally ethernet based and specifically using TCP/IP as communication protocol. Levels 1 and 2 can use TCP/IP or a variety of other ethernet based industrial protocols like DNP3, Modbus TCP or OPC UA.

Field devices are either hard wired to the control or safety systems using typically analogue 4-20mA signals or use serial based (typically RS485) communication protocols like H1, Profibus DP / PA or even Profibus FMS in legacy systems. Hybrid communication like Highway Addressable Remote Transducer (HART) protocol, that uses digital Frequency Shift Keying (FSK) modulated onto the analogue signal, is used in millions of devices worldwide. The figure below shows how the FSK modulation is implemented.

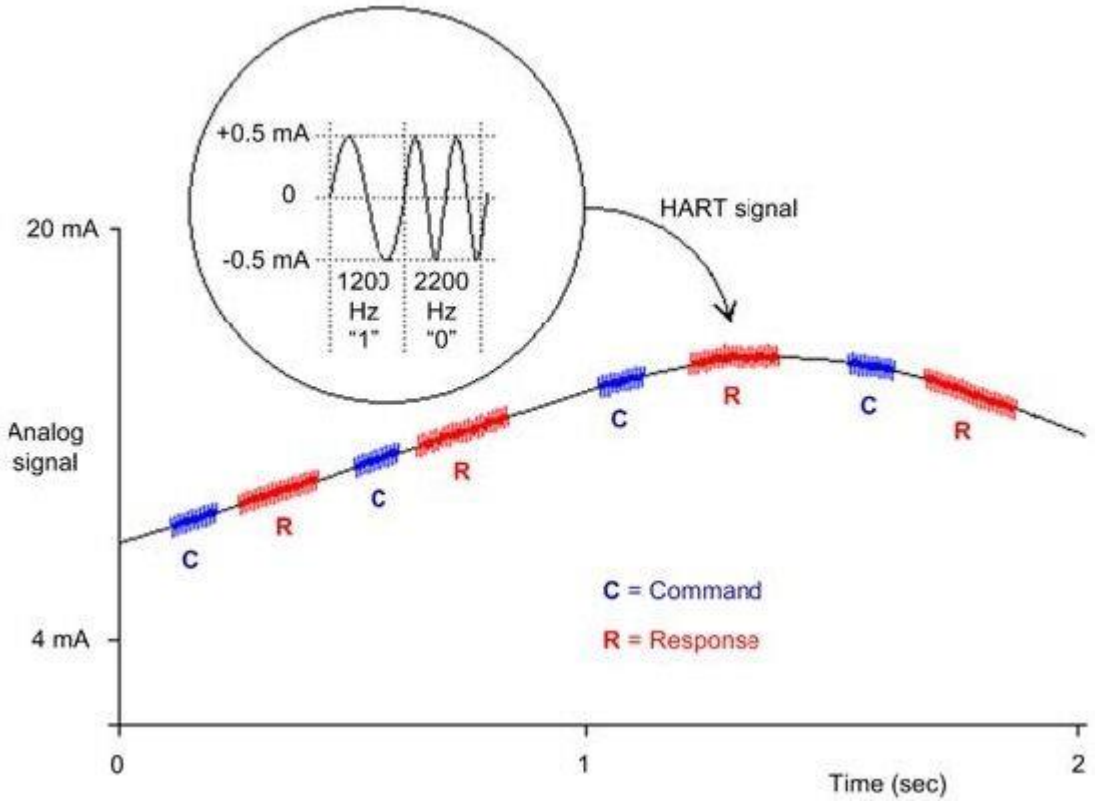

Figure 2 - HART FSK modulation

Incident / Threat vector

While there can be numerous vectors playing a role in a security incident neither the IEC/ISA (in the IEC62443 or ISA99 documents) or ENISA in their well-known threat taxonomy [3], make any mention of field devices. Generally, the input from field devices are implicitly trusted with only safety systems and the associated IEC/ISA standards considering the implications of instrument reliability (in IEC61511 and ISA84). There are preliminary discussions underway between the ISA99 and ISA84 workgroups to determine whether device security should be included in either standard.

The question arises whether instruments or other associated field devices, like Intelligent Electronic Devices (IEDs), should be considered as a credible threat vector or even cause of security incidents.

In 2014 the Russian security researcher Alexander Bolshev [4][5], presented a Proof of Concept (POC) for using a variety of field device protocols, but primarily HART, to infect a control system and eventually download malware to the Enterprise Resource Planning (ERP) system. Until very recently complete circuit diagrams and software for this device, called Corsair, was available online for anybody to use.

This by itself does not translate to a credible threat. There are however additional indications that one should consider the security implications of field devices. In 2019[6], Yokogawa, a worldwide supplier of field instruments including those used in safety critical

applications, made the announcement that, like 2014, there was an incidence of counterfeit transmitters. Aside from the operational deficiencies that result from poor quality, it would be a trivial exercise to implement the Corsair functionality on the counterfeit instrument HART module.

The other concern is that widely used IEDs in industrial electrical systems might also be subjected to similar, albeit different communication, type vectors[7]. It should be noted that the cited information is being questioned by several parties.

None of the widely used industrial security suites, by companies like Tenable, Dragos or Kaspersky, monitor or check for instrument level issues. As mentioned, the information from the instrument is trusted implicitly. One possible check is to include full range operational checks of the instruments as part of periodic maintenance, but the concern with this is that, as shown with Volkswagen Dieselgate, it is theoretically possible for the instrument to detect simulation conditions and change reaction accordingly.

Did / are instrument failures cause(ing) security incidents?

Eric Byres started collecting incident data to analyse and classify incidents. This database (ISID) and its successor, Repository of Industrial Security Incidents (RISI) was eventually made part of eXida[8]. Unfortunately updates to the database stopped in early 2015, but the information is still the most complete repository of its kind available.

There have been several papers published analysing the data of the 242 incidents described. One of these by Ogie [9], is particularly interesting as aside from the analysis for industry it also contains information on four (Korean Air B747, Air France flight 447, Spanair flight 5022 and a Qantas Airbus 330) incidents that caused particularly large loss of life. The recent Boeing 737 Max MCAS crashes is similar to the cited incidents. This seem to imply that instrumentation problems are a major contributing factor, but it does not provide confirmation of it.

The industry distribution from the paper shows that all industries are affected , but that the Critical Infrastructure (petroleum, power transportation and water) industries are particularly vulnerable to incidents.

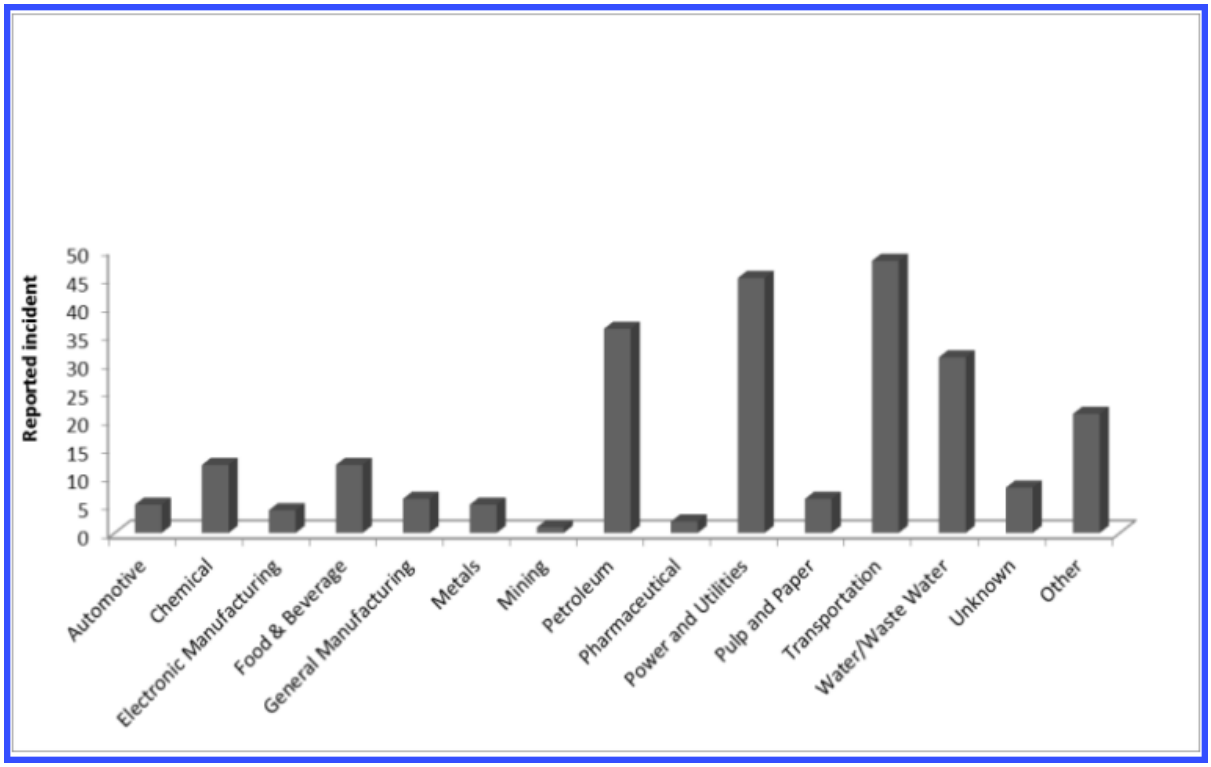

Figure 3 - Industry type incidents Ogie from RISI

Neither the distribution analysis of the method or the perpetrator gives a clear indication of whether instrumentation or other field devices contributed significantly to incidents.

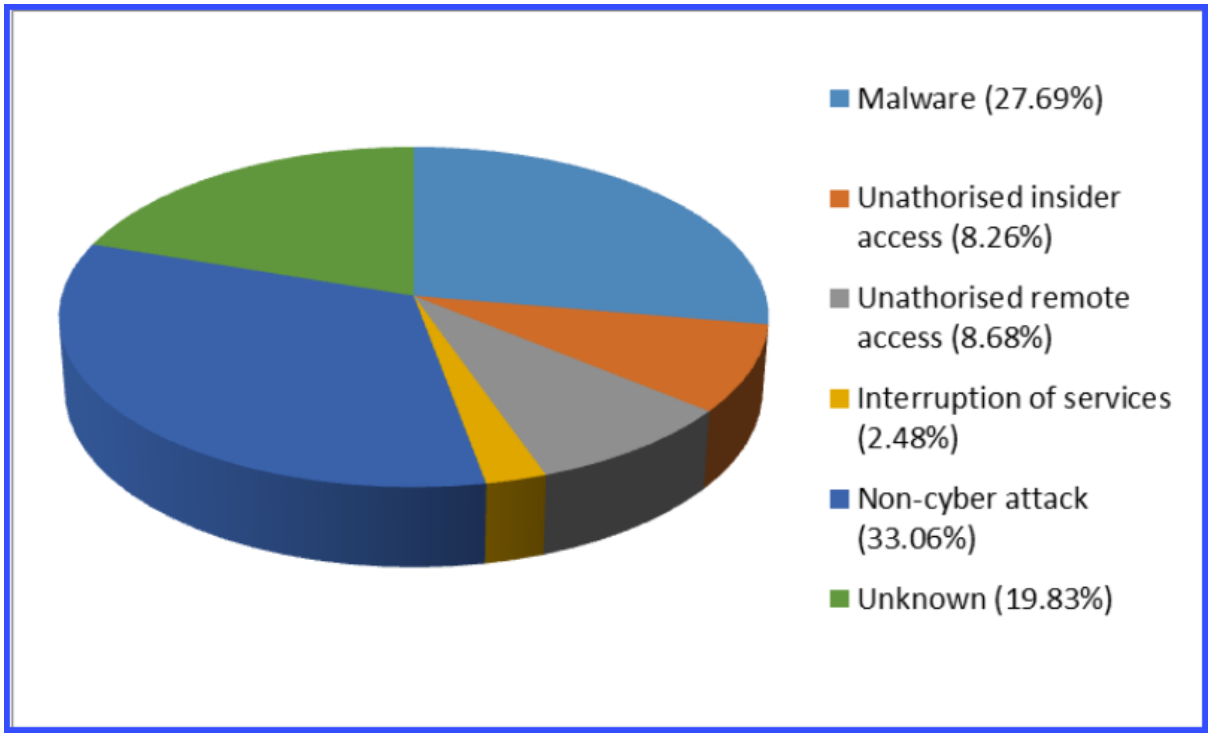

Figure 4 - Security incidents by method of operation Ogie from RISI

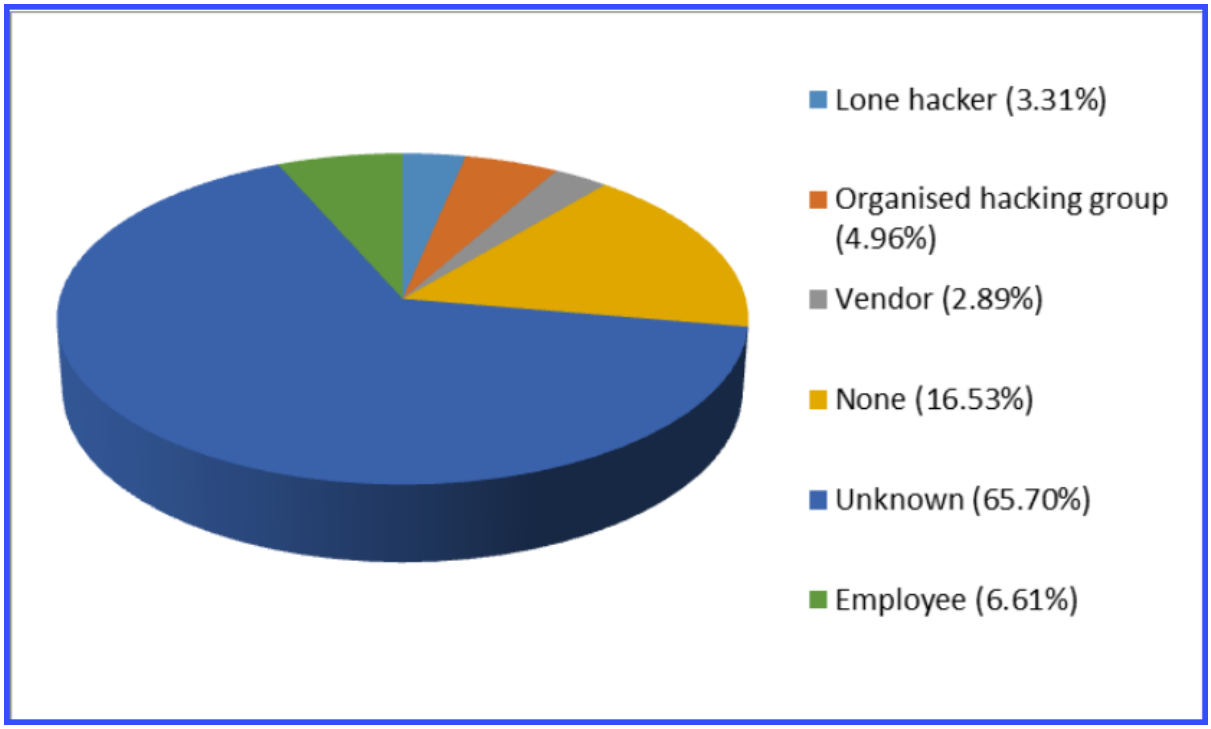

Figure 5 - Security incidents by type of perpetrator Ogie from Risi

To answer the question requires a relook at the original data.

RISI analysis

For the analysis of the RISI data a few changes were made to limit the data set:

- Only Confirmed Incidents were analysed (Likely but unconfirmed, Unlikely and Other including hoax incidents were excluded)
- A limited number of duplicate entries were consolidated to avoid skewing of results
- Specific effort was made in identifying “sensor” or “instrument” related incidents or “glitches” to determine the incidence of occurrence

This resulted in the analysis of 198 incidents versus the complete dataset of 242 incidents. The reader should bear in mind the definition of a cyber incident as given at the beginning of the article.

The results are as follows.

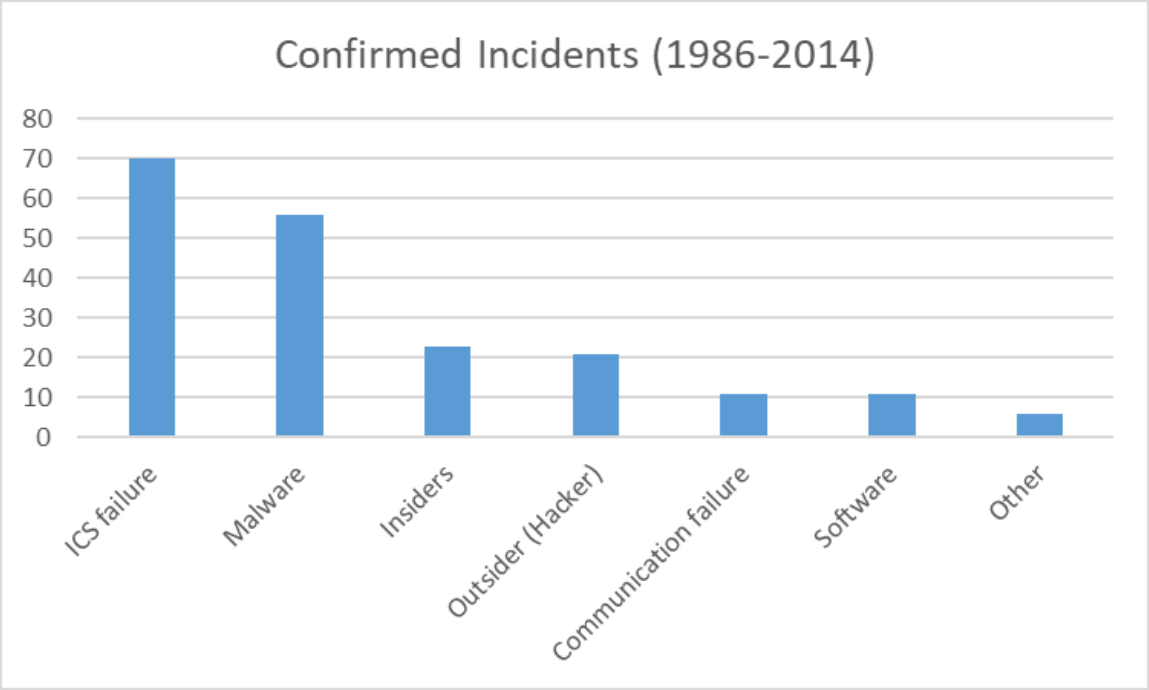

Figure 6 - Number of incidents per cause from RISI

Plotting the results as a percentage contribution results in:

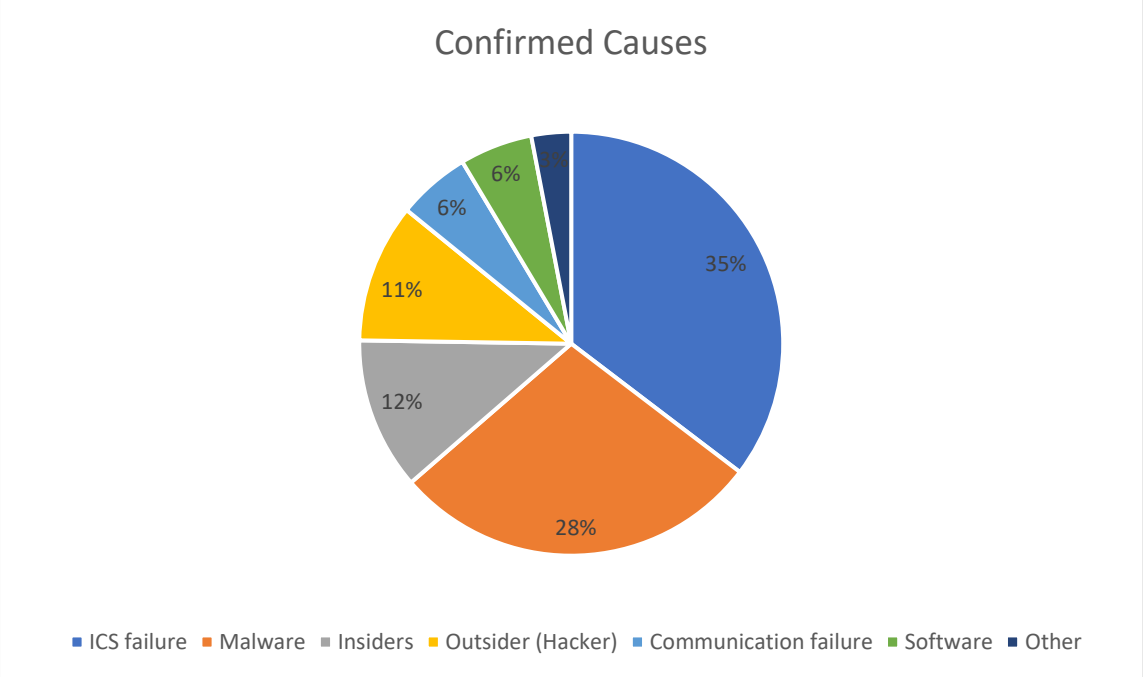

Figure 7 - Distribution of incidents per cause from RISI

Considering the 70 (or 35%) incidents that involved system failure, further analysis of these incidents determined that 48 of the 70 incidents (or 68%) involved failure or misrepresentation of field / process data by the field device or sensor. Almost a quarter of incidents in the database involved field device malfunction of some kind.

This implies that a quarter of incidents will not be detected or alerted by the current industrial security suites.

What was the impact of these incidents?

- Reported monetary loss, including fines and production loss: $485 million
- Injuries: 419 people
- Fatalities 416 people

The impact was substantial.

Current situation

Unfortunately, more recent information is not readily available, so it is almost impossible to provide an accurate analysis of the current situation. Kaspersky [10] is one of the few companies that periodically publish results of detections in their industrial deployments. This is primarily based on malware detections (which we saw accounts for about 28% of total incidents). The figure below shows the incidence of malware on industrial systems:

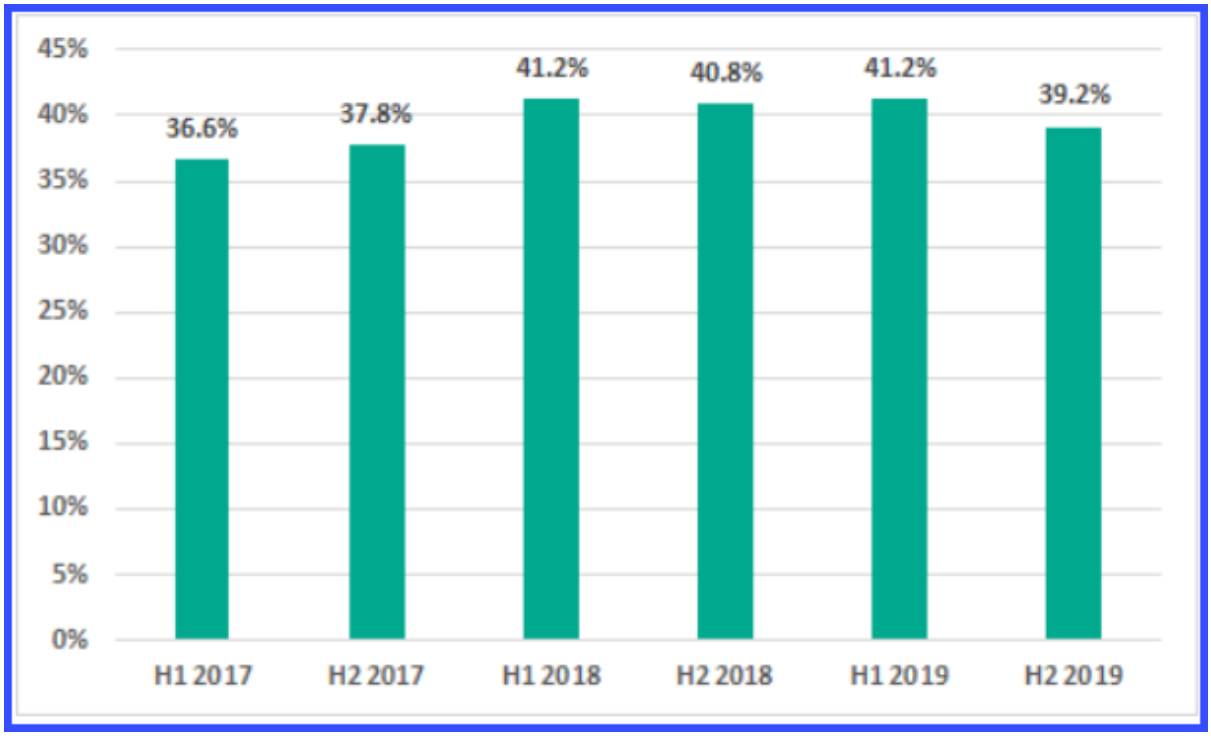

Figure 8 - Percentage of ICS computers on which malicious objects were blocked source Kaspersky

South Africa is slightly better off than average (at about 30% of system affected) as shown in the geographical distribution.

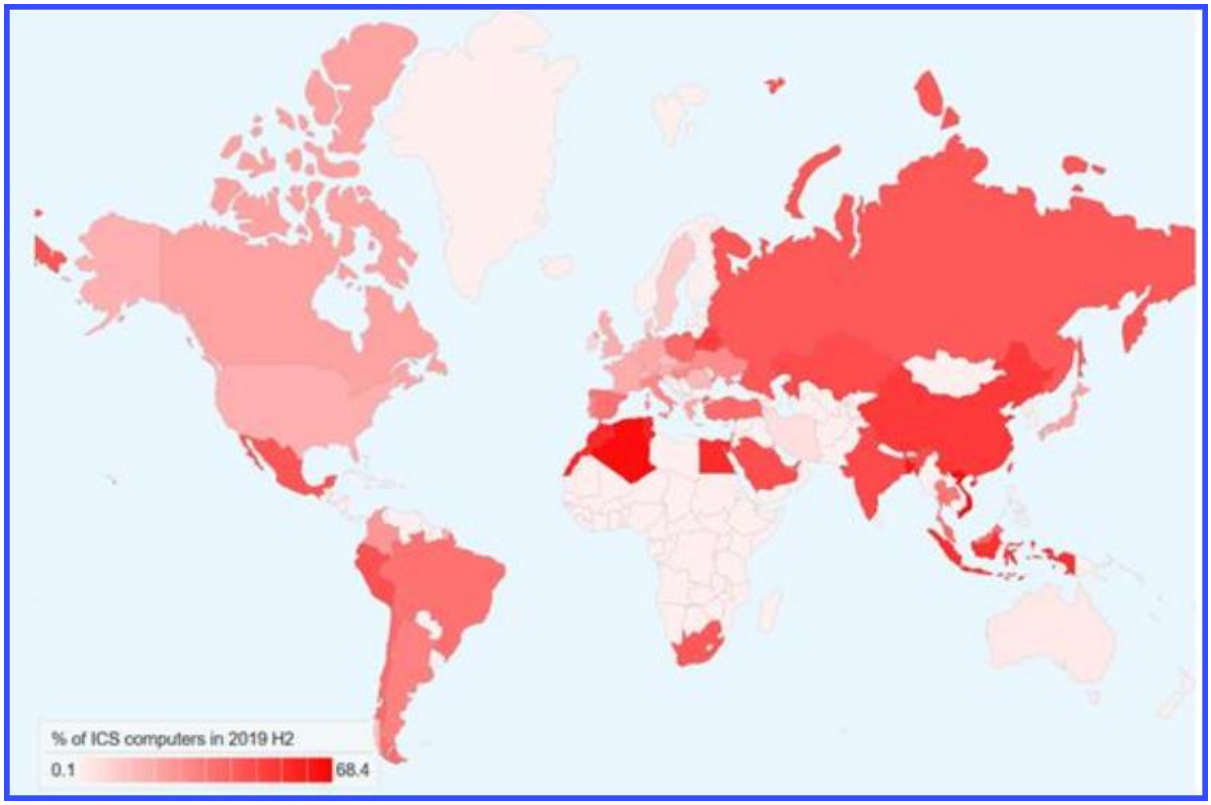

Figure 9 - Geographical distribution of attacks on industrial automation systems, H2 2019 source Kaspersky

Revisiting the IEC definition of an incident *"adverse event in a system or network, or the threat of the occurrence of such an event"* these detections would qualify as incidents. If the trends stay true, we expect that instrument or field device issues would cause a similar number of incidents.

Conclusion

It is clear that field equipment has a significant impact on the number of incidents. While we can deduce the size of the problem from historical data it is difficult to quantify it. Special attention should be paid to primary and field devices to prevent or limit additional cybersecurity impacts.

References

1. https://alpinesecurity.com/blog/what-is-the-origin-of-the-word-cyber/, Retrieved 2020/09/02
2. https://blog.isa.org/the-internet-of-everything-delivers-smart-manufacturing, Retrieved 2020/09/02
3. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view, Retrieved 2020/07/16

4. https://dale-peterson.com/2014/03/11/s4x14-hart-as-an-attack-vector/, Dale Peterson, Retrieved 2020/09/08
5. Alexander Bolshev, ICSCorsair: How I will PWN your ERP through 4-20 mA current loop, https://dsec.ru/presentations/hart-as-an-attack-vector-current-loop-to-application-layer/ , Retrieved 2020/09/01
6. Joe Weiss, Unfettered Blog, https://www.controlglobal.com/blogs/unfettered/the-ultimate-control-system-cyber-security-nightmare-using-process-transmitters-as-trojan-horses/, Retrieved 2020/02/03
7. Joe Weis, Unfettered blog, https://www.controlglobal.com/blogs/unfettered/emergency-executive-order-13920-response-to-a-real-nation-state-cyberattack-against-the-us-grid/, Retrieved 2020/06/06
8. The Repository of Industrial Security Incidents, 2019. Accessed online on December 2, 2019. http://www.risidata.com/
9. Ogie, R. I. (2017). Cyber Security Incidents on Critical Infrastructure and Industrial Networks. ICCAE '17: Proceedings of the 9th International Conference on Computer and Automation Engineering (pp. 254-258). New York, United States: ACM.
10. Kaspersky ICS CERT, Threat landscape for industrial automation systems, H2 2019, published 2020/04/24