Cyber Security – What our systems are trying to tell us, and why we need to listen.

David Allen MSc Computer Science and Cyber Security,
ABB UK Cyber Security Team Lead,
ABB UK, St Neots, PE19 8EU
United Kingdom

The rising popularity of big data in analysing and predicting the behaviour of complex process control systems to mitigate the effects of unwanted system trips has brought with it a new category of process safety concerns.

The increasing interconnection of process devices and safety controllers with the wider industrial automation control system (IACS) network and data collection servers exposes the safety and control systems to new threat vectors. In addition to the core functional safety requirements that guides the assignment of SIL rated safety functions, to reduce the estimated safety risk, it is now essential to explore the risks introduced by cyber security threats and incorporate appropriate mitigation measures and awareness to combat them throughout the safety system lifecycle.

As a part of this presentation, we shall investigate where the Operational Guidance 86 (OG86) fits into the picture along with what an OG86 risk assessment consists of, discussing such elements as, assigning criticality, assessing potential threats, and looking at opportunities which can allow room for future development in the ever-evolving threat environment. It will also cover some of the limitations of the OG86 cyber security risk assessment and what further areas may need to be explored to provide a well-rounded cyber security picture.

HSE's current OG86 advises the incorporation of a cyber security risk assessment for assessing sites with hazards that have the potential to cause a major accident or could cause the loss of an essential service. As observed by OG86, increased functionality of the process safety systems provides an increased attack surface that needs specialised cyber security risk assessment processes to reduce the risks.

This presentation will probe a little deeper into how the OG86 cyber security risk assessment process can be part of a holistic approach to protect both the systems and our people.

Keywords – Cyber Security, OG86, IEC62443, Operational Technologies, IACS, IEC61511

Introduction

The Industrial Internet of Things has been around for two decades. In 1999 it started to gain significant momentum and the world very quickly evolved to utilise this technology and connected devices for everyday living (Karmakar, et al., 2019). In recent times, when smart devices and integrated smart appliances, such as event monitoring and security, have become widely available, it should come as no surprise that the operational technology (OT) industry has also adopted these innovations with the introduction of the industry 4.0 (Geissbauer, et al., 2016), which is also known as the Industrial internet of things (IIoT).

This revolution has undoubtably led to the rise of interconnectivity between network layers, the introduction of new and advanced big data analysis and of course, new areas of connectivity, such as, wireless devices. However, this interconnectivity has also left the door ajar to allow new attack vectors for cyber criminals with fast ways of exploring the systems.

A very basic view of a network can be envisaged as starting at Level 0 where the physical input/output (I/O) process devices reside, moving up into Level 1 in which the OT plant controllers sit. Level 2 hosts the Supervisory control and data acquisition systems (SCADA) and then the Level 3 which contains the operational controls and system management controls (Security information and event management systems, Network monitoring etc.). Finally, Level 4 for this example would be the interconnection to the enterprise level (IT systems). It is important to note that the implementation of new connections on OT systems between the network Level 4 enterprise and Level 3 or even Level 2 is becoming the new normal. An example can be seen in figure 1 below highlighting the different network levels and common devices which reside in each.

Cyber security is one of the fastest growing concerns for the world when it comes to technology. The threats posed by cyber-attackers not only affect our personal digital lives such as online banking and social media, but also affect our professional lives such as utilities and process automation systems (Jones, et al., 2021). Between 2020 and 2021 there was a 102% increase of ransomware attacks globally with the utilities sector being one of the highest targeted sectors (TechRepublic, 2021).

This paper aims to explore a little deeper into some of the cyber security risks in OT systems along with discussing varying elements of the Health and Safety Executive (HSE) OG86 risk assessments such as, assigning criticality, assessing potential threats, and what limitations might be encountered when running an OG86 risk assessment.

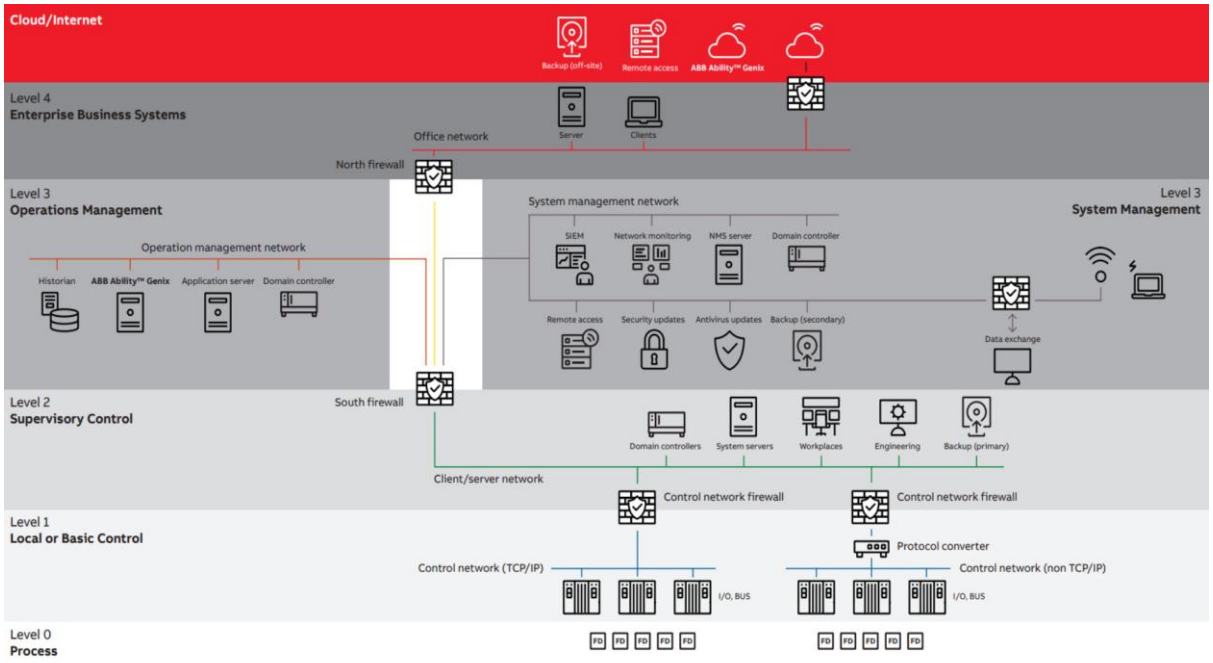

Figure 1 - Example Purdue model Reference Architecture

OT Cyber Security

When thinking about cybersecurity it often means different things to different people, certainly when you consider the vast range of OT systems that exist. In one respect, cyber security is often portrayed as implementing electronic protections to stop attackers, such as implementing anti-virus or network monitoring. However, cyber security really encompasses a much larger area and requires not only suitable electrical/electronic protections, but also cultural cyber awareness and implementation of cyber security management and planning too.

Unfortunately, there is no easy cyber security solution in which a singular product can be purchased and installed solving all your potential cyber security problems; cyber security must be considered as a continuous journey. It requires a harmonious combination of technical solutions, management processes and system expertise to understand the potential OT cyber security risks faced by a system.

In 2019, Verizon issued a cyber report and found that an estimated 85% of all cyber-attacks had some form of social engineering aspect involved (Verizon, 2021). This helps to reinforce the importance of not only protecting systems digitally, either via technologies or limitations but ensuring that a good cyber culture is also implemented.

When looking at the systems with a functional safety hat on, it can be observed, from an assessment point of view, that there is clear and very real need to consider cyber security protections (IEC, 2010). However, the standard IEC61508-1 does not directly state exactly what cyber security must be covered but mentions that any events of “abnormal or infrequent modes of operations” shall be considered. If we then look at section 7.4.2.3 within IEC61508-1, it also mentions ensuring correct security measures but does not elaborate further.

The IEC61511-1 standard for process control, specifically part 1 clause 8.2.4, we can again see an explicit requirement in place for conducting a security risk assessment. However, it still does not cover exactly how cyber security shall be addressed, although the hall marks of needing to consider cyber security are heavily implied.

IEC61508-1 and IEC61511-1 standards provide detail in understanding the functional safety requirements and of course, when considering a wider picture starts to cover cyber security (IEC, 2016). However, the standards do not provide a concise and detailed understanding or guidance in what exactly must be considered when trying to protect IACS (Industrial automation & control systems) from cyber security threats and leaves it largely open ended only mentioning further guidance can be seen in the IEC62443 series and the ISO/IEC 27001:2013.

An additional point that needs to be considered when discussing functional safety and cyber security is that traditionally functional safety looks at two key types of failures. These are classified as systematic failures in which the failure of the system manifests from a design flaw or pre-existing system state and random hardware failures where a device fails randomly based on its hardware failure rate probability distribution (Meany, 2017). When we consider cybersecurity and functional safety, we need to ask about a third type of failure in which an attacker deliberately or accidently tries to exploit a systematic failure which could also potentially result in a hardware failure or alternatively manipulates a device to function in an undesired manner thereby causing an unpredicted failure.

The Stuxnet incident of 2010 can be used as a well-known public example of attackers specifically targeting SCADA systems with PLCs in a hazardous environment leading to extensive damage in the control system equipment (Chen, et al., 2011). Unfortunately, this is just one example of the many types of attacks happening daily. As such, as a community, we must evolve to meet this new challenge.

What keeps our machines up at night?

One of the first questions often asked when looking at implementing cyber security on a system is "What do I need to protect?". With systems now more than ever having additional data monitoring and data packaging passing data between the OT system and enterprise systems, we first need to take a small step back to understand where the devices (nodes) within the system reside and how they are communicating. Equipped with that information, we can then begin to observe the types of risks and vulnerabilities that might be present.

Cyber threats come in many types and forms, from system vulnerabilities, poor network configuration and all the way through to targeted attacks exposing existing vulnerabilities.

Each day in 2022 more than 450,000 new malicious programs are being registered (The Independent IT-Security Institute, 2022) and unfortunately, this is only the tip of the iceberg as the type of cyber-attacks faced are as easily varied.

In April 2022, the National cyber security centre (NCSC) reported that the amount of ransomware attacks had doubled since 2020. The report also went on to show that phishing attempts are currently the most common threat vector followed closely by denial of service (DoS), malware and ransomware attacks (Ell, et al., 2022).

Cyber Vulnerabilities

We can generalise cyber vulnerabilities as weaknesses in the system in which the CIA (Confidentiality, Integrity and Availability) triad is affected. So, when looking at cyber vulnerabilities, it is a case of assessing the system for weakness in the equipment or design that could allow an attacker to gain unauthorised access. This could be anything from incorrect networking, poorly managed devices or even lack of physical protections in place, such as unrestricted access.

The above description can then be further broken down into more specific categories such as:

Human factor vulnerabilities in which the users of the system present a major risk. It can be observed that human factor constitutes a major threat to systems. The UK Government's yearly cyber survey in 2021 which reviewed a wide range of companies and charities showed that the most common type of attack faced in 2021 was phishing attacks followed very closely by impersonation attacks (Jones, et al., 2021).

Network vulnerabilities are where the network design of the system presents weak areas of communication or access, allowing data to be intercepted and lost or unauthorised access to be gained. Network vulnerabilities can often result in increased damage during a system attack as poor networking can allow increased transitioning between layers during an attack (assuming a network with layers has been implemented).

System vulnerabilities encompasses the main industrial control system (ICS) which might have been misconfigured, lack maintenance or have unsecure hardening techniques implemented. Common system vulnerabilities could be poor patching schedules, unmaintained user accounts (elevated privileges), misconfigured connections, weak authorisation techniques or insider threats.

Supply chain vulnerabilities are often overlooked, however when considering IIoT there is a requirement to check that the equipment being supplied is from a controlled and reliable supplier. If the equipment being installed has already been compromised before deployment it is unlikely that the system protections implemented will catch that threat.

The last vulnerabilities to discuss are physical vulnerabilities. As systems are as much at risk from physical attacks as they are from digital attacks, we need to ensure they are considered too. When considering physical vulnerabilities, we need to consider the potential threat actors such as insider attacks, 3rd party clients and unauthorised access as they can be just as likely to affect the CIA triad.

What is OG86? and who needs to know?

The operational guidance 86 (OG86) was originally published by the Health and Safety Executive (HSE) in 2017 covering industrial automation and control systems (Health and Safety Executive, 2021). In 2018 a second edition of the standard was released based on industry feedback which contained increased guidance on how to use the document.

The OG86 document is designed to support HSE assessors in conducting inspections in a consistent manner along with providing guidance to operational duty holders. This guidance helps ensure that duty holders are implementing suitable cyber protections on sites with a potential to cause a major accident (MA) or loss of essential service (LES). For sites which fall under COMAH (Control of major accident hazards), OG86 is considered as a sensible starting point for tackling cyber security.

The OG86 guidance was designed to include the regulatory requirements of NIS (Network information systems) and sets the minimum ICS cyber security requirements that the HSE expects the duty holders of COMAH sites to conform to. These requirements are to help minimise the likelihood and potential subsequent safety impact of an attack.

It should of course be noted that in the OG86 guidance it does acknowledge the development of other standards such as the IEC62443 standard, and states that duty holders may follow these other standards if the protections implemented provide equivalent protections as mandated in the OG86 standard.

This is clearly shown in Appendix 1 of the OG86 standard where the first step highlighted in the OG86 process is either OG86 or alternately accepts approaches detailed as IEC62443, IAS84.00.09 and BSEN 61511 Ed 2 (Health and Safety Executive, 2021).

The OG86 process is designed to review the sites' management systems highlighting areas of implementation in cyber security governance, processes, polices, detection and reduction of incidents. The risk assessment section below will predominately look at section B and C of the OG86 standard.

OG86 Risk Assessment the Overall Process

The first step in understanding the process is examining what the OG86 risk assessment can ultimately achieve and assessing the value it provides. Every duty holder will have their own reasons for conducting an OG86 risk assessment, such as for HSE compliance or for understanding the system better. However, there are a few other good reasons for conducting one.

Conducting a risk assessment helps operators to understand the potential impact of different types of cyber-attacks. It provides guidance on where to implement system upgrades to reduce cyber risk. The risk assessment also highlights and provides an estimated prediction on the safety severity of loss to your organisation. Additionally, as mentioned above, it is one of the requirements in achieving compliance whilst utilising both industry best practices and regulatory requirements.

By conducting a risk assessment, sites are provided with insight into potential system blind spots alongside enabling further development of the cyber security program.

OG86 Preparing for the assessment

Before starting the risk assessment, a bit of pre-work is required. This firstly involves identifying personnel within the company who are required to particate in the assessment. The OG86 guidance does not explicitly state who should be involved in the assessment and there is no "one perfect solution" as each organisation will have its own organisational structures. However, using industry best practice, we can narrow down some of the pre-requirements.

Conducting an effective cyber security risk assessment will require the support of different site experts. It will need a project lead who will drive the assessment by arranging participation; this ideally should be the responsible person onsite for OT cyber security. A key aspect of the risk assessment will be managing communication between the teams designated as responsible for cyber security and those who have the power to make and approve the risk decisions that will be raised by the assessment (NCSC, 2017).

In addition to the site responsible cyber security owner, it is advisable to build a varied team consisting of technical system experts such as functional safety, operations engineers, maintenance engineers, telecoms specialists and including system vendor support where 3rd party systems are used.

Alongside the OT team it is advantageous to include the company's IT team when there is a system connection between the OT system and enterprise level. This additional support not only provides an even better understanding of data exchanges between the levels but also enhances the ability to identify potential threats from both sides.

The support from each functional area is essential in providing a well-rounded picture of the system under discussion and a broader understanding of the site, environment and systems installed. A pragmatic approach should of course be taken with regards to who is invited to the assessment as the risk assessment will be discussing sensitive security related information. Also, a large number of participants can result in wider areas of discussion than is required and can result in the assessment drifting off-topic. Where possible participants should be limited to a selected 'core team' with specific experts involved where needed.

If using a third-party company to facilitate the cyber security assessment, they will most likely take the lead in organising the required meetings, however, will still require the site responsible cyber security owner to be involved to advise who, from their organisation, should represent the various disciplines during the assessment.

In addition to site expertise, some essential documentation will be required to support the discussion and ensure it is conducted in a methodical manner. As a minimum, the risk assessment will require a site reference architecture or high-level network diagram identifying the different zones and conduits as these will be assessed during the criticality phase. An asset inventory should also be available to enable the identification of different systems onsite and to ensure all systems are reviewed and considered from a cyber security perspective.

When following the OG86 process, it puts a large emphasis on the need for Purdue model diagrams - an example of this can be seen above in Figure 1. This requirement can clearly be seen throughout the guidance along with example Purdue model network diagrams listed in the OG86 Appendix (Health and Safety Executive, 2021).

It is important to note that any additional systems not listed in the network diagrams or asset inventory should be recorded separately as a part of the risk assessment. This is to ensure that all parts of the system under consideration (SuC), applicable to cyber security, are explored during the assessment.

OG86 Understanding Cyber Criticality

An OG86 risk assessment has four key objectives, the first of which is identification of zones that directly or indirectly perform functions that protect against major accidents (MA) or loss of essential services (LES) (Health and Safety Executive, 2021).

In order to meet this objective, the assessment must review the asset inventory and network diagrams to define the IACS scope along with grouping the systems into logical groups. This of course will be easier if the network diagram already follows the OG86 recommendations using zones and conduits.

If a zones and conduit drawings does not currently exist, it would be advisable to create one at this stage from the existing site piping and instrumentation diagrams (P&ID), network diagrams and site technical knowledge.

Once the zones and assets have been identified, the zone consequence and criticality level can be assigned to each, in turn allowing them to be designated as either MA/LES or Non-MA/LES. This is important as we are at this stage identifying which zones require additional cyber security focus.

During this part of the assessment, it's important to identify if the zones are also relevant or critical. This is also important as it defines whether a zone is directly (Critical) or indirectly (Relevant) in supporting the areas identified as MA and/or LES.

The OG86 provides a good definition of what should be considered MA and LES. The guidance also explains how you can represent Non-MA/LES. The option is either classifying them as Non-MA within the marked zone or alternatively excluding them from the defined IACS boundary.

Upon completion of this activity, MA/LES and Non-MA/LES should have been clearly established along with the assets within the identified zones. This is an important part of the risk assessment process as it must be clear that the Non-MA/LES zones have been considered even though they are not considered for the remainder of the assessment when looking at the applied countermeasures.

Zone	**Consequence**	**Criticality**	**Comment**
SCADA Control System	MA	Critical	Identified as MA as identified risks reside within BPCS (Basic Process Control System) zone.
Safety Instrumented System	MA	Critical	Identified as MA as identified risks reside within SIS zone.
DMZ (Demilitarized zone)	Non-MA	N/A	Categorised as Non-MA from a cyber security point of view, as identified risks are outside of the DMZ system, segregated by firewall protections.

Table 1 - Example Zone Criticality Output

OG86 Understanding Potential Threats

To understand the potential threats, we need to define what a threat is. If we refer to the IEC62443 standard, threats are defined as "the potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm" (IEC, 2020).

With this in mind, we then need to look at each of the identified MA/LES zones and start to identify what threats might be posed against each. At this stage, it will be a case of going through the identified zones and looking at the threat scenarios that are applicable to each one.

As a part of this process the types of threat actors that are likely to affect the systems under consideration must be identified. An example of this would be considering who is likely to be able to affect the system and what threat would each identified actor present.

A few common examples that can be considered are:

- Hackers who are likely to present a deliberate misconfiguration or deploy malicious software.
- Insider attackers who could tamper with the system or deliberately cause a release.
- Physical intruders who may be able to gain access to the system resulting in tampering or damage to the system along with potential loss of system confidentially and integrity.

The three examples above provide a varied contrast showing that when considering threat types, you need to consider not only digital threats but physical and potential insider threats too.

The OG86 guidance provides some threat examples such as unauthorised access, deliberate misconfiguration, Denial of service, etc. However, it will be down to the duty holder to assess, on a case-by-case basis, which threats are applicable for the identified MA/LES asset.

During the assessment, discussions may also lead to new threat scenarios being added or removed based on both documentation and site experience. Before moving onto the next stage or assigning countermeasures, it is important to ensure that all reasonably foreseeable threat scenarios have been considered that are relevant to the site.

OG86 Pulling it all together and assigning countermeasures

The final step in the OG86 risk assessment will be to assign the identified technical and physical countermeasures along with consolidating all the information into a final report.

When assigning countermeasures, it is good to start by entering the identified zones which have been designated as MA and or LES into a table and then adding in the identified threat actors and threat scenarios as discussed above. With these key parts filled into the table we can then start to introduce the countermeasures (CM). It should be noted at this stage that the HSE have an expectation that multiple countermeasures should be considered where possible rather than relying on one single solution.

The HSE have broken down the overall Cyber Security Management System (CSMS) into four sections; managing security risk, protecting against cyber-attack, detecting cyber security events and minimising the impact of cyber security incidents. Guidance on most system countermeasures can be found in sections B and C. These countermeasures are directed towards the protection of the required system and detection of security events.

A list of expected countermeasures to be considered can also be found in Appendix 5 of the OG86 document. The list is comprised of guidance from the NCSC Network & Information Systems regulations (NIS), IEC62443-3-1 and other industry best practices. It should be noted that the list is not designed to be an exhaustive list and the HSE advises that in the future the list may be updated as the cyber threat landscape evolves (Health and Safety Executive, 2021). The risk assessment of course can include additional countermeasures that may not have been considered in the current HSE guidance.

At this stage of the assessment, each of the CMs against the zone and asset should have been assigned along with a record of whether the identified countermeasure has already been implemented or not. This may consist of two columns, one showing the existing identified CMs and another with ‘ideas for improvement’.

The final risk assessment report will need to include the findings from the criticality phase along with the defined zones, threat scenarios, asset components and identification of technical countermeasures required. It should also include all the documented findings from the workshops and discussions to highlight that the risk assessment has been conducted in an appropriate manner.

From the findings, wherever the countermeasures implemented are not sufficient, recommendations should be made to address the short comings and to help identify where additional controls are required.

At the end of the assessment, the organisation should have a report identifying the cyber security risks faced, along with consideration for appropriate protections and recommendations for areas of improvements to protect the site from the identified potential cyber security threats. It is worth remembering at this stage that once the assessment is completed, it should be reviewed every three to five years or anytime a major system modification is undertaken in a zone that may have changed designation.

OG86 Risk assessment limitations

OT cybersecurity is relatively new in comparison to that of the IT industry which has been developing for decades. Therefore, it should be no surprise that there are limitations with the OG86 approach as there are equally with IEC62443, NIS and other standards as cyber security in OT is still finding its feet. The NCSC alludes to this fact that all risk assessments have their strengths and weaknesses, and that it is our responsibility to make sure we are aware of them (NCSC, 2017).

One of the major limitations with conducting an OG86 risk assessment is that the assessment is based around the severity of a zone being affected. This results in providing more of a hazard assessment rather than a risk assessment as it does not consider the likelihood of the risk. An example of this limitation can be observed by considering two zones both identified as having the potential to cause a MA, however one zone is connected to an external source such as the internet and the other zone is only affected by a user accessing a controlled area with a USB device. With an OG86 assessment both zones will be identified as MA and the consequence may be the same, however in reality we can see one zone has a much higher risk and should be prioritised.

Another limitation that can be observed regarding the OG86 assessment is that it is predominantly concerned with the health and safety risk category. It goes without saying that health and safety is a critically important aspect of cyber security. However, it is not the only part that could be considered when assessing cyber threats. Other risk assessments often explore beyond this and consider additional areas of risk such as, financial, and reputational impacts, and environmental impacts along with disclosure of confidential information.

These additional areas of risk will not necessarily have a health or safety impact and therefore can often be overlooked in an OG86 assessment. However, they can still have a devastating impact on the business with potential long-term implications. Financial risk and loss of production are commonly the largest risks faced as considerable effort is put into safety systems ensuring they fail safe protecting life. They are not however designed to prevent the loss of sensitive information.

A further limitation of the OG86 Risk assessment is that once all the countermeasures are defined the assessment concludes. This results in no further investigation into identifying the strength of the countermeasures implemented and if they meet all

the required levels of protection needed. An alternative approach can be observed in the security levels as defined by the IEC62443 standard which helps duty holders to identify the level of risk posed to their systems along with the required target level. This in turn allows more appropriate protections to be implemented based on not only how the identified risk affects the system but also looking at the likelihood of the risk too.

The OG86 assessment, by its nature of not weighing the threat against potential risk, results in a challenge of prioritising tasks. When comparing this against an IEC62443 assessment we can see that the criticality is assigned by applying a rating against each category for each identified system. This in turn then provides guidance in prioritising which systems require more dedicated attention.

System Under Consideration	**Category**	**Criticality**	**Rational and Comments**
SCADA Control System	Health & Safety	High	Identified as high risk due to the potential of causing major loss of life, current protections fail to adequately protect the system.
Batch Control System	Financial	High	Identified as high risk due to the potential of causing major financial loss and significant impact on production affecting quality and/or availability.
Training System	Confidentiality	Very Low	Identified as very low risk due to system having 'view only' access rights with no confidential information stored on system.

Table 2 - Example IEC62443 Criticality Assessment

Summary

Revisiting what we have discussed so far, it is clear that cyber security is an important topic. It needs to be considered, not just because cyber threats are increasing, but because cyber threats can seriously affect our existing protections and mitigation layers. This is why OG86 is critical in the development of OT cyber security around health and safety.

As the prevalence of IIoT increases and its popularity grows, so will the threats that are related to them. This interconnectivity, as discussed earlier, poses a risk, and therefore also needs to be considered from a cyber security point of view. As we move further away from decentralisation and onto more advanced controls (Artificial Intelligence), process data analytics and mobile connectivity, our protections must also evolve.

By performing cyber security risk assessments, it not only helps to reduce and manage the impact of attacks but also provides a methodical approach to continuously assess and address risks. Additionally, it reduces the potential financial impacts faced, as undertaking a risk assessment will provide better visibility of potential risks and enables an organisation to more efficiently plan actions to address those risks before being impacted.

As mentioned before, performing cyber risk assessments is a regulatory requirement especially for COMAH sites. Avoiding cyber security risk assessments leaves you not only potentially vulnerable to risks but also failing to comply with the required cyber security standards.

For site owners who are looking to further understand their systems regarding cyber security beyond the health and safety aspect, additional standards may also be worth reviewing in tandem with the OG86 guidance. Some additional established good practices and standards to review would be the IEC62443 standard, NCSC guidance or NIS Framework, all of which provide further guidance and practices in developing cyber security understanding and compliance.

Cyber security needs to be viewed as a continuous journey where it is built-in as one of the foundational structures of a system, much in the same way that function safety is a crucial part of a safe site design.

References

Chen Thomas M and Abu-Nimeh Saeed Lessons from Stuxnet [Article] // Computer. - Swansea USA : IEEE, 2011. - 4 : Vol. 44.

Ell Maddy and Gallucci Robbie Cyber Security Breaches Survey 2022 [Report]. - London : Department for Digital, Culture, Media, and sport, 2022.

Geissbauer Reinhard et al. Industry 4.0: Building the digital enterprise [Report]. - Munich : PWC, 2016.

Health and Safety Executive OG86 - Cyber Security for Industrial Automation and Control Systems (IACS) [Online]. - 1 October 2021. - 31 January 2022. - https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf.

IEC Functional Safety – Safety instrumented systems for [Book]. - [s.l.] : International Electrotechnical Commission, 2016. - Vol. 2.

IEC Functional Safety of Electrical/Electronic/Programable Electronic Safety-Related Systems - Part 1 [Book]. - [s.l.] : International Electrotechnical Commission, 2010. - Vol. Edition 2.

IEC IEC 62443 International Standard [Book]. - Geneva : International Electrotechnical Commission (IEC), 2020. - 1.0.

Jones Emma and Smart Harry Cyber Security Breaches Survey 2021 [Report]. - London : Department for Digital, Culture, Media, and Sport, 2021.

Karmakar Avish et al. Industrial Internet of Things: A Review [Conference] // 2019 International Conference on Opto-Electronics and Applied Optics (Optronix). - Kolkata : [s.n.], 2019. - pp. 1-6.

Meany Tom Functional Safety and Industrie 4.0 [Conference] // 28th Irish Signals and Systems Conference (ISSC). - Ireland : IEEE, 2017.

NCSC Get the basics right: risk management principles for cyber security [Report]. - London : NCSC.GOV.UK, 2017.

NCSC NCSC Secure design principles: Design principles and Operational Technology [Report]. - London : NCSC.GOV.UK, 2020.

TechRepublic Ransomware: A cheat sheet for professionals [Report]. - Nashville : TechRepublic, 2021.

The Independent IT-Security Institute Malware Statistics & Trends report [Report]. - [s.l.] : AVTEST, 2022.

Verizon Verizon 2021 Data Breach Investigations Report. - New York : Verizon, 2021.