INDUSTRIAL CONTROL SYSTEMS
Community of Interest

# Vulnerability Management in Industrial Control Systems / Operational Technology Environments.

## Introduction

NCSC has generalised vulnerability management guidance which can be found here - Vulnerability management, while this article is part of a series of Industrial Control System (ICS)/Operational Technology (OT) specific guidance articles on vulnerability management. In this article we shall be focussing specifically on the vulnerability management challenges that exist within ICS/OT environments and how they can be addressed.

This article is written to not only inform staff with Information Technology (IT) backgrounds on the different approaches required for vulnerability management in ICS/OT environments, but also for those with ICS/OT environments experience who are now responsible for the cyber security of these environments.

As a guidance document it presents potential mitigations against vulnerabilities within the context of an ICS/OT environment. Recommendations are framed within this environment and consider the operating constraints and requirements of such an environment. For the purposes of this document the term software encompasses both software and firmware loaded onto devices.

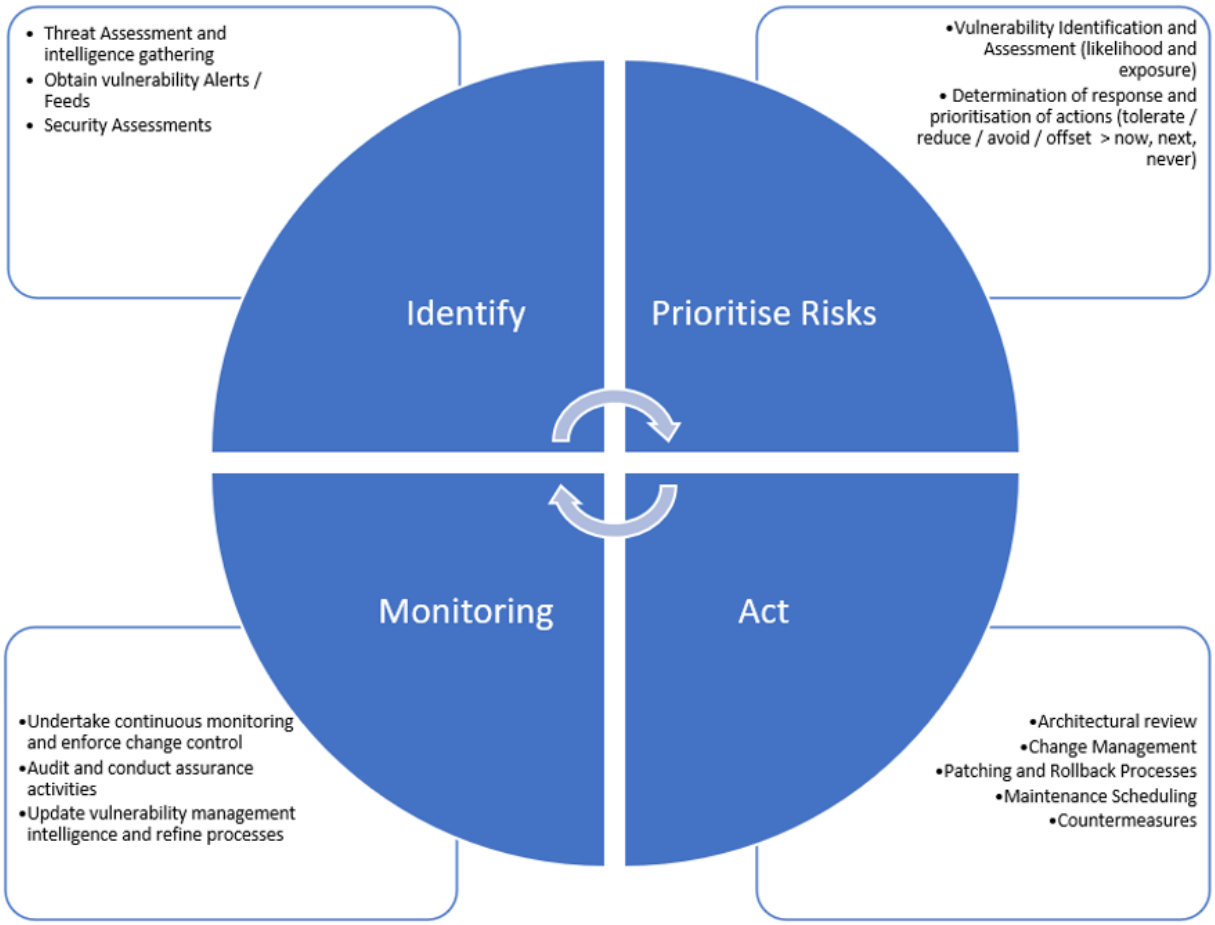
It is important to note that this guidance document does not cover vulnerability management for Privileged Access Workstations (PAWs) that should be used to securely configure and maintain ICS/OT environments. NCSC has published separate guidance for the secure use of PAWs that can be found here: https://www.ncsc.gov.uk/collection/principles-for-secure-paws.

Having a formally defined vulnerability management approach is critical for ICS/OT asset owners and the supply chain to ensure that vulnerabilities affecting assets are identified, rationalised and mitigated accordingly to minimise the potential for an adversary to target vulnerable assets. This approach requires accurate, meaningful threat intelligence to allow stakeholders to evaluate the capabilities and techniques used by threat actors, while assurance enables ICS/OT asset owners and the supply chain to proactively identify vulnerabilities and fix the vulnerability, or if not possible, apply compensating controls to mitigate the risk of exploitation. When a potential threat is identified, applying mitigation strategies further assists in minimising the impact of exploitation.

It is essential that ICS/OT asset owners and the supply chain make active efforts to manage vulnerabilities when they are identified given the protection of these systems is vital for the day-to-day operation of an organisation and the essential functions it provides.

# Vulnerability Management Process

Effective management of vulnerabilities within an ICS/OT environment requires asset owners and operators to identify, prioritise and mitigate, to reduce the likelihood of exploitation and ensure the safety and reliability of critical systems are maintained. This process is detailed in the diagram below:




This requires regular assessment of all assets against known exploited vulnerabilities requires collaboration with Threat Intelligence, System Owners and Architects for a complete assessment of exploitability and exposure, along with the identification of recommended mitigations. To achieve this aim, it is necessary to be able to:

- understand the assets within the ICS/OT environment (related ICS COI guidance can be found here)
- identify relevant vulnerabilities and if they are being exploited,

- assess and prioritise appropriate responses,
- undertake the identified responses to mitigate or otherwise while continuing to monitor the assets.

## Challenges of ICS/OT vulnerability mitigation

Many organisations have developed a mature, well-defined capacity for vulnerability mitigation within the IT domain. This typically focuses on timely implementation of incremental software updates and system updates as they become available. Unfortunately, the nature of the systems and operating requirements of the ICS/OT environment presents several challenges that prevent the adoption of traditional IT approaches all together.

ICS/OT environments have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses. ICS/OT environments have different performance and reliability requirements and use Operating Systems (OSs) and applications that may not be typical in an IT environment.

The following lists some special considerations when considering vulnerability mitigation for ICS/OT.

**Availability Requirements -** Many ICS/OT processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or years in advance. Pre-deployment testing is essential to ensure high availability (i.e., reliability) for the service provided. ICS/OT systems often cannot be stopped and started without affecting production. Therefore, typical IT approaches (e.g., rebooting a component) are usually not acceptable for ICS/OT environments due to the adverse impact on the requirements for high availability, reliability, and maintainability. Some ICS/OT environments employ redundant components, often running in parallel, to provide continuity when primary components are unavailable, but this cannot be assumed. (Where there are redundant components, this can significantly enhance the ability to test patches and upgrades).

**Complexity of ICS/OT Environments. -** ICS/OT environments can have complex interactions with physical processes and where field devices (e.g., Programmable Logic Controllers (PLCs), operator stations, Distributed Control Systems (DCS) controllers) are

directly responsible for controlling physical processes. Many existing ICS/OT installations are unique to the asset being managed and consist of multiple bespoke applications and functions side by side with complex dependencies and low levels of change to ensure stability. While an approved patch/update may be compatible with a number of hosted applications, it may not be compatible with all applications. Applying patches/updates in these situations can have significant negative impacts to the safety and/or availability demanded within operational environment. Introducing any form of change into the environment, if not fully understood, can lead to consequences in the ICS/OT domain that manifest in physical events. In the case of safety-critical systems, application of patches/updates often requires extensive testing to verify the patch/update does not impact on the required functionality of the system being updated. Where necessary this can require formal certification of engineering hardware and software applications to verify the correct operation of the system. Regression testing should be performed before deployment on a representative/pre-production system and verified once deployed to live (to ensure that it was successfully implemented as tested). It is common for ICS/OT devices to not be backed up regularly, if at all, (because of this then there is apprehension to roll out changes because regressing back may have never been fully tested).

**System Operation. -** staff operating ICS/OT environments are often quite different from their IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel. Assumptions that differences are insignificant can have disastrous consequences on system operations.

**Managed Support. -** For ICS/OT, service support is in some instances available only from a single vendor. In some cases, third-party security solutions are not allowed due to ICS/OT vendor licensing and service agreements, and loss of service support can occur if third-party applications are installed without vendor acknowledgement or approval.

**Testing Environments** - Quite often Operators have a lack of a mature security testing environments for their ICS/OT environment, and this can hinder the testing of vulnerability patches, upgrades and mitigations, this challenge also impacts the confidence and time to react.

**Component Lifetime -** Typical IT components have a lifetime on the order of three to five years due to the quick evolution of technology. For ICS/OT where technology has been developed in many cases for specific uses and implementations, the lifetime of the deployed technology is often in the order of 10 to 15 years, and sometimes longer. The related hardware warranties match this lifetime.

**Component Location -** Most IT components and some ICS/OT components are located in business and commercial facilities physically accessible by local transportation. Remote locations may be utilised for backup facilities. Distributed ICS/OT components may be isolated, remote, and require extensive transportation effort to reach (e.g. an offshore oil rig or an offshore wind farm). Component location also needs to consider necessary physical and environmental security measures.

The following table summarises some of the typical differences between IT and ICS/OT systems:

| **Category** | **Information Technology** | **Industrial Control System / Operational Technology** |
|---|---|---|
| **Performance Requirements** | Non-real time<br><br>Stochastic<br><br>Response must be consistent.<br><br>High throughput is demanded.<br><br>High delay and jitter may be acceptable.<br><br>Emergency interaction is less critical.<br><br>Tightly restricted access control can be implemented to the degree necessary for security. | Real-time<br><br>Determinism with Real Time<br><br>Response is time critical.<br><br>Modest throughput is acceptable.<br><br>High delay and/or jitter is not acceptable.<br><br>Response to human and other emergency interaction is critical.<br><br>Access to ICS/OT environments should be strictly controlled but should not hamper or interfere with human-machine interaction.<br><br>Response to Environmental changes<br><br>Responses to Asset changes |

| | | |
|---|---|---|
| **Availability (Reliability) Requirements** | Responses such as rebooting are acceptable.<br><br>Availability deficiencies can often be tolerated, depending on the system's operational requirements. | Availability deficiencies can often be tolerated, depending on the system's operational requirements. |
| **Risk Management Requirements** | Manage data.<br><br>Data confidentiality and integrity is paramount.<br><br>Fault tolerance is less important – momentary downtime is not always a major risk.<br><br>Loss of data confidentiality (Secret information, Intellectual Property, PII) leading to significant fines, reputational impact, loss of competitive advantage. | Control physical world.<br><br>Fault tolerance is essential; even momentary downtime may not be acceptable.<br><br>Major risk impacts are regulatory non-compliance, environmental impacts, and loss of life, equipment, or production. |
| **System Operation** | Systems are designed for use with typical OSs.<br><br>Upgrades are straightforward with the availability of automated deployment tools. | Systems often use differing and possibly proprietary OSs, sometimes without security capabilities built in.<br><br>Software changes must be carefully made, because of the specialized control algorithms and perhaps modified hardware and software involved. |

| | | |
|---|---|---|
| **Communications** | Standard communications protocols<br><br>Primarily wired networks with some localized wireless capabilities<br><br>Typical IT networking practices | Many proprietary and standard communication protocols<br><br>Several types of communications media used, including dedicated wire and wireless (radio and satellite)<br><br>Complex networks that sometimes require the expertise of control engineers |
| **Change Management** | Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated. | Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the ICS/OT system is maintained. ICS/OT outages often must be planned and scheduled days/years in advance. |
| **Managed Support** | Allow for diversified support styles. | Service support could be via a single vendor. |
| **Component Lifetime** | Lifetime on the order of three to five years | Lifetime on the order of 10 to 15 years |
| **Components Location** | Components are usually local and easy to access. | Components can be isolated, remote, and require extensive physical effort to gain access to them. |

When looking to address vulnerabilities in any live production ICS/OT environment a cross-functional team of control engineers, control system operators, and IT security professionals must work closely to understand the possible implications for the installation, operation, and maintenance of vulnerability mitigations where it is essential that the potential safety or reliability impacts of introducing changes into the environment are fully understood.

In some cases, these limitations can delay timely implementation of system updates and patches considered normal in an IT environment. Limitations may mean that patches/updates cannot be applied leaving a system vulnerable to compromise. Therefore, new strategies and techniques should be considered alongside conventional IT vulnerability management programmes to ensure the resilience of ICS/OT environments.

## Asset Management and understanding

Key to understanding the vulnerabilities within an ICS/OT environment, is also the knowledge of the assets that make up the ICS/OT environment. Further information on helping understand the assets within an ICS/OT environments, can be found in the ICS COI series on Asset Management. Critical to allow any asset knowledge base to support vulnerability management, is the ability to link to Common Vulnerabilities and Exposures (CVE). To facilitate this asset knowledge base must be Common Platform Enumeration (CPE) compliant.

Asset Management is key to understanding:

- Threat Intelligence/Advisory focus
- Location of asset and potential exposure
- Last patch or upgrade information

## Information on System and Component Vulnerabilities

System vulnerabilities can be discovered in any of the hardware, firmware and software used within an ICS/OT environment and have the potential to compromise the security of all devices in use. There are a range of sources that can provide information on system and component vulnerabilities, a selection is presented below:

**Vulnerability Lists -** Vulnerability lists provide a free, searchable, publicly available list of cyber security vulnerabilities. Each vulnerability is uniquely identified and is linked to software or hardware versions, most commonly through the CVE list maintained by MITRE, and supplemented by the National Vulnerability Database (NVD). CISA also have a Known Exploited Vulnerabilities Catalogue, that helps provide understanding if the vulnerability has been exploited in the wild. The purpose of the CVE Program is to identify, define, and catalogue publicly disclosed cybersecurity vulnerabilities. The Common Weakness Enumeration (CWE) is a list of software and hardware vulnerabilities that serves as a common language for describing and identifying weaknesses. Most ICS/OT vendors are

named as CVE numbering authorities, where an advisory will be issued with a CVE identifier.

Vendors and operators should look to join the CERT/CC Vulnerability Information and Coordination Environment (VINCE)

The NVD, provided by NIST, supplements the CVE information with a list of affected products (via CPE), and references to public documentation, the Common Vulnerability Scoring System (CVSS) score, and a vendor advisory. While additional information such as descriptions, references, remediation advice and severity scores are included from other sources. It should be noted that the severity score is from the perspective of traditional IT environment, with confidentiality of primary concern, whereas this is often not the case within ICS/OT environments, where availability is often the primary concern. Therefore, these ratings should be used as an indicative guide only and organisations should also factor in the impact exploiting the vulnerability will cause, and their own particular context of operation. In many cases there is a requirement to fully address the individual ICS/OT environments, recognising that the impact of the same vulnerability on different ICS/OT assets won't always be the same. Similarly, the remediation solution is often related to patching or updating software, which is not always a viable option for ICS/OT equipment.

The industrial vulnerability scoring system (IVSS) is a derivative of the CVSS. Currently in BETA, the IVSS, however, is designed specifically for industrial control system vulnerabilities. The organisation will have to determine their own risk acceptance threshold for patching or updating of equipment. Whilst NVD and the MITRE CVE database provide an authoritative source for vulnerability information, errors may exist, where many vendors have a dedicated product cyber security team, publishing advisories to customers, which provides dedicated, accurate, information on the vulnerability and may be updated in a more frequent cycle to the National Vulnerability Database. In some cases, vendor advisories may be restricted to authenticated users, or those with a support contract.

**Cyber Threat Information sharing -** Cyber threat information sharing is the exchange of knowledge about threats, incidents, vulnerabilities, mitigations, leading practices, or tools relevant to a technology-based/technology-leveraged risk set. By participating in information sharing schemes organisations are able to take a collective defence approach, receiving information to aid them in the protection of their own networks. NCSC provides a CISP platform to support sharing of threat related information to operators.

**Open-Source information -** Often information on common vulnerabilities and threats to systems can be found by analysing information available on public websites. Several

websites provide the results of scanning of devices connected to the internet or maintain incident databases. This information is then compiled into a searchable database and made available. Any systems identified by these sources should immediately be investigated and risk assessed to determine if they should remain externally connected and ensure that they have sufficient protection in place. To help identify threats from low resource threat actors, organisations can monitor the availability of freely available hacking tools. Analysis of these can provide an insight into the capabilities available to all threats. Similarly, regular searching of version control repositories can show what is readily available to attackers. The US Cyber Security and Infrastructure Security Agency (CISA) provides vulnerability advisories for ICS/OT environments.

**Vendors – Generic -** One of the main sources of information on vulnerabilities within hardware/firmware is the vendors themselves. Most vendors will maintain a database of vulnerabilities, these must be carefully analysed before use as multiple CVEs are often addressed through a single bulletin. Information is delivered through a variety of sources. Complete historical datasets can usually be found through a vendor's website, which should be consulted whenever new assets are added to the system. Most companies also offer mailing lists that will send out information on the latest patch/update and vulnerabilities in a timely manner. It is recommended that subscriptions to mailing lists either go to a shared e-mail address or to more than one employee to remove a single point of failure if an employee leaves the company.

**Vendors - Third Party -** Where organisations have maintenance contracts with third party vendors it is recommended that the service provision includes vulnerability disclosure and management associated with the equipment under contract. This could provide useful information if components covered under the contract are in use in other systems within the organisation. Third parties often have a wider view of the threats across the industry sector and any vulnerabilities identified can be used to benefit multiple organisations. If existing contracts do not include the notification of identified vulnerabilities within their products, then clauses should be added to any future contractual terms.

**Paid for feeds -** Many external cyber security companies offer subscription-based services providing the latest threat information, including not just vulnerabilities but adversarial identification, indicators of compromise and more. Whilst there are far more services covering the IT sphere an increasing number of companies are now offering ICS/OT specific vulnerability management solutions as additional services. To further enhance the usefulness of this information many organisations also offer threat intelligence feeds. This information is tailored to your systems and reduces the effort of identifying applicability to

your estate.  As with any solution there may be gaps within the threat intelligence. Without proper understanding of your assets, you may end up trying to view too much information which can be overwhelming therefore, and you sift through masses of information not applicable to you. Needs to be targeted and include information regarding your systems.

## Vulnerability Prioritisation Strategies

Once you understand the assets within your ICS/OT environment and have married them up with relevant vulnerability information, the next stage is then to prioritise those elements that need attention. Vulnerability prioritisation to aid remediation within an ICS/OT environment should include:

- **Contextual Prioritisation** - Understanding the Vulnerabilities - their impact and likelihood.
- **Risk-Based approach** - Assessing the risk to the organisation, the value of the asset and consequence of the exploit.
- **Exploitation Status** - understand if the vulnerability is or likely to be exploited.
- **Threat** - Who is likely to or able to attack or exploit the system/vulnerability?
- **Regulatory requirement** - Critical assets may require prompt remediations/replacements due to regulatory requirement or compliance to industry standards.

A more detailed list of elements to consider is included in the Assessment Criteria section below.

Carnegie Mellon University's Software Engineering Institute, in collaboration with the US's Cybersecurity & Infrastructure Security Agency (CISA), created the Stakeholder-Specific Vulnerability Categorisation (SSVC) system in 2019 to provide the cyber community a vulnerability analysis methodology that accounts for a vulnerability's exploitation status, impacts to safety, and prevalence of the affected product in a singular system. Further information on how CISA use SSVC can be found here https://www.cisa.gov/sites/default/files/publications/cisa-ssvc-guide 508c.pdf, while information on how to apply in a non-CISA specific manner can be found here.

## Scheduled Downtime

As many processes require continuous operation it is vital that any solutions are incorporated into scheduled downtime. Where this is possible the prioritisation strategies can be used to determine which are the most critical vulnerabilities to remediate and what options to fix the vulnerability should be explored. Vulnerabilities that are deemed so critical that they cannot wait for scheduled downtime and therefore a mitigation is required within a very short period of time. Where this is the case, it may not be possible to fix the vulnerability and instead the most appropriate option to reduce the exploitability must be chosen.

## Assessment Criteria

Identifying critical systems is crucial for making these prioritisation decisions. Do not simply assume that given a systems relative criticality it must prioritised. Often these assets carry the highest operational or safety risk if impacted by any mitigation applied. Provided "secure by design" practices were adopted when developing the ICS/OT architecture (although it is important to note that this is quite often not the case), it is likely that these assets are well defended, sat behind multiple levels of protection that can reduce the likelihood of any exploit being realised. Owners and operators should consider a range of factors to establish an overall risk scoring for prioritisation based on operational risk. For example, assets in Purdue Level 3.5 (DMZ) and Level 3 (Plant supervisory) have greater exposure to external networks, but more often provide supervision of engineering or remote access tools which are often not real-time systems. So have an overall lower risk of interruption but higher risk of exploit, therefore, may be identified as high priority. With assets that are connected systems in the ICS/OT environment, either connected to third parties, different vendors, and the outside world, especially if a path to the internet exists on these assets, are typically at the highest risk to many of the ICS/OT vulnerabilities that surface. Other considerations to be assessed may be whether there are mitigating factors to the operational risks that would support timely patching/updating. For example, systems that have redundancy built in could potentially go higher up the priority list if they are relatively easy to take offline. In many cases, realisation of an unacceptable consequence (e.g. operational disruption, causing a safety incident) requires an interaction with the physical environment. This allows for a wide range of mitigating actions to be considered.

When assessing vulnerabilities, factors that should be taken into consideration include but are not limited to:

- **Severity** of the threat.  Whilst common practice across both IT and ICS/OT, it is important to note that the impact to engineering processes cannot be adequately represented through the likes of CVSS scoring, due to the diversity of the ICS/OT environment.  Therefore, the CVSS should be weighted less than in IT provisions with greater emphasis placed on the environment. As previously mentioned IVSS tries to rectify this scoring.
- **Environment** of the system it is related to.
- **Significance** of any impact resulting from a compromise of the system.
- **Extent** of connectivity of the system to other assets, especially in relation to the access needed to exploit the specific vulnerability.
- **Existence** of known exploits, and whether those exploits are being actively deployed.
- **Conditions** that are necessary for the vulnerability to be successfully executed including the degree of sophistication required to execute the exploit. If there is remote exploit capability the risk may be deemed higher than if it can only be exploited locally.
- **Risk Appetite** to accept the vulnerability and manage the risk.
- **Exploitability** - Existence of known exploits, and whether those exploits are being actively deployed, and by whom (noting that some organisations will be a higher target for Nation State attacks and should take this into account more than hacktivist/criminal activity).

## Prioritisation

The above factors, especially in relation to the significance of any consequence resulting from a compromise within the ICS/OT environment, can be factored into an assessment process that prioritises vulnerability mitigation based on Now, Next and Never.

- **Now** - The significance of the consequence, and the ease with which it can be exploited, presents an unacceptable risk that requires mitigation(s) to be implemented immediately.
- **Next** - The significance of the consequence, and the ease with which it can be exploited, presents a tolerable risk that requires the mitigation to be implemented at the next scheduled routine opportunity (e.g. maintenance window, plant outage).
- **Never** - The significance of consequence, and the ease with which it can be exploited, presents an acceptable risk that requires no further mitigation to be implemented.

In all cases, a record of the assessment should be kept, especially in relation to those vulnerabilities for which it is chosen not to undertake any action.

With regards to timelines, good practice would be looking to achieve the following from a perdue model perspective:

Levels 5 and 5 - follow the standard NCSC Vulnerability Management guidance timelines:

- Internet-facing services and software equal 5 days,
- Operating system and applications equal 7 days,
- Internal/air-gapped service and software equal 14 days

Level 3.5/DMZ – follow the standard NCSC Vulnerability Management guidance timelines:

- Internet-facing services and software equal 5 days,
- Operating system and applications equal 7 days,
- Internal/air-gapped service and software equal 14 days

Level 3 - follow the standard NCSC Vulnerability Management guidance timelines:

- Operating system and applications equal 7 days,

Level 2, 1 and 0 - follow the triage and assessment process outlined in the section "Assessment Criteria".

## Controls and Mitigations

When seeking to mitigate vulnerabilities within an ICS/OT environment, elimination of the vulnerability should be the priority. Where it is not possible to eliminate the vulnerability (e.g. due to an operational constraint) it may be possible to prevent exploitation of the vulnerability through the application of mitigations and controls which reduce or eliminate the ability for the vulnerability to be exploited (often referred to as "virtual patching". Any mitigation strategy adopted should consider how to respond to an exploit of the vulnerability by providing containment and further controls to constrain or negate the impact if exploited.

Within ICS/OT environments the option of fixing the vulnerability is not always possible. Where, for example, the availability of source code and or compatible hardware limits options available to resolve flaws. This is frequently the situation for systems that

have dropped out of active support from the original system integrator or manufacturer. Requiring potentially much larger (rip and replace) replacement upgrade strategies to be considered for the environment with associated technical and cost challenges if seeking to eliminate vulnerabilities. It is in these cases where the approach to reduce the ability for the vulnerability to be exploited (isolating the system) come to the fore where the adoption of appropriate and proportionate countermeasures to prevent exploit of the vulnerability may be the most sensible option to take. Managing the risk posed by the vulnerability throughout the operational lifetime.

Mitigations that address vulnerabilities in the system design or alternatively measures used to establish additional layers of defence, in general, can be assigned to one of three categories: technical control measures, physical control measures or organisational (administrative) control measures. All three categories should be considered when determining suitable mitigations.

- **Technical** control measures are hardware and/or software used to prevent, detect, mitigate the consequences of an intrusion or another malicious act. Technical controls can include effective segregation, segmentation, firewall rules, airgaps, and flow control.
- **Physical** control measures are physical barriers that protect installations and supporting assets from physical damage and unauthorised physical access. Physical control measures include locks, physical encasements, tamper indicating devices, isolation rooms, gates, and guards.
- **Administrative** control measures are policies, procedures and practices designed to protect assets by providing instructions for actions of employees and third-party personnel. Administrative control measures specify permitted, necessary, and forbidden actions by employees and third-party personnel. Administrative control measures may include operational and management control measures. (It is worth noting that administrative controls may not be followed by employees of third-party personnel and therefore are not effective by themselves).

## Fixing the vulnerability

In general, options for mitigating actions to fix a vulnerability are listed below; however, the chosen mitigation strategy will be dependent on practical considerations:

- Remove the vulnerable component.
- Upgrade the component to a version not containing the vulnerability. Note - An upgrade may contain patches and new/improved features. Upgrades may be hardware, software or firmware.
- Re-engineer the component to eliminate the vulnerability.
- Patch/update the vulnerability. A patch/update is a piece of software which prevents a vulnerability or vulnerabilities being exploited – it may do this by removing the vulnerability.

Consideration of the most appropriate option should take into account the following:

- If the software component is obsolete and not supported by the Original Equipment Manufacturer (OEM) the only mitigation for an unacceptable risk is to replace the software component or ensure it cannot be exploited.
- If the software component is obsolete but still supported by the OEM it may be possible to patch/update, but consideration should be given to upgrading.
- If the software component is relatively new and still supported by the OEM it is probably better to patch/update where patches/updates are provided.

Some manufacturers do not release patches but only upgrades, sometimes referred to as ‘rolling releases’. These upgrades will include patches as well as new or improved features.

Deploying patches/updates to ICS/OT environments requires additional considerations for organisations, including testing and validation to ensure the patches/updates do not impact operational capabilities or safety. Where vendor supplied patches/updates are deployed, you should always look to ensure the patch/update is validated by the vendor, and ensure any requirements identified in release notes are implemented. Installation of a patch/update is then treated as a modification and should follow the recognised change management process which includes appropriate validation, certification as well as contingency (rollback) plans. As with any modification, whenever possible, patches/updates should be tested on an off-line system (test environment) to ensure they function correctly, and do not cause problems before being deployed to a production system.

When deploying patches/updates on ICS/OT systems it is advisable to plan patches and updates during scheduled maintenance windows for the environment and ensure that a recovery plan for the ICS/OT component or system being patched/updated is available.

## Reducing Exploitability of new vulnerabilities

Examples of mitigating actions to reduce the ability for the vulnerability to be exploited are listed below; however, the chosen mitigation strategy will be dependent on practical considerations:

**System Isolation -** Isolating the systems into a separate security zone with compensation controls applied. This isolation could be through:

- Isolation of the system by disconnection from a network
- Implementation of firewalls to segment the network

One potential solution is the implementation of additional security zones as defined by IEC62443. Any device with an identified vulnerability could be placed into either an entirely separate zone or a sub-zone of the existing configuration along with other devices with a low security level. A layer 2 device such as a switch can be segmented into VLANs, however, it cannot act as a conduit between the VLANs. A layer 3 switch or router is required for this.

The traffic passing between the low security devices and higher Security Level (SL) zones through the conduit will be monitored by intrusion detection systems. Traffic within the zone can be restricted using firewall rules on a default deny basis, any required exceptions added must be included in the zoning documentation to ensure compliance with IEC-62443-3-2.

**Virtual Patching -** Virtual patching can be an effective method to reduce risk in the time between discovery of a vulnerability and implementation of any preferred longer term mitigation strategy to eliminate the vulnerability from the environment.

Virtual patching is effectively creation of a security policy enforcement layer which prevents the exploitation of a known vulnerability. The security enforcement layer analyses interactions between nodes and blocks attacks in transit, so malicious traffic never reaches the intended target. While the actual component has not been modified, the effect of applying the additional security policy is to render the exploit vector ineffective.

Virtual patching can be implemented through the application of:

- firewall rules (preventing systems from being accessed using vulnerable ports (this could be on a host-based or network-based firewall),
- an Intrusion Prevention System (IPS) (blocking known exploits),
- application layer filter,

each designed to protect the network from the exploitation of specific vulnerabilities. In all cases, monitoring and logging of the applied control should be implemented.

Adopting this approach, the risk of exploitation can be reduced in the short to medium term, allowing time to evaluate the risk the vulnerability poses to the operational environment, it may not even be exploitable, while developing a longer-term mitigation strategy.

In some cases, the organisation will be able to address the vulnerability at the component or application level which will allow virtual patching rules for that vulnerability to be removed.

In other situations where a correction to the mechanics of the network is not feasible (proprietary code, legacy system, prohibitive cost, patch unavailable) the rules specific to that vulnerability may remain in effect as part of an overall defence in depth approach to security.

Whilst it may be tempting to leave in place a virtual patch rather than seeking to eliminate the vulnerability, virtual patching should not be seen as a long-term fix for security vulnerabilities. As the network changes due to operational demands, systems are updated and reconfigured; the effectiveness of the virtual patch may not be maintained, exposing the vulnerability to a successful attack vector. There are also risks associated with the configuration of the security policy itself. A policy that is more restrictive, one that blocks more traffic across a network for example, has a higher chance of blocking legitimate traffic and interrupting normal operation.

Benefits of deploying virtual patching within ICS/OT environments include:

- **Rapid Response to Threats** - Virtual patching enables immediate protection against newly discovered vulnerabilities. This rapid response is crucial in ICS/OT environments where applying traditional patches can be delayed due to operational constraints. (This very much depends on whether you have the network architecture

to support this. Another important point is that in a well architected network with connectivity limited to the minimum necessary, this wouldn't be needed. This illustrates the importance of prioritising a secure network architecture for the ICS/OT environment, over software firmware updating for security purposes)

- **Minimises Downtime** - Traditional patching often requires system downtime, which can disrupt critical operations. Virtual patching reduces the need for such downtime, maintaining operational continuity.
- **Extends Life of Legacy Systems** - Many ICS/OT systems are legacy systems that no longer receive vendor support or updates. Virtual patching provides an essential layer of security for these systems, ensuring they remain protected against modern threats.
- **Compliance and Risk Management** - Virtual patching helps operators meet regulatory requirements and manage cyber security risks effectively by addressing known vulnerabilities promptly and continuously.

**Enhanced Monitoring and alerting -** Application of enhanced monitoring and alerting, potentially further enhanced using rules to identify known remote exploit attempts. Implementing additional monitoring of network traffic, allows a response to be initiated to prevent exploitation of a vulnerability from realising an unacceptable impact.

Where it's not possible to prevent malicious traffic reaching the component, additional monitoring for known exploits can be implemented, along with appropriate response arrangements that ensure that any undesirable activity resulting from the vulnerability being exploited can't be realised.  Coupled with this is the additional training requirement to ensure that operators understand the information presented by the Intrusion Detection/Prevention System and can react accordingly.

**Changes to Administrative/Access controls -** Implement more stringent access management to reduce potential impact of exploitation.

The implementation of Identity and Access Management (IDAM) solutions as a mitigation technique should be targeted at higher risk assets in conjunction with network architectural controls to separate and segment assets to ensure that unauthorised connections to vulnerable endpoints are minimised. Ideally the availability of the services will already exist within an ICS/OT environment, if not the cost deployment of such techniques should be balanced against risk reduction achieved for the protection afforded given that network segregation and separation may offer greater opportunity for risk reduction.

Additional measures can also be implemented to better control physical access to the component, restricting access to those who have authority to access the system for a legitimate purpose.

**Respond and Recover -** Implement appropriate Respond and Recover controls to mitigate the impact of a vulnerability.

Whilst it is obvious to many that the need to prevent an incident resulting from a vulnerability is paramount, it cannot be understated that there is no such thing as 100% protection. When an incident does occur, there is only the ability to swiftly and effectively return to normal operations.

To ensure a return to operational business as quickly as possible, careful consideration should be made to the back-up system and the schedule to which it is set. Traditional daily/weekly/monthly scheduling that is used for office automation environments do not necessarily transfer appropriately to ICS/OT environments. An ICS/OT back-up strategy should be considerably different to that of the office system due to the varied priorities of the environment. (See ICS/OT Specific IR guidance)

The rate of change for ICS/OT environments may be a lot lower and the data that is required to be "saved" is more likely to be configuration of assets rather than the actual information. All of this should be considered when the routine scheduling is being defined.

Additionally, a full back-up of the asset should be taken prior to any change or update (such as patching) so that a failed change/patch can be reversed easily. Once an update or patch has been confirmed successful, another full back-up should be taken so that the latest known good configuration is then available for recovery.

It is necessary to define the ICS/OT environment recovery priorities to ensure that the correct assets are returned to normal operating in a timely manner. Therefore, the back-up and recovery strategy should define the Short-Term Recovery procedure for Critical Systems, followed by the Long-Term Recovery for the rest of the environment.

Where mitigating actions are providing additional Protect (as defined in the NIST Identify, Protect, Detect, Respond, Recover framework) controls, it is often also necessary to implement additional Detect (and associated Respond) controls, e.g. monitoring of network traffic to ensure configured rules aren't being by-passed, to ensure the risk is adequately mitigated.

## Conclusions

As previously highlighted, ICS/OT assets and environments are fundamentally different from their IT counterparts, solutions designed for IT vulnerability mitigation can be applied to IT based Hosts/servers/applications within ICS/OT environments but are not suitable for use on ICS/OT assets. Tailored strategies and processes are therefore required, where this document highlights how these may be achieved. It is important to note that when selecting the most appropriate mitigation, the urgency and criticality of that vulnerability must be considered in the context of the environment, which ultimately informs the appropriate mitigation to be taken. When the immediate threat of exploitation has passed, the vulnerability will remain, where a transition to longer-term solutions can be implemented, or the vulnerability remains a managed risk.

Vulnerability management is but one of many contributing functions which underpin ICS/OT security, where regular asset and infrastructure reviews drive decision making to proactive improvements to reduce the risk of exploitation, and the risk of an asset in general. Effective logging and monitoring, coupled with a rigorously tested and exercised recovery plan enables ICS/OT asset owners to identify potential exploitation, and subsequently recover in the case where a vulnerability cannot be mitigated in time before exploited. Vulnerability management, therefore, is a critical function that supports asset owners, and the supply chain manage cyber security risk to their infrastructure and asset estate, supported by pre- and post-incident measures.

## Related Standards

In ICS/OT environments, the criticality of effective vulnerability and patch /update management is reflected in standards such as:

- NERC CIP-007 (System Security Management)
- NERC CIP-010 (Configuration Change Management and Vulnerability Assessments)
- NIST SP 800-40 Rev. 3 (Guide to Enterprise Patch Management Technologies)
- ISA/IEC TR 62443-2-3 (Patch Management in the Industrial Automation and Control System Environment)
- ISO29147 (Vulnerability Disclosure)
- ISO30111 (Vulnerability Handling Techniques)

## CAF IGP Summary

This guidance discusses measures that contribute to the following CAF IGPs:

- B4D.A01 - You maintain a current understanding of the exposure of your essential function(s) to publicly known vulnerabilities.
- B4D.A02 - Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly.
- B4D.A03 - You regularly test to fully understand the vulnerabilities of the network and information systems that support the operation of your essential function(s) and verify this understanding with third-party testing.
- B4D.A04 - You maximise the use of supported software, firmware and hardware in your network and information systems supporting your essential function(s).
- B4D.PA03 - Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.
- B4D.PA04 - You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology.

## Statement of support

This guidance has been produced with support from NCC Group, Scottish Power Energy Networks, Bridewell Consulting, members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by NCC Group, Scottish Power Energy Networks, Bridewell Consulting, the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.