ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

MANAGING CONFLICTS IN VULNERABILITY AND PATCH MANAGEMENT FOR IT AND OT

Robert Kemp
De Montfort University, United Kingdom
rob.kemp1@hotmail.com

Richard Smith
De Montfort University, United Kingdom
rgs@dmu.ac.uk

Abstract

All organisations need to manage vulnerabilities and a keyway to do that is to patch their assets. However, for critical infrastructure organisations that have Information Technology (IT) and Operational Technology (OT) devices and a strong focus on both safety and security ensuring those controls are implemented can be difficult. This paper will analysis the requirements of patching and vulnerability management and establish conflicts that can occur for IT and OT. A process to manage these conflicts will be created, including calculations to establish vulnerability and patch ratings. A case study will be used to show the controls being implemented. The paper concluded that conflicts and issues can be resolved and provided methods to resolve them. Often the conflicts are related to if a control goes wrong rather than a control that is implemented correctly causing a conflict. The process created will allow critical infrastructure organisations to implement the required controls without impacting safety and security.

Keywords: Vulnerability management, patch management, safety, security, IT, OT

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors

Introduction

Often organisations look to balance Information Technology (IT) security risks with the need for the organisation to operate its core business. Whereas organisations that manage critical infrastructure need to also balance safety risks and Operational Technology (OT) risks.

Safety, security, IT and OT have similarities and differences, by understanding the similarities and differences organisations will be able to better select controls and mange conflicts between the two areas. Safety and security should not be treated in isolation (Lisova et al., 2019) and will be more effective when controls are applied taking both into consideration.

Two control areas where this can be seen is vulnerability management and patch management. Critical Infrastructure (CI) organisations have safety and security standards they may follow or comply with and the standards especially security will require these two control areas to be implemented.

Vulnerability management is looking to detect and reduce vulnerabilities. One way to do this is via patch management which is focused on applying code known as patches to software used by the CI organisation. The number of vulnerabilities and patches continue to raise (Furnell, 2016) which adds more pressure for organisation's to manage the vulnerabilities and patches promptly as the risk is increasing.

Problem and Novelty of Solution

The main problems this paper is going to resolve are IT and OT are managed and configured differently (Homeland Security, 2016) which means the security controls that are applied to IT can conflict with safety objectives and cause issues for OT. It can be difficult to implement the controls and comply with safety and security standards (Kanamaru, 2020) as they have different aims and objectives.

This aim of this paper is to propose a process that will work for both IT and OT while maintaining both safety and security. To create this process the paper will highlight conflicts and issues and ways to resolve those issues. Another solution to the problems will be to use calculations to establish the OT vulnerability risk rating and the patch assessment rating which will establish how critical the patch is and the impact on the organisation of patching.

There are processes that describe how to create a vulnerability and patch management process (National Institute of Standards and Technology, 2013), but they are designed for standard organisation's and not CI organisation's. Even when a process does consider CI it does not resolve many of the conflicts that IT and OT have and usually just recommends the same controls are applied on IT and OT. This is often not possible or could impact the operation of the CI organization.

The rest of the paper is organized as follows section 2 will discuss the differences between safety, security, IT and OT. Section 3 will introduce the case study that is used to show the controls being implemented. Then section 4 will explain the controls for vulnerability and patch management. The conflicts and issues and how to resolve them will be presented in section 5. Section 6 will present two calculations that have been created to help assess vulnerability and patch management. The final section in the paper is section 7 the conclusion.

Differences with Safety, Security, IT and OT

Safety and Security

ISO 2700 - Information security management systems (International Organization for Standardization, 2017) defines security as "preservation of confidentiality, integrity and availability of information" while IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems (International Electrotechnical Commission, 2010) define safety as "freedom from unacceptable risk" they are both quite high level statements but in general safety is usually seen as protecting people from harm while security is seen as protecting data the organisation has.

Safety has in the past been seen to focus on accidental risks while security on intentional risks (Kriaa et al., 2015) but that has begun to change. Intentional risks can also cause a safety incident such as a malicious user purposely opening a flood gate. Also, accidental risks such as a flood can impact security's aim to preserve the availability of data, so that difference is now much smaller with them both having more in common.

Often safety risks were considered equipment failure or natural hazards which although are still the case many other threats that are more security related are now in scope of safety risks. Such as data manipulation, or remote access being gained to the safety systems. From a security perspective security risks were considered external threats. Hoeever, now they can also be internal and equipment failure and natural hazards are threats that security teams also need to manage. This shows that differences in the past are now beginning to be less significant with the current way CI organisations are operating.

A difference that also impacts the way safety and security interacts is that they are managed by separate teams who often take a different view and approach to the areas they manage. This can make it more difficult when both areas are converging more and ensuring an efficient way of working is achieved.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

As IT, OT and the components that CI organisations require become more integrated this also brings safety and security closer together as security incidents can now lead to safety incidents which is another reason both areas need to be managed in a more integrated manner.

Vulnerability and patch management will need to be applied to different parts of the CI organisation such as IT, OT, buildings and components such as sensors and valves as a few examples. A large amount of the controls will be aimed at IT and OT so it is important to describe what each one is and the differences they have as by understanding the differences the CI organisation should be able to better understand how to apply the controls to both.

IT and OT

Both terms are overarching terms and within them there are other terms that are used to describe the components that make up IT and OT. For example, in IT terms such as servers, networks and applications are used and within OT some examples can be Supervisory Control and Data Acquisition (SCADA), Human-Machine Interface (HMI) and Programmable Logic Controller (PLC). Within each of the other terms it can be more detailed such as a financial applications or PLC for a sensor etc.

(Kriaa et al., 2015) mentioned that safety and security were two distinct fields, but they are beginning to converge more and will continue to do so and the same can be said for IT and OT. IT systems were used as business tools for activities such as spreadsheets, communication and file storage as examples. While OT were separate and used to manage industrial operations such as physical equipment including valves and pipelines these systems were very different and were often separate from the IT systems (National Institute of Standards and Technology, 2015). For many reasons including efficiency and cost OT systems are being connected to the Internet and beginning to use IT systems such as connecting with laptops which have USB and standard operating systems installed. This has advantages but also disadvantages as the risks that IT systems faced are now being faced by OT systems (Holcomb, 2015). However, as will be described they are not designed to operate in the same way and for that reason cannot always use the same controls in the same manner to manage those risks. Compared to OT (Conklin, 2016) highlights, IT systems have over the years been designed with more security inbuilt or security controls have been created to help protect the IT systems and the information they contain the same cannot be said for OT. The focus on OT was to ensure it was reliable and available when needed to help ensure safety of the components it managed and overall safety of the CI organisation. Due to the way OT was setup security especially Internet based risks were not seen as a major concern. However, as IT and OT converge security is now becoming much more important for OT.

A difference between IT and OT is the lifespan of the technology, OT is expected to have a much longer lifespan it can be over 20 years while IT is usually much shorter such as around 5 years (Owl, 2019). Even though IT systems have a shorter lifespan they have updates applied throughout that time to help them stay secure and resolve vulnerabilities that were not known at the time of release. OT does not apply the same principal on updates to their systems as there is a strong focus on not impacting availability which an update could have. However, security risks can also impact availability, so this difference needs to be overcome.

It does depend on the what the task is for the IT system but in general the monitoring and response of an OT system will be more time sensitive (Bimco, 2020) due to the nature of what it is controlling. An alert on a file server could be reviewed within 24 hours while an alert on a pressure sensor will need to be reviewed almost instantly.

IT systems are more open and have better integration with other IT systems while OT systems tend to use proprietary systems that do not always integrate well with other OT or IT systems. This can mean different OT systems have to be supported by different users and vendors.

Resources is another place IT and OT differ. IT systems can have their resources increased more easily and have enough resources for controls such as anti-virus software to be installed on them. Whereas OT it is not as easy to add resources (National Institute of Standards and Technology, 2015) and, they tend to be created with the necessary resources to do their task and not have extra resources for controls such as antivirus software.

It was mentioned OT systems are focused on safety and IT systems are more focused on security due to this many of the current security controls cannot always be applied to both systems. For example vulnerability scanning takes place on IT but is not as common in OT for fear of impacting the running of the OT systems. Network protocols for IT systems are common and well known while OT are niche and may not be understood by the current network security tools on the market. OT systems connect with physical real-world devices such as sensors and gates while IT systems do not usually manage those devices. This difference can be seen in the strong need for safety controls on OT but not as much in IT systems.

As the previous few sections have shown it will not always be possible to take the IT security controls and place them on the OT systems to make them secure. The differences in the two areas mean that at times this will not be likely and other solutions will be required. Also, the differences between safety and security can cause issues with the implementation of safety and security controls and will require further work.

Case Study

A case study has been created to highlight how controls can be applied and how conflicts can be identified and resolved within the case study.

An electricity company called East London Power (ELP) has a dam and hydroelectric power station in Essex and provides electricity to the local area. They employ 200 people and are based in two locations the first is the location of the dam and hydroelectric power station which is on the River Lea and the other is their office location which is based in East London. They also utilise outsourced support companies.

The company is divided in to three different areas:

- Dam and power station - Area of responsibility is the maintenance of the dam and power station and the production of the electricity.
- Commercial – This part of the business manages the selling of the electricity and handles all account management.

resources to do their task and not have extra resources for controls such as antivirus software.

It was mentioned OT systems are focused on safety and IT systems are more focused on security due to this many of the current security controls cannot always be applied to both systems. For example vulnerability scanning takes place on IT but is not as common in OT for fear of impacting the running of the OT systems. Network protocols for IT systems are common and well known while OT are niche and may not be understood by the current network security tools on the market. OT systems connect with physical real-world devices such as sensors and gates while IT systems do not usually manage those devices. This difference can be seen in the strong need for safety controls on OT but not as much in IT systems.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

As the previous few sections have shown it will not always be possible to take the IT security controls and place them on the OT systems to make them secure. The differences in the two areas mean that at times this will not be likely and other solutions will be required. Also, the differences between safety and security can cause issues with the implementation of safety and security controls and will require further work.

Case Study

A case study has been created to highlight how controls can be applied and how conflicts can be identified and resolved within the case study.

An electricity company called East London Power (ELP) has a dam and hydroelectric power station in Essex and provides electricity to the local area. They employ 200 people and are based in two locations the first is the location of the dam and hydroelectric power station which is on the River Lea and the other is their office location which is based in East London. They also utilise outsourced support companies.

The company is divided in to three different areas:

- Dam and power station - Area of responsibility is the maintenance of the dam and power station and the production of the electricity.

Commercial – This part of the business manages the selling of the electricity and handles all account management

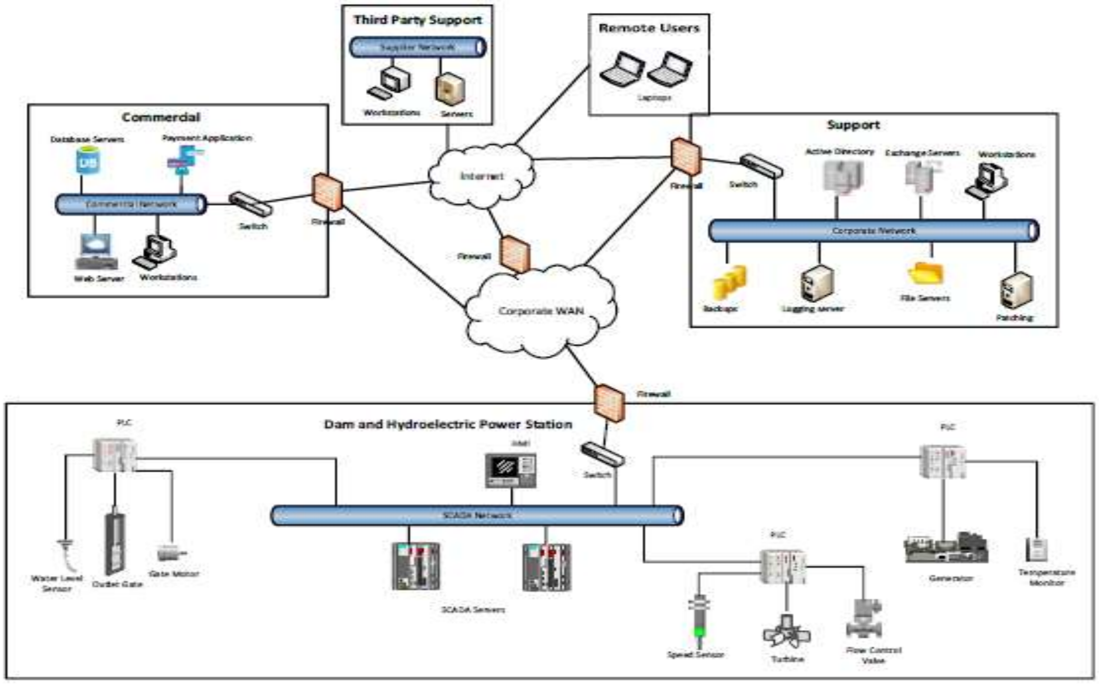


Figure 1 - ELP Network Layout

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

Vulnerability and Patch Management Controls

This section will list the main controls and then use the case study to show how the controls can be implemented and where conflicts can arise. **Error! Reference source not found.** gives a brief description of the control. Control areas often overlap and some controls from another area may be needed for the vulnerability and patch management controls to operate correctly these controls will be highlighted as supporting controls but will not be covered in detail here.

Table 1 - Vulnerability and Patch Management Controls

Control	Description
Asset inventory	A complete asset inventory is required so that the CI organisation knows what assets it has to patch and check for vulnerabilities. This is a control area in its own right and is more a supporting control for this section.
Monitor vulnerability sources	Vendors such as Microsoft, Abode and organisation's such as CVE and NVD release information about vulnerabilities that are discovered. CI organisation's should monitor these sources for information and check them against their systems to see if they are vulnerable.
Vulnerability scans	One of the main controls within vulnerability management is using a vulnerability scanning tool to scan the assets and look for vulnerabilities.
Vulnerability assessments	This can be other types of assessments were vulnerabilities can be identified such as during architectural reviews, lessons learned from incidents, audits and during project planning.
Penetration testing	This is a more advance and intrusive form of assessment. The penetration test will look to exploit the vulnerabilities and the testers will behavior in the same manner an attacker would to look for vulnerabilities in the systems.
Code analysis	If the code for the application is available this can be analysed and vulnerabilities identified.
Patch assessment	This will involve assessing if the patch is required, the criticality of the patch and what systems require it as examples.
Sourcing patches	Before the CI organisation can apply patches, it needs to gather the patches from the appropriate sources. This involves locating and securely receiving the patches.
Patch testing	Before patches are applied to all the production systems it should be tested to ensure it will not impact the systems. Testing should be done on a selection of systems.
Apply patches	One of the main controls of patch management is deploying the patches. This can be via an automated process or manually applying patches to the systems. The patch management configuration is also managed when applying patches.
Verify installation of patches	As potentially thousands of patches will be applied to the systems the CI organisation needs a way to verify the patches have been installed correctly.
Control governance	This is a generic term that captures all the governance tasks around the control such as reporting, establishing the team, metrics and providing remediation tasks to the relevant teams.

This list is just a brief description of each control and each control will have much more details and implementation options that the CI organisation must decide on. Standards such as ISO 27002- Security techniques — Code of practice for information security controls (International Organization for Standardization, 2013), NIST 800-40 Guide to Enterprise Patch Management Technologies (National Institute of Standards and Technology, 2013), and NERC CIP-010-2 - Cyber Security — Configuration Change Management and Vulnerability Assessments (North American Electric Reliability Corporation , 2016) can provide further information on the controls if required. What follows now is a few more details on certain key controls listed in Error! Reference source not found.

The first step is to understand what assets ELP has and identify if they are in scope for vulnerability and patch assessments. ELP has separated out their business into three distinct areas; dam and power station, commercial and support each area has assets that are in scope and selected. The commercial and support areas only have IT assets and have a strong focus on security while the dam and power station section have IT and OT assets and are concerned with safety and security.

A key part of the vulnerability management process is conducting vulnerability scans on the assets. ELP have decided to use a third-party vulnerability scanning appliance and to use a hybrid-cloud approach. The team selected this approach as it reduces the costs and still provides a good level of security. The commercial and support areas of the business will use the cloud version of the vulnerability scanning appliance which is cheaper than having an appliance on site while the dam and power station area will have an appliance onsite scanning the assets within that area. The team decided on this set up as it reduces the external connections into the dam and power station network and also keeps the information from the vulnerability scans internal to the network.

The team will look to use all controls in combination where it can, as this is better than just using one control such as vulnerability scanning only. Penetration testing and code analysis can identity other vulnerabilities that vulnerability scanning would not. Once ELP has identified the patches required for its assets, it needs to assess which patches to install and when. To assess the patches the team will need to consider the following points and from the point of view of installing and not installing the patch.

- Safety
- Security
- Productivity
- Downtime
- Threats
- Vulnerabilities
- Hazards

There are more but this should help the team focus on the main areas, and they are all related such as threats are part of safety and security for example. To help ELP assess their patches, a calculation (Equation 1-1) has been created that is used to give a patch assessment rating for each asset/patch combination. Section 6

Vulnerability and Patch Assessment **Calculations** describes the formula in detail.

A key part of the patch management process is applying the patches on the assets. ELP have decided to use a third-party patch management appliance to help apply the patches, the patching appliance is installed on a server in the head office and is located on the support network area. The patches will either be applied automatically or manually. If the patch is being deployed automatically then the third-party patch management appliance will be used and for the manual deployment the patching team will work with each asset owner and deploy the patches on each asset individually.

The assets that are receiving the patches automatically are located in all three areas of ELP which are commercial, support and the dam and power station. However, it will only be the IT assets in those areas that get them automatically the OT assets within the dam and power station will get them manually.

The patch management process that ELP has created, is designed to assess the risks of patching and not-patching on assets and provide the details needed to carry out the patching. It was mentioned that conflicts and issues can occur in the process between safety and security and between the different types of assets such as OT and IT. Also, problems can arise when patches cannot be applied or cause issues with the assets. The next two sections will focus on these conflicts and issues and provide guidance on what the CI organisation can do to resolve them.

Conflicts and Issue Resolution

The previous section described the controls that CI organisation's can use. This section will now analyses the conflicts that can occur and provide solutions that can be put in place.

Sourcing Vulnerabilities and Patches

Vulnerability and patching sources for OT is not as easy compared to IT. OT vendors do not publish as much detail on their vulnerabilities and in some cases the OT is so old the vendor is no longer providing patches and is unlikely to even be looking for vulnerabilities. The lack of vulnerability sources can mean it is harder to find details on vulnerabilities which in turn makes it harder to detect vulnerabilities within the OT systems.

Some potential solutions to this issue are to use the same vulnerability information that is used for IT as some may be applicable to OT as well. The CI organisation can directly approach vendors if patches do not appear to be available and enquire if and when they will be available. The OT manual can be used to find default settings that may be enabled which can be a vulnerability such as default passwords being used. Another control is to keep a record of when patches were last applied, if it is a long-time, patches may have been missed and should be inspected. Making vendors contractually required to provide patches if possible can be a good way to ensure they continue to provide patches. The CI organisation should build a strong relationship with other CI organisation's so they can share vulnerability and patching information that could impact them both. Other controls such as penetration testing and code analysis can provide vulnerability details. A final control if a vulnerability scan cannot be run on a device would be to use an asset management tool to find software versions and missing patches that way instead.

Sourcing Patches

Not all vendors will consider patching important and may not provide a good level of security around the patches and that can make it difficult for the patch management team to securely source the patches.

If that is the case the following methods can help. The CI organisation should contact the vendor for a secure transfer method instead of downloading from their website. They should analyse the code of the patch to see if there is anything malicious or that looks out of place. The patch should be installed in a sandboxed environment at first to monitor the patch activity and ensure it is as expected. Also, the file size should be checked and scanned for viruses.

Vulnerability Scanning Configuration

The vulnerability scanning configuration for IT will not be the most appropriate configuration for OT and can have conflicting areas. For that reason, the following configuration settings should be made for each area to reduce conflicts and issues.

The vulnerability scans for IT will be carried out monthly while OT scans will be quarterly. IT scans will take place overnight, while OT will depend on water levels and electricity demand and take place when the assets are less utilized. The IT scans will have no users involved and run on their own automatically. Whereas the OT scans have the following users involved:

- Vulnerability team – Monitoring the scan
- OT asset owner – In case of issue with the asset
- Safety and security team – To provide support if needed
- Vendor – On call for support if needed
- Dam and power station users – If issue with asset occurs can complete tasks manually while asset is unavailable

When the vulnerability scans take place, it is likely IT assets may have a backup system as part of other controls. For OT, if there is no backup system in place, the team should be onsite to manually do the job of the asset in case there is an issue and the asset is not available. A final difference is all IP addresses are scanned for IT devices, while only selected IP addresses will be scanned for OT.

Patch Testing

The main conflict for testing is the requirement that patches are tested before they are applied to the assets. There may be times when the patch cannot be tested first as it is only going on the one asset and there are no backup or spare assets for the test to be applied to.

There are several controls that can be put in place to resolve conflicts in patch testing. These are to use a patch assessment rating to understand the impact if the patch goes wrong and an assessment is created in section 6 for this use. That can help the team understand how much of a risk they are taking by patching without testing. The CI organisation could see if other organisation’s have had issues with the patch. To reduce the risk of applying a patch that has not been tested, owners of connected devices should test their device is not impacted and be onsite in case of issues.

Penetration Testing

Penetration testing can impact assets and an issue can occur if no backup or non-production version of the asset is available. To resolve those issues and lower the risk the following controls can be used.

The team carrying out the penetration testing should ensure the owners of the assets backup the data on the live systems before the test is conducted. An appropriate time that would cause minimum issues if the test negatively impacts the asset should be selected. In advance the asset owner should document how to carry out the process of the asset manually incase that is required. High risk tests such as Denial of Service (DoS) will not be carried out. Another option if possible is to use virtual assets for the penetration test instead of the live systems. However, the virtual asset should be an accurate representation of the production system.

Applying Patches

There are many conflicts with trying to apply patches in the same way for IT and OT. The conflicts and ways to resolve them are described in this section.

Some patches cannot work on the patching appliance and instead of being installed on the asset via the appliance will need to be done manually. The CI organisation should patch IT and OT at different times to reduce the risk of issues occurring on both at the same time. Within OT the team should consider whether to stagger the patches or do them at the same time for all devices. Staggering can reduce the risk of multiple devices being impacted at the same time but will require multiple downtimes for the CI organisation. The force reboot that is applied for IT patches should be disabled for OT patches with the asset owners being able to choose when is an appropriate time to reboot. This should be tracked to ensure it does take place.

Separate patching appliances can be setup in different network areas such as one for IT and OT. If there is only one patching appliance for all areas extra security controls should be implemented and care should be taken to ensure the different configuration settings for IT and OT are not mixed up and applied to the wrong areas. Another control is for the backup team to backup the asset before the patching takes place so an up to date backup is ready if needed. An outage could occur at the CI organisation for various reasons and the patching team could take advantage of the fact the devices are not in use and carry out the patching and required reboots at the same time. A potential problem with this control is that depending on what is the cause of the outage it may not be the best time to also carry out patching while the teams are dealing with an outage and the outage could be resolved before the patching finishes. A final control is if the patch is released but is not available for the current version of the asset the team can reverse engineer the patch to see what it is for and then attempt to manually resolve the issue on the asset if appliable.

Verify Patches

Verifying patches for IT can be done via the patch management appliance but as OT is done manually that may not be possible. For this reason, it can be difficult to verify manual patches compared to IT.

The CI organisation should consider the following options. Setting up Security Information and Event Management (SIEM) logging on the OT assets, ensuring any patch related logs are sent to the SIEM which can then report on the patch status. A different approach can be to scan the OT with an asset management tool to see if patches are installed. Also, before applying next month's patches the team can manually check the previous month's patches were applied and installed correctly.

Not Applying Patches

There will be times when a patch cannot be installed or is installed and has to be removed and when this happens other controls are needed. ELP uses a defense in depth approach to safety and security and do not rely on one control only. This means when the control of patching cannot be applied other controls will be used instead to reduce the overall risk.

Some example compensating controls are to increase logging and monitoring, to capture suspicious activity. The team should investigate the ability to upgrade the asset to a newer version. A newer version should be able to be patched. File integrity monitoring can be implemented on the asset to detect changes to files which can be a sign of compromise. Another compensating control is to set up an Intrusion Detection Systems (IDS) both host based, and network based to monitor traffic and actions. If possible remote access should be removed from

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

the asset, so the only way to access the device is in person physical access. The asset owner should disable certain features on the application that are not critical to reduce the attack service. Also, if the patch relates to a specific service look to disable that service or feature so it cannot be exploited. The CI organisation should isolate the system from other devices. This will make it more difficult to access to compromise and can reduce impact if compromised. Also, increasing user awareness so that users look out for suspicious activities.

The controls and activities that have been described in this section are designed to reduce the risks of conflicts or remove the conflicts and allow ELP to still carry out the vulnerability and patch management controls. The controls chosen will be dependent on the risk appetite of the CI organisation and the conflict that is occurring.

Vulnerability and Patch Assessment Calculations

Establishing what the risk of a vulnerability is or how a patch will impact an asset are often difficult to quantify. CI organisation's will have a risk management process which can help but this paper has created calculations specifically aimed at vulnerability and patch management.

Patch Assessment Rating

The patch assessment rating will establish how critical the patch is and the impact on the organisation of patching. Other papers have created patch calculations such as (Shariffdeen, et al., 2020) which created a calculation to apply patches to similar programs and (Wang et al., 2020) were patch correctness was calculated. These were used to help establish what should be considered in this paper's calculation.

For the patch assessment rating, the formula for the calculation is made up of several parts. The first part of the formula is Asset Value (AV) the team will need to understand and assign a value to the asset that is being patched. The AV can be a value between 1-10 with the higher the number the higher value the asset is. It should be noted that value here is not referring to a purely financial value.

The next part of the formula is the Safety Impact (SI) this is the safety impact the patch will have on the asset. The team need to consider will the patch improve the safety of the asset. Such as will it add more stability to the asset, or a new feature. Often patches are a preventative measure so will not improve safety and are more security focused. The team will give a value of 1-5 with the higher the number the more it will improve safety.

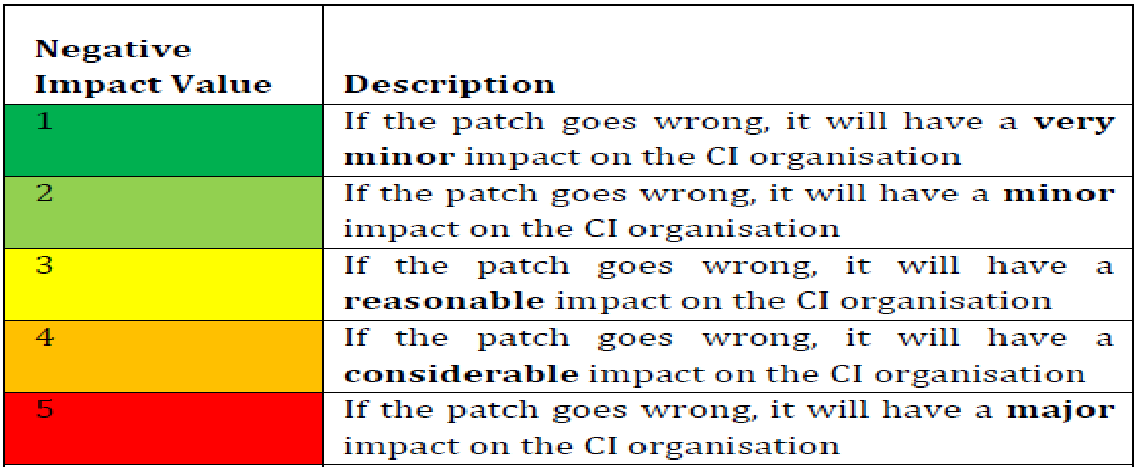
Security Impact (SecI) is similar to the Safety Impact but is based on security. The team will consider how the patch can improve the security of the asset. For example, are their known exploits that are in use for this vulnerability, can the vulnerability be exploited remotely and how difficult is the exploit to do. A major aim of patches are to resolve vulnerabilities and improve security so when the team are deciding on a the SecI they need to consider how big the security risk is that the patch applies to. Patches can also introduce security vulnerabilities even though it resolves one and that should also be considered when assigning a value. The team will give a value of 1-5 with the higher the number the more it will improve security.

The Productivity Impact (PI) part of the calculation is considering the impact the patch will have on the productivity of the asset and the overall organization. For example, will the asset need to reboot for the patch to install, will it remove some features of the software or slow the software or hardware down. The productivity of the asset could improve with the patch being installed, it may resolve issues that caused the software to crash or run slow or add new features that make users more efficient for example. The team need to assess all these issues and provide a value of between 1-5 with the higher the number the more of a positive impact the patch will have.

As with anything there is a risk that applying the patch could have a negative impact on the asset and/or organisation. This is what the Negative Impact (NI) value is focused on. The team need to look at what could go wrong with the patch such as if the asset is no longer able to perform the function that it is designed for, or it has become more unstable and crashes or has a degraded performance. What would be the impact of the CI organisation if that was the case. The team will consider what would be the consequences of an issue with the patch and give a value of between 1-5 with a higher value meaning a bigger impact would be possible. Error! Reference source not found. provides a description of each Negative Impact value between 1-5.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

Table 2 - Negative Impact Value provides a description for each value.



Negative Impact Value	Description
1	If the patch goes wrong, it will have a **very minor** impact on the CI organisation
2	If the patch goes wrong, it will have a **minor** impact on the CI organisation
3	If the patch goes wrong, it will have a **reasonable** impact on the CI organisation
4	If the patch goes wrong, it will have a **considerable** impact on the CI organisation
5	If the patch goes wrong, it will have a **major** impact on the CI organisation

Negative Impact Value Description
1 If the patch goes wrong, it will have a very minor impact on the CI organisation
2 If the patch goes wrong, it will have a minor impact on the CI organisation
3 If the patch goes wrong, it will have a reasonable impact on the CI organisation
4 If the patch goes wrong, it will have a considerable impact on the CI organisation
5 If the patch goes wrong, it will have a major impact on the CI organisation
Table 2 - Negative Impact Value

To establish how critical the patch is and what impact it will have on the CI organisation the following calculation is used:

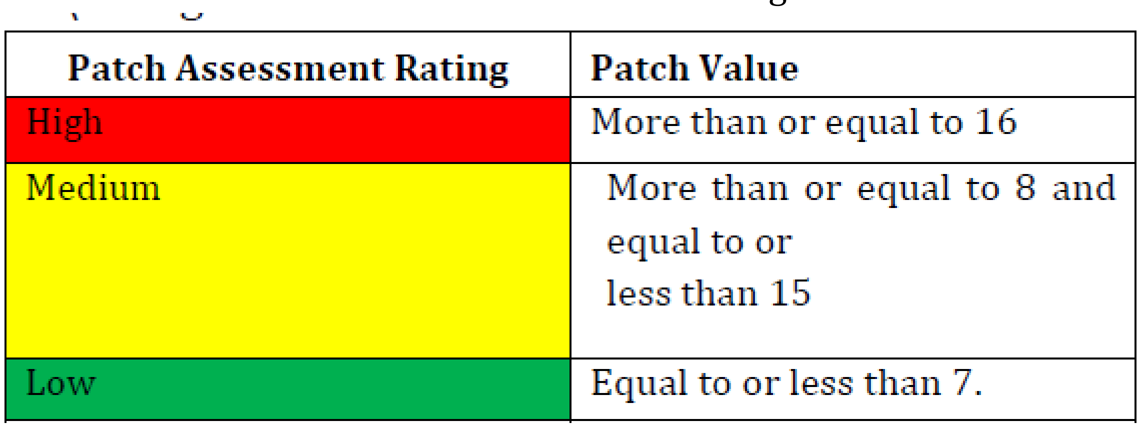
PV =AV+SI+SecI+PI Equation. 1-1

Where PV is the Patch Value. Error! Reference source not found. shows what ELP has decided the patch assessment ratings will equal for the patch value and the details of how the patch assessment ratings can impact patching will be discussed later. A higher patch assessment rating will show the patch has the potential to have a large positive impact on the asset\CI organisation.

Patch Assessment Rating Patch Value
High More than or equal to 16
Medium More than or equal to 8 and equal to or
less than 15
Low Equal to or less than 7.

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

Table 3 - Patch Assessment Rating



Patch Assessment Rating	Patch Value
High	More than or equal to 16
Medium	More than or equal to 8 and equal to or less than 15
Low	Equal to or less than 7.

As there is a risk when applying patches, the team also want to understand how that risk is balanced with the need to apply the patch. That is what the Negative Impact (NI) value that was given earlier is used for, Table 2 - Negative Impact Value shows the description for each value and the team will compare the patch assessment rating and the NI value. There is no set rule for what ELP will do when a certain patch assessment rating and negative impact value are selected for the asset it is just a guide to help the team gain a better understanding of the value the patch will bring and the potential impact if it goes wrong.

The patch assessment process considers many different things as this process is covering both safety and security so it requires assessing areas which may not be considered if it was just patching purely from a security perspective and not looking at both safety and security. The assessment will not be required for every single asset, the team will be able to group similar assets and conduct one assessment for them all. For example, all laptops within the commercial area can use the one assessment rating.

The patch assessment calculation is designed to not only give a value and a rating to the patches and assets but also it makes the users think about safety, security, issues and the assets themselves. This is important as the patches can have a range of positive and negative consequences which the users will consider as they work though the assessment and calculate patch assessment ratings.

OT Vulnerability Risk Rating

To help the CI organisation establish what the potential risk could be to the OT from vulnerability management a calculation has been created which the team can use to rate the risk for each asset. The calculation looks at the controls and OT differences compared to IT and potential solutions. Previous papers have created vulnerability risk calculations such as (Singh& Joshi, 2016) that created a model to estimate the security risk level of the vulnerability. While (Hong et al., 2014) used the Attack Representation Model (ARM) and included Importance Measures (IMs) to calculate what to patch. These papers helped to understand concepts needed for creating a vulnerability risk calculation such as the one used in this paper. The calculation and formulas are described next

Vulnerability Inherent Risk rating (VIRr) is the overall rating for the risk of vulnerability management on the asset before any conflict and issue solutions are applied. That rating is made up of the following figures:

Vulnerability Sources rating (VSr) – This is a rating of between 1 -5 for how well vulnerability sources are currently available for the asset not including the conflict and issues solutions. The higher the number the less resources are available.

Scanner Settings rating (SSr) - This is a rating of between 1 -5 for how well the CI organisation can separate IT and OT and use different scanners and scan settings. The higher the number means the appliances and settings are more likely to be the same for IT and OT.

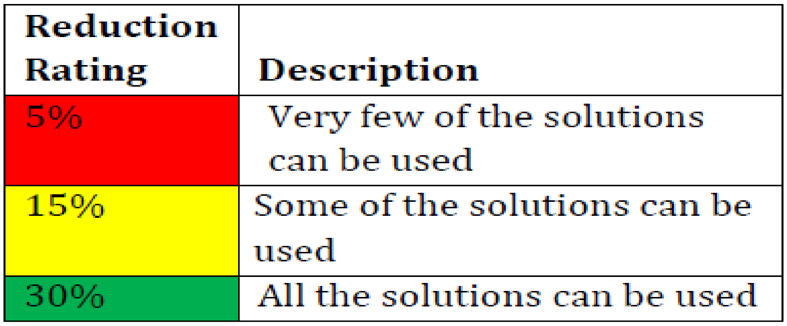
Penetration Test rating (PTr) – This is either a rating of 1 or 5 and it represents if the asset has a backup system that can be used for the penetration test instead of the production system. The rating of 1 is for yes and 5 is for no.

To summarise VIRr=VSr+SSr+PTr

The Vulnerability Rating risk percentage (VRrp) is the overall percentage that the conflict and issue solutions will help reduce the risk of vulnerability management on the asset. The rating is made up of the following figures:

Each rating is taken from Error! Reference source not found.. It can be seen that even with all solutions used the risk is only reduced 30% this is because the solutions cannot ensure the issues will not occur.

Table 4 - Vulnerability Rating risk percentage



Reduction Rating	Description
5%	Very few of the solutions can be used
15%	Some of the solutions can be used
30%	All the solutions can be used

ResearchJet Journal of Analysis and Inventions
https://reserchjet.academiascience.org

Vulnerability Sourcing Solutions (VSS) – Table 4 is used to select the description and rating that best suits the solutions that can be applied to that asset for vulnerability sourcing.

Scanner Settings Solutions (SSS) - Table 4 is used to select the description and rating that best suits the solutions that can be applied to that asset for the scanner solutions.

Penetration Test Solution (PTS) - Table 4 is used to select the description and rating that best suits the solutions that can be applied to that asset penetration solutions.

To summarise VRrp =VSS+SSS+PTS

N is the sum of the calculation of VIRr and VRrp.

Operational Technology Risk (OTr) –is the overall OT risk score of using vulnerability management on the asset. The higher the number the higher the risk is, each CI organisation can decide on their risk appetite and what level of risk they can have.

The formal calculation for the OT risk is:

$(VIRr \div 100) \times VRrp = N$

$VIRr - N = OTr$

These calculations can provide ratings for assets and allow CI organisation's to prioritize vulnerabilities and patches and also identify which are the higher risk and will require more controls.

Conclusion

A key aim of this paper was looking for conflicts in safety and security as well as within IT and OT. The controls that vulnerability management includes should improve safety and security. The main risk is around availability and if an asset becomes unavailable that could impact safety but that could impact security as well. The issues only occur if the control goes wrong rather than a control that is implemented correctly having a conflict with safety.

There can be various remediation activities depending on the vulnerability and they could cause safety conflicts or could have issues working on both IT and OT. It is important to understand remediation work from vulnerability management may in itself cause conflicts and issues and even more than the vulnerability management controls themselves. The team can use the vulnerability management calculation to help them prioritize the vulnerability findings and provide a risk rating for them.

The patch assessment calculation will help the CI organisation establish several important pieces of information including:

Asset value

Will it improve safety and security

What impact will it have on productivity

What are the consequences if the patch goes wrongWhat happens if the patch is not applied

Overall patch assessment rating

All of this information is used throughout the patch management process to help decide what other actions are required and how each patch and asset will be managed. The patch assessment phase has the potential during the assessment to identify conflicts and/or issues. For example, the assessment could highlight that an asset requires a patch but has no way for the patch to be tested before deployment. The Conflict and Issue Resolution section provided guidance that can be used when the patch assessment identifies those issues.

It is important to note that the conflicts and issues that are being discussed in this paper can apply to OT and IT. Often OT are the assets that have these issues but IT assets can also have conflicts and issues that means a patch cannot be applied or a server has no backup and requires high uptime but requires a reboot. The controls here can also be used for IT and OT, the key is to assess each asset\patch and calculate the risk and controls required to reduce that risk.

If patches are not applied this can impact security and safety. Often patches are aimed at a security vulnerability so not patching will be a security risk. However, it can also be a safety risk as if that device is compromised due to the missing patch a malicious user could take control of the connected assets such as the spillway gate and cause a flood which will be a safety issue. There is also the conflict that by applying the patch to improve security it could cause an issue with the asset which then impacts safety, the controls and issue resolution section has provided guidance on how to lessen that risk and resolve the conflict.

This paper has shown controls that can be applied for vulnerability and patch management and used a case study to demonstrate the controls being implemented. The conflicts and issues that could occur and ways to reduce those conflicts or lessen the risk of a safety or security incident were given.

The calculations that were presented can be used to help identify the level of risk involved and then the CI organisation can decide if more controls are needed to reduce the conflict or if the control will not be implemented at all and other compensating controls will be used instead.

Safety and security are very important for CI organisation's and with IT and OT playing a key part in both. Organisation's need to manage conflicts that can occur and find ways to implement controls while ensuring safety and/or security are not compromised.

References

1. Bimco. (2020). The Guidelines On Cyber Security Onboard Ships V3, Accessed 2020,https://www.bimco.org/about-us-and-ourmembers/publications/the-guidelines-on-cyber-security-onboard-ships
2. Conklin, W. (2016). IT vs. OT Security: A Time to Consider a Change in CIA to Include Resilienc. 2642-2647. 10.1109/HICSS.2016.331.
3. Furnell, S. (2016) Vulnerability management: Not a patch on where we should be?, Network Security, 5-9. DOI: 10.1016/S1353-4858(16)30036-8.
4. Holcomb, J. (2015). Definitive Guide to Cybersecurity for the Oil & Gas Industry, 2015, Accessed 2020, https://www.ciosummits.com/Online_Assets_Leidos_Definitive_Guide_to_Cyber_for_Oil_and_Gas_eBook.pdf
5. Homeland Security, (2016) Dams Sector Cybersecurity Capability Maturity Model (C2M2).
6. Hong, J., Kim, S., &Haqiq, A., (20014). What Vulnerability Do We Need to Patch First?. Proceedings of the International Conference on Dependable Systems and Networks. 684-689. 10.1109/DSN.2014.68.
7. International Electrotechnical Commission, (2010). Functional safety of electrical/electronic/ programmable electronic safety-related systems - Part 1: General requirements.
8. International Organization for Standardization. (2013). Security techniques — Code of practice for information security controls.
9. International Organization for Standardization, (2017). Information security management systems — Overview and vocabulary.
10. Kanamaru, H. (2020). Requirements for IT/OT Cooperation in Safe and Secure IACS. 39-44. 10.23919/SICE48898.2020.9240295.
11. Kriaa, S., Bouissou, M., Piètre-Cambacedes, L., & Halgand, Y. (2015). A Survey of Approaches Combining Safety and Security for Industrial Control Systems,

Reliability Engineering System Safety. DOI: 139. 156-178. 10.1016/j.ress.2015.02.008.

12. Lisova, E. Šljivo, I. & Causevic, A. (2019). Safety and Security Co-Analyses: A Systematic Literature Review. 833-833. 10.1109/COMPSAC.2019.00122.
13. National Institute of Standards and Technology, (2013), SP 800-40 Rev. 3 Guide to Enterprise Patch Management Technologies.
14. National Institute of Standards and Technology (2015). SP 800-82 REV. 2 Guide to Industrial Control Systems (ICS) Security.
15. North American Electric Reliability Corporation. (2016). CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments.
16. Owl. (2019). Protecting Critical Infrastructure in the DoD Landscape, Accessed 2020, https://owlcyberdefense.com/wp-content/uploads/2019/06/19-OWL-W013-V1-CI-in-the-DoD-Landscape.pdf
17. Shariffdeen, R. Tan, S. Gao, M & Roychoudhury, A. (2020). Automated Patch Transplantation. ACM Transactions on Software Engineering and Methodology. 30. 1-36. 10.1145/3412376.
18. Singh, U. & Joshi, Ch. (2016). Quantitative Security Risk Evaluation using CVSS Metrics by Estimation of Frequency and Maturity of Exploit, Proceedings of the World Congress on Engineering and Computer Science 2016 Vol I WCECS 2016, San Francisco, USA, October 19-21, 2016, ISBN: 978-988-14047-1-8, ISSN: 2078-0958 (Print), ISSN: 2078-0966 (Online).
19. Wang, S. Wen, M. Lin, B. Zou, D. Xiaoguang, M. Jin, H. Wu, H & Qin, Y. (2020). Automated Patch Correctness Assessment: How Far are We?. 10.1145/3324884.3416590.