Journal of Network and Information Security
10 (1) 2022, 12-28
http://www.publishingindia.com/jnis

# Combining Security and Safety Risk Management in Critical Infrastructure

Robert Kemp[1*] and Richard Smith[2]
[1]De Montfort University, Leicester, England, United Kingdom. Email: p2548837@my365.dmu.ac.uk
[2]De Montfort University, Leicester, England, United Kingdom.
*Corresponding Author

**Abstract: Within the critical infrastructure sector, risk management for safety and security are often treated as disjoint processes. Separating these processes creates duplication of effort when safety and security concerns align, and it will obscure the situations where a trade-off between safety and security needs to be resolved. This paper proposes a risk management process that enables an organisation to carry out safety and security risk assessment within one combined process. The results show that this is possible, but changes need to be made within the organisation and the process for it to be successful. Some examples of the changes are around terminology used, culture and how threats and hazards are assessed. The combining of the risk management process for safety and security can also support compliance to safety and security standards. Often organisations will need to comply with both standards and can leverage the combined risk management process to allow compliance without creating two separate risk management processes.**

**Keywords: Critical infrastructure, Risk Management, Safety, Security, Standards.**

## I. Introduction

The nature of Critical Infrastructure (CI) is that security is critical, most CI has a safety dimension as well. To help a CI organisation ensure safety and security is appropriate and managed properly, risk management processes need to be implemented. Often a separate safety and security risk management process is carried out, often driven by compliance needs from disparate standards. However, there is overlap in the safety and security domains [1] and they both have the goal of protecting the public from harm. Although there is overlap there are also differences, Pettersen [2] uses the example of safety risks being well known and consistent such as a component failure. While security risks are more unknown with a wider range of risks.

### *Problem and Novelty of Solution*

This paper presents a framework for joint safety and security risk assessments. This resolves a number of problems. One is removing the duplication of work within the safety and security risk management process [3], which requires the resolution of the subsidiary problem that the two areas tend to use different terminology [4], and this will be harmonised in this paper. The joint approach to safety and security will also address the problem that conflicts can arise [5] when trying to implement both safety and security controls.

Impact rating scales for safety and security will be combined in a single scale covering six attributes, from which an overall impact can be calculated using a proposed formula.

Risk treatment options will include safety and security controls and actions that can be carried out depending on the risk rating. This will ensure the controls are not considered in isolation. During the implementation of safety and security controls conflicts can occur. This risk management process will find and resolves conflicts and can identify conflicts before the controls are implemented.

This paper presents a risk management framework that combines the risk processes of both safety and security and will allow the CI organisation to carry out the assessment on both areas at the same time. The risk management process will also be in line with certain safety and security standards so that it can be used for CI organisations that also want or need to be compliant with a standard.

The standards that will be used are:

- ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [6].
- IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems [7].
- NERC Critical Infrastructure Protection (CIP) Standards [8].
- International Electrotechnical Commission, 61513:2013 Nuclear power plants — Instrumentation and control important to safety — General requirements for systems, 2013 [9].

These standards were chosen because they represent a good combination of a well-known general security standard (ISO

27001) and a well-known general safety standard (IEC 61508). NERC is a security standard aimed at CI and IEC 61513 is a safety standard aimed at nuclear power plants that are part of the CI sector. These standards will cover the type of standards that will be used by organisations and should have similarities and differences that will need to be managed.

Section III Current Literature analyses the various papers that have investigated safety and security risk management. It shows that although many papers have looked at it, few covers both areas and the whole risk management process. The approach proposed here is novel in combining the full security and safety risk management processes while also proposing a way to identify and resolve conflicts which is lacking in the papers that cover both areas.

The rest of the paper is organized as follows: Section II will provide the background on critical infrastructure. Section III will survey the current literature in the area of safety and security risk management. The proposed risk management framework is presented in Section IV. The conclusion and analysis of the proposed risk management framework will be the final section of the paper Section V.

## II. Critical Infrastructure

Each country may have a slightly different definition or list of industries that fall within CI. For example, in the United Kingdom the Centre for the Protection of National Infrastructure (CPNI) has defined Critical National Infrastructure as "facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends" and lists 13 national infrastructure sectors [10]. In the United States, the Department of Homeland Security defines it as "the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety" and states there are 16 critical infrastructure sectors [11]. They all cover roughly the same industries which include energy, health, water and finance as a few examples.

Incidents at CI organisations can have a large impact on society as they may lose access to basic services, they require for a normal standard of living such as running water or power. While their importance means security in CI is paramount, failures in CI can also lead to increased risk of injury or death, which implies there is also a dimension of safety. In 2010 the Macondo Oil Well [12] had a fire which resulted in 11 deaths and 17 serious injuries. To ensure the services are available and people are safe, security and safety in CI must be appropriately managed.

## III. Current Literature

There is extensive literature on security risk management, as well as on safety risk management. Discussion of the two areas in combination or contrast occurs much less frequently. Derock [13] discusses the similarities in the risk management processes in security and safety standards. They argue that ISO 27005 (Information technology — Information security risk management), is closely aligned with the risk management framework of ISO15026 (Systems and software engineering — Systems and software assurance). More so then the other safety standard ISO 61508 (Functional safety of electrical/electronic/programmable electronic safety-related systems). They then create at a high level a risk management framework that could be used by all standards. However, it does not go into enough detail. For example, it touches on how a common vocabulary is needed but does not explain how that will be achieved.

Stoneburner [14] offers two security and safety frameworks and also feels that they can be combined to cover safety and security but similar to Derock [13] does not go into the detail of how this can be achieved.

Taking a well-known safety methodology and adding security to that is one approach that can be used. Howard [15] proposes the use of the System-Theoretic Process Analysis (STPA) methodology as a base to build on to analyse security and safety requirements in CI. The paper takes a view of using a safety model as a base and adding security whereas Subramanian [16] uses a different approach and builds off a non-functional requirement model. A gap with the Subramanian [16] methodology is that it is very focused on the safety side. For example, it discusses hazard but has no mention of risks from a security perspective. Taking an already used methodology is a good approach but it is important not to get constrained within the methodology. Important security requirements such as threats to the integrity of the data such as data manipulation and key security concepts such as least privilege need to be included in the methodology.

Young [17] takes the hazard analysis technique STPA and adds security elements to it to create a new technique called STPA for Security (STPA-Sec). It looks at safety and security at a tactical level and does not consider confidentiality violations, but the author feels this can be added in later work. This technique on its own would not be enough to cover safety and security in CI as it focuses on software and lacks the does not consider confidentiality violations and safety and security standards and risk management processes would also be needed.

Friedberg [18] is building off the work of Young [17] and integrates safety analysis (STPA) and security analysis (STPA-sec) into one framework called STPA-SafeSec. The authors have tried to improve on STPA-Sec and have resolved some of the gaps it had. Such as introducing security constraints to the analysis and by mapping the abstract control level of the system that is analysed by STPA to real components. However, the model is more for analysing the risks to a system and not using standards and makes no mention of conflicts between safety and security or compensating controls that could be needed.

Risk management is a key area in both safety and security implementations. Merrell [19] like Derock [13] asserts that

risk management is important to define security risks in CI. However, the authors argue that many risk assessments become simplified, and the goal of the risk assessment is undermined. They propose an assurance assessment approach as the best method to conduct the risk assessment. As assurance cases have already been used in safety, Merrell [19] talks about using it for security. A future piece of work could be to see if assurance cases could be combined into one for both areas of safety and security. The assurance case method is a good approach to be used by individuals who are less knowledgeable on safety and security. As it will create the goals and questions that can then be asked to the relevant teams. However, you need knowledgeable individuals to create those goals and questions first.

Not all authors agree with Merrell [19], others feel a risk management approach is the best method. Poletykin [20] proposes a risk assessment method that can be used for security, safety and reliability. The author has created a formula-based risk assessment method. All threats and vulnerabilities would need to be collected from different sources such as security standards. The author mentions they tested the risk assessment method but does not provide many details on the results of the test, it would have been good if they said how it went, gaps found or if it covered all areas needed.

There are many elements to risk management, and they are not all touched on equally. Cherdantesva [21] has conducted a survey in risk assessment methods for Supervisory Control and Data Acquisition (SCADA) systems. A key finding is that the majority of the risk methods used are based on the risk identification and risk analysis stages. This leaves gaps in the other areas especially risk evaluation and treatment.

Another opinion on risk management is Kriaa [4] which states that risk assessment is one of the areas were safety and security differ. The authors states that the security functions are not meant to cope with physical hazards and failures. However, disaster recovery and business continuity which do focus on those areas are included in security standards. ISO 27001 has both the respective control areas within the control family.

There is a range of papers on CI in general and others that are focused on a particular area of CI. Litherland [1] is one paper that is focused on a specific sector which in this case is nuclear power. Litherland [1] states that security and safety have many features in common such as defense in depth but also differences such as security having more qualitative risk assessments compared to safety. However, quantitative risk assessments have been carried out for security such as the work done by Staalduinen [22]. The author states having safety does not ensure security and vice versa. Litherland [1] highlights that nuclear power plants are connected and rely on corporate business IT networks; this means there is a need for general security standards as the CI is interfacing with corporate networks that utilise general security standards.

Several safety standards talk about safety integrity levels and these are used in journal papers. Marcin [23] suggests a method to integrate safety and security by creating Security Assurance Levels (SAL) and they can be used similar to how Safety Integrity Levels (SIL) are. In this method you must take into consideration the SIL and SAL when assessing security and safety. The paper was very focused on the safety aspect and did not explain the SAL or how to consider security threats into the model. The authors mention selecting a SAL but then not how to decide on the SAL and what security controls would be required. Looking at the references used there is mention of several safety standards but not a single security standard has been referenced or used within this paper which highlights the focus was on safety.

The model is a good starting point and the idea of SAL is something that has been used in other journal papers, standards\ frameworks and especially maturity models. Similar to Marcin [23], Barnert [24] recommends leveraging SIL to link to security. This paper was only looking at safety and security from a functional safety analysis point of view and not the wider view of the complete CI infrastructure which this paperis.

Compared to Marcin [23], Barnert [24] did include security into the process but it was still a safety-first perspective with security added on rather than a complete integration of both the processes.

Reichenbach [3] asserts that for safety and security requirements in CI taking a separate approach is not the best way to do it and harmonizing the processes is the best way. The paper proposes taking the safety integrity levels (SIL) and integrating it in with the Threat Vulnerability and Risk Assessment (TVRA) method.

Risk management is mentioned in many papers and is a key part of both safety and security, however very few papers cover the full spectrum of risk management the only paper that did in the review was Derock [13]. Cherdantesva [21] reviewed many risk assessments papers and not one of those covered the full risk management process. Most papers instead focus on certain areas such as Reichenbach [3] that focused on the risk analysis section only or Poletykin [20] which does not look at risk treatment.

## IV. Combined Security and Safety Risk Management Process

The approach this paper is taking when creating the risk management framework is to ensure the framework will be detailed enough that it can be used with minimal changes from the users except if they require changing the ratings for example. In the literature review papers such as Derock [13] and Stoneburner [14] have created frameworks but they are not detailed enough and would be difficult to implement without more work. This framework will also cover all elements of the risk management process as Cherdantesva [21] highlighted that other papers do not cover all elements equally and will focus on one area only such as risk identification.

There are three main risk analysis methods that are generally used in risk management:

- Quantitative
- Qualitative
- Semi-quantitative

This framework has taken the approach of using the semi-quantitative method. The reasons for this are that to successfully use the quantitative method requires detailed and accurate figures on all parts of the process. For example: cost of controls, impact of risk, likelihood and residual risk. It can be difficult and, in some cases, impossible to put an accurate figure to the question.

Another reason the semi-quantitative approach was chosen was even when accurate figures can be gathered the time and resources required to produce those figures can be high. For example, the costs of controls can take a lot of time, if the CI organisation had decided a safety control was to improve the protection walls of the nuclear power plant and they wanted to install a concrete floor base and special steel walls. To cost this out would require specialist teams coming onsite doing an inspection and providing quotes on materials and labour. All of this would take time and if that had to be done for every control that was considered it would take a lot of time.

The option of a purely qualitative approach was considered as that does not have the issues with finding exact figures but instead relies on the team deciding on what they feel the cost would be or the likelihood as examples. However, safety and security do not need to be considered in such a subjective manner as although there may not be enough information in all areas that is required for a quantitative method there is some information out there which can help move it beyond a complete qualitative method. For example, certain countries have good statistics on the chances of natural disasters, or figures on the amount of cyber-attacks organisations can expect to face such as phishing emails. Fines for data breaches and costs to clean up CI incidents are also public knowledge and can help during the assessment process.

For these reasons a semi-quantitative approach has been selected for this framework. This framework created ratings that also use a numerical value. This approach removes the need to capture detailed information which is not always possible but makes the use of a pre-defined ranking system less subjective by including a numerical value as well.

Fig. 1 - Risk Management Framework shows the main steps of the framework. The first section is harmonisation.

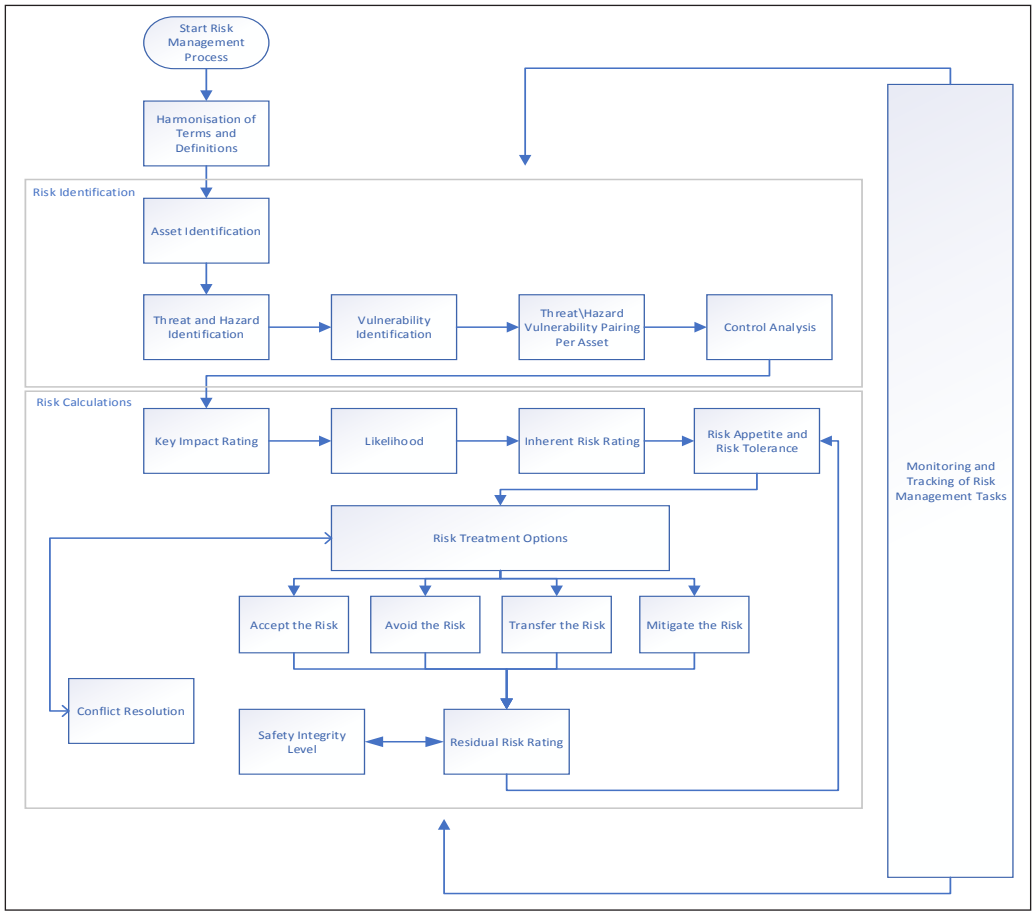


Fig. 1: Risk Management Framework

### *A. Harmonisation*

Safety and security risk management methods use different terminology. Terminology harmonisation involves users making a subjective decision and it is possible other users would come to a different conclusion or choose to harmonise in a different way. One aim of this method is to lessen the potential for different users to come to different conclusions and to allow the process to be more repeatable and remove some of the subjectiveness from it.

A method to harmonise the terms used in the four selected standards was created. The methodology was at a high level:

- Go through the terms and definitions of each applicable standard and create a harmonisation document that lists key terms or terms that have the potential to be used in more than one standard.
- In the harmonisation document the definition from each standard can be compared with the definition given in other standards.
- A new definition is then created that covers the definitions used in all the standards or if one of the standards definitions is good enough to cover the definitions used in the other standards that definition is used.
- There will be a list of terms and definitions that can be used across all standards the organisation is going to use. There will still be other terms in the standards that are used but the key or common terms will be covered in the terminology harmonisation process.

For risk management some of the key terms and the definitions the four standards use that should be checked, include:

- Risk
- Threat
- Hazard
- Likelihood
- Control
- Safety function
- Asset
- Vulnerability

Table I - Example Terms and Definitions shows a few example terms and definitions found in the four chosen standards that will be of key relevance within the risk management process. There are others that the CI organisation will need to take from the harmonisation process but the below are good examples of how the process works.

Column 1 Terms is the terms that are mentioned in the four standards. Columns 3-6 list the four standards and the definition of the term in column one. If they are blank that means the standard does not have a definition for that term. Column 2 New Framework is showing the new definition that will be used for the applicable terms.

TABLE I: EXAMPLE TERMS AND DEFINITION

| Terms | New Framework | ISO 27001 | IEC 61508 | NERC CIP | IEC 61513 |
|---|---|---|---|---|---|
| Control | Action that modifies risk. | Measure that is modifying risk. | | | |
| Safety-related system | | | Designated system that both<br>– implements the required safety functions necessary to achieve or maintain a safe state for the EUC; and<br>– is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external. | | |
| Safety function | | | Function to be implemented by an E/E/PE safety-related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event. | | |

| Terms | New Framework | ISO 27001 | IEC 61508 | NERC CIP | IEC 61513 |
|---|---|---|---|---|---|
| EUC risk | Combination of likelihood and impact of a positive or negative event. | | Risk arising from the EUC or its interaction with the EUC control system. | | |
| Risk | | Effect of uncertainty on objectives. | Combination of the probability of occurrence of harm and the severity of that harm. | | |
| Threat | Potential cause of an unwanted incident, which may result in harm to a system, person or organisation. | Potential cause of an unwanted incident, which may result in harm to a system or organisation. | | | |
| Hazard | | | Potential source of harm. | | Event having the potential to cause injury to plant personnel or damage to components, equipment or structures. Hazards are divided into internal hazards and external hazards. |

For the harmonisation method the risk management process has harmonised the definitions and left the individual terms of each standard separate. The reason the terms have been left and the definitions harmonised is because that will allow each standard to use the terms that are written in its standard so when external auditors audit they will see terms they recognise. However, the CI organisation will need to highlight the definition has been changed slightly to accommodate the other standards, but the new definition should still cover what the old definition was saying so should not be an issue. An example of this would be the terms control, safety-related system and safety function in Table I. If the term control was used in respect of IEC 61508 as that standard does not use the term control the auditor could read that and say they are not sure what this is referring to as IEC 61508 uses safety functions to help manage risks. Safety-related systems can be seen as controls or a system that has controls in it that are designed to reduce the risk for the assets. To resolve this, the CI organisation has two options they can include in the standard documentation the harmonisation work and show that control, safety-related system and safety function have the same definition so can be used interchangeably and mean the same thing. Or they could use the term safety function when discussing safety as an action that modifies risk from a safety point of view and control when talking from a security point of view. They can still include the harmonisation method in the standard documentation so that the auditors and other users understand even though two different terms are being used they are both referring to actions that modify risk.

### *B. Asset Identification*

Asset identification is very important because if the CI organisation does not know about the asset it will not be able to protect the asset. The assets should be broken down into categories, the list of categories should include:

- Information
- Locations
- People
- Physical
- Systems and Software
- Third Parties

The list of categories are not an exhaustive list and has been created from the authors previous experience in identifying assets for risk assessments. The list provides a good grounding and should cover the majority of assets within those categories. The CI organisation can add as many as they feel is needed for them to conduct the risk management process.

### *C. Threat and Hazard Identification*

The next step is to identify the threats and hazards that apply to the assets.

Many of the threats and hazards can be interconnected and the realisation of one may lead to others. For example, the hazard

of an explosion would then lead to the hazard of a fire. Another example if the threat of an SQL injection attack could then lead to unauthorised access as the first threat was able to get login credentials that they use to access other system.

The framework provides many methods that can be used to identify the threats and hazards including Hazard and Operability Analysis (HazOp), Failure mode and effects analysis (FMEA) and previous incidents as some examples. The methods need to cover both safety and security and will involve teams from all areas to ensure threats and hazards are found and the team does not focus on one area such as safety more than security.

### *D. Vulnerability Identification*

The next step which is closely related to the previous section is identifying vulnerabilities.

The aim of this section is to take the assets, threats and hazards that have been identified and use them to help identify vulnerabilities.

The framework has many vulnerability identification methods including assessing threats\hazards, review configuration of IT/OT devices, checklists and audits as a few examples from the created risk management framework.

The final task is to pair the vulnerabilities discovered in this section with the threats and hazards of each asset which were identified in section 5.3 to create the threat\hazard vulnerability paring per asset.

### *E. Control Analysis*

The CI organisation will already have controls in place for security and safety and to conduct this risk management process the CI organisation will need to analysis those controls. In the earlier vulnerability identification section, the controls have been assessed and any weaknesses that could lead to vulnerabilities have been documented.

Some ways to assess controls are to carry out a gap assessment. Another method is to interview and request information directly from control owners on what they do, any weaknesses they know of and include that information in the risk management details.

Penetration testing is a good way to assess if a system has any control deficiencies.

In this section the CI organisation should also link the controls to certain assets or groups of assets. For example, an Intrusion Detection System (IDS) may be in place for a certain part of the network only meaning certain servers have this control but not others. It is important to know which controls are applicable to what assets especially in the risk calculation and risk treatment sections.

The CI organisation also requires a good understanding of the controls to help identify and resolve conflicts that can occur between safety and security.

### *F. Risk Calculations*

The following sections describe the risk calculations that are needed to provide risk ratings for all the information that has been gathered so far. The risk calculations include:

- Key impact rating
- Likelihood
- Inherent risk rating
- Residual risk

The risk calculations are an important part and connect with the other sections such as risk tolerance and risk treatment options.

#### *Key Impact Rating*

This section is going to be looking at the impact compromises could have on six key impact attributes. The attributes will be discussed here and the team carrying out the risk management process will give a rating to each of the six key attributes, which will be used as part of the risk management process.

To calculate the key impact measures the CI organisation needs to use what it has created so far in the risk management process and in particular:

- List of threats\hazards and the assets they are applicable to.
- Details of the threat\hazard vulnerability pairings.
- List of controls and assets they are applicable to.

The CI organisation now needs to take each individual threat\hazard and the applicable asset and establish what the impact ratings will be. The key impact attributes are listed below:

Confidentiality – The attribute is about the asset not being disclosed to unauthorised parities.

Integrity – This attribute is focused on the accuracy and completeness of the asset.

Availability – This attribute is concerned with the asset being available when required.

Human Welfare – This attribute is concerned with the safety of human life or injury.

Environmental – This attribute is about the environment (natural and man-made) around the asset.

Social – The social attribute considers the wider impact on society for that asset.

The attributes have been selected from the authors experience and cover both areas well. The first three attributes are more

commonly considered with security and the final three with safety. Although from a key impact rating point of view there are many assets that will cover both sections and have a rating in both the safety and security attributes.

Each attribute will be measured against the individual threat\ hazard and applicable asset and given a rating which is described below. The rating will be an impact rating of that attribute for that asset. Not all attributes will be applicable to all assets however they should still be considered and if not applicable the lowest rating would be selected.

When assessing the impact rating the team will need to consider the controls that are applicable to the assets and how they may change the impact. Some risk management standards recommend assessing the impact with no controls then with controls in place. However, this risk management framework removes that part as it is unrealistic and will create a higher impact for a large amount of threats\hazards. For example, a threat\hazard of corrupt data will be less if the data is backed up and the corruption is noticed before it is also backed up, or a loss of a facility will have less of an impact if a hot site is in place. The team needs to consider that the existing set of controls, could be incomplete or less than ideal and so do not remove the impact completely. Without considering the current controls the impacts will always be higher and the team then has to do another assessment with controls to get a more representative impact rating.

The ratings and descriptions for the asset and the attributes are given in Table II - Ratings and Descriptions below.

The descriptions given for each impact has been kept at a high-level description such as minor, reasonable and catastrophic. The reason for this is that each CI organisation is then free to choose what these impacts are they can either keep them high level, replace with figures or define what the high-level impact is in more detail.

For example, the human welfare attribute instead of minor impact (rating 1) it could be classed as no deaths and less than 10 people injured, whereas a major impact (rating 3) could be up to 10 people killed and 30 injured and other values could be given for each rating.

TABLE II: IMPACT RATINGS AND DESCRIPTIONS

| | Definitions | | | | |
|---|---|---|---|---|---|
| Rating / Attribute | 0 | 1 | 2 | 3 | 4 |
| Confidentiality | A loss of confidentiality on this asset would have *no impact* on the organisation. | A loss of confidentiality on this asset would have *a minor impact* on the organisation. | A loss of confidentiality on this asset would have *a reasonable impact* on the organisation. | A loss of confidentiality on this asset would have *a major impact* on the organisation. | A loss of confidentiality on this asset would have *a catastrophic impact* on the organisation. |
| Integrity | A loss of integrity on this asset would have *no impacton* the organisation. | A loss of integrity on this asset would have *a minor impact on* the organisation. | A loss of integrity on this asset would have *a reasonable impact* on the organisation. | A loss of integrity on this asset would have *a major impact* on the organisation. | A loss of integrity on this asset would have *a catastrophic impact* on the organisation. |
| Availability | A loss of availability on this asset would have *no impact* on the organisation. | A loss of availability on this asset would have *a minor impact* on the organisation. | A loss of availability on this asset would have *a reasonable impact* on the organisation. | A loss of availability on this asset would have *a major impact* on the organisation. | A loss of availability on this asset would have *a catastrophic impact* on the organisation |
| Human | A compromise of this asset would result in *no impact* to human welfare. | A compromise of this asset would result in *a minor impact* to human welfare. | A compromise of this asset would result in *a reasonable impact* to human welfare. | A compromise of this asset would result in *a major impact* to human welfare. | A compromise of this asset would result in *a catastrophic impact* to human welfare. |
| Environmental | A compromise of this asset would result in *no environmental impact.* | A compromise of this asset would result in *a minor environmental impact.* | A compromise of this asset would result in *a reasonable environmental impact.* | A compromise of this asset would result in *a major environmental impact.* | A compromise of this asset would result in *a catastrophic environmental impact.* |
| Social | A compromise of this asset would result in *no impact* to society. | A compromise of this asset would result in *a minor impact* to society. | A compromise of this asset would result in *a reasonable impact* to society. | A compromise of this asset would result in *a major impact* to society. | A compromise of this asset would result in *a catastrophic impact* to society. |

The overall key impact rating is the sum of all six attributes. Also, the CI organisation can use individual attribute ratings if they ever require focussing on a particular area. For example, if they wanted to focus on assets that would have an impact on human welfare then they could just look at the individual rating for that one.

Threats, hazards, vulnerabilities and assets interact and can impact each other. When looking at risks the CI organisation needs to consider this and also consider how the controls will interact and cover multiple areas. For example, if the sensor failed on the flood protection system, the flood could then damage the electrics and take out the CCTV which will lead to other risks around security and safety.

The calculation was touched on earlier and the formal calculation is:

$$Cr + Ir + Ar + Hr\ Er + Sr = Tlr \quad (1)$$

Equation 1 – Key Impact Rating Calculation.

Where Cr is the Confidentiality rating, Ir is the integrity rating, Ar is the availability rating, Hr is human welfare rating, Er is environmental rating, Sr is social rating and TIr is total impact rating.

Once all the threat\hazards applicable to each asset have been assessed the CI organisation should record and document the impact ratings for each asset. This risk management process allows the CI organisation to document these results however they prefer. As long as the ratings are available for the remaining stages of the risk management process.

*Likelihood*

In this section the CI organisation is going to decide the rating for the likelihood of the threat\hazard and vulnerability pairings taking place.

Controls at the CI organisation were looked at in the threats and hazards section and especially in the vulnerability identification section. Knowledge of the controls currently in place are needed for rating the likelihood of a threat\hazard exploiting a vulnerability for a particular asset. If the likelihood was rated on the basis of no controls being in place many of the pairings would be rated as very likely.

A large factor in coming to a decision on the likelihood rating is what is the threat\hazard and using the team members knowledge and expertise to decide how likely it is to occur. The other information given here is all relevant but sometimes there is not a lot of actual data and the team will have to decide using their own experience.

Another major factor is the vulnerability itself and much like the threat\hazard, the team managing the risk management process will rely on their knowledge and experience to help decide the effect on the likelihood.

Each threat\asset vulnerability paring will be measured against the asset and given a rating which is described below. The rating will be a likelihood of that paring exploiting a particular asset over the course of a year. The CI organisation using the tool it has selected such as a spreadsheet, risk management tool etc. will take each pairing and asset use all the information and methods mentioned in this section and decide what description is best for that parring\asset and document what the rating is.

The ratings and descriptions for the paring and the asset are given in Table III - Likelihood Rating and Description. When using Table III, the CI organisation should keep in mind what was said for the asset value assessment rating table (Table II). The descriptions have been kept high-level with terms such as unlikely and fairly likely. Each CI organisation is free to choose what these descriptions are they can either keep them high level or replace with figures.

Table III: Likelihood Rating and Description

| Rating | Description |
|---|---|
| 1 | Threat\hazard vulnerability pairing is *highly unlikely* to exploit the asset in a calendar year. |
| 2 | Threat\hazard vulnerability pairing is *unlikely* to exploit the asset in a calendar year. |
| 3 | Threat\hazard vulnerability pairing is *fairly likely* to exploit the asset in a calendar year. |
| 4 | Threat\hazard vulnerability pairing is *highly likely* to exploit the asset in a calendar year. |
| 5 | Threat\hazard vulnerability pairing is *almost certain* to exploit the asset in a calendar year. |

This framework recommends keeping the description high-level as it can be difficult for the team carrying out the risk management process to work out for certain pairings if it would occur once a year or three times. However, the team could still have issues with people needing to understand what the difference is between fairly likely and unlikely.

At this stage in the risk management calculation process the CI organisation has assigned a key impact rating and likelihood

ratings for threat\hazard vulnerability parings for the assets. The next step is where the risk ratings take place.

*Inherent Risk Rating*

In the Key Impact Rating section, an impact rating was given to assets for each individual threat\hazard using six attributes. Then in the likelihood section the threat\hazard vulnerability pairings for the assets were given a likelihood rating.

This section takes each individual threat\hazard vulnerability paring for an asset and gives it a risk rating. This will be the inherent risk rating.

The inherent risk is calculated using the earlier previous rating calculations which are the total impact rating and the likelihood rating. The formal calculation is:

$$\text{Tlr} \times \text{Lr} = \text{IRr} \quad (2)$$

Equation 2 – Inherent Risk Rating Calculation.

As a reminder TIr is Total Impact rating and Lr is Likelihood rating and IRr is Inherent Risk rating. By multiplying the total impact rating with the likelihood rating the CI organisation will calculate an inherent risk rating for each threat\hazard vulnerability pairing for an asset.

For each threat\hazard per asset the total impact rating will stay the same, but the likelihood rating is threat\hazard vulnerability pairing per asset and can be different.

The reason for this is that when the CI organisation considers what the impact of the threat\hazard will be that impact is going to be the same for that asset regardless of what vulnerability is exploited. For example, the impact of having data destroyed will be the same regardless if the threat exploited poor access control or malware. However, what would be different is how likely each of those vulnerabilities were to be exploited and thus different likelihood ratings are needed and that is why they are worked out threat\hazard vulnerability pairing per asset.

The risk management documentation should now be updated to show inherent risk rating for each threat\hazard vulnerability pairing per asset. Now the CI organisation has the inherent risk ratings it needs to decide what to do with all the risks.

*Risk Tolerance*

The risk tolerance is where the inherent risk ratings will become classed as high, medium or low risks depending on the risk tolerance rating set by the CI organisation. The risk tolerance rating is connected with the risk treatment options discussed in the next section. Depending on what the risk tolerance rating is will impact what the risk treatment options are.

The first time the CI organisations sets the risk tolerance rating for what is classed as high, medium and low risk can be difficult to decide on.

The highest possible inherent risk rating for a threat\hazard vulnerability pairing of an asset is 150 and the lowest is 1, so the CI organisation needs to set it within that range. If the CI organisation was very risk adverse they would set the risk tolerance to be low such as any inherent risk rating over 20 has a high risk tolerance rating and is classed as a high risk. Whereas a CI organisation with a higher risk appetite may say any risk with an inherent risk rating over 50 has a risk tolerance rating of high. It is likely most CI organisations will be risk adverse and have a lower risk tolerance.

The risk tolerance rating is not fixed and can be changed over time. Table IV - Risk Tolerance Rating shows the risk tolerance ratings. These are compared to the inherent risk ratings and depending on the inherent risk rating will decide which risk tolerance rating it falls under and what type of risk it will be classed as.

A CI organisation may decide they have a different risk tolerance for safety and security and want to have different tolerance ratings for each. This framework would not recommend that as security can impact safety and so it cannot be seen as less important or being able to take a higher risk tolerance rating then safety. As if that is the case then a security risk could lead to a safety incident and as they are so intermingled, a loss of security could impact safety so the CI organisation should consider their risk tolerance to be one of the same.

The main work for the CI organisation in this section is to decide on what the risk tolerance ratings will be. Once the CI organisation has that they can go through all the threat\hazard vulnerability pairings per asset and use their inherent risk rating to establish what their risk tolerance rating is and what risk class the pairing will fall under.

TABLE IV: RISK TOLERANCE RATING

| Risk Tolerance Rating | Inherent Risk Rating |
|---|---|
| High Risk | More than 40. |
| Medium Risk | More than or equal to 15 and equal to or less than 39. |
| Low Risk | Equal to or less than 14. |

*Risk Treatment Options*

Now that all the threat\hazard vulnerability pairings have been assessed and given an inherent risk rating and risk tolerance

rating. The next step is for the CI organisation to decide what to do with all the results. This is called risk treatment and the CI organisation will have a few different options on how to handle the risk:

- Accept the risk
- Avoid the risk
- Transfer the risk
- Mitigate the risk

The risk treatment option descriptions can be different depending on what the risk tolerance rating is. For example, a threat\hazard vulnerability pairing that is classed as a high risk could only have the risk accepted by a select group of senior managers while for a low risk the risk accepting could be done by the risk owner.

An example of the details on the risk treatment options for a high risk is shown in Table V - Risk Treatment Options High Risk and the other options for the medium and low risks can be found within the risk management framework.

*Risk Tolerance Rating – High Risk*

Table V: Risk Treatment Options High Risk

| Risk Treatment Option | Description |
|---|---|
| Accept the risk | Can only be accepted by the CI organisation's board or C-level team.<br>These risks must be reviewed every 6 months to decide if the risk treatment option should be changed. |
| Avoid the risk | CI organisation chooses to stop or change plans to avoid the risk. Action to avoid the risk should be completed within 3 months of the risk being identified or it will need to be escalated to the CI organisation's board or C-level team. |
| Transfer the risk | Can only be transferred outside the organisation by the CI organisation's board or C-level team. Transfer must be completed within 3 months of the risk being identified or it will need to be escalated to the CI organisation's board or C-level team.<br>These risks must be reviewed every 6 months to decide if risk treatment option should be changed. |
| Mitigate the risk | High risks can be mitigated by the risk owner. Mitigation choices will need to be reviewed and approved by the Head of Security and Safety Risk Management.<br>The mitigation activity should be completed within 3 months of the risk being identified or it will need to be escalated to the CI organisation's board or C-level team.<br>These must also be reviewed every 6 months if outstanding for that long. |

The treatment options can be tailored to suit each individual CI organisation. The CI organisation may already have a team that approves certain activities and they may be more suited then saying board or C-level team members. Also, times can be changed to reflect how comfortable the CI organisation is with the risk staying in its current form.

As the risks move from high, medium to low the people\teams that review and approve become less senior to represent the change in risk. Also, to ensure certain people\teams only focus on the highest risk and do not lose interest or as they see so many risks, begin to take them less seriously.

When the CI organisation works through the risk treatment options for the individual findings, they need to also look at the wider impact. Do certain controls cover many risks? Or are many risks linked to the same root cause and it would be better to resolve that then implement many individual controls?

It is likely that many threats\hazards, vulnerabilities and controls cover many assets. So, the CI organisation will be able to leverage that and use one control to reduce the risk across many findings. For example, the control of encryption could reduce the risk of network sniffing, data theft and data manipulation as a few examples.

During the risk treatment stage, the teams need to think of both safety and security controls depending on the risk they are assessing. There may be times when a security control can also resolve safety risks and vice-versa. It's important that all teams are involved in deciding and selecting the risk treatment option for both safety and security and the teams do not just look at their own areas as this is how conflicts can occur or go unnoticed.

*Residual Risk*

The risk treatment section discussed four treatment options and three of them (avoid, transfer and mitigate) reduce the inherent risk rating. This is what the residual risk is, it is the remaining risk rating after the treatment options have been calculated.

To calculate the residual risk the CI organisation will need to consider what treatment options have been put in place. The most likely treatment option is to mitigate the risk using controls and this will be discussed in more detail next.

When the mitigate option has been chosen the risk management team will consider what control is being implemented and establish does the control reduce the likelihood, impact or both. They also need to consider how much the control will reduce those ratings. This can be subjective, trying to establish how much a control will reduce the impact or likelihood. It is best to involve users in the process who have knowledge on the area being discussed. Such as safety and security engineers, asset owners and risk assessors as examples.

The reduction ratings and descriptions for the risk treatment options are given in Table VI - Reduction Ratings and Descriptions these ratings are used to calculate the residual risk.

Table VI is the first table to have a rating that is an actual percentage. The percentage represents how much the inherent risk score will be reduced by the treatment option. As with the descriptions these figures can be changed to fit how the CI organisation feels the treatment option are reducing the inherent risk. However, this framework recommends at least one very low percentage and a high percentage but not 100% as no treatment option (except avoid) can reduce the risk 100%.

TABLE VI: REDUCTION RATINGS AND DESCRIPTIONS

| Reduction Rating | Description |
|---|---|
| 5% | Risk treatment option will have a *very minor* impact on inherent risk rating. |
| 10% | Risk treatment option will have a *minor* impact on inherent risk rating. |
| 20% | Risk treatment option will have a *reasonable* impact on inherent risk rating. |
| 40% | Risk treatment option will have a *considerable* impact on inherent risk rating. |
| 60% | Risk treatment option will have a *major* impact on inherent risk rating. |
| 90% | Risk treatment option will have a *massive* impact on inherent risk rating. |

The residual risk rating is calculated using the inherent risk rating and the reduction rating. The formal calculation is:

$$(IRr \ / \ 100) \ X \ Rrp = N$$

$$IRr - N - RR$$

Where IRr is the Inherent Risk rating, Rrp is the Reduction rating percentage, N is the sum of that calculation and RR is the residual risk.

Once the CI organisation has the residual risk they can decide if they want to reduce it even more or if it has been reduced enough. The risk can also be worked on again in the future and so it could potentially have an even lower residual risk in future years if in each year new controls are added.

After the residual risk rating has been calculated the CI organisation needs to see where the risk is now rated based on the risk tolerance rating in Table VII - Residual Risk Rating. The ratings are the same as they were in Table IV in the Risk Tolerance section, but the second column is now titled residual risk rating instead of inherent risk rating.

TABLE VII: RESIDUAL RISK RATING

| Risk Tolerance Rating | Residual Risk Rating |
|---|---|
| High Risk | More than 40. |
| Medium Risk | More than or equal to 15 and equal to or less than 39. |
| Low Risk | Equal to or less than 14. |

What the CI organisation will be aiming for is that the risks have now moved to a lower risk tolerance rating due to the risk treatment options bringing the risk rating down. Resulting in a residual risk rating that is in a lower risk tolerance rating. Even if the risk tolerance rating does not change the residual risk rating will be lower than the inherent risk rating and so the risk has been reduced.

The flow diagram in Fig. 2 - Risk Calculations shows the main steps of the risk calculations at a high level and how they are all connected and the results from one part connects with the other part. Details for each part of the flowchart can be found in the earlier sections.

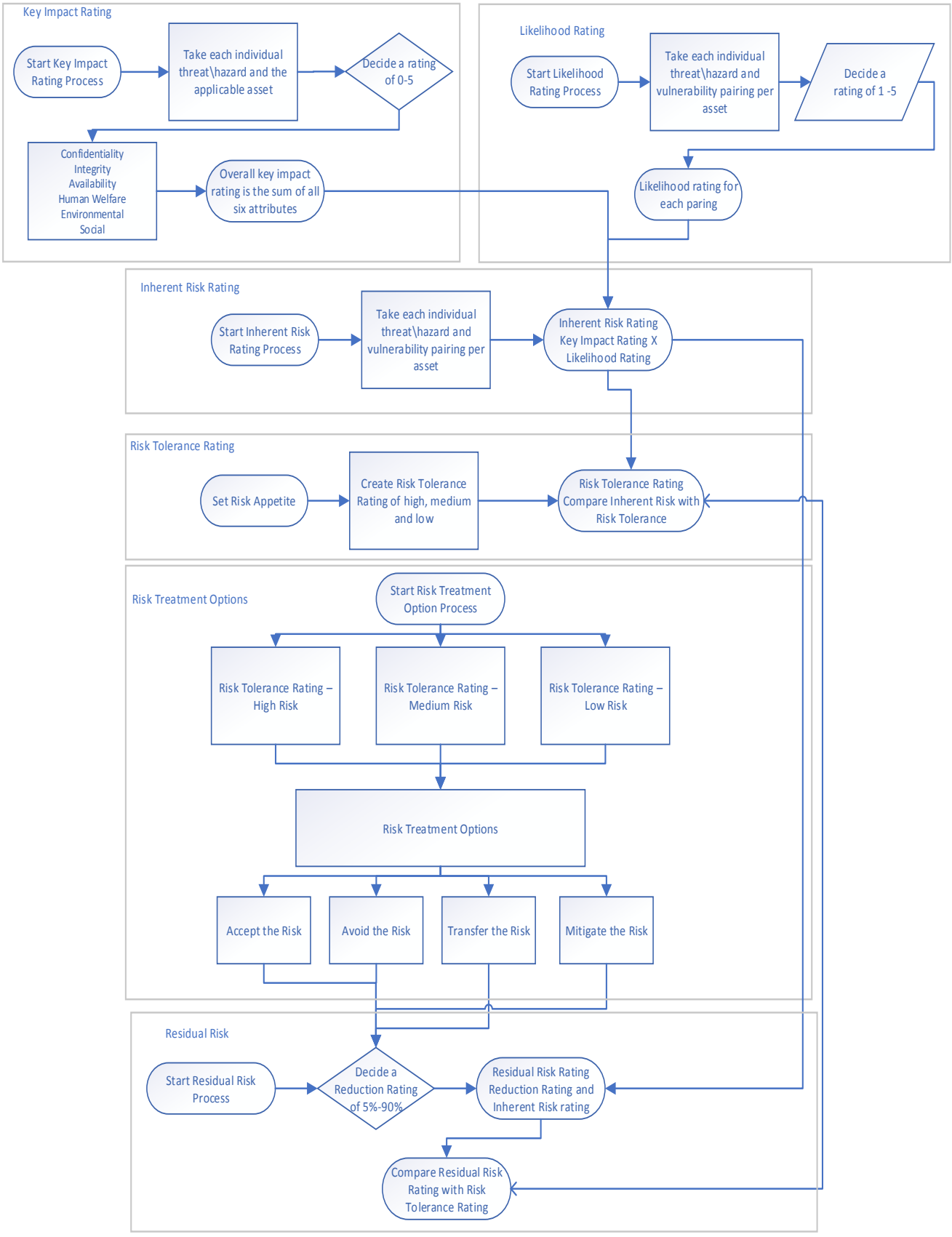


Fig. 2: Risk Calculations

*Conflict Resolution*

This section is focused on finding and resolving conflicts within the risk management framework. Conflicts can occur because at times security and safety have different goals and the controls that are implemented to achieve one goal can then stop the other goal being achieved.

Some examples of conflicts that can occur are:

- A manual override controller has been put in place to be used if the generator malfunctions and it can take control and configure the generator instead of the generators computer system. This is a safety control designed to ensure the generator can be managed even if the main system that is used fails or the generator stops responding to it. The conflict will arise when the security control that ensures no assets can be accessed without being authenticated first such as by username or password or biometrics. The manual override can be done by anyone as in an emergency the ability to override and shut down the generator is needed.
- For safety reasons in an emergency at the facility an alarm sounds, and doors unlock to allow people to exit the building. However, this can create a security risk as people could enter the building through an unlocked door or even set off the alarms to gain entry and bypass many of the controls that are usually in place. This conflicts with the security control of controlling physical access to the facility and all entry and exit points being locked.
- Users want the ability to manage systems remotely in case of an emergency but many of the systems are old and vulnerable to Internet facing attacks. By enabling remote access safety controls can be implemented from a remote safe place during an incident, however having an insecure Internet facing system can create a lot of security risks.
- The safety systems are bespoke and are not connected with the main access identity system. Meaning user accounts are entered manually and not in line with the security policy such as locking out after failed attempts, password expiry and disabling when users leave as examples.

The first step in the conflict resolution process is to be able to identify conflicts. There are several places conflicts can be identified one of the main places is the risk treatment options section. That is where controls for all the threats\hazards for safety and security will be selected. The main users who should look for conflicts are the users that will be implementing the controls so this will include safety and security team members. They will be best placed to identify if one control is going to be in conflict with another.

To identify conflicts the CI organisation will not at first have to find a safety and a security control in conflict. It will be more likely they will see either a safety or security control and they realise it would potentially be conflicting with security or safety then they can look for the conflicting control. To achieve this the teams will need to have the experience and knowledge to see one set of controls and understand it could raise conflicts and should be investigated more. Using the examples above if the team saw the control for the manual override of the generator that can be actioned by anyone if needed they should think that goes against the security principle of least privilege within access control and look for were that control is mentioned and document the conflict.

Another place conflicts could be seen is in the threat\hazard and vulnerability identification sections. As the CI organisation is identifying threats, hazards and vulnerabilities the teams need to be thinking if a conflict could occur between safety and security and make a note for it to be investigated more in the risk treatment and this conflict resolution process.

The current controls are also analysed and here if a control is lacking and the CI organisation is looking to improve it this could also signal a conflict is going to occur. Using the examples earlier if the CI organisation identified that physical access control on the doors was lacking during an emergency the team may realise one way to resolve it may conflict with the safety control of getting all users out of the building as quickly as possible.

Many of the ways to identify conflicts discussed so far have relied on the team's experience and knowledge. A way to make the process achievable for less experienced users is for the CI organisation to create a knowledge base that highlights areas where conflicts have occurred in the past or where conflicts are more likely to be seen. For example, areas such as access control, physical safety, testing and technology patching and upgrading. As the CI organisation identifies conflicts, themes will appear such as conflicts arise around this asset or control area and the knowledge base can provide details on checking closely when controls in these areas are being selected as risk treatment options.

Once the conflicts have been identified the next step is to resolve the conflict. The resolution for each conflict will be unique to that set of controls but this section will describe some important concepts that can be used to help resolve the conflicts.

Although the protection of human life should always take precedence the CI organisation needs to understand that security controls also have a role to play in safety. If a breach takes place due to lacking security controls this can lead to an incident that could result in harm or loss of human life. Due to this resolving conflict is not as simple as always selecting the safety control.

When looking to resolve conflicts the CI organisation should look at what is the goal of each control. This will allow them to see if there are other controls that can be selected instead and if these controls do not cause a conflict then the conflict has been resolved and controls for both safety and security are in place. At times the alternative controls put in place may not be as effective or may not reduce the risk rating as much.

An option the CI organisation has but is not recommended is to drop or not attempt to comply with either the safety or security control. In the earlier examples the conflict of doors opening in an emergency the CI organisation could choose to allow the safety control to remain but not enforce a security control for it. This should only be done when no other option is possible as often the lack of security can impact safety and still puts safety at risk.

Once compensating controls have been selected or a control has been selected to be removed completely the team carrying out the conflict resolution needs to update the risk treatment options for the applicable risks. As the controls have been changed the reduction rating and residual risk rating also needs to be recalculated to get a new rating. The CI organisation then needs to review the rating and decide if the new rating is fine or if they want to change the control to reduce the rating even more. This part of the conflict resolution can involve the same steps and teams as the risk treatment options and residual risk sections did.

Conflict resolution is an important part of this risk framework as it is aiming to combine both safety and security into the one risk framework. This will create conflicts that are not seen when these processes are done separately. The CI organisation needs to take their time identifying and resolving the conflicts and ensuring the residual risk ratings are updated, as for future risk assessments these conflicts could re-occur if they are not documented.

Fig. 3 - Conflict Resolution Process below shows the process for conflict resolution which has just been covered in this section.

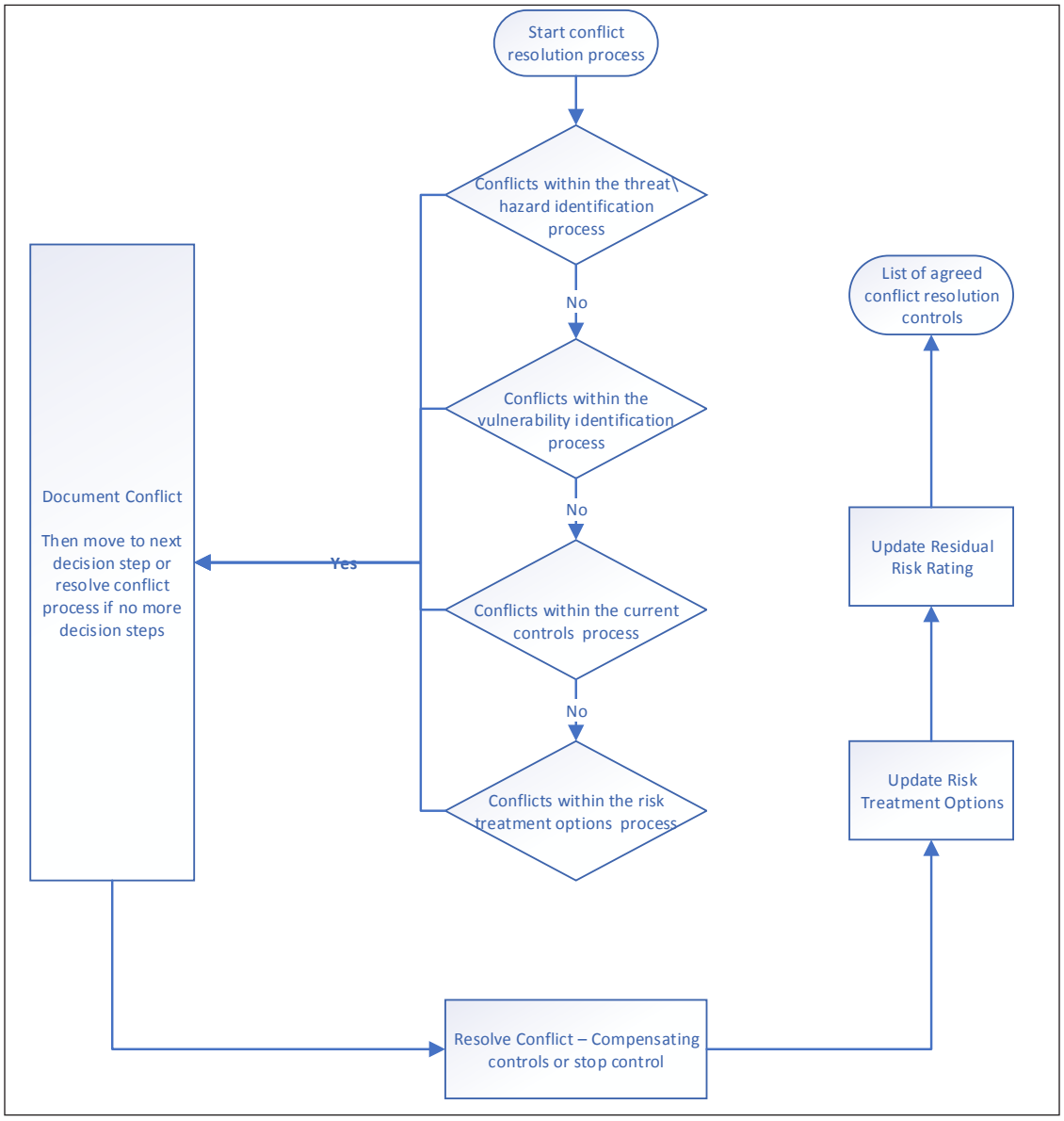


Fig. 3: Conflict Resolution Process

## V. Conclusion

This paper was looking to combine risk management for safety and security and has shown that it is possible if the CI organisation makes changes. Some changes are part of the risk management process and others are cultural. Some of the changes in the risk management process are around the terms and definitions that are used and having a conflict resolution process in place. Some of the cultural changes are around getting team members that are often siloed to work together, sharing information and considering how security impacts safety and vice-versa.

Some of the section's crossover such as threat and hazard identification and vulnerability identification and several of the methods used will identify both.

One downside of this approach is there is going to be a lot of options to work out as there will be many threat\hazards vulnerability pairings for multiple assets. However, tools may help make this more manageable by cascading certain ratings etc. One advantage is that in the risk treatment options section as the risk are for a particular vulnerability it can be easier to decide what controls to select.

For future work this risk management framework could be applied to a tool that allows workflows and calculations to be automated and connections between assets and controls highlighted by the tool. At the moment this framework would need to be done manually but it can be used as a base and be implemented into a risk management tool.

## References

[1] P. Litherland, R. Orr, and R. Piggin, "Cyber security of operational technology: Understanding differences and achieving balance between nuclear safety and nuclear security," in *11th International Conference on System Safety and Cyber-Security (SSCS 2016),* London, 2016, pp. 1-6, doi: 10.1049/CP.2016.0856.

[2] K. Pettersen, and T. Bjørnskau, "Organizational contradictions between safety and security - Perceived challenges and ways of integrating critical infrastructure protection in civil aviation," *Safety Science*, vol. 71, no. Part B, pp. 167-177, 2015, doi: 10.1016/J.SSCI.2014.04.018.

[3] F. Reichenbach, J. Endresen, M. Chowdhury, and J. Rossebo, "A pragmatic approach on combined safety and security risk analysis," in *Proceedings of the IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*, 2012, pp. 239-244, doi: 10.1109/ISSREW.2012.98.

[4] S. Kriaa, M. Bouissou, L. Pièrre-Cambacedes, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering and System Safety*," vol. 139, pp. 156-178, 2015, doi: 10.1016/j.ress.2015.02.008.

[5] M. Bartnes, "Safety vs. security?," in *Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management,* New Orleans, Louisiana, USA, May 14-18, 2006.

[6] International Organization for Standardization, *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, 2nd ed. American National Standards Institute, 2013.

[7] International Electrotechnical Commission, "61508-1 2010 Functional safety of electrical electronic programmable electronic safety-related systems," 2010.

[8] NERC, "CIP standards," 2021. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

[9] International Electrotechnical Commission, "61513:2013 Nuclear power plants - Instrumentation and control important to safety - General requirements for systems," 2013.

[10] Centre for the Protection of National Infrastructure, "Critical national infrastructure," 2020. [Online]. Available: https://www.cpni.gov.uk/critical-national-infrastructure-0

[11] United States Department of Homeland Security, "Critical infrastructure sectors," 2020. [Online]. Available: https://www.cisa.gov/critical-infrastructure-sectors

[12] United States Chemical Safety and Hazard Investigation Board, *Drilling Rig Explosion and Fire at the Macondo Well*. 2016.

[13] A. Derock, "Convergence of the latest standards addressing safety and security for information technology," in *On-line Proceedings of Embedded Real Time Software and Systems (ERTS2 2010)*, Toulouse, France, 2010.

[14] G. Stoneburner, "Toward a unified security-safety model," *Computer*, vol. 39, no. 8, pp. 96-97, 2006, doi: 10.1109/MC.2006.283.

[15] G. Howard, M. Butler, J. Colley, and V. Sassone, "Formal analysis of safety and security requirements of critical systems supported by an extended STPA methodology," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Paris, 2017, pp. 174-180.

[16] N. Subramanian, and J. Zalewski, "Assessment of safety and security of system architectures for cyberphysical systems," in *Proceedings of the IEEE International Systems Conference (SysCon),* 2013, pp. 634-641, doi: 10.1109/SysCon.2013.6549949.

[17] W. Young, and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13),* ACM, New York, NY, USA, 2013, pp. 1-8, doi: 10.1145/2523649.2530277.

[18] I. Friedberg, K. Mclaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications*, vol. 34, no. Part 2, pp. 183-196, 2017, doi: 10.1016/j.jisa.2016.05.008.

[19] S. A. Merrell, A. P. Moore, and J. F. Stevens, "Goal-based assessment for the cybersecurity of critical infrastructure," *2010 IEEE International Conference on Technologies for Homeland Security (HST)*, Waltham, MA, 2010, pp. 84-88, doi: 10.1109/THS.2010.5655090.

[20] A. Poletykin, "Cyber security risk assessment method for SCADA of industrial control systems," in *2018 International Russian Automation Conference (RusAutoCon)*, Sochi, 2018, pp. 1-5, doi: 10.1109/RUSAUTOCON.2018.8501811.

[21] Y. Cherdantesva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Computers & Security*, vol. 56, pp. 1-27, 2016, doi: 10.1016/j.cose.2015.09.009.

[22] M. Staalduinen, F. Khan, V. Gadag, and G. Reniers, "Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure," *Reliability Engineering & System Safety*, vol. 157, pp. 23-34, 2017, doi: 10.1016/j.ress.2016.08.014.

[23] S. Marcin, and P. Emilian, "Functional safety with cybersecurity for the control and protection systems on example of the oil port infrastructure," *Journal of Polish Safety and Reliability Association Summer Safety and Reliability Seminars*, vol. 9, no. 3, 2018.

[24] T. Barnert, K. T. Kosmowski, and M. Śliwiński, "The impact of security aspects on functional safety analysis / Wpływ Aspektów Ochrony Informacji Na Wyniki Analiz Bezpieczeństwa Funkcjonalnego," *Journal of KONBiN*, vol. 1, no. 21, pp. 27-40, 2012, doi: 10.2478/jok-2013-0003.