
# A Framework for creating a Safety and Security Management System (SSMS)

**Robert Kemp*, Richard Smith**

[1]Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, Gateway House, Leicester, LE19BH

Email: p2548837@my365.dmu.ac.uk , rgs@dmu.ac.uk

**Abstract**

Safety and security risks to critical infrastructure organizations are well known, and incidents in both fields have taken place. To help critical infrastructure organizations manage these areas, safety and security standards have been created. The main aim of this paper is to present a framework that has been created to manage both safety and security by providing guidance on how to create a Safety and Security Management System (SSMS). The framework identifies and remediates conflicts and issues between IT, OT, safety, and security. While also creating processes that can combine safety and security compliance to standards to reduce duplication of work and allow one process to manage both areas. A survey was carried out to understand if the framework would be of use to organizations and to better understand the issues users have with managing safety and security and how they manage conflicts that can occur. The survey showed key areas of concern for organizations and how the framework can be of use to them. It identified six themes from the research and identified improvements opportunities for the framework that can be implemented.

**Keywords:** Safety, Security, Critical Infrastructure, Management Systems

## 1. Introduction

Management systems have been used by organisations for decades with management systems being dedicated to specific areas such as financial and environmental [1]. This paper is focused on management systems for the areas of safety and security. These are commonly known as Safety Management Systems (SMS) and Information Security Management Systems (ISMS). Often these are implemented as two distinct management systems and managed separately [2]. However, in certain industries and as new technology is developed there is becoming more cross over with both disciplines and this can lead to conflicts and issues and also opportunities such as reducing duplicative processes and knowledge sharing.

One industry that has a strong need for both a SMS and a ISMS is the Critical Infrastructure (CI) industry. The safety of people working within the facilities and the wider public is paramount and to ensure safety the CI organisation will also need to be secure. Technology changes such as Operational Technology (OT) and safety devices becoming connected to Information Technology (IT) and the Internet has also meant that cyber security threats can now impact the safety of the CI organisation [3]. In the past due to the technology being isolated from IT and the Internet these risks were less likely to occur.

To aid with the creation and implementation of SMS and ISMS, standards having been created some of the more well-known standards are:

- ISO 27000: information security management system



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

- IEC 62443: Industrial communication networks - IT security for networks and system
- IEC 61508 Functional safety
- IEC 61513 Nuclear power plants – Instrumentation and control important to safety

These are just a few example standards, and some would not strictly be considered a management standard but rather a standard in the field of safety or security but can be used to guide controls and processes that would make up the management system.

This paper will present a framework that has been created to allow CI organisations to create a Safety and Security Management System (SSMS). This management system combines the standalone processes into one process and resolves conflicts that can occur when the processes are combined. Results from a study that was carried out on the framework will also be presented.

## 2. Related works

There are many definitions on what a SMS is with one of the first definitions being from Kysor in 1973 [4] there has been many others given since then. Although all different they have core themes around policies, processes, and activities [5]. A key part of the SMS is managing risk [5] this helps the CI organisation decide on the controls required and sets the tone for policies and processes that need to be implemented.

As mentioned, SMS can be created for specific areas such as a Fire Safety Management System (FSMS), [6] showed they have many similarities to general SMS but have a focus on safety and risks for that particular area such as fire. Also, specific industries have mandated the use of an SMS such as the International Civil Aviation Organization (ICAO) who made it mandatory that all members states use an SMS [7].

[8] states that many safety-management systems standards are based on quality-management principles attributed to W. Edwards Deming. The reasons SMS are implemented can be varied a main reason is to improve safety, but it can also be a regulatory requirement. Research by [9] found that the top reasons where it was a client requirement, required by an insurance company or their employees wanted it.

Some benefits that have been noted by having an SMS are they improve communication, productivity, and overall safety in organisations [10]. They can also reduce the costs of incidents that occur. A survey conducted by [10] showed that organisations that adopted an SMS performed better in key areas of safety compared to organisations that did not have an SMS. This helps to show that a SMS helps organisations manage their safety and although it can be done without an SMS the overall performance of managing safety is improved with the use of one.

Some issues with SMS are that implementing an SMS can be considered costly [11] but the SMS can supplement safety processes that are already in place which can reduce costs. The complexity of the SMS and the processes it created can go against the organisations core activities [12]. Several authors [13, 14] have stated that the standards are too bureaucratic, and organisations became compliance focused rather than managing safety. Although these issues are raised the authors still feel SMS should be used but they need updating [15].

All management systems follow a similar design and principle, but the actual content will be different. For example, an ISMS would require objectives, and policies just like a SMS but the actual content of the objectives and policies would be different. An ISMS should be flexible enough to adjust to other security requirements and legislation [16]. The risk-based approach that is taken for an ISMS allows controls to be added as required.

Although there are many positive aspects of implementing a ISMS there has also been issues highlighted such as:

- Difficult to find users with the required experience to implement an ISMS [17].
- Users can be against change and the new processes and activities that it can introduce.



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

- The cost and time to implement an ISMS can also be a factor that limits the uptake of them [18].
- The standards can be vague, and organisations can struggle to understand what is required [19].

Due to the amount of work that can be required for an ISMS, techniques have been created to reduce the workload such as automation of certain areas. [20] created a framework and tool that is based on risk and reacts to changes in the organisation. The tests carried out were on a SME, but it looked to provide a way to manage certain aspects of an ISMS. Organisations have the option to either certify to standards such as ISO 27001 or they can just align and follow the standards to create their ISMS but not certify to them. An ISMS can be opposed by users of the organisation who are concerned it will negatively impact their day-to-day work. A study by [21] showed that a user centric ISMS can overcome some of the challenges users of an organisation could have with an ISMS being implemented. All management systems should be closely integrated with the organisational goals and objectives if they are not it will likely fail.

## 3. Safety and Security Standards Framework for Critical Infrastructure

The Safety and Security Standards Framework for Critical Infrastructure (SSS Framework for CI) allows CI organisations to manage both their safety and security standards. It leverages general safety and security standards and CI specific safety and security standards. The SSS Framework for CI details controls that are needed and how to deal with conflicts that arise when attempting to comply with both safety and security standards. By using the framework CI organisations can create a Safety and Security Management System (SSMS).

### 3.1 Framework Processes

The SSS Framework for CI has, 14 Processes, 22 control areas and over 1000 conflicts, issues and resolutions for those conflicts and issues. The framework can be used in two different ways the first is to follow each part of the framework in order. This is a good approach if the CI organisation is starting without a current management system in place. They follow the links in order and complete each section as they go. The other approach is to go straight to an area of interest, this can be appropriate if the CI organisation only needs guidance on a particular area. Figure 1 - Processes within the framework shows the 14 processes and the logical order they follow. The CI organisation may choose to follow a different order or do some parts in parallel as long as all parts are complete that is the key objective.



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022


**Figure 1- Processes within the framework**

### 3.2 Framework Controls

The next section of the SSS Framework for CI was the Controls section. This has four main parts. The first is Control Implementation and Operation, there are thousands of potential controls that can be put in place for safety and security. As well as new controls that can be implemented, controls that are already in place can be improved or have weakness that can be resolved. Implementing a control is only one part



**Doi : https://doi.org/10.54216/JCIM.090201**
Received: February 2, 2022 Accepted: March 05, 2022

of the process, once the control is implemented it needs to be managed some controls require more managing then others. The guidance given in the Control Implementation and Operation section will explain how controls should be implemented, operated, maintained, and decommissioned. Specific controls will be used as examples but due to the varied nature of controls it will not be possible to go through the process for all possible controls that could be used within safety and security.

The Control Implementation and Operation section is not usually a requirement within standards but the controls themselves need to be implemented and operated correctly to ensure compliance to the standards. Often poor control implementation and/or operation can lead to incidents such as the attack on a water utilities company in the US. Attackers gained access to cellular routers and run up a large bill, they could have impacted the faciality but did not, they were able to do due to poor network controls and not patching the routers [22]. For that reason, the author added this section which covers important considerations that should take place when controls are implemented.

The next section is Control Modification. Once the controls have been implemented changes in the environment, risk appetite, threats or organisation objectives as examples could all mean the controls needs to be changed. Modifying a control can impact many parts of a standard including the risk management section, as depending on the change it could increase or decrease the risk to the CI organisation. For this reason, the modifying of controls should be managed as strictly as the implementation and operation of controls are. The guidance given in the Control Modification section will explain how controls should be modified. Control modification has a lot in common with the Control Implementation and Operation Section. This is to be expected as when a control is modified it can be similar to installing it for the first time or depending on the control it can be similar to decommissioning it. For that reason, some of the guidance given in those sections can be leveraged but in the context of modification.

**3.3 Framework Case Study**

The third key part in the Controls section is the Case Study. The main purpose of the case study is to be used as a way for the SSS Framework for CI to show an example of how the controls described within the framework would be applied to a CI organisation and how conflicts and issues could occur and be remediated. The rest of the Controls section is then made up of 22 control areas. Each of the control areas is laid out in the following format:

- Overview – Brief description of what the control area is focused on.
- Controls –Controls for the control area will be listed here with a brief description of the control and a link to where more details can be found if needed
- Case Study Implementation - The case study will be used to show the controls being implemented and to highlight issues and conflicts that can occur between IT and OT and safety and security.
- Conflict and Issue Resolution - Covers the controls and conflicts highlighted in the case study implementation section and describes how to resolve the issues to ensure controls are implemented in some manner while not impacting the safety, security or running of the CI organisation.

The reason for these four main headings and the details within them was to allow the majority of the SSS Framework for CI to focus on the novel aspects of the framework and not information that is common to many. For example, the first two headings provide brief details on the control area and a list of the controls. Information on the controls can be found in many standards and several are referenced in each control area if the reader wants to find more details. The case study implementation section allows the reader to see how the controls can impact safety and security and the difficulties of implementing them on both IT and OT. It then highlights conflicts that can occur which is often lacking from standards which either will just describe the control and expect it to be implemented on both IT and OT or say there may be conflicts and issues but not what they are. The conflict and issue resolution section also provides hundreds of ways to resolve the conflicts and issues and gives more than one way so the CI organisation has options they can select which are best for them and their risk appetite.

The SSS Framework for CI is not static, updates will be required due to new technology, updates in standards, and new controls as examples. Any section of the framework can be updated and as part of the



Doi : https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

SSMS that each CI organisation will create from the SSS Framework for CI the SSMS itself will require regular updates and changes as part of an efficient SSMS.

## 4. Research Results

To get a better understanding of how well the SSS Framework for CI could be used by organisations, research was carried out to validate if the framework operated as expected.

### 4.1 Research Approach

Thematic analysis was selected as the data analysis method and the sampling selection approach was purposive sampling. A survey was selected as the main method to use within the research validation. Due to the type of questions the survey has and the answers that are produced a mixed method of using both quantitative and qualitative research approaches will be used. Using a mixed method can allow the strengths of both methods to be gained and they can complement each other [23]. Quantitative research approaches will be used on questions that provide a numerical response or can be quantified, while qualitative research approaches will be used for the more verbose answers and where gaining an understanding of what users are thinking is required.

Ensuring the research is trustworthy and identifying the bias's and assumptions of the researchers was also carried out. This is important as these need to be understood to ensure they do not occur or at least limit the impact of them.

### 4.2 Thematic Analysis Themes

The research was undertaken, and thematic analysis was carried out on the results and there were 6 main themes that were identified. Each will be now be analysed and the connection between the themes will also be evaluated.

### 4.3 Gaining Assurance

The strongest theme that was identified was *Gaining Assurance*. The participants described methods they use to gain assurance that the controls and processes they have in place are working correctly. The sub-themes described some of the key methods that were identified from the data. They were *application testing, audit, logging and monitoring* and *phishing tests.* The responses from the participants were already part of the framework and shows that the framework would be a good solution to use by an organisation and could be followed to help gain assurance.

The sub-theme of *application testing* has been documented in the SSS Framework For CI, in the Vulnerability Management and System Acquisition, Development and Maintenance areas. In total those areas found 8 conflicts and issues that can occur and provided solutions to resolve or reduce the risk of those conflicts. The framework also produced an auditing process that was created to handle both safety and security audits. It dealt with all aspects of the process including harmonising the terminology, creating an audit team for both areas, and producing the reports. The created auditing process could be used for the sub-theme of *audits* that was identified. Another sub-theme that the SSS Framework For CI had produced a section on was *Logging and Monitoring*. This was one of the control areas within the framework, 18 conflicts and issues were identified and documented in the framework. The SSS Framework For CI did not create those controls\processes exclusively to gain assurance they were created for various reasons such as to capture vulnerabilities, detect malicious insiders and for certification, but they can also be leveraged for gaining assurance and the analysis showed this was a key requirement for the participants when it comes to the use of safety and security frameworks.

### 4.4 Conflict Resolution

The next theme was *Conflict Resolution*, there was various conflicts that were highlighted which helped developed the theme. Such as ones between safety and security or between the business and the control area and conflicts in costs for the control\process. The concept of conflicts is a major area of the framework. The thematic analysis identified three sub-themes which were *Return on Investment (ROI), Risk Assessments* and *Team Discussions.* This highlights the need for a strong conflict resolution process within the SSS Framework For CI. In the framework, conflict resolution is part of the risk management process which many of the participants did comment was where they manage it, and it was one of the



Doi : https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

sub-themes that was created. However, an improvement to the framework could be for the conflict resolution process to not be focused or managed within one process such as risk management but be integrated into more areas so the other sub-themes of *ROI* and T*eam Discussion* can also be part of the framework, as these areas are currently lacking within the framework. This theme showed that to resolve conflicts will involve more than just the teams involved in the conflict itself. Other teams can help resolve what can become an impasse between teams directly involved in the conflict. As well as other teams' information such as financial benefits and threats and vulnerabilities can be used to help resolve the conflict. The SSS Framework For CI produced a new risk management process that combined both safety and security in to the one process. The survey results analysis showed that risk management is used in many areas within organisations and thus it is important a clearly defined process is in place. Guidance on how to create and improve a current risk management process would be of use as the participants use risk management within their own processes.

**4.5 Framework Challenges**

The implementation of a safety and/or security framework can be difficult, and the theme *Framework Challenges* was identified from the survey results. Six sub-themes also emerged around what the participants found challenging when it came to implementing the framework. The themes showed that the challenges can range from control specific challenges such as *Remote Access* and *Asset Management* to concepts such as *Availability* and *Knowledge.* People can also be a challenge which was shown in the *Senior Management* theme and technology can also impact the framework as shown by *OT Issues.*

The two-control specific sub-themes of *Remote Access* and *Asset Management* are covered within the SSS Framework For CI. The remote access is covered within Access Control and Asset Management within its namesake. The use of the framework would help resolve issues with the controls in general and provides conflict and issue specific guidance. Within Access Control 12 conflicts and issues were established and Asset Management had 6. The solutions to the conflicts could help resolve the challenges the themes highlight could occur. For example, a participant highlighted gaining access in a secure manner remotely can be difficult. The SSS Framework For CI recommends using a jump host if the end point device cannot have the secure access such as multiple factor authentication implemented on it.

The *Availability* sub-theme can be a concern for all organisations, but the thematic analysis of the survey results showed that it is of particular concern to CI organisations. Also, implementing safety and security frameworks can be challenging due to the risk of it impacting the availability of the organisation. The *Knowledge* sub-theme occurred within the data often with it being linked with a lack of knowledge for implementing\maintaining controls or an issue with finding people with knowledge in both safety and security. The SSS Framework For CI is designed to reduce the dependency on people's knowledge, people will still have to have an understanding and knowledge but the framework can assist with providing information and guidance and can be used to improve people's knowledge as well. For example, it can describe the process how to combine areas and how to resolve issues and give example solutions that can be used.

The safety and security risks and issues of OT have been raised before [24, 25] and were also a sub-theme within the data. The entire SSS Framework For CI is designed to consider both IT and OT and the challenges that can occur when trying to implement controls that are usually only applied to IT systems and non-critical infrastructure industries. As the analysis has shown that the participants have experienced *OT Issues* when using frameworks, it shows there is a need for a framework like the SSS Framework For CI. The SSS Framework For CI has over 1000 conflict\issues and solutions with many helping resolve OT specific issues. The final framework challenge that was identified was *Senior Management* and user resistance to the framework, the analysis showed that without senior management support all aspects of the framework can be more challenging which can then increase user resistance in general. The SSS Framework For CI has several sections which were designed to ensure senior management support such as the Management Commitment section and also the Roles and Responsibilities and Communication process sections can ensure general users and senior management understand their role and are more involved in the success of the framework implementation.

**4.6 Framework Improvements**



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

The next theme was *Framework Improvements* as the participants were only given a section of the SSS Framework For CI to review this theme has to take in to consideration the improvement themes that were identified may be covered in other sections of the framework they did not see. Of the improvements sub-themes that were identified and covered elsewhere they were *Authentication Improvements, Increased Monitoring, Network Segmentation* and *OT Security Weaknesses.* This shows that four of the six sub-theme improvements identified are already in place and shows the SSS Framework For CI had established important control areas that would be required. Another sub-theme that showed the framework had covered the areas well was *No Improvements* this was a strong sub-theme that many participants highlighted stating they could not see any areas missing or requiring improving. The final sub-theme was *Knowledge Assessment* and having that included within the framework. Connected with this sub-theme is the sub-theme from the *Framework Challenges* theme of *Knowledge* and finding people with the right level of knowledge for the implementation and maintenance of the framework.

**4.7 Controls in Place**

Understanding what controls, the participants currently have in place within their organisations is important to help establish what are the areas organisations currently struggle with or which are common within the SSS Framework For CI and their organisation. The theme *Controls in place* identified what those controls were. The thematic analysis defined a sub-theme of *Majority of Controls* this covered participants who stated that the majority of the controls within the SSS Framework For CI that they reviewed where in place. This underlines what other themes have shown such as *Gaining Assurance* where many of the areas discussed were already part of the SSS Framework For CI, that this framework is comprehensive and covers the controls and processes required.

Other sub-themes identified were *Logging and Monitoring, Network Controls* and *Password Resets.* It is expected that organisations would have these controls in place to some degree it was not established if these controls are in place across the entire organisation or only certain areas or how effective the controls are working. Each of these sub-themes and the potential conflicts and issues with them are part of the SSS Framework For CI, even when controls are in place a gap assessment can be done to see if specific controls in the section are not in place or offer alternative controls that can be implemented if needed.

**4.8 Controls not Implemented**

The final theme identified was *Controls not Implemented* these controls were specific controls within a control area. It showed that the control area itself would be in place in some form which is also shown with the earlier theme of *Controls in Place* but a certain more detailed control would not be. For example, access controls are in place but not multi factor authentication. A sub-theme for the *Controls not Implemented* area was *Conflict Resolution* the analysis showed that this was identified as an area that organisations are lacking. Although there were themes identified for how to resolve conflicts this shows that not all organisations are doing it and the ones that are it may be too informal to consider it an implemented control.

Other sub-themes were due to the fact that OT and/or safety were not applicable to the organisation. For example, the sub-theme *Harmonisation* is less likely to be required if the organisation does not have safety standards to also comply with which would require the terminology in the safety and security standard to be harmonised. However, it is possible that between only security standards terminology can differ [26] and harmonisation is required. The other sub-theme of *OT Specific Controls* emerged but if the organisation has no OT that would be why they have no requirement for those controls.

For the remaining sub-themes, they were detailed controls such as *Three Factor Authentication, Network Access Control (NAC)* and *Vendor Relationship.* Organisations will have reasons for not implementing them such as too user impacting which was highlighted for three factor authentication, or other controls are in place instead which was mentioned for vendor relationships with regards to vulnerability management. If a control was not implemented as the organisation had not considered it before the SSS Framework For CI can present the control and implementation guidance to help the organisation decide if the control is needed and how to implement it.

**4.9 Theme Relationships and Connections**



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

**Error! Reference source not found.** shows all the themes and sub-themes that were identified during the thematic analysis. It also shows the relationship between the themes and the impacts they each have.

The *Conflict Resolution* theme is connected to both the *Controls in Place* and *Controls not Implemented* themes. The *Conflict Resolution* theme will result in updates to both the other two themes and at a minimum they will be considered as part of the conflict resolution process. Two other themes that have a relationship with the theme *Controls in Place* is *Gaining Assurance* and *Framework Improvements. Gaining Assurance* evaluates the controls that are in place to understand if they are operating as expected, this then leads to the connection between *Gaining Assurance* and *Framework Improvements* the results from *Gaining Assurance* theme can advise the *Framework Improvements* theme of any changes that are required. This then leads the *Framework Improvements* to have a relationship with the *Controls in Place* and advises on new controls or changes to current controls. **Error! Reference source not found.**shows that the theme *Framework Challenges* is connected with the *Controls not Implemented* theme, as the framework challenges can impact the framework and cause certain controls not to be implemented. This in turns forms the final relationship of the *Controls not Implemented* theme with *Framework Improvements* controls that are not implemented have the potential to form improvements to the framework which can lead to controls being implemented.

The themes are inter-related and show how each theme and sub-themes can impact other themes which then results in changes to other themes. It shows the areas that can impact the implementation and maintenance of safety and security frameworks and how if the relationships are managed correctly they can result in a better more appropriate framework. If any of the themes are lacking or the relationships are not in place issues can occur. For example, if the relationship between *Gaining Assurance* and *Framework Improvements* was not in place when the gaining assurance theme identifies deficiencies in the controls a process to make the required changes may not occur.



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

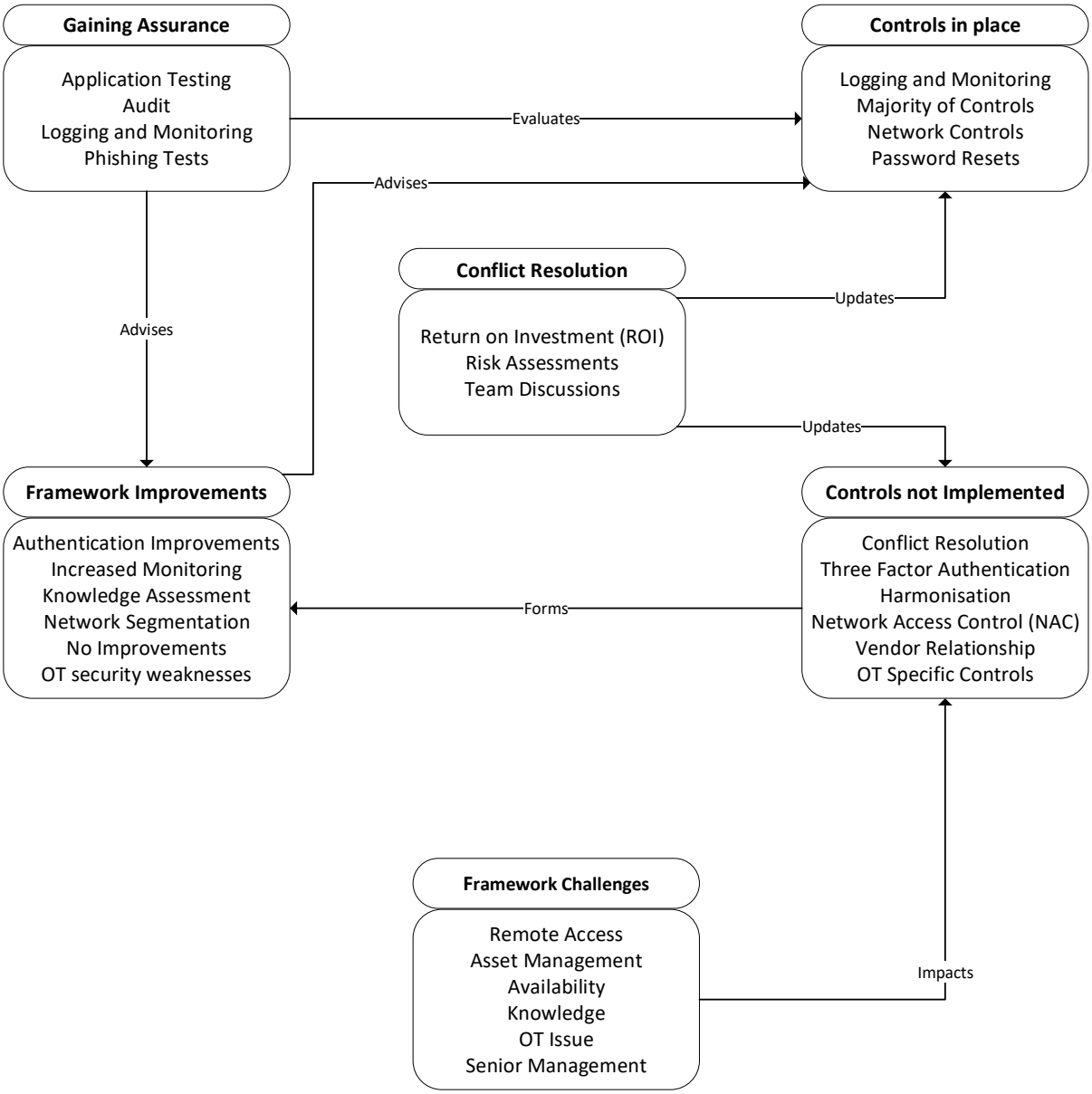


**Figure 2 - Themes and their relationships**

## 3. Conclusion

This paper has presented the SSS Framework for CI and the main parts of the framework and how they can be used to create a SSMS for CI organisations.

A survey was carried out with safety and security professionals to validate that the SSS Framework For CI would be useable for their organisations and to gain a better understanding of what is required to create a SSMS. The analysis of the survey results showed there were 6 key themes identified which were:

- Gaining Assurance
- Conflict Resolution
- Framework Challenges
- Framework Improvements



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

- Controls in place
- Controls not Implemented

The research validation showed that the SSS Framework For CI covered many of the issues or requirements of users. It also identified several potential areas of improvement, which were:

- Have the SSS Framework For CI highlight more the various ways the controls and processes within the framework can be used to gain assurance that other parts of the framework are operating correctly.
- Move the conflict resolution process out of the risk management process into the wider framework process and add ROI and team discussions to the process.
- Create a knowledge assessment process to help CI organisations establish the required level of knowledge for the control or process and to assess if the people have that level of knowledge, especially when safety and security are combined.

The results of this paper have shown that the SSS Framework for CI would be of use to users who need to create a management system that covers safety and security. Even if they only had a requirement for a SMS or ISMS the SSS Framework for CI would be of use but some of the areas may not be needed. The themes have highlighted what is required from a framework and challenges and controls that are applicable to organisations that need a SSMS.

**References**

[1] C. Coglianese, 2010, Regulating from the Inside. 10.4324/9781936331345.

[2] V. Holubová, 2016, Integrated safety management systems. Polish Journal of Management Studies, 14(1), pp.106-118.

[3] T. Kutzler, A. Wolter, A. Kenner, & S. Dassow, 2021, Boosting Cyber-Physical System Security. IFAC-PapersOnLine. 54. 976-981. 10.1016/j.ifacol.2021.08.117.

[4] H.D. Kysor, 1973, Safety management system. Part I: the design of a system. Nat. Safety News. 108, 98–102.

[5] F. Guldenmund & Y. Li, 2017, Safety management systems: A broad overview of the literature. Safety Science. 103. 94-123. 10.1016/j.ssci.2017.11.016.

[6] J. Santos-Reyes & A. Beard, 2002, Assessing safety management systems. Journal of Loss Prevention in the Process Industries. 15. 77-95. 10.1016/S0950-4230(01)00066-3.

[7] S. Smith, 2005, Safety management systems - New wine, old skins. 596- 599. 10.1109/RAMS.2005.1408428.

[8] H. Floyd, 2011, Safety-Management Systems, in IEEE Industry Applications Magazine, vol. 17, no. 3, pp. 19-24, May-June. 10.1109/MIAS.2010.939622.

[9] W. K. Law, A. Chan & K. F. Pun, 2006, Prioritising the safety management elements: A hierarchical analysis for manufacturing enterprises. Industrial Management and Data Systems. 106. 778-792. 10.1108/02635570610671470.

[10] E. Bottani, L. Monica & G. Vignali, 2009, Safety management systems: Performance differences between adopters and non-adopters. Safety Science. 47. 155-162. 10.1016/j.ssci.2008.05.001.

[11] H. Wolf, 2012, The emerging role of Safety Management Systems in aerospace. 10.1109/AERO.2012.6187419.

[12] [DM17] D. Maurino, Accessed 2021, Why SMS: An Introduction and Overview of Safety Management Systems. https://www.itf-oecd.org/why-safety-management-systems



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022

[13] J. Lappalainen, Overcoming Obstacles to Implementing SMS, Accessed 2021. https://www.itf-oecd.org/overcoming-obstacles-implementing-sms

[14] J. Pariès, L. Macchi, C. Valot, & S. Derhavengt, 2019, Comparing HROs and RE in the light of safety management systems. Saf. Sci. 117, 501–511.

[15] B. Accou & G. Reniers, 2020, Introducing the Extended Safety Fractal: Reusing the Concept of Safety Management Systems to Organize Resilient Organizations. International Journal of Environmental Research and Public Health. 17. 5478. 10.3390/ijerph17155478.

[16] J. Broderick, 2006, ISMS, security standards and security regulations. Information Security Technical Report. 11. 26-31. 10.1016/j.istr.2005.12.001.

[17] B. AbuSaad, F.A. Saeed, K. Alghathbar & B. Khan, 2011, Implementation of ISO 27001 in Saudi Arabia–obstacles, motivations, outcomes, and lessons learned", in Proceedings of the 9th Australian Information Security Management Conference, Perth Western Australia, pp. 1-9.

[18] K. Alshitri & A. Abanumy, 2014, Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. ICISA 2014 - 2014 5th International Conference on Information Science and Applications. 1-4. 10.1109/ICISA.2014.6847396.

[19] S. Aleksandrova, V. Vasiliev & M. Aleksandrov, 2020, Problems of Implementing Information Security Management Systems. 78-81. 10.1109/ITQMIS51053.2020.9322896.

[20] M. Brunner, C. Sillaber & R. Breu, 2017, Towards automation in information security management systems. 10.1109/QRS.2017.26.

[21] I. Bongiovanni, 2020, Designing User-Centric Information Security Management Systems in Financial Services Organisations. 192-199. 10.1109/CIC50333.2020.9492732.

[22] A. Hassanzadeh, A. Rasekh, S. Galelli, M. Aghashahi, R. Taormina, A. Ostfeld & K. Banks, 2020, A Review of Cybersecurity Incidents in the Water Sector. Journal of Environmental Engineering. 146. 10.1061/(ASCE)EE.1943-7870.0001686.

[23] G. Brown, J. Munro, H. Kobryn & S. Moore, 2017, Mixed methods participatory GIS: An evaluation of the validity of qualitative and quantitative mapping methods. Applied Geography. 79. 10.1016/j.apgeog.2016.12.015.

[24] H. Mokalled, C. Pragliola, D. Debertol, E. Meda & R. Zunino, 2019, A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems. 10.1007/978-3-319-95597-1_3.

[25] K. Su, I. Liu & J. Li, 2021. The Security Challenges with The Widespread Use of IT Infrastructure in ICS. Proceedings of International Conference on Artificial Life and Robotics. 26. 413-416. 10.5954/ICAROB.2021.OS7-1.

[26] [RR20] R. Ramirez & N. Choucri, 2020, Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review.



**Doi :** https://doi.org/10.54216/JCIM.090201
Received: February 2, 2022 Accepted: March 05, 2022