Audit, Validation, Verification and Assessment for Safety and Security Standards

Robert Kemp[1], Richard Smith[1]

[1] De Montfort University, Leicester, UK
Emails: p2548837@my365.dmu.ac.uk ; rgs@dmu.ac.uk

.

Abstract
Internal auditing is important for ensuring compliance to multiple safety and security standards. The problem is that although safety and security have similarities when it comes to auditing, they also have differences that makes auditing both areas under the same process difficult. This paper has shown how to overcome those differences and leverage the similarities to create one auditing process for both safety and security. The paper has harmonized the different terminology between safety and security and showed how the new auditing process can allow compliance to IEC 61508, ISO 27001 and IEC 62443.

Keywords: audit; security; safety; critical infrastructure, standards; assessment

1.Introduction

Auditing is a mandatory requirement for compliance to many safety and security standards. If an organization need to know in detail how processes and parts of the organization are working, they can gain an independent opinion on that process. One potential method to obtain this information is through audits, either external or internal, however gaining an independent opinion from an internal audit may not always be possible. It is dependent upon the specific audit criteria and who was carrying out the internal audit. Other potential methods are validation, verification, and assessments. All of these methods can allow an organization to examine and evaluate processes to provide an opinion on how the process is operating. Safety audits are important and have been shown to reduce injuries [1] and security audits can provide assurance that systems are secure and operating as expected [2].

An industrial sector particularly concerned with ensuring that safety and security are in place and functioning correctly is the Critical Infrastructure (CI) industry. The UK Cabinet Office defines CI as [3]:

Those critical elements of Infrastructure, the loss or compromise of which would result in major detrimental impact on the availability, delivery, or integrity of essential services, leading to severe economic or social consequences or to loss of life.

CI has many different aspects such as information technology, operational technology, mechanical systems, buildings and people as a few examples. All of these areas need to be audited, assessed, verified and validated.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

However, it can be costly and complex [4] to carry out these activities. Nevertheless, safety and security must be managed within CI as when it is not the consequences can be severe. Examples of this are the security incident of the attack on the Ukraine power grid [5] or the safety incident at the Oroville Dam when it was damaged and over 180,000 people living downstream from the dam had to be evacuated [6].

1.1 Problem and novelty of solution

This paper addresses the problem of managing the different terminologies that are used between safety and security [7] by creating a common lexicon to remove ambiguity and conflict that might occur in the process. The terms and definitions have been assessed and harmonised were possible. This will allow both areas to use a single terminology within the auditing process. This in turn helps make the other steps in the process easier to understand as they will be using unified terms.

By combining safety and security audits the challenge of finding auditors with suitable skillsets to perform joint audits becomes more difficult [8]. This paper presents a methodology for the assessment and classification of the suitability of auditors allowing organizations to choose the correct author to ensure that their requirements are met.

The scoping and scheduling [9] of two distinct areas is not something organizations would traditionally attempt and can be problematic as planning to audit the safety and security of Operating Technology (OT) simultaneously can impact resources and require significant coordination. This paper presents the criteria required for auditing activities in detail. This allows the issues that can occur when combing both safety and security to be identified, reduced, and managed better. This is coupled with a risk profile calculation that has been developed to make reporting on safety and security more formal and repeatable.

Safety audits have additional requirements, such as verification and validation, which are not usually required in a security audit. Calculating a risk score is already a complicated task [10] but expanding the scope for an audit covering two areas poses more challenges. Cases where the security area has no findings, but safety does can make the results look inaccurate for certain areas.

Within the domain there exist many different standards and requirements [11], which leads to the final problem of complying with all the clauses within different safety and security standards in a single process. Many of the issues will be new to teams that only cover safety and not security. This paper performs an analysis of safety and security standards and presents a novel methodology to resolve the problems and issues arising from the use of multiple standards.

1.2 Context

The aim of this paper is to create a process that allows a CI organization to carry out internal audits, validation, verification and assessments that will cover the safety standard IEC 61508-1:2010 Functional safety of electrical/ electronic/programmable electronic safety-related systems; the security standards of ISO 27001:2013 Information technology — Security techniques — Information security management systems and IEC 62443-2-1:2010 Industrial communication networks IT security Network and system security. Establishing an industrial automation and control system security program.

Figure 1 - Auditing Process Flow illustrates the process at a high level. The process will be termed Combined Safety and Security Internal Audit (C-SSIA) and has been created by the author. An audit represents a significant undertaking on the part of the organization, both in terms of time and resources. Due to the nature of the areas there exists a significant amount of overlap and dependencies between the two but both audits would take place separately leading to inefficiencies and wasted effort.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Most research has focused on either security such as [12] that created a security framework to manage and audit Information security. Or safety like [13] that looks at the auditing process by interviewing auditors and auditees to find improvements. However, none have looked at the auditing process of both safety and security at once. [14] has looked at approaches for combining safety and security for industrial control systems at a high level but not with a focus on auditing.

The rest of the paper is organized as follows. Section 2 will discuss the different standards that will be incorporated into the methodology. Section 3 will harmonise the different terms and definitions. Then section 4 will analyse the standards identified in section 2 to demonstrate how the process will meet the requirements of those standards. Section 5 will present the C-SSIA process that has been created. The final section 6, provides the conclusion.

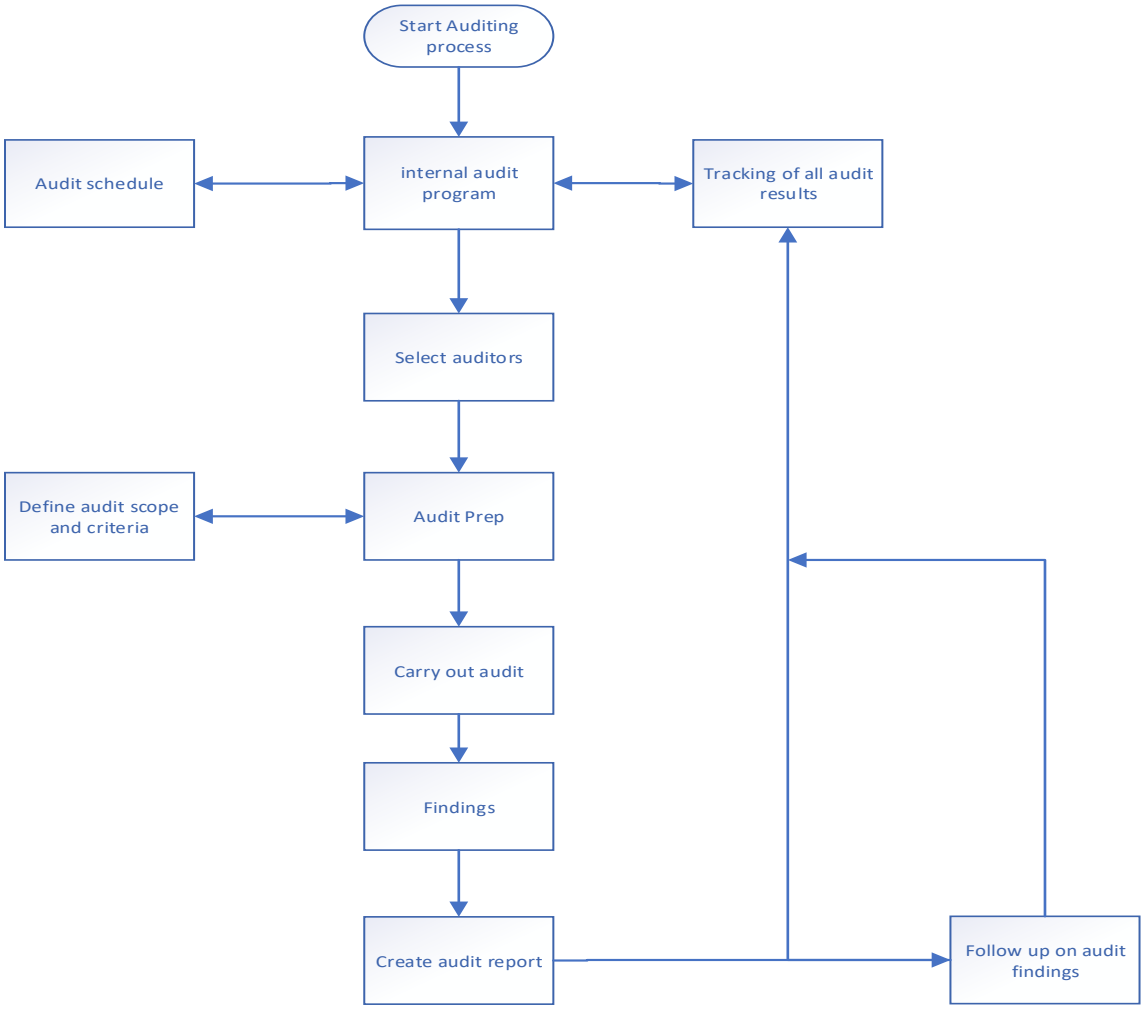

Figure 1 - Auditing Process Flow

2. Standards

The standards to be addressed in this paper are:

- IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems [15]

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

- ISO 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [16]

- IEC 62443-2-1:2010 Industrial communication networks. Network and system security. Establishing an industrial automation and control system security program [17]

These three standards were selected as they each cover a key area, with IEC 61508 ensuring safety activities are implemented in systems. ISO 27001 is focused on general security for organizations and IEC 62443 is aimed at cyber security for CI. Whilst other standards exist in the series, the three chosen standards provide the greatest coverage.

2.1 IEC 61508

IEC 61508 is a high-level functional safety standard. It is designed to be used across different industries, allowing them to create domain specific safety standards such as IEC 61513 Nuclear power plants - Instrumentation and control important to safety. As it has been designed for use across different industries a lot of the actual implementation decisions are left up to the end user [18]. It looks to cover the whole lifecycle of safety activities including all elements that make up the safety-related system by ensuring the engineering principles and requirements from the standards are applied to ensure the safety of the systems.

IEC 61508 is focused on functional safety of electronic and the software components of the electronics. Functional safety identifies potentially dangerous conditions, situations or events that could have a negative impact [19]. IEC 61508 is made up of a series of 7 standards: parts 1-3 make up the requirements of the standard; part 4 covers definitions; while part 5 provides examples on how to establish the safety integrity levels. Part 6 and 7 provide supporting information for parts 2 and 3.

2.2 ISO 27001

The number of organizations gaining certification to ISO 27001 has been increasing annually [20]. The standard is designed for organizations that want to create an Information Security Management System (ISMS) and is the main standard in a family of ISO 27000 standards. ISO 27002 is often used in conjunction with ISO 27001 although it is not mandatory, and compliance can be achieved without it. ISO 27002 lists recommended controls in various areas of security such as: incident management, access control, backups etc.

ISO 27001 has been designed to be applicable to organizations of all sizes and industry. The management system that ISO 27001 creates will help ensure the security controls that are already in place are also managed correctly. Some of the key areas of ISO 27001 are leadership commitment, risk management, metrics and corrective logs.

2.3 IEC 62443

IEC 62443 are a series of standards aimed at securing Industrial Automation and Control Systems (IACS). The four main parts of the standards are [21]:

- General
- Policies and Procedures
- Systems
- Components

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

The standards are comprised of technical requirements for the systems used as well as processes for other activities such as risk assessments. For example, part 4 is around the development of devices while parts 2 and 3 provide requirements on the overall CI system and how to secure it.

2.4 Comparison

The three standards have many similarities and in the case of IEC 62443 and ISO 27001 they are connected. Throughout IEC 62443 it mentions ISO 27001 as supplementary guidance and recommends it being used to help create the ISMS [22]. ISO 27001 is more general and aimed at the organizational level and creating the management system while IEC 62443 is more focused on individual systems. However, both consider the overall organization and systems, just not to the same degree of detail. Hence they can be used together to ensure good coverage of both areas. This is not the case with IEC 61508 and ISO 27001.

IEC 62443 and IEC 61508 also have parallels, both focus on the systems under test, have target levels and provide requirements for the achieving the levels.

Many similarities between IEC 61508 and ISO 27001, for example they both consider risk assessments, risk reduction and certification. They do have minor differences which will need to be considered during this paper, but both provide good base documents for their respective areas which other standards have been built on.

Auditing is an important part of being compliant with standards. External audits of the safety and security standards are required if the CI organization wants to gain certification. Internal audits can be done by the organization to check if they are in compliance with the applicable standard and find and resolve issues before they are picked up in the external audit where they could impact the organizations compliance status.

3. Terms and Definitions

In this section the terms and definitions from IEC 61508, ISO 27001 and IEC 62443, will be described and where possible harmonised.

Table 1 - Terms and Definitions shows the standard terms and the new definition that will be used for the C-SSIA in this paper.

Table 1 - Terms and Definitions

Term	New Definition	ISO 27001 Definition	IEC 61508 Definition	IEC 62443 Definition
Audit\ Functional safety audit	**Systematic and independent examination of evidence and relevant processes to establish if the requirements have been met.**	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.	Systematic and independent examination to determine whether the procedures specific to the functional safety requirements to comply with the planned arrangements are implemented effectively and are suitable to achieve the specified objectives.	independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Functional safety assessment			Investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities	
Validation	**Confirmation by examination and objective evidence that the requirements for a specific intended use or application have been fulfilled.**	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.	Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.	
Verification	**Confirmation by examination and objective evidence that specified required have been fulfilled.**	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.	Confirmation by examination and provision of objective evidence that the requirements have been fulfilled.	

IEC 62433 includes only one of the terms defined in the standard: audit. In both ISO 27001 and IEC 61508 validation and verification have very similar definitions and for that reason the new definition did not require significantly updating to cover both.

For the auditing and assessment, the new definition covers the terms audit, functional safety audit and Functional safety assessment. The original definitions were all very similar, the new definition has reduced the focus on safety or security focus allowing it to cover all 3 terms mentioned. IEC 61508-4 page 25 [23] even states that a functional safety audit may be carried out as part of a functional safety assessment. An assessment is different from an audit as the assessment focuses on the product\system, whereas an audit focuses on the organization. The new term has been defined to encompass both approaches. Although, the work to carry out either task will be different many of the concepts such as selecting auditors, criteria etc. will remain the same.

ISO 27001 and IEC 61508 have a limited number of defined requirements for an audit (security) and a functional safety audit. IEC 61508 requires defining:

a) the frequency of the functional safety audits;

b) the level of independence of those carrying out the audits;

c) the necessary documentation and follow-up activities.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

While IEC 61508 clause 8 – a functional safety assessment contains many more requirements. This highlights that although the new definition has been written to cover all three terms and their original wordings, the actual implementations include some differences. The main advantage of harmonising the defintion is that it allows the concepts that are covered by all areas to be discussed using common terminology.

For the remainder of this paper and in the C-SSIA process the term audit will be used when discussing the terms in Table 1 - Terms and Definitions but if there is a need or the section is only talking about one term in particular such as verification that will then be highlighted.

4. Standards Analysis

This section will now look at the clauses in IEC 61508, ISO 27001 and IEC 62443 and show how the C-SSIA in section 4 complies with those standards.

4.1 IEC 61508

IEC 61508 has a number of clauses that have requirements based around audits.

Clause 6.2.7 Management of function safety. The requirement is for functional safety audits to take place and a process should be created that covers the frequency, auditors and documentation. Each of which are covered in the C-SSIA process in section 4.

Clause 7.8 - overall safety validation planning. Clause 7.8 requires a plan for safety validation of the safety-related systems. The C-SSIA process created can be used to comply with this clause such as scheduling dates when the audit should take place and getting the correct auditors to carry out the validation. The focus in the validation process is on the product compared to the audits which are focused on the process.

The standard is focused on safety validation and as mentioned in section 3 the definition of validation is confirmation by examination and objective evidence that the requirements for a specific intended use or application have been fulfilled. This means that the CI organization will need to define the asset and requirements that are in scope, the same as audits, but should also include the modes of operation between the asset and control for example start-up, shut down, manual and automatic. Each mode may have different requirements that need to be assessed and evidence gathered. The auditor should document the technical steps they will take in the assessment and confirm that the requirements are in place for the use case. This is important as the auditor needs to ensure none of the tests or techniques to gather evidence will have a negative impact on the control or asset.

Clause 7.14 - overall safety validation, is taking the validation process discussed in clause 7.8 and is performing the process to validate the assets meet the safety requirements defined in the earlier clauses of the standard. If the team carrying out the validating are using equipment to generate quantitative measurements, they need to ensure the equipment is configured to the vendor specification or a national standard.

The C-SSIA in section 4 recommends how to document the audit\validation activities, including the results of the audit\validation. In the previous paragraph it was discussed how equipment may be needed, the tools and equipment used should also be documented including the configuration. Any differences between the expected and actual results will be investigated and if needed will be raised as a non-conformity and remediation work can take place to ensure the results are as expected.

Clause 7.15 - overall operation, maintenance and repair, has a requirement 7.15.2.2 that requires audits to take place and refers to clause 6.2.7 mentioned earlier. Auditing is important here to ensure correct operation and maintenance of systems. Also, requirement 7.15.2.3 requires documentation of the audits to be created and maintained.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Clause 7.18 – verification, details how to prove that each phase of the control lifecycle has met the objectives and requirements of that phase. The C-SSIA that has been described can be used to create a plan to verify all phases have been completed per the standard. The criteria of these audits was discussed earlier in the C-SSIA and clause 7.14 covers tools that will be needed for the validation activities.

Clause 8 – Functional safety assessment. Following the C-SSIA process to carry out safety audits will ensure compliance with this clause. It is worth highlighting that audit and functional safety assessments have the same defintion in the harmonised terminology in Table 1 - Terms and Definitions. The functional safety assessment will cover all phases of the control's lifecycle and clauses in the standard. As the C-SSIA process has shown, the auditors will need to analyse the assessment results to determine if the objectives and requirements of IEC 61508 have been met.

Clauses 8.2.15 to 8.2.18 consider independence of the auditors. IEC 61508 covers much more detail as to the level of independence required and it is tied to the consequence or safety integrity level of the control. The independence can range from a person, department or an organization. For example, if the consequence is very high then only an independent organization can carry out the assessment. The reason for the independence category selection should be documented.

4.2 ISO 27001

The only relevant clause in ISO 27001 is clause 9.2 - internal Audit. It is fairly high level like most clauses within ISO 27001. It makes audits mandatory but leaves it up to the organization to decide on the exact details, such as frequency of audits and methods of the audit. It requires the internal audit to check conformance to ISO 27001 and the organizations own requirements, as they may differ from the standard in some places. The clause requires the audits to be planned and reported along with other additional requirements.

The C-SSIA process created in section 4 will help comply with clause 9.2. The CI organization should also consider previous audits when it comes to planning the audit program.

It is also a requirement of this clause that the audit process and results are documented and retained as evidence.

Due to the high-level nature of clause 9.2, a CI organization would often require more guidance to successfully implement an auditing scheme. C-SSIA provides more detailed explanations to aid organizations in the design and implementation of their scheme and also facilitates the creation of a contextual process, one that can be adapted to suit the organization, such as who conducts audits, finding ratings and frequency of audits while still remaining compliant to clause 9.2.

4.3 IEC 62443

IEC 62443 has one main clause for auditing which is 4.4.2 - conformance. It has numerous sub clauses many of which have similar requirements to ISO 27001. Examples of this are competence of auditors, scheduling audits and creating an auditing methodology. KEMP ensures compliance with all of these sub-clauses.

Clause 4.4.2.4 states that punitive measures for non-conformance should be established. This means the organization should define what a non-conformance is and how it will be managed.

Verification and validation of systems is mentioned in Annex A of IEC 62443. Annex A provides guidance for developing the elements of a Cyber Security Management Systems (CSMS). Although the two terms are not mentioned in the main clauses of the standard they are required to create the CSMS and will be needed.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Table 2 - Mapping between standards and C-SSIA process shows the clauses discussed in this section and what sections of the C-SSIA process covers that clause.

Table 2 - Mapping between standards and C-SSIA process

Standard	Clause No.	Clause Details	C-SSIA Process
IEC 61508	6.2.7	Requirements for periodic functional safety audits shall be specified	4.2.2 Audit schedules 4.1.1 Auditor requirements 4.4.4 Remediation tracking
IEC 61508	7.8	Overall safety validation planning	All of the C-SSIA process will help comply with this clause
IEC 61508	7.14	Overall safety validation	4.1.6 Defining audit scope 4.1.7 Defining audit criteria 4.4.1 Audit report
IEC 61508	7.15.2.2	The carrying out, periodically, of functional safety audits (see 6.2.7)	4.2.2 Audit schedule 4.1.1 Auditor requirements 4.4.4 Remediation tracking
IEC 61508	7.18	Verification	4.1.7 Defining audit criteria 4.4.1 Audit report
IEC 61508	8	Functional safety assessment	4.1.1 Auditor requirements 4.1.2 Internal auditors 4.1.3 External auditors 4.1.4 Suitability of auditors 4.2.4 Audit schedule 4.4.1 Audit report
ISO 27001	9.2	Internal Audit	4.1.1 Auditor requirements 4.1.2 Internal auditors 4.1.3 External auditors 4.1.4 Suitability of auditors 4.1.6 Defining audit scope 4.1.7 Defining audit criteria 4.4.1 Audit report
IEC 62443	4.4.2.1	Specify the methodology of the audit process	All of the C-SSIA process will help comply with this clause
IEC 62443	4.4.2.2	Conduct periodic IACS audits	4.3 Conducting audits
IEC 62443	4.4.2.3	Establish conformance metrics	4.1.7 Defining audit criteria
IEC 62443	4.4.2.4	Establish a document audit trail	4.1.9 Questions and evidence
IEC 62443	4.4.2.5	Define punitive measures for non-conformance	4.3.2 Findings
IEC 62443	4.4.2.6	Ensure auditors' competence	4.1.2 Internal auditors 4.1.3 External auditors 4.1.4 Suitability of auditors

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

It can be seen that IEC 61508 has more clauses and requirements around auditing than ISO 27001 and validation, verification and assessments are all mentioned. IEC 62443 has in the main part of the standard similarly high level requirements as ISO 27001. The detailed Annex A however provides more detail on what should be audited and also verification and validation, which is not a part of ISO 27001. This makes it more closely aligned with IEC 61508 than ISO 27001. However, as the SMSS shows it is possible to cover these areas in the standards across one process it just requires looking at each step from both a safety and security perspective.

5. Safety and Security Management System Internal Auditing Process

CI organizations need to manage both safety and security by applying the applicable standards. When these areas are being managed separately a safety management system would be created for safety and a security management system for security. Safety and security should not be treated in isolation [24] and will be more effective when managed together.

Combining an Information Security Management system (ISMS) and a Safety Management System (SMS) in this paper is termed a Safety and Security Management System (SSMS).

The SSMS is considered to incorporate all of the processes, policies, documentation, technology, people and controls of the system. This means the SSMS will impact all parts of the CI organization; from the technology used to the controls that are placed on people. There will exist many different parts to the SSMS and the interdependencies between them will impact the way the SSMS operates. For example, a policy will describe a security requirement, which will be implemented by a control, which uses technology and a documented process, which is all managed by people.

To ensure the SSMS operates correctly and is complying with the applicable safety and security standards the CI organization will carry out internal audits. When these areas are manged separately the audits will also be managed separately, however as they are now being combined the CI organization will need to combine the internal audit processes. This can be a challenge for organizations used to managing them individually.

This section defines the C-SSIA process that can be used for both safety and security. This is a list of the topics covered in the upcoming section and a few example activities that are discussed:

- Audit preparation – Including selecting auditors and evidence requests
- Audit schedule – Creating audit program and timings of audits
- Conducting audits – Covers interviewing and observing activities
- Audit reporting – Creating the report and tracking.

5.1 Audit preparation

The audit is more likely to be successful when it is well planned out and the CI organization has prepared for what they want to achieve. This section will look at:

- Auditor requirements
- Internal auditors
- External auditors
- Suitability of auditors
- Establishing support for the audit
- Defining audit scope

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

- Defining audit criteria
- Gaining approval for the audit
- Creating questions and evidence requests

5.1.1 Auditor requirements

One of the first steps to prepare for an audit is to have an auditor or in most cases a team of auditors. Before the CI organization selects the auditors they need to consider the following about the auditors:

- Knowledge
- Independence
- Availability
- Experience

Knowledge - It will be very unlikely that the auditor will have knowledge in all areas covered by the standards, even more so as the C-SSIA process is covering both safety and security. The standard ISO 19011 Guidelines for auditing management systems provides useful requirements for understanding the knowledge the auditors need. The standard also provides guidance on other key stages of the auditing process which have been expanded on in this paper.

The CI organization may find an auditor with knowledge in one of the standards or areas but to find an auditor knowledgeable in both safety and security will be difficult. The auditor(s) selected must have the required knowledge to cover all the areas being audited. If the auditor does not understand an area they are auditing they will be unlikely to do a thorough audit. For example, it would be better if the auditor had knowledge of firewalls and network security if they were going to audit those processes within the CI organization.

Independence - As the audits are internal, the independence of the auditor is important. The auditor should not be involved or have been involved in the area being audited. For example, if the auditor helped set up the Intrusion Detection System (IDS) for the network they should not audit it. This would create a conflict of interest, because they may not want to identify any issues as that will be highlighting things they potentially missed when they set up the IDS. The line management of the auditor is also important, if the area being audited is also managed by the auditor's line manager they may be under pressure to ensure a positive audit report. To ensure independence the auditor should be free of any potential conflicts like the ones mentioned here. Also, they should not audit friends or family as that can impact their impartiality as well.

For independence of auditors some standards such as ISO 27001 require they are impartial but do not define the level of independence required. Whereas IEC 61508 has very detailed levels of independence that are required. With the three levels being person, department and organization. Section 5 discusses these clauses in more detail.

Availability - The auditors need to be available to audit the CI organization; certain audits may only be able to take place at specific times. For example, if the auditor wanted to audit the fail over of the facility to the backup one they would need to be available to attend. The CI organization will not be always be able to schedule the audits at a time that suits the auditor. Planning for audits will be discussed later.

Experience - As well as the auditor having knowledge it is best if they have experience in either auditing the areas or have worked on those areas in the past. Often auditors who have real world experience in the area they are auditing can provide better audits as they know what to expect and where issues can usually occur they can then look out for these in the audit. It is likely the CI organization will need multiple auditors for the reasons discussed here.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

5.1.2 Internal auditors

Whoever is selected to conduct the internal audits should be evaluated against the above. The CI organization may already have an internal audit department and they could ask them to lead the process and select auditors. This can be the simplest way as the CI organization can leverage what the internal audit team already have such as audit reports, processes etc., and all that will be required is the right auditors. If the CI organization does not have an internal audit department, they can look to use different users within current teams. Some issues with this is that while it is likely that the users will have the experience and knowledge in the area they are auditing they may not have actual auditing experience which will be required. A bigger problem will be ensuring independence the users may have to audit colleagues or areas managed by their line manager or they may have in the past worked on that area so having independence can be difficult. Without that it can be difficult to have assurance that the audit results are correct.

5.1.3 External auditors

Even though this section is talking about internal audits it does not mean that the auditors have to be internal to the organization. The CI organization can hire external auditors or use an external consultancy firm to carry out the audits. This has many advantages, independence can be more easily achieved, and the CI organization should be better able obtain auditors with the relevant knowledge and experience. The main downside to this approach is the additional cost that will come with paying for the auditors.

5.1.4 Suitability of auditors

Considerable research has been conducted in to how to build successful teams and the criteria that is needed to create those teams. Such as [25] that defines three attributes of team members and creates a quantitative method to help select the best team for the particular engineering project. [26] used the fuzzy number approach to establish the suitability of workers in industrial environments. Another paper that used fuzzy theory was [27] to assess the audit risk which considered the auditors and what impact the auditor attributes can have on the overall audit. Two papers that focused specifically on auditing are [28] and [29]. [29] does not focus on suitability of auditors however, it does have formulas and requirements for audit scheduling and those concepts and ideas helped to create the suitability of auditor's formula. [28] focuses on creating an audit team with the correct required skills. They create a formula using four skills types to determine the suitability of each potential auditor for the particular audit.

The suitability of auditor's calculation was developed from the concepts of [28] but expanded to use different criteria other than just the auditor's skill set to decide on their suitability and a different calculation was created to determine their suitability. The authors professional experience helped decide on the criteria and weightings for them.

A calculation (Eq. 4-1) has been created to show the suitability of the auditors. It uses the following formula:

Suitability of Auditors (SOA) gives a rating of the auditor's suitability for the auditing, a higher rating the more suitable they are to conduct the audit.

Knowledge Rate (Kr), a higher rating means the auditors are more knowledgeable for the audit. The rating can be between 1-5.

Knowledge Rating Score (Krs) is the knowledge rating after the weighting has been calculated.

Independence Rate (Ir), a higher rating means the auditors are more independent for the audit. The rating can be between 1-5.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Independence Rating Score (Irs) is the independence rating after the weighting has been calculated.

Availability Rate (Ar) a higher rating means the auditors have better availability for the audit. The rating can be between 1-5.

Availability Rating Score (Ars) is the availability rating after the weighting has been calculated.

Experience Rate (Er) a higher rating means the auditors have more experience in the area of the audit. The rating can be between 1-5.

Experience Rating Score (Ers) is the experience rating after the weighting has been calculated.

The knowledge and experience of the auditors are considered more significant than independence and availability and so are given a higher weighting within the calculation. Knowledge and experience use a 0.3 value while independence and availability have a value of 0.2. It can be easier to resolve an availability issue or reduce the risk of a conflict of interest compared to a lack of knowledge and experience. Also, those two areas will impact more how suitable the auditor is for the audit.

$$\begin{aligned} \boldsymbol{Kr} \times \mathbf{0.3} &= \boldsymbol{Krs} \\ \boldsymbol{Ir} \times \mathbf{0.2} &= \boldsymbol{Irs} \\ \boldsymbol{Ar} \times \mathbf{0.2} &= \boldsymbol{Ars} \\ \boldsymbol{Er} \times \mathbf{0.3} &= \boldsymbol{Ers} \end{aligned}$$

$$\boldsymbol{SOA} = \frac{\boldsymbol{Krs} + \boldsymbol{Irs} + \boldsymbol{Ars} + \boldsymbol{Ers} \times \mathbf{100}}{\mathbf{4}} \qquad \textbf{Eq. 4-1}$$

The ratings of 1-5 can be documented and described so the CI organization will be able to select the applicable rating.

5.1.5 Audit support

As well as the creation of the auditing team, the CI organization needs to have the buy in of the areas under audit. An audit can only be completed successfully if the teams that are being audited are involved and provide the required resources. The teams need to have the time, information and understanding of their own systems and be open with the auditors. If the teams being audited hide information or evade the auditor's questions it can result in either delaying or reducing the accuracy of the audit. To combat this senior management must ensure everyone understands the importance of the audit and users fully understand their roles and responsibilities. If the areas being audited do not provide the required assistance to conduct the audit this should be recorded in the audit report.

5.1.6 Defining audit scope

The next step in the C-SSIA is defining the audit scope. Each audit will have to be scoped to clearly identify will and will not be included in the audit. The aim of these internal audits are to help check the SSMS is operating correctly and complying to the selected safety and security standards. Each standard will have certain clauses that are mandatory when completing the audit. These mandatory clauses must be included in the scope of the internal audits.

For example, if the CI organization decided it was going to audit IEC 61508 clause 7.15 -overall operation, maintenance and repair for the facilities pipes and tanks this would be included in the scope. It is then the responsibility of the CI organization to establish which elements of the organization manage everything

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

covered by the scope. Also, within ISO 27001 clause 7.5 -documented information has mandatory requirements that documentation must follow, this should also be included within the scope and ensure IEC 61508 clause 7.15 also meets the required documentation requirements.

5.1.7 Defining audit criteria

At this stage the CI organization should have the auditors in place, support of the areas being audited and understand how to define the audit scope. Once the scope is defined the audit criteria will be established.

The audit criteria are linked to the scope and define what the audit will be based upon. What are the auditors going to audit against to determine whether the CI organization is in compliance. In the example earlier the audit criteria would be the requirements of IEC 61508 clause 7.5 and also any policies or procedures the CI organization has created to help comply with that clause, including requirements on the controls themselves. The auditor would then audit against the defined scope and criteria to determine compliance.

The next step is to gain approval for the audit.

5.1.8 Audit approval

Several different users will be required to approve the audit:

- The auditors themselves need to approve it and state they are happy with it.
- The team being audited should approve and the safety and/or security teams may also want to review and approve the planned audit.

Gaining approval is important as it helps gain support for the audit and also ensures all parities understand and have agreed upon all aspects of the audit.

5.1.9 Questions and evidence

To prepare for the audit the auditors will need to prepare questions, identify the evidence they require and areas they are going to focus on. The audit scope and audit criteria will help the auditors decide what is relevant. They can base their questions off the policies and procedures of the areas within scope. For example, the scope was to assess the storage of combustible material at a facility and the CI organization's policy requires all material to be stored in a specific building. During the audit the auditor could ask the team where they store the material to determine if their answer aligns with the policy. Another example could be if the audit was on the logical access controls to the network. The auditors could ask for evidence of the monthly access control reviews which the CI organizations are required to do. The requirements of the standard will also be used to create questions or evidence requirements. The questions asked by Auditors will dynamically change dependent upon answers provided.

5.2 Audit schedule

All three standards selected have requirements the CI organization are required to meet. These requirements will apply to the areas of the organization that are within the scope of the standard.

5.2.1 Audit scope schedule impact

The CI organization has many things to consider when it defines the scope some examples are:

- Which parts of the organization require certification [30]
- Are there resource constraints such as people and budget.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

- Which parts of the organization are considered high risk and require the standards being applied to them [31]
- Which systems and processes are key to the safety of the CI organization
- Where is data that is valuable to the organization kept and how is it managed
- What key interfaces and dependencies does the organization have

The wider the scope, and the more processes and areas are included will have a direct impact on the auditing requirements. For example, if the scope included two separate network segments the auditors would need to audit both. The control processes such as firewalls and router configurations on both networks would be assessed. This will impact the audit schedule and resources could be increased or the audits spread out over a longer period.

5.2.2 Audit schedule considerations

Most audit schedules would not have to manage both safety and security scopes but changing one scope can impact the other. For example, to ensure the safety of a system new security controls from the relevant standard would need to be applied and verified via an audit or assessment. The CI organization will need to ensure it covers all areas as required and the areas are aware of when they will be audited so they can prepare for it. For these reasons an audit schedule should be created listing all areas to be audited and when it will take place.

The internal audit program can be based on locations and clauses of the applicable standards. Each standard may have a different certification cycle, but all areas of the standard must be internally audited within the certification cycle. Some sections of the standard may be considered more high risk or important and require auditing more often such as once a year. Similarly, if an area can impact both safety and security it may be considered a higher risk and require more frequent auditing.

The CI organization needs to not only balance the resources of the audit team but also the impact on the teams being audited; it will require a significant investment of time and effort by the team members to be audited. Where teams fall under the remit of both safety and security audits a decision must be made whether or not to collocate the two to save time or introduce a time delay between the two to reduce the workload on staff.

5.2.3 Identifying conflicts

Auditing has the potential to identify conflicts arising between safety and security. For example, a security control of no shared accounts is not being enforced as it would impact the safety team who require the use of the shared account for a safety system. The auditors would raise a non-conformity due to the security control not being implemented. As an informal solution staff simply stopped implementing the security control, the audit can identify situations such as this and raise the issue up to the conflict resolution process. Auditing can also identify when areas of safety and security are duplicating work. The C-SSIA is being created to stop that happening. However, if the audit teams realise a safety and security team are both generating the same evidence or monitoring the same logs for example this could be identified and the efficiency of the SSMS could be improved.

5.3 Conducting audit

The next step in the C-SSIA is to carry out the audit.

5.3.1 Carrying out audit

The audit questions\evidence that have been defined in section 4.1 shall be checked and tested by verifying the existence of procedures and processes and witnessing evidence of these in action. All items recorded as

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

part of the audit shall be objective, (based on factual evidence) and not subjective (based on opinion). The auditors can carry out the audit in many ways:

- conduct interviews
- user observation
- request evidence

The auditors need to analyse all evidence, both primary and secondary, during the audit as at times users will try to cover up gaps or may not realise they are not compliant. The auditors need to be able to take the information from the audit and identify not only non-conformities but opportunities for improvements.

When the auditors auditing a particular area, they can perform verification and validation. For example, they may audit a control such as the safety release valve at the power station and check it meets the required requirements. All the guidance given here can be applicable to verification and validation.

5.3.2 Findings

As the auditors are carrying out the audit there will be findings. A finding is an area that is not in compliance with the standard or policies of the CI organization. Each finding should be assigned a severity based on a criterion set by the CI organization. The guidance given here is an example and can be changed as required. In ISO 27000:2017 Information technology — Security techniques— Information security management systems — Overview and vocabulary it defines a non-conformity as *"non-fulfilment of a requirement" and defines a requirement as "need or expectation that is stated, generally implied or obligatory"*. ISO 9000 Quality management systems Fundamentals and vocabulary has the same definitions for non-conformity and requirements. It also has a definition for audit findings, and it states, *"Audit findings indicate conformity or nonconformity"* This highlights that the audit findings should show if requirements are being achieved by the organization or not. Both standards talk about non-conformities however, they do not specify the type of non-conformity such as major or minor. A grading for non-conformities is discussed in ISO 19011:2018 Guidelines for auditing management systems, stating the context of the organization and its risk can help determine the non-conformity rating. They can be quantitative and qualitative and the example of minor and major is given.

External bodies that provide audit and certification of management systems apply grading to non-conformities. ISO 17021-1:2015 Conformity assessment -Requirements for bodies providing audit and certification of management systems has a definition for both a minor and major non-conformity. The terms are also used in [32] [33] [34] were they discuss audits and findings for management systems.

For the criterion used in the C-SSIA process the major and minor non-conformities that were discussed in the various ISO standards, were developed and given a more detail definition. Also, the professional experience of the authors allowed other audit finding criterion to be created to better represent that the audits where covering both safety and security such as a critical non-conformity finding.

The severities can be:

- Critical Non-conformity – A critical non-conformity is when a safety or security finding has the potential to cause an immediate risk to a person's life or cause serious injury. These are reported as soon as they are discovered, and action must be taken to resolve them before the audit and normal operation of the CI organization can continue.
- Major Non-conformity - A major non-conformity is where a systematic breakdown has occurred within one or more of the controls, or there is a failure of one of the management system elements.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

- Minor Non-conformity - A minor non-conformity is where an isolated failure has occurred of a particular control within the organization. Generally, the control has been working effectively, however the isolated elements create a reasonable risk. A failure of documentation controls within the management system or individual processes will also cause a minor non-conformity.
- Observation - An observation is provided when although the CI organization is compliant with the requirements of the standard there are opportunities to improve the process. There is no requirement to implement these observations, however they should be formally considered and logged

5.4 Reporting on the audit

Once the audit has taken place, the results of that audit need to be documented in a report.

5.4.1 Audit report

Some of the key pieces of information that should be documented in the audit report are:

- Date of Audit – Start and end dates the audit took place
- Name of Auditor – Name of auditors that were involved
- List of Auditees – Names of anyone who was involved in the audit
- Number of Findings assigned to Actions Log – An action log can have different names, but the main aim of this heading is to list how many findings have been logged and tracked for remediation.
- Audit Risk Profile – This is the overall risk profile that is given for the audit, it can be low, medium or high. An example what can be classified as low, medium or high is given at the end of these example headings for the audit report. This is a good way for users to see at a glance whether the audit had any findings or not.
- Purpose of Audit – This describes the aim of the audit, such as to gain assurance that maintenance is carried out.
- Control Areas in scope –any specific controls or standard clause numbers that were audited should be listed.
- Assets within Audit Scope – The actual assets will be listed here, such as buildings, or names of systems in scope of the audit.
- Exclusions from the Audit – Lists anything that has been excluded from the audit and states why.
- Audit Summary – In this section a description of what was audited, and number of findings and any other relevant information can be included here.
- Summary of Tests Conducted – Lists any tests done such as checking certain logs, looking at samples of data etc.
- Audit Findings Summary – all major and minor non-conformities and observations are listed here.

The C-SSIA recommends creating an audit risk profile of low, medium or high and using descriptions like those shown in Table 3 - Audit Risk Profile. The audit risk profile takes into considerations the findings from section 4.3.2 to determine the overall audit risk profile. The more findings the higher the audit risk profile will be. Audit risks have been looked at in other areas such as [35] which created an audit risk scorecard and considered many areas to create the risk score. For this audit risk profile in table 3 the authors professional experience supported creating the profile levels considering the impact each audit finding could have on the overall risk to the CI organization. If a more detailed formal method is required the calculation given in the next section (4.4.2) can be used.

CI organizations may alter the definitions to match their risk appetite. As an example, safety findings may be considered more serious then security findings unless the security finding can impact the safety of the CI

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

organization. The CI organization could set safety non-conformities to high while security are medium or low. The aim of the audit risk profile is to help the CI organization tell at a glance especially if many different audits have taken place which ones are higher risk and have more findings.

Table 3 - Audit Risk Profile

Level	Definition
High	There were many minor non-conformities or a critical non-conformity or major non-conformity which leaves the CI organization exposed to high levels of risk.
Medium	Most controls were in place and there was nothing found that was likely to cause significant risk to the CI organization. A few minor non-conformities were found.
Low	All controls were in place as expected

5.4.2 Risk profile score

Instead of using Table 3 - Audit Risk Profile or in combination with this the CI organization can look to use a formal calculation to establish the audit risk profile. A calculation (Eq. 4-2) has been created and it uses the following formula:

Risk Profile Score (RPS) is the overall score for the audit which will be used to set the audit risk profile at either high, medium or low.

Critical Non-conformity (CNC) is a critical non-conformity finding from the audit. These have a value of 5.

Number of Critical Non-conformities (NCNC) will be the number of critical non-conformities identified in the audit.

Major Non-conformity (MNC) a major non-conformity finding from the audit. These have a value of 4.

Number of Major Non-conformities (NMNC) will be the number of major non-conformities identified in the audit.

Minor Non-conformity (MINC) a minor non-conformity finding from the audit. These have a value of 2.

Number of Minor Non-conformities (NMINC) will be the number of minor non-conformities identified in the audit.

Criticality of Audit (COA) is how critical is the audit, a low number means more critical for example an audit of explosive material would be more critical than an audit of new hire background checks. The rating will be between 1-5.

$$RPS=((CNC \times NCNC)+ (MNC \times NMNC)+(MINC \times NMINC))/COA$$

Eq. 4-2

The CI organization can set the RPS to fall in to either high, medium or low depending on the score.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Audit risk can also be established before an audit takes place to help identify if the audit is of a higher risk and for example extra resources will be required. The methods and considerations that go into that audit risk process can be leveraged to create the audit risk profile. [36] creates calculations that include the importance of different criteria and different weighting for different audit factors. Another paper that calculates the audit risk for a risk based audit is [37] it uses fuzzy logic to help establish what the audit risk rating will be. This paper was not approaching the audit risk in the same manner as [36] and [37] as they were establishing the potential risk to help decide how to approach the audit and what resources are required. In this paper the audit risk profile is a calculation that determines the overall risk that comes from the audit findings. However, the concept of establishing audit risk and using a calculation helped created the calculation used in this paper. The values are different for each non-conformity with the higher value being assigned to the more serious non-conformities. Also, the criticality of the audit value will be lower for more critical audits, by doing this it will mean the risk profile score will be reduced for less critical audits.

5.4.3 Audit report review

Once the audit report is complete it should be provided to the auditees for review and they then have a chance to raise any inaccuracies they find in the report. They can also respond with potential remedial actions and activities. Audit reports can contain confidential information and should be shared on a least privilege basis, with the appropriate controls in place such as limiting who can access it and encryption. Audits should also highlight positive findings for example if the CI organization is doing something particularly well it should be included in the audit report.

5.4.4 Remediation tracking

As well as documenting the audit results and producing the audit report all major and minor non-conformities and the observations should be logged and tracked. The main objective is to have all the findings tracked, even if in the case of observations the CI organization chooses to do nothing with them. By recording them the CI organization has shown that it has considered them, and a comment can be added as to why no action was taken.

The auditor should follow up on the audit findings in a timely manner. The severity of the finding and when it was scheduled to be resolved will determine the timeframe for the follow-up. The remediation work should be verified to ensure they have met the original non-conformity effectively.

Section 5 has covered many areas that are required to ensure an efficient and effective internal audit process is created. Figure 2 - Internal Audit Considerations has all the key points and the details of each can be found in the C-SSIA process.

6. Conclusion

Internal auditing is necessary because the SSMS can change over time, mistakes can happen, malicious actions may be taken, and improvements to the SSMS should be done where possible. Internal auditing can help in all these areas and more and is a requirement in many safety and security standards. The C-SSIA process created can be used to audit both safety and security, often the biggest challenge for internal auditing is getting experienced, impartial auditors. However, once the auditors are in place the benefit for the CI organization not only in complying to the standards but also, to providing assurance that the SSMS is working effectively. By combining safety and security it is hoped duplication of work will be reduced and the two teams will become closer and share more information which is needed in both areas as they are converging more and more.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

This paper has created a process for auditing, validating, verifying and assessing an SSMS in a CI organization.

The terms and definitions in both safety and security standards are similar and can be harmonised to have a single defintion that covers them all. IEC 61508, ISO 27001 and IEC 62433, although covering different areas and having different requirements, also have similarities, such as leaving many of the implementation details up to the individual organization. This means two CI organization could create different auditing processes, but both still be compliant as long as they cover the clauses in the way best suited to them.

A future piece of work could be to include in the C-SSIA a way to capture the unique clauses in the standards that the process does not already cover and highlight any new definitions for the terms.

For example, standards are often updated, and new clauses added, or current ones modified. A part of the process could be a way to identify them and update the C-SSIA process to reflect the changes in the standards.

In order to help resolve the problem of finding auditors to cover both safety and security the calculation (Eq. 4-1) can be used to determine the suitability of auditors. The C-SSIA also showed an audit schedule and what should be considered to help the CI organization audit both areas concurrently. It was shown how the audit team can find it difficult to define an audit risk profile for audits on safety and security and an audit risk profile calculation (Eq. 4-2) was created that the audit team can use to help them establish a profile rating. The terminology section presented that verification and validation are terms found in safety, but this process was created to ensure that both areas are still captured in the process and therefore the audit team can be compliant to the relevant standards.

Another future piece of work is the calculation's that were created in this paper could be validated by being tested by auditors and see what works well and what improvements to the calculations are needed.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

Figure 1 - Internal Audit Considerations

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

References

[1] K. Mearns, S.M, Whitaker and R. Flin, Safety climate, safety management practice and safety performance in offshore environments. Safety Sci. 41, 641–680, 2003.

[2] M. Petterson, The keys to effective IT auditing. Journal of Corporate Accounting & Finance, 2005.

[3] Public Summary of Sector Security and Resilience Plans, 2017, Cabinet Office, Accessed 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

[4] H. Hemantha and H. Tejaswini, IT security auditing: A performance evaluation decision model. Decision Support Systems, 2014.

[5] United States Department of Homeland Security, ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure, Access 2019, https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

[6] F. Mcintyre, Learning from Failure | Oroville Dam spillway, 2017, Accessed 2019, https://www.newcivilengineer.com/archive/learning-from-failure-oroville-dam-spillway-14-11-2017/

[7] A. Waring, Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. Safety Science. 132, 2020. 104942. 10.1016/j.ssci.2020.104942.

[8] J. Rajamäki, Challenges to a Smooth-Running Data Security Audits. Case: A Finnish National Security Auditing Criteria KATAKRI, Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014. 240-243. 10.1109/JISIC.2014.45.

[9] I. Livshitz, K. Nikiforova, P. Lontsikh, E. Drolova and N. Lontsikh, The optimization of the integrated management system audit program. 121-124, 2016. 10.1109/ITMQIS.2016.7751919.

[10] R. Sabillon, J. Serra-Ruiz, V. Cavaller and J. Cano M, A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM), 2017. 253-259. 10.1109/INCISCOS.2017.20.

[11] B. Duncan and M. Whittington, Compliance with standards, assurance and audit: Does this equal security?. ACM International Conference Proceeding Series. 2014. 10.1145/2659651.2659711.

[12] T. Pereira and H. Santos, A Security Framework for Audit and Manage Information System Security. 3. 29 – 32, 2010. 10.1109/WI-IAT.2010.244.

[13] L. Allford,The auditing of process safety. Journal of Loss Prevention in the Process Industries, 2016. 43. 10.1016/j.jlp.2016.07.001.

[14] S. Kriaa, M. Bouissou, L. Piètre-Cambacedes and Y. Halgand, A Survey of Approaches Combining Safety and Security for Industrial Control Systems. Reliability Engineering System Safety, 2013. 139. 156-178. 10.1016/j.ress.2015.02.008.

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

[16] International Organization for Standardization, Information technology — Security techniques — Information security management systems — Requirements, Second edition, 2013.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

[17] International Electrotechnical Commission, 62443-2-1:2010 Industrial communication networks. Network and system security. Establishing an industrial automation and control system security program.

[18] K. G. L. Simpson and D. J. Smith, The Safety Critical Systems Handbook : A Straightforwrd Guide to Functional Safety : IEC 61508 Guidance, 2016, Elsevier Science & Technology, Oxford. Available from: ProQuest Ebook Central.

[19] International Electrotechnical Commission, Functional safety Essential to overall safety, 2015.

[20] International Organization for Standardization, 03. ISO/IEC 27001 - data per country and sector 2006 to 2017 Functions, https://isotc.iso.org/livelink/livelink?func=ll&objId=21413346&objAction=browse&viewType=1 Accessed 2020.

[21] International Electrotechnical Commission, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers, 2019.

[22] Thales UK, Thales Report Department of Energy & Climate Change Cyber Security: IACS Product Assurance, 2016.

[23] International Electrotechnical Commission, 61508-4 2010 Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations, 2010.

[24] A. Kornecki, N. Subramanian and J. Zalewski, Studying interrelationships of safety and security for software assurance in cyber-physical systems: approach based on Bayesian belief networks, Proceedings of the federated conference on computer science and information systems (FedCSIS), p.1393–9, 2013.

[25] J. Chen and L. Lin, Modeling Team Member Characteristics for the Formation of a Multifunctional Team in Concurrent Engineering. Engineering Management, IEEE Transactions on, 2014.

[26] S. Yaakob and S. Kawata,. Workers' placement in an industrial environment. Fuzzy Sets and Systems, 1999.

[27] C. Tian, H. Li, S. Tian and T. Fangyuan,. Risk Assessment of Safety Management Audit Based on Fuzzy TOPSIS Method. Mathematical Problems in Engineering. 2020.

[28] T. Dereli, A. Baykasoglu and G. Daş, Fuzzy quality-team formation for value added auditing: A case study. Journal of Engineering and Technology Management, 2007.

[29] B. Dodin, A. Elimam and E. Rolland, Tabu search in audit scheduling, European Journal of Operational Research, 1998.

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

[31] A Calder, Nine Steps to Success - An ISO 27001: 2013 Implementation Overview, IT Governance; 3rd edition, 2016.

[32] E. Lomas, Information governance: Information security and access within a UK context. Records Management Journal, 2010.

[33] M. Othman, Effectiveness of Safety Management System (SMS) by Malaysian shipping companies in compliance to the International Safety Management (ISM) code, 2021.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021

[34] E. Akyuz, and M. Celik,. A hybrid decision-making approach to measure effectiveness of safety management system implementations on-board ships. Safety Science. 68. 169–179, 2014.

[35] P. Saha, I. Bose,, P. Ray, A. Mahanti and B. Bhushan, A risk scorecard framework for E-auditing in Indian banking sector, AIS Journals Joint Author Workshop in PACIS 2013, 2013.

[36] M. Bradbury and P. Rouse, An Application of Data Envelopment Analysis to the Evaluation of Audit Risk. Abacus, 2002.

[37] Z. Hajiha, Fuzzy audit risk modelling algorithm. Management Science Letters, 2011.

DOI: 10.5281/zenodo.5205713
Received: February 21, 2021 Accepted: August 01, 2021