International Journal of Cyber-Security and Digital Forensics (IJCSDF) 10(1): 42-54
The Society of Digital Information and Wireless Communications (SDIWC), 2021 ISSN: 2305-0011

A Process for Performance Monitoring and Measuring in Safety and Security

Robert Kemp and Dr Richard Smith
Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, Gateway House, Leicester, LE19BH
P2658837@dmu.ac.uk and rgs@dmu.ac.uk

ABSTRACT

It can be difficult to measure the performance of a management system as organisations may not know what to monitor and measure or understand the quality of the information they are receiving and making decisions on. A management system that is combing safety and security which this paper has termed as a Safety and Security Management System (SSMS) is even more problematic as it requires measuring both safety and security. This paper will examine a proposed process to monitor and measure the performance of an SSMS and identify the problems with trying to achieve this and how the process overcame those problems.

KEYWORDS

Performance monitoring, Metrics, Security, Safety, Critical infrastructure, Measuring

1. INTRODUCTION

Critical Infrastructure (CI) is vital to the safe and efficient running of countries and for this reason requires protection. However, safety and security risks are increasing for CI and so are the attacks on them [1], [2]. To help CI organisations manage safety and security, standards that specialize in these areas can be used. A requirement of standards is to monitor and measure the performance of the management system in place. Standards such as ISO 27001 Information security management systems - Requirements has clause 9.1 Monitoring, measurement, analysis and evaluation and IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems has clause 6 Management of functional safety that makes monitoring a requirement.

Management systems are considered to be all the processes, policies, documentation, technology, people and controls in the defined scope of work. Management systems are an effective way to manage assets [3] and many organisations will implement them.

As management systems are complex and made up of different parts it can be difficult to establish if they are as effective as possible and operating as expected. Measuring the performance can be a good way to establish this [4]. Often safety and security are measured as two distinct areas, but they do have many concepts in common [5] and it can be possible to integrate safety and security into the same management system. A management system like this can be named a Safety and Security Management System (SSMS).

For organisations that do integrate both safety and security into the same management system they will also then want to monitor and measure that management system with the same process.

1.1. Problem and Novelty of Solution

The main problems this paper is going to resolve are it can be difficult to establish what should be measured or monitored for safety and security [6].

If the organisation measures too much it can be difficult to see important information as it can get lost within all the results. If they measure too little, they may miss the important information.

Organisations can gain a false sense of security if the monitoring is not showing any issues, they can assume everything is fine, but monitoring will not see everything, and issues can still occur.

They take time and resources to implement and maintain [7]. The users may be use to measuring and monitoring one area but will need to understand both safety and security processes.

This paper is going to help resolve those problems and provide a contribution in the performance monitoring and measuring area by these activities within the proposed process:

- Identifying activities to monitor – Breaks down how to establish the areas were monitoring activities will be required. Helping to resolve the issue of establishing what to monitor.

- Monitoring considerations – Monitoring tasks can have different criteria and this process describes them in detail. This allows the activities to be monitored in an efficient manner.

- Quality of Monitoring – This takes the earlier information in the process and uses it to calculate the quality of the monitoring activity. This will help organisations select the correct activities to monitor and ensure they are monitored successfully.

- Measuring Threshold - A calculation has been created to identify when a measuring activity has breached its threshold. This allows issues to be identified quicker and easier.

- Differences between monitoring and measuring – Helps establish the differences enabling organisations to better understand when to monitor or measure the activity.

This paper is going to examine the proposed monitoring and measuring process for a CI organisation that covers safety and security. The entire process will not be repeated here but key parts will and how they help resolve the problems and how it combines safety and security activities will be highlighted.

The process provides a baseline that CI organisations can use and will help with compliance to safety and security standards that require monitoring and measuring to take place.

Most research has focused on either security such as [8] and [9] or safety only such as [10]. However, none looked at the performance monitoring and measuring of the management system of both safety and security.

The safety of an organisation can be determined in different ways it could be base on the number of injuries and deaths that occur or near misses. Other factors can be based on safety equipment and faults that arise. It is best to use a combination of these and others that suit the CI organisation. The process in this paper is designed to provide flexibility for the CI organisation to select the best options for its circumstances.

The rest of the paper is organized as follows section 2 will describe what monitoring and measuring is and why it is needed. Section 3 will present the process for performance monitoring. Section 4 will cover performance measuring and the final section of the paper section 5 is the conclusion.

2. MONITORING AND MEASURING

Monitoring and measuring are two distinct processes. Monitoring involves observing processes, controls and alerts [11] as a few examples. Whereas measuring is assigning a value to something [12] for example measuring the number of safety incidents or faults per month. These will both produce information that needs to be analysed and decisions made based on the analysis of the information.

Monitoring will be discussed first in this paper, however there is a lot of cross over in the activities of both monitoring and measuring and the activities can be combined and implemented at the same time. This paper has separated them out to make the steps clearer.

Monitoring and measuring are important activities for the following reasons:

- [13] states they can help an organisation establish if they’re meeting their goals

- Rationalise expense and budget

- Ensuring the management system is producing expected results is a benefit [14] highlights

- [15] claims it can improve decision making

- Identify events before they become incidents

- Improve accountability is a benefit [16] showed was possible
- Help discover opportunities for improvement
- Show compliance with safety and security standards
- Help track issues or areas that require senior management attention

These are some of the main reasons monitoring and measuring takes place.

3. PERFORMANCE MONITORING

The performance monitoring process is aimed at the components that make up the Safety and Security Management System (SSMS). These were briefly mentioned in the introduction and are:

- Processes – such as how to assign a safety integrity level
- Policies – this includes the safety and security policy
- Documentation – this tends to be part of the other components such as a documented policy or evidence from a control as examples
- Technology – such as distributed control systems and firewalls
- People – can include engineers, managers and clients as examples
- Controls – for example air pressure release valves and encryption

As can be seen each part is not exclusive and they all interact to make the SSMS operate correctly.

3.1. What to Monitor

One of the first problems mentioned around monitoring and measuring is for the CI organisation to decide what to monitor. As this is covering both safety and security this can be even more difficult as different teams will need to be involved from both the safety and security areas.

The process recommends as a first step to establish what to monitor, the CI organisation should consider what are the aims and objectives of the SSMS. As by knowing what the SSMS has been created to achieve will help the CI organisation decide what they should monitor to see if that has been achieved. For example, if an objective of the SSMS was to ensure all safety systems are tested annually the CI organisation would look to monitor the safety systems with regards to their testing status.

The components of the SSMS should be separated out and the CI organisation can analyse each one individually to understand what should be monitored to show the performance of the SSMS. By breaking down each component of the SSMS it will make it easier to identify the activities to monitor. This is especially the case for a SSMS as the aims and objectives will not just be security focused which is normally the case for an Information Security Management System (ISMS).

The first component will be processes, the SSMS will be made up of many processes and it will not be possible to monitor all processes only key ones. The process gives examples of key processes such as risk management and examples of activities that could be monitored including:

- Risk treatment options that miss key dates in the remediation work
- New conflicts that occur between safety and security
- Changes in the CI organisations risk tolerance and risk appetite

The next component of the SSMS being considered is policies. It is a mandatory requirement of most safety and security standards to have policies. Policies can shape the entire SSMS and for that reason they are very important. The process highlights that the monitoring is for the policies themselves and not the requirements they create for the rest of the SSMS as they will be monitored in their own component. For example, a policy requirement would be to have a risk management process in place and operating but that can be monitored via the process component and not the policy component here.

The next component of the SSMS that the process covers is documentation. Documentation interacts with all the other components and in some frameworks would not be defined as a separate part of the SSMS. However, this process has because it is so critical by having it as a standalone component it will allow the CI organisation to consider it in detail.

As there will be a lot of documentation produced the CI organisation may choose to only monitor certain key documents. Documents that most impact the aims and objectives of the SSMS would be good choices such as documented evidence that will be required by the external auditors or ensuring all out of date documents are not in use as that could lead to an incident.

The technology component includes all technology involved in safety and security for CI organisation's and should not be limited to traditional Information Technology (IT). This means when it comes to monitoring of technology it should cover Operational Technology (OT), IT, hardware such as sensors, safety hardware and physical security. This is not an exhaustive list and the CI organisation should take a wide view when considering technology.

The process gives some examples of activities that could be monitored:

- Technology that is no longer under warranty
- Damage to the water flow release handle
- Resource capacity of technology such as memory
- SCADA goes offline

Technology is vital to achieving the aims and objectives of the SSMS and for that reason there are many aspects of technology that could be monitored. If an objective was to have high up time, monitoring for when technology goes offline would be important especially for technology that has the potential to cause an outage.

People are a major part of the performance of the SSMS. People can also be more unpredictable then technology and policies and will require monitoring to detect for that. The process highlights that certain monitoring tasks for people is done at a more granular level such as monitoring access control logs, the monitoring described in the process is more directed at the overall performance and objectives of the SSMS.

The monitoring activities can be linked to objectives such as ensuring a safe environment or having trusted, and trained people work at the facility.

The final component is controls, which can vary and often controls work in a defence in depth manner and one control on their own is of limited use, but the real strength is within the layers of controls.

Monitoring of controls in itself is a control but here the focus will be on the main controls that either impact the aims and objectives of the SSMS or are high level such as control exceptions which is monitoring for when an exception is put in place to not follow a control which could lead to an incident or increase the risk of the CI organisation.

Going through the potential activities by SSMS components such as processes, documentation etc. has shown that many activities can cross over into multiple components. This is not an issue as when the monitoring is defined, they can all be listed together and do not need to be categorised under each component that is just a way to help think of activities to monitor.

This stage in the process will allow the CI organisation to produce a list of activities that they would like to monitor to establish the performance of the SSMS. The next step is to create the monitoring process for the selected activities.

3.2. Considerations for Monitoring

It can be problematic for CI organisations to take the activity they want to monitor and create a monitoring process within the required resources they have and still capture what is required.

To help with this issue the process gives details on what the CI organisation should consider, and these will be used later to help calculate the quality of the monitoring activity.

When deciding how to monitor the performance of the SSMS, the process states the CI organisation should consider the following:

- Reliable
- Automated and manual if possible
- Repeatable
- Have alerts
- How accurate is the data being monitored
- Does the data come from multiple sources
- How often does monitoring take place
- Escalation and reporting
- Who conducts the monitoring
- What resources are required to carry out the monitoring
- Does the required data for monitoring already exist or does it need to be created
- How to monitor the monitoring

Reliable –If the monitoring detects a control failure it should be able to detect the same control failure each time. It is not just the detection that must be reliable all parts of the monitoring process should perform the same each time.

Automated and manual if possible – Monitoring should be configured as either automated, manual or both.

Automated monitoring is often considered the better of the two options as it is usually more efficient to monitor an activity automatically then to manually do it. Also, more information can be monitored by an automated system then a user could manually monitor. Not all activities can be monitored in an automated way and the only way will be a manual method. In situations like this the CI organisation needs to ensure the manual method will be able to monitor the activity efficiently. Automated monitoring is not perfect and can still fail or miss things for that reason a combination of automated and manual monitoring should be considered.

Repeatable –The monitoring activity should be repeatable as the CI organisation will want to monitor the activity more than once.

Have alerts – The monitoring activity should have a way to create or raise an alert when it detects something. Depending on the activity being monitored will decide if alerts are needed but for some activities the CI organisation will want to know if the monitoring detects something right away and for that an alert can be created.

How accurate is the data being monitored – The process highlights the monitoring can only be as good as the data it is monitoring. If the data is corrupt or incorrect the monitoring will use the incorrect data to make its decisions on what is being monitored.

The reliability of the data is very important, and the CI organisation should take steps to ensure it is accurate they can do this in various ways. They can manually check the information at the asset and check what is being received by the monitoring method, another method would be to ask the asset owners to look at the data to ensure it looks accurate. They can also get data from multiple sources which can help show if data is correct.

Does the data come from multiple sources – To increase accuracy and reliability the CI organisation should look to monitor data from multiple sources. This way if each source has different data that could be a sign something of an issue whereas only using one source it may go undetected. Multiple sources can also help if one source of data fails the monitoring can continue as the other source is still able to send the data. It will not always be possible to get data from multiple sources or it may be too resource intensive to produce the data in two places.

How often does monitoring take place –How often monitoring takes place and across what time frame can be impacted by many factors. Often the more monitoring that takes place the more resources are required (although not always the case with automated monitoring), the data required for monitoring may only be available at certain times such as once a week meaning the monitoring can only happen then as well.

The CI organisation may decide that the activity being monitored is not time sensitive and only needs to be monitored monthly for example. It may take a lot of effort to create the data to be

monitored and for that reason the monitoring is limited to how often it can take place.

Escalation and reporting – This will be covered in more detail in section 3.4.

Who conducts the monitoring – For the monitoring there should not be a conflict of interest with the person doing the monitoring being involved in the activity that is being monitored as they may try and supress results from the monitoring for various reasons.

The process recommends different monitoring activities being carried out by the most appropriate person\team and then another person\team is in charge of the overall monitoring process and takes the information provided by the individuals and correlates it and presents it as required by the CI organisation.

What resources are required to carry out the monitoring – The resources required can be affected by how easy it is to create the data to be monitored, how often the monitoring takes place, how the monitoring takes place; does a whole new system need to be created or is it done by email for example these will impact resources needed, and how much data is produced.

The CI organisation will need to look at how much resources they have for all monitoring activities and like any task balance the resources required with the resources they have. They may decide to monitor less activities or change the monitoring to monthly, do less manual and more automated monitoring as examples to change resource requirements as needed.

The process is helping to highlight the resources and the CI organisation will then have to manage them within the constraints they have.

Does the required data for monitoring already exist or does it need to be created – This can impact the other areas discussed. For some monitoring activities the data will be created as part of the normal activity. Whereas other activities may not generate the required data and the CI organisation will first need to spend resources creating the data for it to be monitored.

This process recommends were possible to use data that is available but recognises at times this will not be possible and the data required for monitoring will need to be created, when this is the case the monitoring team should work with the team that manages the activity to find the best way to create the data needed.

How to monitor the monitoring – The CI organisation will use the information from the monitoring to decide on the performance of the SSMS and safety and security decisions. For this reason, it is important the monitoring is accurate

The CI organisation needs a way to monitor for this, the process recommends:

- Audits
- Spot checks
- If automated monitoring is taking place switch to manual and see if results stay the same
- Ask the team running the activity if they have seen any issues.

Looking at the things the process recommends considering a lot of them can impact each other. For example, if the data needs to be created and come from multiple sources that would then increase the resources required. For that reason, when deciding how to monitor the activities all these items need to be considered together. Another factor to consider is when deciding how to monitor is to consider the risk, for example the CI organisation may choose to monitor an activity continuously in real time as it is a high risk but another activity the CI organisation may take a risk based approach and decide not to use alerts and just check the data when needed.

What the process aims to achieve in this section is to guide the CI organisation through one of the more difficult parts of the monitoring process. By giving examples and listing the key considerations the process will allow the organisations to select the most appropriate methods to create a monitoring task.

3.3. Assessing the Monitoring Results

The next topic in the process is assessing the monitoring results. The process recommends taking the monitoring results from all the separate

activities and centralising them in one place. The monitoring results will be different some may be numerical, others may be a description, and the results will be created at different times.

For the assessing to be effective the CI organisation must decide what it is looking for in the monitoring, what is expected and what would require escalation or remediation. This will be unique to each activity that is monitored.

For each of the activities the CI organisation needs to decide what are the expected results of the monitoring activity and then compare that against the actual result. This is the main part of the assessment for the monitoring. The user doing the monitoring will assess the results and then if the results are expected they will do what the process has defined for that situation. Which may be to just make a note the monitoring took place, and nothing was found or add the results to the report as examples. If the assessment of the monitoring shows an issue then the user should follow the process for that such as taking remediation action, informing a team or senior management as examples.

Assessing the monitoring results, reporting on the monitoring results and actions taken on the monitoring results are all separate tasks, although they are all connected. Assessment is the first of the three steps and has just been discussed. After the assessment, reporting and actions are the next steps.

3.4. Reporting and Actions

Reporting is done once the monitoring results have been assessed. The report can be any type of report such as a simple spreadsheet, dashboard, custom data visualisation tools, word documents and emails. The reporting can take place as soon as each activity is monitored, or the CI organisation can gather up all the assessment results and publish them at once. The process leaves it up to the CI organisation to decide.

The CI organisation should consider the organisations documentation and communication policies when it comes to documenting and communicating the performance monitoring reports. The reporting should provide enough details so that the users can understand what is being shown.

The aim of the reporting is to allow the CI organisation to present the assessment of the monitoring results in a clear manner and if needed it can lead on to the next step which is actions taken on the monitoring results.

The reporting will mention what action is taken. The CI organisation can take different actions depending on the results. If the results in the report are what is expected, then no action may be required.

The CI organisation should define an escalation path as another potential action, the escalation path can be used when the report is showing that the monitoring results require escalation beyond having the results in the report. Once escalated the person\team that it is escalated to should investigate what has happened and see what the cause of the monitoring results were. The next action the CI organisation could potentially take after it has been escalated if needed is take remediation action. This will depend on what the activity is and what remediation is needed.

3.5. Quality of Monitoring

The previous sections have discussed the main parts on the monitoring process for the SSMS. However, the CI organisation will want to establish if the monitoring activities they have created using the process are of a good quality. For that reason, the process created a calculation (Eq. 1) to show the quality of the monitoring activity.

The overall formal calculation is:

$$\boldsymbol{QMA = \frac{(COM \times AOM)}{RA}} \qquad \textbf{(Eq. 1)}$$

Where Quality of Monitoring Activity (QMA) is the overall rating of quality for the monitoring activity a higher rating means a better-quality monitoring activity.

Considerations for Monitoring (COM) uses the information in section 3.2 such as reliability, repeatability etc. and the user needs to decide how well the monitoring activity satisfies those considerations. A rating of between 0 (poor) – 10 (good) is given.

Assessment of Monitoring (AOM) looks at section 3.3 and how the monitoring activity can be

monitored. If the activity is difficult to assess it will receive a lower rating the rating is between 1-5.

Remediation Activity (RA) is focused on section 3.4 and the remediation work. There are 3 figures that can be used here which are if the remediation work did not resolve the issue a 6 is given, if it slightly resolves it a 4 is the figure and if the remediation work resolved the issue a 2 is given.

Figure 1 - Performance monitoring steps shows a flow chart showing the main steps that have been discussed in this document for performance monitoring of the SSMS.

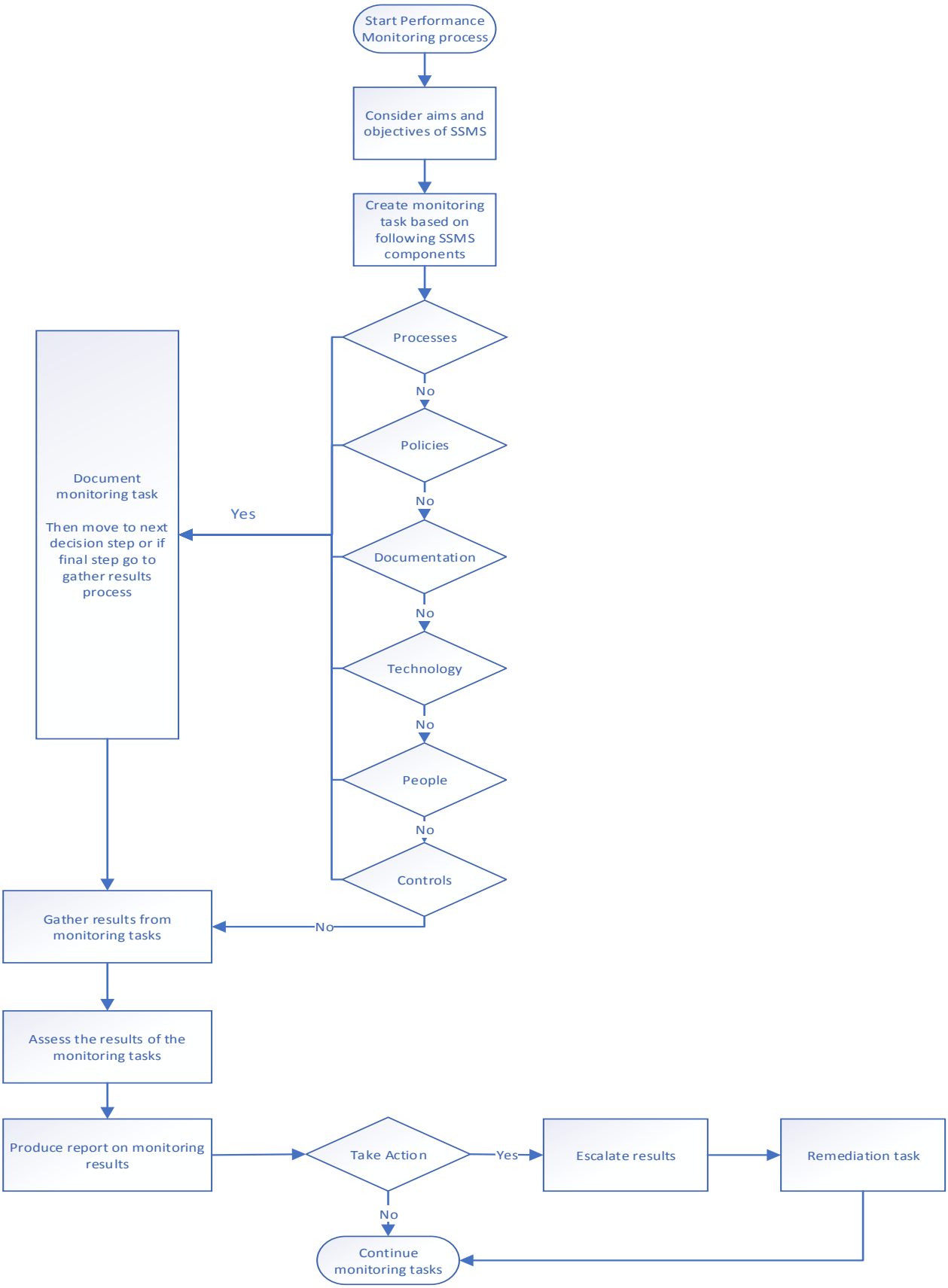

Figure 1 - Performance monitoring steps

4. Performance Measuring

The process next covers performance measuring of the SSMS. It states that the CI organisation should have created the monitoring tasks and they can leverage much of that work to measure the performance of the SSMS, measurements could even have been done at the same time. This section will cover the unique performance measuring activities.

The CI organisation needs to establish what to measure to evaluate the effectiveness of the SSMS. Much like monitoring, the aims and objectives will be good to be reviewed, and so will the components of the SSMS.

The process recommends using metrics to measure the SSMS effectiveness, a difference between creating monitoring tasks and metrics is that when considering metrics, the CI organisation will be looking for activities that produce something that can be measured. Monitoring tasks may monitor something that will not create anything whereas metrics tend to assign expected values to the activity.

Some example metrics that the CI organisation could create are:

- Percentage of servers with the two latest virus definitions
- Number of high risks open on the risk register
- Number of risks closed
- Number of emergency changes
- Average overall patching compliance percentage for servers
- Percentage of systems behind maintenance schedule
- Number of faults reported
- Number of audit findings open
- Percentage of injuries caused by missing safety equipment

A difference with how these will be managed compared to monitoring activities is that they are not monitored but rather values provided on each one on a time scale decided by the CI organisation.

Each metric selected will have an owner and they will be responsible for providing the measurement results to the person\team who is managing the metrics. This may or may not be the same team that manages monitoring. As well as a metric owner a rational for why the metric has been selected should also be documented. For example, the metric of number of emergency changes, could have a rational that this demonstrates the effectiveness of the change management process.

Next a threshold measurement needs to be created by the metric owner and the team managing the overall measurement process. The threshold should be a value that if the actual result is higher or lower than that threshold it should be reported. The process recommends using a red and green status to help identify more clearly measurements that are not within their thresholds.

The CI organisation can select a time frame for how often the measurements are collected. A recommend timeframe would be monthly any shorter than that may use too many resources and also may not allow for many measurements to be taken but each CI organisation should select the timeframe that works for them.

Once the CI organisation has all the measurements they need to be put in a report. Like the monitoring report the CI can present the information from the measurements how they prefer.

For the action taken on the metrics, the CI organisation can decide what is the most appropriate action. When a measurement

goes above/below its threshold and is marked red the CI organisation does not always have to take any action. They can wait and see if it continues to stay red in the following months and then take action to investigate further or remediate. At times the CI organisation may decide the threshold needs to be changed as the original was not realistic or the team may have improved the activity and now the threshold can become stricter. When changes to the threshold are made all relevant users should be informed so they can voice any concerns they have.

Some differences with measurements compared to monitoring tasks can be seen here which are timeframes, some monitoring tasks can be real time whereas metrics are more static and take place at the same time. Another difference is the assessment for metrics it is just comparing the metric to its threshold and marking it red or green.

Performance measuring is important for the reasons discussed in section 2 and it can complement performance monitoring and allow the CI organisation to gain a good understanding of the effectiveness of the SSMS.

4.1. Measuring Threshold

The measuring process requires a threshold to be created for when the performance of the SSMS may be negatively impacted. When this occurs the CI organisation will want to identify the issue quickly and ensure the alerts are correct.

For that reason, the process created a calculation (Eq. 2) to identify when a measuring activity has breached its threshold.

The overall formal calculation is

$$PMT = MA > TR \quad \textbf{(Eq. 2)}$$

Where Performance Measuring Threshold (PMT) is the result of the calculation and will either show the results are within the threshold limit or have breached them.

Measuring Activity (MA) is the results from the measuring activity. This can be any figure depending on what the activity is. For example, 5 malware incidents or 3 accidents at the plant.

Threshold Rating (TR) is the rating that the threshold has been set at. Measuring activities can be set to be higher or lower than the threshold. Following on from the example above the MA could be 5 malware incidents and the TR is 3. This will then result in a PMT showing the measuring activity has breached its threshold.

Then the team can use the results and act if required and update the reports.

The measuring process created allows the CI organisation to use much of the earlier information from the monitoring process. This is an efficient way to decide on what requires measuring and the threshold calculation could be automated within the measuring reports and tools to send out alerts if required.

5. CONCLUSION

This paper has analysed the process created to measure and monitor the performance of Safety and Security Management Systems (SSMS) in CI organisations which was the aim of this paper.

This paper has shown the difference between monitoring and measuring as they are often considered to be the same thing. Monitoring is around observing process while measuring is assigning values to activities, both are important and work together to show how efficient and effective the SSMS is.

The process looked to resolve the problems with monitoring and measuring by providing guidance on how to select activities to monitor and the criteria that can help create the monitoring\measuring tasks.

Due to the added complexity of the management system covering both safety and security the process placed on emphasis on including aims and objective for both areas. It also created calculations that can be used for monitoring\measuring and ensuring activities in both areas are managed resourcefully.

The process analysed in this paper should gain the benefits discussed in section 2 and help with overcoming the issues mentioned such as what to monitor and measure, checking results and managing resources.

The process listed a lot of detail such as all the components of the SSMS that can be used to help select what to monitor\measure. Also, all the information on how to monitor activities that the CI organisation must consider such as reliability, sources of data, how often etc. CI organisation will need to consider how their organisation will handle each section and customise the activities to suit.

The results can be used to make decisions such as if the results are showing that patching is not taking place or faults take a long time to be fixed. Senior management may invest more resources into those areas then once the results improve, they can look at other results and make more investment decisions based on those results.

A key part in the whole process of monitoring and measuring is the actions, as they should lead to improvements. Another way to look at it is if nothing is raised that can give confidence the SSMS is working well although there should always be improvements that can be made.

Assessing, reporting and taking action are different tasks and this paper has highlighted that. They follow from one to the other, first the CI organisation assesses the monitoring results, they then report on the results of the assessment and if needed take action.

Measuring the performance of the SSMS allows the CI organisation to see how key aspects are performing and can be a good way to measure how the performance changes over time. Often when organisations begin collecting metrics, they will have a lot of red results, but the metrics will bring the activities to users' attention and work will be done to improve the performance and the activities and then the metrics will begin to improve as well.

As this process is about complying with both safety and security standards, the CI organisation can produce the report combing both safety and security results this will help bring the teams together and share important information. Safety and security working closely is becoming more important as more attacks take place on them such as the attacks on oil refineries [17] in the United Arab Emirates (UAE).

Conflicts could occur in the monitoring or measuring of safety and security when it gets to the action part of the process. Often an action will be to remediate the finding which could involve a control or changing a process which could impact either safety or security and create a conflict. In situations like that the CI organisation should follow its conflict resolution process.

Existing methods for monitoring and measuring are focused on either safety or security and not both. Such as ISO 27004 - Information security management — Monitoring, measurement, analysis and evaluation which is focused only on security. Or they focus on either monitoring or measuring only such as [18] and [19]. This process has covered all areas within the one process to make measuring and monitoring safety and security management systems more efficient and no longer two distinct processes.

A future piece of work could be for the monitoring and measuring process to include a step in the action section that checks for conflicts and if identified directs the user to the conflict resolution process.

This paper has shown that safety and security have enough similarities and goals in common that a joint performance monitoring and measuring process can be used. By having both areas covered together it will reduce duplication, make more efficient use of resources and allow the two teams to work closer and manage the SSMS better.

6. References

1. A. Ofori, Cybercrime and Risks for Cyber Physical Systems. International Journal of Cyber-Security and Digital Forensics, 2019. 8. 43-57. 10.17781/P002556.

2. A. Humayed, J. Lin, F. Li, Fengjun and B. Luo, Cyber-Physical Systems Security -- A Survey, IEEE Internet of Things Journal, 2017. DOI: 10.1109/JIOT.2017.2703172

3. H. Susanto, M. N. Almunawar and Y. Tuan, Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical Computing Sciences, 2011.

4. J. Andress, and M. Leary, Building a Practical Information Security Program, Chapter 10 - Information Security Program Metrics, Pages 169-183, Syngress, 2017.

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

6. W. Knowles, D. Prince, D. Hutchison, D. Pagna and K. Jones, A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection., 2015. 9. 10.1016/j.ijcip.2015.02.002.

7. L. Svensson, U. Snis, C. Sørensen, H. Fgerlind, T. Lindroth, and M. Magnusson, The Challenge of Metrics Implementation, 2000.

8. S. Fukushima, Proposal and Evaluation of Method for Establishing Consensus on Combination of Measures Based on Cybersecurity Framework. International Journal of Cyber-Security and Digital Forensics, 2016. 5. 155-165. 10.17781/P002209.

9. C. Krag and G. Hinson, Pragmatic security metrics: applying metametrics to information security. Auerbach Publications, 2016.

10. Y. Luo, and M. Brand, Metrics Design for Safety Assessment. Information and Software Technology, 2016. 73. 10.1016/j.infsof.2015.12.012.

11. W. Chen and J. Li, Jing, Safety performance monitoring and measurement of civil aviation unit, Journal of Air Transport Management, 2016. DOI: 10.1016/j.jairtraman.2016.08.015

12. S. Sultana, B. Andersen and S. Haugen, Identifying safety indicators for safety performance measurement using a system engineering approach, Process Safety and Environmental Protection, 2019. DOI: 10.1016/j.psep.2019.05.047

13. S. Melnyk, Metrics and performance measurement in operations management: dealing with the metrics maze, Journal of Operations Management, 2004. DOI: 10.1016/S0272-6963(04)00010-5

14. N. Karanikas, Critical review of safety performance metrics. International Journal of Business Performance Management, 2016. DOI: 10.1504/IJBPM.2016.077244

15. W. Jansen, Directions in Security Metrics Research, 2010.

16. I. Tashi and S. Ghernaouti, Security metrics to improve information security management, Proceedings of 6th Annual Security Conference, 2007.

17. A. Neaimi, A Framework for Effectiveness of Cyber Security Defenses, a case of the United Arab Emirates (UAE).. International Journal of Cyber-Security and Digital Forensics, 2015. 4. 290-301. 10.17781/P001502.

18. F. S. Özdemir, A Conceptual Model for a Metric Based Framework for the Monitoring of Information Security Tasks' Efficiency, The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, 2019.

19. M. Shamim, A. Buang, H. Anjum, I. Khan and M. Athar, Development and quantitative evaluation of leading and lagging metrics of emergency planning and response element for sustainable process safety performance. Journal of Loss Prevention in the Process Industries, 2019. 62. 103989. 10.1016/j.jlp.2019.10398