

Development of a process model for a modern control room

EL Hugo

 **[orcid.org/ 0000-0001-8685-1890](https://orcid.org/0000-0001-8685-1890)**

Dissertation accepted in fulfilment of the requirements for the degree *Master of Engineering in Development and Management Engineering* at the North West University

Supervisor: Prof JEW Holm

Co-supervisor: Prof PW Buys

Graduation: June 2021

Student number: 27235270

Acknowledgements

I wish to thank my promotor, Professor Johann Holm for his guidance, support and involvement on a professional and personal level. Thank you for supporting my goals and helping me achieve them. Secondly, I would like to thank Dr Rossouw van der Merwe and the team at Jericho systems for funding my position at the SAIIE conference and thank you for your support and insights.

I would also like to thank my grandmother for copyediting my thesis and my grandfather for making provision for me to study. I will forever be grateful. My significant other, Lana, for your love, understanding and support. Finally, I would like to thank God for the blessings and opportunities that were given to me this year. Thank You for always letting things fall into place according to Your plan - the best one.

Abstract

We are in the midst of the fourth industrial revolution, which raises the question of the relevance of intelligent technologies in modern-day control room systems. Control rooms in multiple industries perform tasks of event management – which is the most important function of control rooms. A loosely integrated security control room system is analysed in this research and defined generically. This system is constructed and validated in a simulation environment with historical data from a real-world control room system. This conventional control room system is referred to as the “AS-IS” model in this research.

Research topics in the literature study include human factors and industry 4.0 technology such as various forms of artificial intelligence and augmented cognition. These topics show that intelligent technology that may be applicable to control room systems is widely available and successful in many other settings. This finding provokes multiple sensitivity analyses on the “AS-IS” system to understand the anticipated impact of technological alterations. The impact of changes to the “AS-IS” system is recorded with influential output variables including the time incidents are not under control, the operational wastage, and the costs involved.

This research is intended to act as a catalyst for future, more comprehensive studies. The objective is, therefore, to illustrate that intelligent technologies may be suitable in many control room industries, and to identify the areas of the system where they would be most applicable and why.

Keywords:

Modern control room

Industry 4.0

Process model

Artificial intelligence

Operations modelling

Opsomming

Ons staan midde van die vierde industriële rewolusie, wat die vraag opbring of intelligente tegnologie in 'n moderne, hedendaagse beheerkamer relevant is. Beheerkamers in veelvuldige industrieë vervul take in voorvalbestuur – die belangrikste funksie van beheerkamers. 'n Losweg-geïntegreerde sekuriteitsbeheerkamer word in hierdie navorsing ontleed en generies gedefinieer. Die stelsel word saamgestel en gevalideer in 'n gesimuleerde omgewing met historiese data uit 'n werklike beheerkamer. Hierdie konvensionele beheerkamerstelsel word na verwys as die “AS IS” model.

Navorsingsonderwerpe in die literatuurstudie bevat onderwerpe soos menslike faktore, industrie 4.0, en ander onderwerpe soos bv. verskillende vorms van kunsmatige intelligensie en aanvullende kognisie. Hierdie onderwerpe toon aan dat intelligente tegnologie vryelik beskikbaar is om aangewend te word in beheerkamers, en ook suksesvol is in ander toepassings. Bevindinge, wat uit die analyses volg, lei tot veelvuldige sensitiviteitsanalises van die “AS IS” stelsel om die impak van veranderinge ten volle te begryp. Die impak van veranderinge aan die “AS IS” stelsel op uitsette van die stelsel, insluitend tyd, bedryfsverliese, en koste word gedokumenteer.

Die navorsing sal dien as 'n katalisator vir toekomstige, meer omvattende studies. Die doelwit is dus om te illustreer dat intelligente tegnologie volhoubaar aangewend kan word in industrieë waar beheerkamers voorkom, en om areas te identifiseer waar intelligente tegnologie mees toepaslik sal wees, asook redes waarom dit die geval sal wees.

Sleutelwoorde:

Moderne beheerkamer

Industrie 4.0

Prosesmodel

Kunsmatige intelligensie

Bedryfsmodellering

Table of contents

Chapter one: Introduction.....	1
1.1 Background.....	1
1.2 Chapter layout	2
Chapter two: Research Methodology	3
2.1 Chapter overview.....	3
2.2 Design methodologies	3
2.2.1 Design Science Research.....	3
2.2.2 Action Design Research	4
2.3 Research management methodology.....	7
2.3.1 Research validation matrix (RVM).....	7
2.4 Conclusion.....	10
Chapter 3: Literature study.....	11
3.1 Chapter overview.....	11
3.2 Control room systems	11
3.2.1 Functions of control rooms.....	11
3.2.2 General control room systems	12
3.2.3 Event management.....	15
3.2.4 Technology in security control room systems.....	17
3.3 Human factors	19
3.3.1 Control room related factors.....	19

3.3.2	Psychomotor learning	21
3.4	Technology and industry 4.0 methods.....	22
3.4.1	Video scene analysis	22
3.4.2	Artificial intelligence (AI).....	23
3.4.3	Augmented cognition	26
3.4.4	AI costing.....	28
3.4.5	Tiny AI	29
3.5	Computing in networks	30
3.6	Signal-to-noise ratio	31
3.7	Information and data fusion.....	32
3.8	Systems engineering	34
3.8.1	Cognitive systems.....	34
3.8.2	Cognitive systems engineering	34
3.9	Risk terminology	36
3.9.1	Terminology	36
3.9.2	Qualitative methods	37
3.9.3	Quantitative methods.....	38
3.9.4	Semi-quantitative methods.....	39
3.10	Scales of measurement	39
3.10.1	Nominal scale	41
3.10.2	Ordinal scale.....	41

3.10.3	Interval scale.....	41
3.10.4	Ratio scale.....	41
3.11	Decision trust.....	42
3.12	Simulation modelling.....	44
3.12.1	Simulation software.....	44
3.12.2	Finite-state machines.....	44
3.12.3	Monte Carlo Simulations.....	45
3.13	RVM part one.....	46
3.14	Conclusion.....	48
	Chapter 4: System modelling	49
4.1	Overview.....	49
4.2	System trade-offs.....	49
4.2.1	Trade-off triangle	49
4.2.2	The model trade-off.....	53
4.3	The bin-theory.....	59
4.4	Analysis and modelling process.....	65
4.5	The “AS-IS” system.....	67
4.5.1	Step 1: Define the “AS-IS” system	67
4.5.2	Step 2: Build the “AS-IS” system in the simulation environment.....	74
4.5.3	Step 3: “AS-IS” model validation	85
4.6	RVM part two.....	87

4.7	Conclusion.....	88
	Chapter 5: Experimental analysis.....	90
5.1	Overview.....	90
5.1.1	Step 4: Experiment 1 - “AS-IS” event logic comparison.....	90
5.1.2	Step 5: Experiment 2 - Industry 4.0 technology on-site	96
5.1.3	Step 6: Experiment 3 - Human-inspired AI in the control room.....	102
5.1.4	Step 7: Experiment 4 - Augmented cognition in the control room.....	107
5.1.5	Step 8: Experiment 5 - Tiny AI possibilities	110
5.2	Conclusion.....	116
	Chapter 6: Conclusion.....	118
6.1	Research summary.....	118
6.2	Validation.....	119
6.3	Recommendations for future research and notable remarks	123
	Appendix A	125
	Appendix B	128
	Appendix C	134
	Appendix D.....	135
	References.....	147

List of figures

Figure 1: Design Science Research framework adapted from [2] and [3]	3
Figure 2: The elaborated ADR cycle adapted from [5].....	6
Figure 3: The four elaborated ADR stages with multiple entry points adapted from [5].....	7
Figure 4: RVM matrix	9
Figure 5: Proactive and reactive control rooms adapted from [10].....	12
Figure 6: Swim lane illustration of a common nuclear control room functions adapted from [12]	13
Figure 7: Accident management process in the traffic control industry adapted from [13]	14
Figure 8: Loosely integrated security control room	15
Figure 9: Detailed general event management flowchart adapted from [15]	16
Figure 10: The relevance of specialised and generic applications	17
Figure 11: Animation of a centralised computing system.....	30
Figure 12: Animation of a distributed computing system	31
Figure 13: Illustration of information fusion in the control room.....	33
Figure 14: Field of attention versus the level of abstraction adapted from [49]	35
Figure 15: The driving factors of complexity taken from [50].....	36
Figure 16: Qualitative risk matrix adapted from [1, 56]	38
Figure 17: Semi-quantitative risk matrix adapted from [1, 56].....	39
Figure 18: Generic FSM.....	45

Figure 19: RVM part one of this research.....	47
Figure 20: Trade-off triangle.....	50
Figure 21: Trade-off to have more certainty	51
Figure 22: Trade-off to have a lower cost.....	52
Figure 23: Trade-off to spend less time processing event	53
Figure 24: Analysis of the model trade-off.....	55
Figure 25: Iterative risk evaluation.....	58
Figure 26: Density of informative information in bins emphasised in the model trade-off.....	60
Figure 27: Bin illustration.....	63
Figure 28: Sensitive and normal areas of a loosely integrated security control room.....	65
Figure 29: Flowchart of the analysis and modelling process.....	66
Figure 30: Derived event management flowchart for the loosely integrated security control room setting	68
Figure 31: Generic alarm-handling SOP for a functional unit.....	69
Figure 32: Architecture of a loosely integrated security control room system	72
Figure 33: Finite state machine for the attention of alarms	73
Figure 34: Event types	75
Figure 35: Loosely integrated security control room system SIMIO model	75
Figure 36: Functional unit processing logic flowchart	82
Figure 37: Comparison of the annual number of events for model validation	86
Figure 38: Comparison of the incident-to-false-alarm ratios for model validation.....	87

Figure 39:RVM part two – The validation of the “AS-IS” simulation model.....	88
Figure 40: Comparison of the best performers of each input device system.....	93
Figure 41: Cost comparison of the input device systems.....	95
Figure 42: Bins before and after being treated by video scene analysis on-site.....	97
Figure 43: The Impact of industry 4.0 technology on conventional CCTV systems.....	99
Figure 44: The Impact of industry 4.0 technology on conventional SID systems	100
Figure 45: Observations in waste reduction	102
Figure 46: Impact on the system if a functional unit transition is made from a human to human- inspired AI	106
Figure 47: Impact on the system if a functional unit transition is made from a human to an augmented human	109
Figure 48: Tiny-AI-setup.....	111
Figure 49: Simulated impact of the Tiny AI sensitivity analysis.....	114
Figure 50: Simulated change in resource wastage and response efficiency with the implementation of tiny AI	115
Figure 51: RVM Matrix part 3 - Experiments	117
Figure 52: Work breakdown structure	120
Figure 53: Complete RVM.....	122
Figure 54: Process for accepting or rejecting an event.....	128
Figure 55: Maximum cost allocation	128
Figure 56: Event creation process.....	128

Figure 57: Event interpretation process.....	129
Figure 58: The original bin	130
Figure 59: Define the iR value.....	130
Figure 60: Process to determine the perceived risk score	131
Figure 61: Functional unit processing logic	133

List of tables

Table 1: Comparison of humans to various AI systems adapted from [37]	24
Table 2: Examples of areas of application taken from [30]	25
Table 3: Comparison of augmented cognition categories taken from [32]	27
Table 4: Scales of measurement adapted from [57]	40
Table 5: Risk categories and their corresponding actions	58
Table 6: Volatility table based on the operator class	71
Table 7: Residual site risk classes	77
Table 8: Top 10 scenarios based on the incident escalation factor.....	91
Table 9: Top 10 scenarios based on the response efficiency	94
Table 10: "What-if" alterations for the "AS-IS" transition to the "TO-BE" candidate with video scene analysis.....	98
Table 11: Sensitivity analysis of the virtual control room "TO-BE" candidate	104
Table 12: Sensitivity analysis of the augmented control room "TO-BE" candidate.....	108
Table 13: Sensitivity analysis of the tiny AI experiments	113
Table 14: Combinations of possible "Best 'AS-IS'" models.....	125

Chapter one: Introduction

1.1 Background

Many industries use control rooms to monitor and manage their daily operations. Of the many operational tasks control rooms face daily, one fundamental task is of major importance: event management. Events are abnormalities that trigger alarms on the site or sites which the control room serves. The role of a control room is to identify the causes of alarms, classify them, and manage it accordingly.

Depending on the industry, ineffective event management may result in significant monetary and intangible losses as an event may be unfavourable. In this research, unfavourable events are referred to as *incidents*. Events that trigger alarms may be incidents or false alarms caused by pests and other non-malicious events. It is, therefore, the duty of the control room to process an event as quickly and effectively as possible in order to ensure that incidents are identified and managed appropriately.

Industry 4.0 technologies and methods are rapidly advancing and these modern findings are consistently proving to be successful in many domains. Control rooms are advancing at a much slower pace and outdated technology is common in many systems. Limited research has been done on industry 4.0 technologies in control room environments. The success in a large number of environments, however, leads one to believe that they may enhance control room operations. This raises the research question:

Can currently available industry 4.0 technologies improve conventional control room operations?

The research question can be addressed by constructing a generalised framework for a control room system and observing the impact of guided changes to the system. How a generalised framework is defined may differ between individuals. In this research, however, a systems engineering approach is followed to improve operational efficacy.

1.2 Chapter layout

Chapter 2 provides an overview of the research methodologies used in this research to effectively address the research question. Design methodologies such as design science research and action design research are followed to guide the emergence of the research artefact in the form of a simulation model. A research validation matrix is used to qualitatively guide research efforts in a structured manner, to ensure that literature topics have dedicated focal points and that the research is managed in a structured and planned manner.

Chapter 3 contains important literature findings to provide context related to control room systems. The research problem is validated in this chapter and concept solutions are identified at a high-level. Relevant technologies and their expected effect on input variables are also explored in this chapter.

Chapter 4 is an analysis of key literature findings that are presented concurrently with an in-depth evaluation of a loosely integrated security control room system. During the system analysis of the control room, trade-offs are identified and new concepts and theories such as the bin-approach are presented. An investigation flowchart is presented, which also includes the contents of chapter 4 and 5. In chapter 5, the “AS-IS” model is defined, built in the simulation environment and validated. Chapter 4 is concluded with a research validation matrix as suggested by the quality research management approach.

Chapter 5 contains the experiments shown in the investigation flowchart defined in chapter 4. Multiple experiments are done in the form of sensitivity analyses in a simulation environment to evaluate the impact of industry 4.0 technologies in various sections of the “AS-IS” control room system. These impacts are mainly evaluated by identifying trends.

Chapter 6 contains a summary of the work done in this research and the notable findings that were made. A work breakdown structure is also presented to recapitulate what was done in this research and the sequence in which tasks were conducted. Recommendations are made for future, more comprehensive studies and other noteworthy remarks are mentioned regarding the contents of this research.

Chapter two: Research Methodology

2.1 Chapter overview

This chapter contains an overview of the research methodologies followed in this research. Research methodologies are included to ensure both the sound development of an artefact and the structured management and allocation of literature. Design methodologies including Design Science Research (DSR) and Action Design Research (ADR) are considered, since they are methods for solving real-world problems by guiding the emergence of an artefact. Quality Research Management is consulted to manage the research efforts qualitatively.

2.2 Design methodologies

2.2.1 Design Science Research

DSR is a commonly used research tool that enables the researcher to perform *directed* and *structured* research on problems in the physical world [1]. It is included in this research since there is an ongoing interaction between the physical world and the knowledge base to create an artefact. The DSR framework was created to ensure that an artefact is developed and continually evaluated within the DSR framework by addressing accomplishments in the knowledge base together with the requirements of the physical world. The DSR cycle is showcased in figure 1 below.

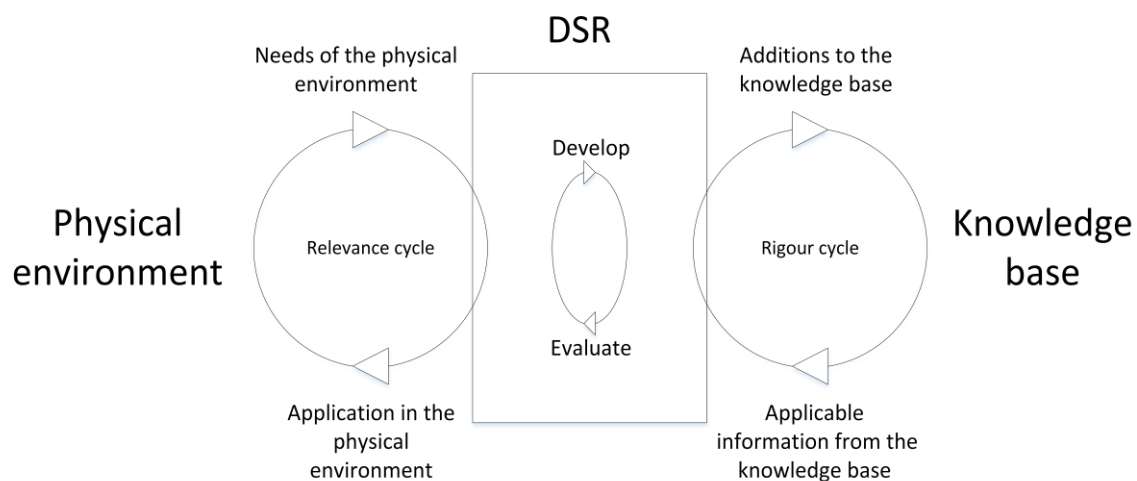


Figure 1: Design Science Research framework adapted from [2] and [3]

By following the DSR framework, the researcher may, during the research process, gain knowledge from literature and make new additions to the knowledge base. This is known as the “Rigour cycle” and it is performed concurrently with the rigour cycle. The Relevance cycle repeatedly surveys the artefact to ensure that the requirements of the physical world are addressed. These two cycles are the main drivers for the principal *develop-and-evaluate* cycle.

The physical world typically includes people and their roles, organisational processes and infrastructure of technology. DSR is often evaluated by case studies, experiments, field studies or simulation [2]. The DSR framework ensures that the synthesis of an artefact is theoretically grounded and that the problem in the physical world is effectively addressed.

2.2.2 Action Design Research

2.2.2.1 Traditional ADR

The traditional ADR method was developed to act as a design methodology with the goals of *building innovative artefacts in an organisational context and learning from the intervention of the organisation* [4]. This method is researched since an artefact must be created for a physical, organisational context. The ADR method consists of four stages which are each grounded by their distinct fundamental principles.

Stage 1: Problem formulation

This stage is initiated when a problem is recognised in practice or envisioned by researchers. It includes defining the initial scope, formulating the prospective research questions and defining the roles of the participating parties [4].

The first principle grounding the problem formulation phase is *practice-inspired research*. This principle encourages problems in practice to be viewed as knowledge-creation opportunities. The second fundamental principle of this stage is the development of a *theory-ingrained artefact*. The emphasis of this principle is that the primary informant for the creation of an artefact is the knowledge base [4]. This principle corresponds with the before-mentioned rigour cycle of DSR.

Stage 2: Building, intervention, and evaluation (BIE)

The main focus of this stage is to ensure the integration and overlapping of the construction of artefacts, expected and unexpected intervention within the organisation, and the continual evaluation of progress [4]. The ADR method identifies two endpoints for the research design

sequence, namely *the creation of an innovative technological design and the generation of design knowledge*.

Stage 2 is grounded by three principles. The first is *reciprocal shaping*, where the ADR team may engage and disengage in recursive cycles of decisions, at various levels of detail [4]. This is natural since problems are better understood, and the resources become more specialised as the research process advances. The second grounding principle is *mutually influential roles*. The focus of this principle is the continuous learning and informing among all relevant project participants. The final grounding principle of the second stage is *authentic and concurrent evaluation*. This principle is emphasised, since research – in many cases – is evaluated at its end, often resulting in wasted resources and time as issues may arise here and reworking may be needed. With ADR, evaluation is done persistently throughout, and it is not considered a separate, single stage.

Stage 3: Reflection and learning

This stage runs parallel to the previous two stages. The goal of this stage is to regard how the artefact is being built, and which *lessons learnt* are of relevance. One principle, namely *guided emergence*, grounds this stage. This principle focusses on the ongoing shaping of the artefact, by all relevant parties, to ensure that not only the preliminary design challenges are focussed on, but also that new challenges that arose from the continual evaluation are taken into consideration [4].

Stage 4: Formalisation of learning

In the fourth and final stage of the traditional ADR method, the researchers formalise learning by outlining the accomplishments of the artefact and describing the organisational outcomes. The only fundamental principle in this stage is *generalised outcomes*. The creators of the traditional ADR method argue that an artefact is a solution that addresses a problem, and both a solution and a problem can be generalised. This stage aims to move from “specific-and-unique” to “generic-and-abstract” outcomes [4].

2.2.2.2 Elaborated ADR

Mullarkey and Hevner [5] state that the details of the BIE stage in the traditional ADR method are largely open to interpretation by the researcher. These researchers emphasise that *intervention* is a core concept in the traditional ADR process and that it should be occurring in each ADR cycle.

They further argue that the tasks of learning, evaluation, and reflection are prominent in every intervention cycle. Moreover, they find that all the stages in the traditional ADR methodology supports multiple iterations of the intervention cycle, as shown in figure 2 below.

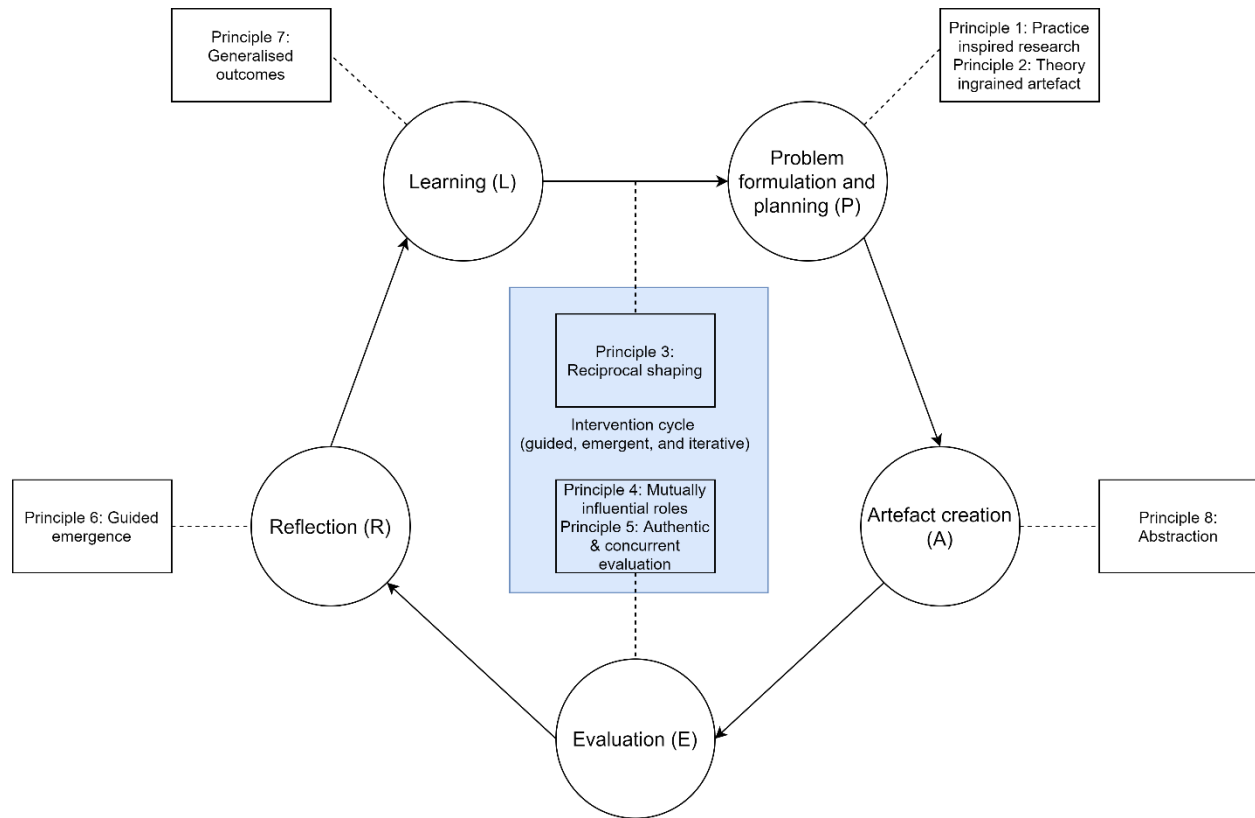


Figure 2: The elaborated ADR cycle adapted from [5]

The seven grounding principles of the traditional ADR are complemented with an eighth principle in the elaborated ADR process, namely *abstraction*. This principle supports the creation of different levels of artefact abstraction for the current state of research goals in the problem environment [5, 6]. The traditional four stages of this ADR process are redefined by Mullarkey and Hevner [5] as:

- *Diagnosis* instead of *problem formulation*;
- *Design* instead of *building, intervention and evaluation*;
- *Implementation* instead of *reflection and learning*;
- *Evolution* instead of *formalisation of learning*.

Two critical learning areas of the diagnosis stage include the *awareness of the existing knowledge base* and a *clear understanding of the application domain of the project* [5]. The design stage is focussed on the identification and conceptualisation of the proposed artefact design. This stage may be iterated as the solution to the problem evolves. The implementation stage supports the implementation of artefacts in the physical environment. Finally, the evolution stage is proposed as the artefact evolves with changes in the problem environment. Figure 3 illustrates the four elaborated ADR cycles.

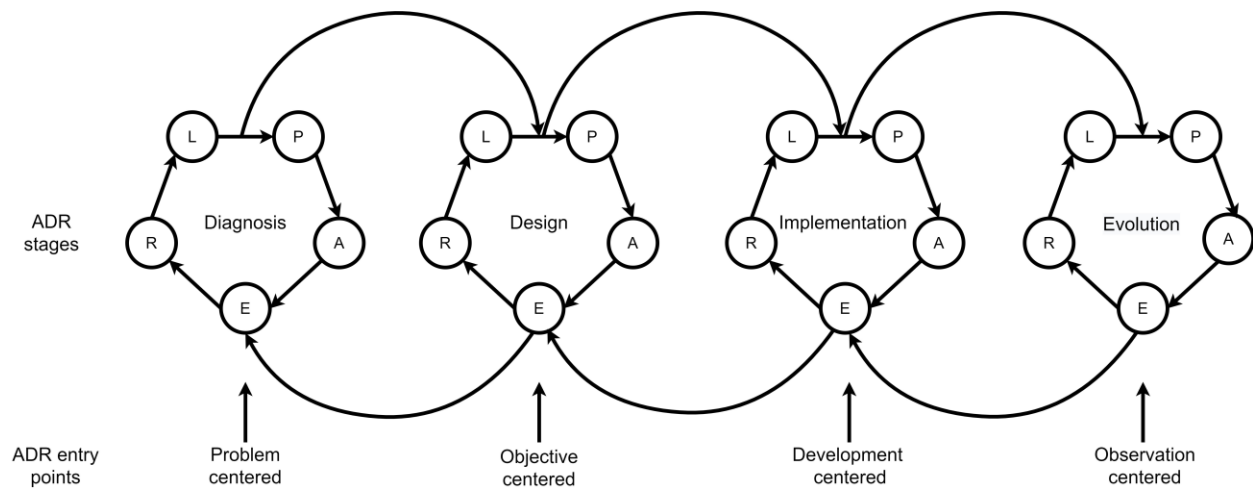


Figure 3: The four elaborated ADR stages with multiple entry points adapted from [5]

The relevance of multiple entry points is emphasised in the progression of the ABR process model. This adds to the flexibility of the elaborated ADR process model to ensure that researchers may start anywhere along the timeline of ensemble system instantiation, since, in practice, input from several contributing participants may be required at various stages of the project [5].

2.3 Research management methodology

2.3.1 Research validation matrix (RVM)

An RVM is a supporting tool used to manage research efforts in a structured and visual manner [7]. It is included in this research to ensure that no unnecessary or irrelevant research is done and that the reason for inclusions is visible in a single matrix. The framework simplifies research concept solutions, solution validation, the traceability of information sources by indicating whether it contributed to research challenges, research concept solutions and solution validation.

1. Research challenges

Several sources such as literature and industry experts may indicate that the problem at hand is indeed a problem of interest. These sources individually contribute to the piecemeal validation of the research problem. A sufficient number of sources are required to prove that each major aspect of the research problem is truly in need of being addressed. The shortfalls derived from the research problem are commonly referred to as *research challenges*. Literature from the knowledge base may contribute toward the verification of the research question through the verification of individual research challenges.

2. Research concept solutions

Additionally, literature findings may contribute to the concept solution. Research concept solutions directly address research challenges in the QRM framework and they synthesise into a single solution.

3. Solution validation

The research solution can be validated through physical experimentation, case studies, simulation etc.

A remarkable feature of the RVM framework is that it represents a matrix, which allows the reader to easily locate any element of the research effort on a single page and observe its areas of contribution and application. The correlation feature of the matrix ensures that the researcher is guided while performing iterative methodologies such as DSR and ADR. A recent study [7] showed that quality research management improves the effectiveness of design science research.

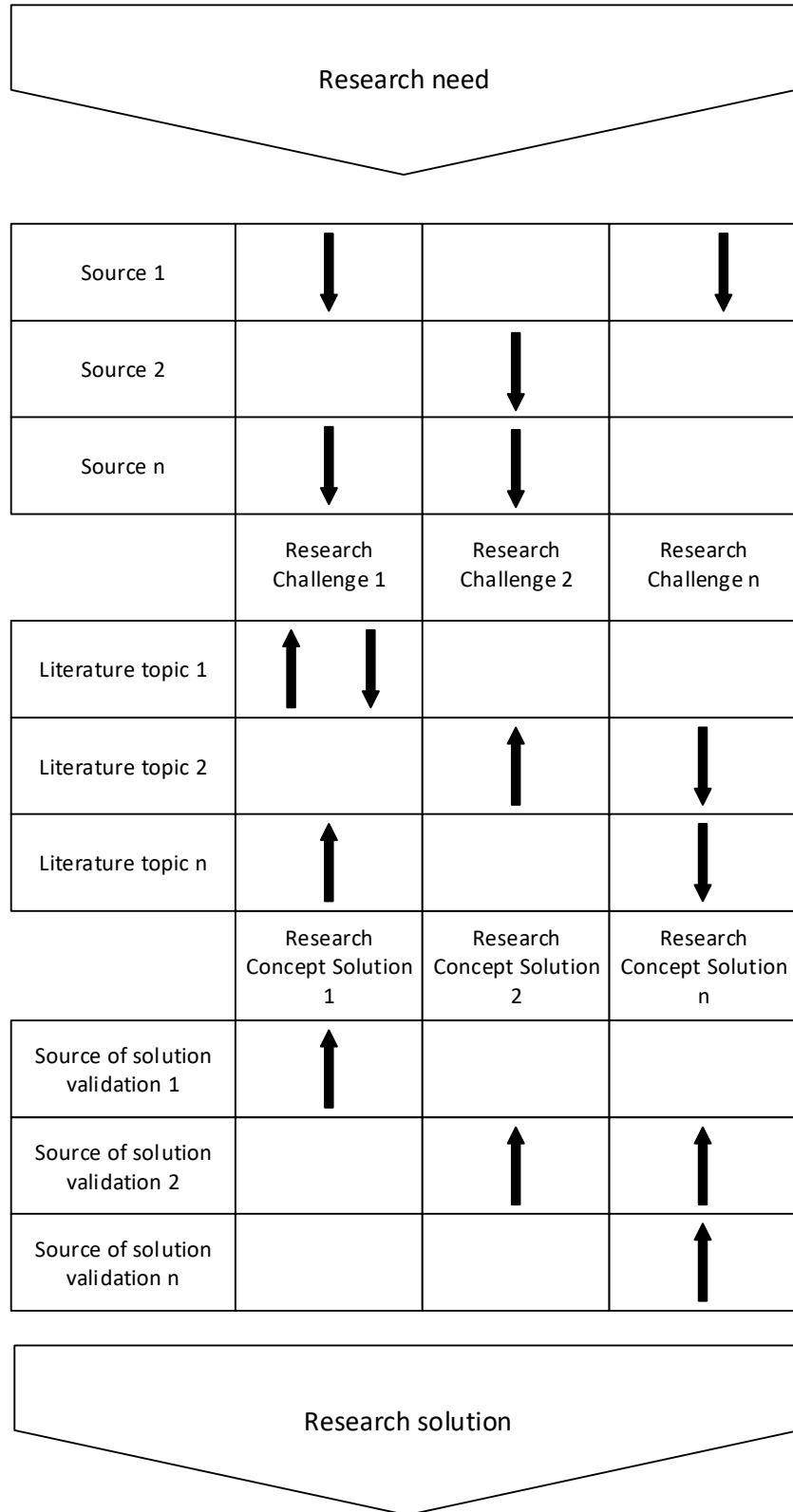


Figure 4: RVM matrix

Figure 4 illustrates the framework of a common RVM. The direction of an arrow in the research validation matrix indicates whether elements of the most left column (literature topics and sources) contributed to the immediate header or the footer of the column. For instance, consider Literature topic 1 in Figure 4; the arrows indicate that this topic contributes to both research challenge 1 and research concept solution 1.

Sources of the problem are only used to validate research challenges and they may expose new research challenges that may be validated by other sources of the problem. Literature topics may also validate research challenges and contribute to concept solutions. Various sources are used to validate the concept solutions to ensure a justifiable artefact is synthesised.

2.4 Conclusion

This chapter presented an overview of the design science research (DSR), action design research (ADR), and research validation matrix (RVM) methods. These methods were discussed in general and their roles in this research were presented. DSR and ADR will be consulted to ensure a valid artefact is created, which provides value in the physical world and is theoretically sound, and an RVM will be created for the reader to easily understand the value of the literature topics.

Chapter 3: Literature study

3.1 Chapter overview

This chapter provides background on current control room systems in selected industries. The functional architectures of control rooms are compared with the focus placed on core control room operations. Similarities between industries are identified and the security industry is chosen to be investigated for this research.

Since operators are currently key functional units in control rooms, human factors relevant to control rooms are examined. Furthermore, industry 4.0 technology available at the time of this research and deemed applicable to control room systems is investigated in this chapter. Systems engineering is reviewed and its applicability to the control room environment is elaborated upon.

Theories that are not traditionally related to control rooms or engineering are reviewed, since they will be adapted and utilised if deemed valuable. Simulation modelling is researched to ensure that verified software is considered together with sound simulation methodologies.

3.2 Control room systems

An improved control room system through complete, or partial, industry 4.0 technology integration is the main focus of this research. The topic of control room systems is evaluated to identify a suitable real-world functional control room model.

3.2.1 Functions of control rooms

This section of literature is included since control rooms must be understood at a functional level to simulate an “AS-IS” system and to evaluate candidate “TO-BE” systems. Control rooms are traditionally defined as a physical structure where operators use control room facilities to perform tasks of monitoring and centralised control [8], or “a functional entity with an associated physical structure, where the operators carry out centralised control, monitoring and administrative responsibilities” [9]. The nature of control room tasks can be proactive or reactive in nature, or a combination of both. Figure 5 gives a high-level indication of which control room industries are typically more proactive than reactive, or vice versa.

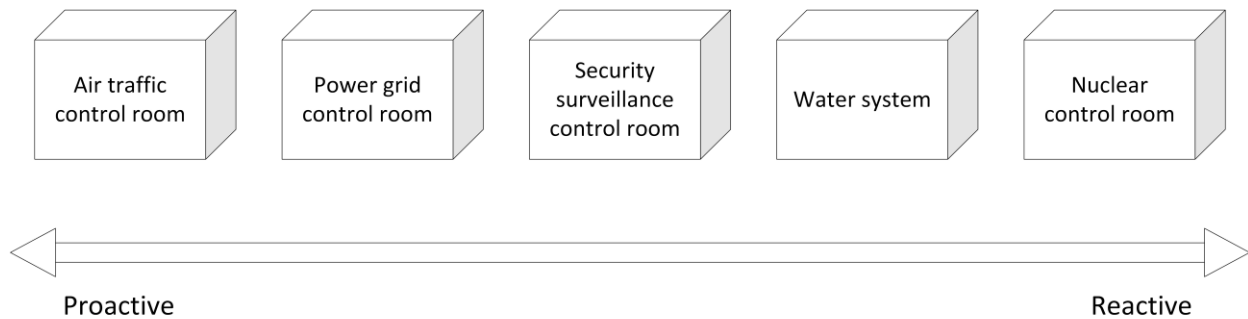


Figure 5: Proactive and reactive control rooms adapted from [10]

Air traffic control rooms proactively manipulate aircraft primarily just before take-off and just before landing, in an attempt to prevent collisions and other unfavourable events. Contrarily, nuclear control rooms follow a more reactive approach since monitors inform operators that an abnormality is present, and the operators react to this information accordingly [10].

The remoteness of control rooms relative to the sites being monitored depends on the number and geographic locations of the sites. Nuclear control rooms are typically on-site, as they only control one plant in a tightly integrated way. Differently, traffic control rooms are remotely connected and loosely integrated, as it is impractical to be physically present at multiple sites simultaneously.

Tightly integrated security control rooms use both reactive and proactive measures in an attempt to avert unwanted scenarios. Airport security control rooms may proactively use closed-circuit television (CCTV) to identify abnormal behaviour such as leaving a bag unattended for a certain amount of time and reacting to the potential threat of a bomb, whereas CCTV footage from a parking lot may be used reactively to review a crime scene in that area [11].

Typically, security control rooms in a loosely integrated system do not perform high levels of proactive surveillance, but rather monitor reactively. This is natural since a few operators cannot keep track of the real-time phenomenon on literally thousands of distributed sites. Therefore, these control rooms act largely on a *reactive* basis, where the focus is on events originating at these sites.

3.2.2 General control room systems

General control room systems are researched in this section to identify overlapping functions of control rooms of different industries. A nuclear plant is not considered an abstract environment,

since all the possible complications are stipulated in detail beforehand, and operators are trained to handle each of these complications according to specific codes. There are no “first-of-a-kind” incidents in nuclear control rooms since all the activity in nuclear reactors are closely controlled and the reactor (site) can be manipulated quickly. Due to the inherently complex nature of nuclear plants, many of the redundant and high-risk functions had already been automated. Modern nuclear control rooms are automated to such an extent that abnormalities are pinpointed and displayed to operators on-screen, together with probable causes. This makes it possible for operators to manage events and with high levels of certainty.

The designers of nuclear control rooms realise that humans make mistakes, and the more complicated a control room setting is for an operator, the more likely mistakes will occur. Incorrect management in nuclear power plants can result in catastrophic failure, and these control rooms have therefore been improved and designed around this awareness of human fallibility.

Nuclear control rooms are tightly integrated to further reduce the risk of human error. In effect, nuclear plants in the modern day are considered reasonably safe. As an example, figure 6 contains a diagram of the high-level functions of a nuclear control room in the case of a reactor going into a critical state.

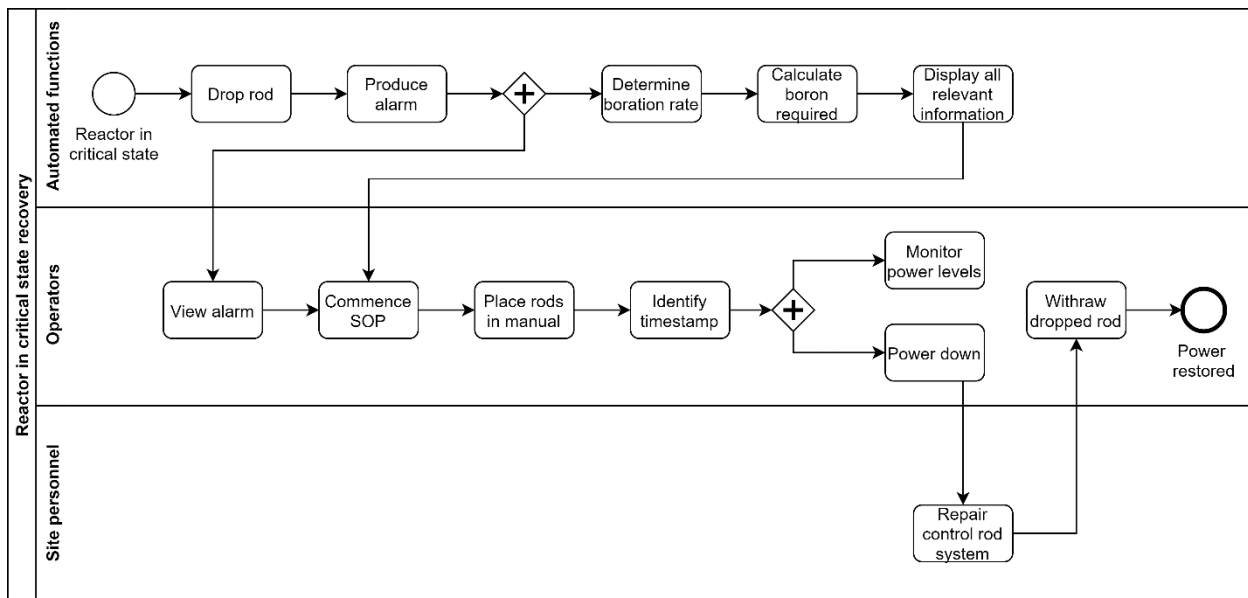


Figure 6: Swim lane illustration of a common nuclear control room functions adapted from [12]

Figure 6 illustrates one of the many tasks a nuclear control room faces periodically. The reactor is automatically disengaged when it enters a critical state to avert disaster. The term “dropping a

rod” is one of many common reactivity perturbation methods. It is then the role of the operator to control the restoration of power in a safe and timely manner.

A traffic control room is typically loosely integrated and it serves many sites where sensors and other devices provide data to a centralised control room. Figure 7 contains a derived process of a traffic control room where some event triggered an alarm.

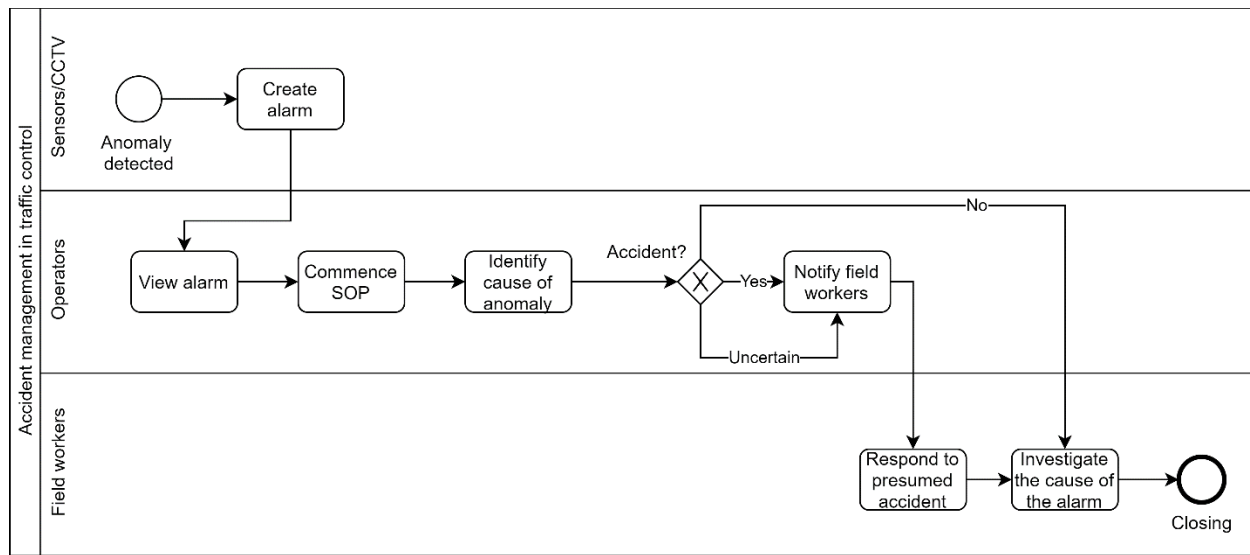


Figure 7: Accident management process in the traffic control industry adapted from [13]

If an anomaly (an atypical event) is present on a site, an alarm is signalled and the control room operators are notified. The operators then follow an SOP to identify the cause of the event. This task must be done quickly and effectively, as lives may be at stake if it is indeed a traffic accident that occurred.

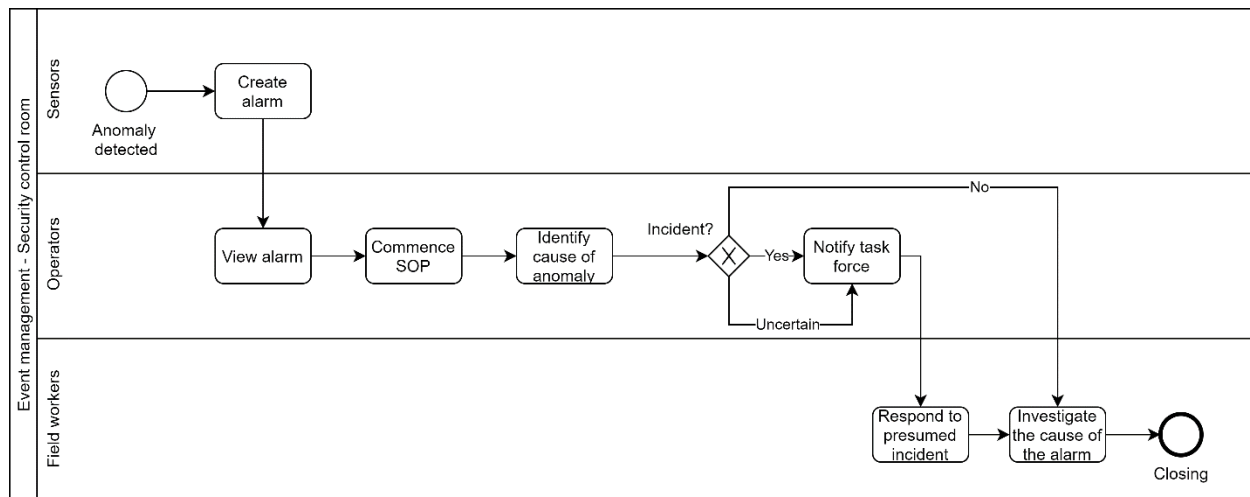


Figure 8: Loosely integrated security control room

Figure 8 contains the operational flow of a loosely integrated security control room system. Typically, loosely integrated control room systems are generally less complex relative to tightly integrated systems such as nuclear control rooms, and the risks associated with the sites of loosely integrated control room settings justify the choice of remote monitoring and control. This does not imply that risks are not involved, as the impact of burglaries and car accidents are largely unfavourable. This does, however, imply that the risk associated with individual sites does not justify building individual control rooms for every site.

It is unheard of to assign an entire tightly integrated traffic control room for one corner of a road in a large city, or an entire tightly integrated security control room for a single house. However, in the case of nuclear and energy control rooms, tightly integrated control rooms are justified by their risk and complexity.

The purpose of the illustrations shown above on the operational flow of control rooms in these different industries is not to promote the detailed individual steps of the process, but rather to identify the similarities between control room systems. Clearly, these multidisciplinary systems have one main function in common, namely *event management*.

3.2.3 Event management

Event management is important in the control room environment, as the operational worth of a control room is dependent on its ability to manage events occurring on the sites it monitors. This topic is further researched in this section, since it is the main overlapping function of control rooms

operating in different industries. The most important goal of event management is to restore the system to its normal operating conditions as quickly as possible [14]. This is to ensure that the best possible levels of service are provided and that minimal downtime is present.

In the security control room environment, an important goal is to lower the allowed incident escalation time by timeously reacting to an event. This is not only the case for security control rooms, as incidents in other industries also escalate over time. Examples include an attack on confidential information in the IT industry and a road accident in the traffic control industry. The objective is, therefore, to manage events effectively to get incidents under control and arrest escalation.

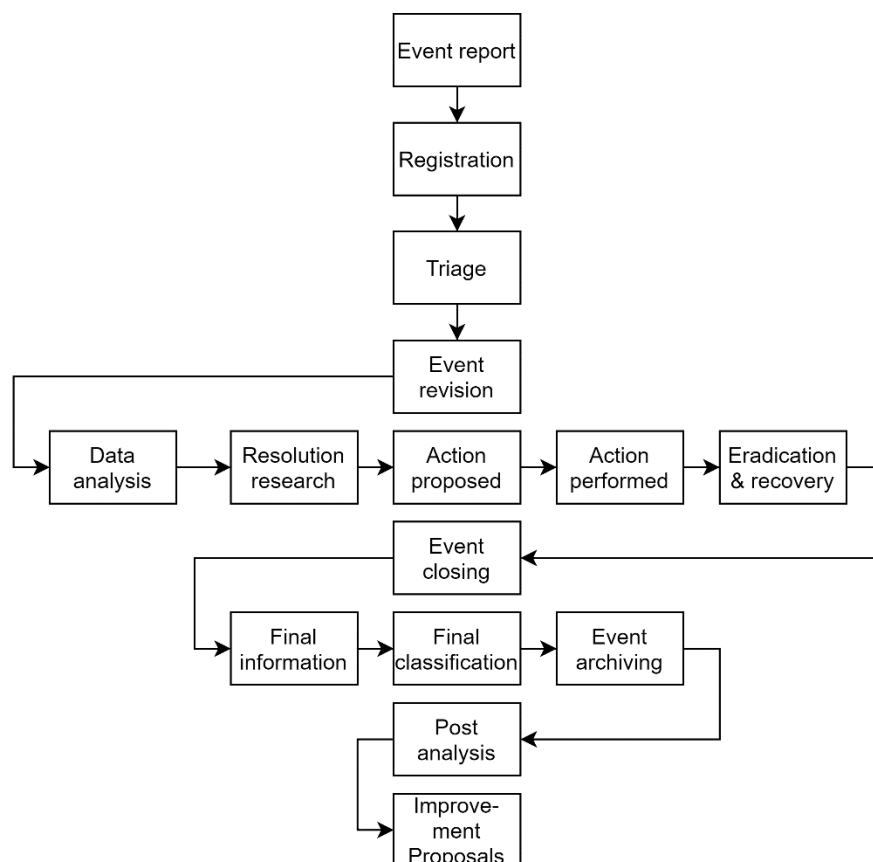


Figure 9: Detailed general event management flowchart adapted from [15]

The steps in an event management process are shown in the flowchart in Figure 9. After (i) an event has been reported, (ii) a decision is made as to its severity, after which (iii) appropriate action is taken, and (iv) the event is closed. Should an event be a false alarm, its severity is negligible, and no action is taken at the time. However, in the case of an actual incident, the type

of incident will determine the severity, and reaction personnel are dispatched to get the incident under control. The additional steps that are shown above (on the management of an event over its life cycle) do not directly influence the escalation of incidents, as these steps only occur after the event is under control.

To address the research challenge, a loosely integrated security control room model was selected as an abstracted model, as it best represents the real-world model to be analysed. Although explicit generalisation cannot be made between control rooms operating in different industries, the basic event management functions of these control rooms are similar and it should be possible to convert a generalised model into a specialised model with limited effort.

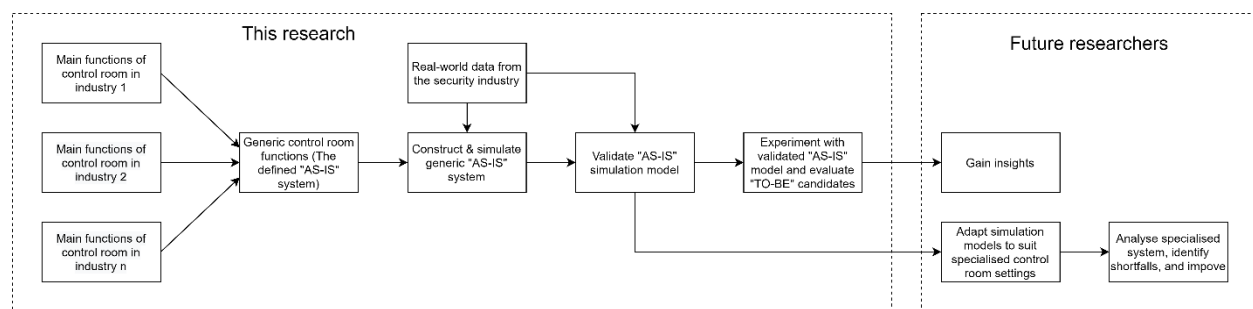


Figure 10: The relevance of specialised and generic applications

Figure 10 provides clarity on the scope and purpose of this research. The similarity of control rooms over various industries was found to be event management. The artefact will be a simulation model on the event management functionality as observed in control rooms. This generic model will then be adjusted slightly to represent a loosely integrated security control room system, and it will be validated with actual data from a real-world control room. “TO-BE” experiments will be inspired by literature findings and the “AS-IS” model will be adjusted to form these “TO-BE” models. Future researchers can then easily adapt the generic artefact to suit specialised control room systems, which will in turn provide value in specific settings. Chapter 4 contains the detailed analysis and modelling process followed in this research, and it is created by considering the goal illustrated in figure 10.

3.2.4 Technology in security control room systems

This research aims to leverage modern technologies in a simulation environment to improve conventional control room operations. Therefore, typical technological systems in security control

rooms are evaluated in this section to identify possible additions in the form of industry 4.0 technology.

Intrusion detection systems (IDS) are electronic alarm systems designed to alert a user that an entity is identified in a monitored area of relevance [15]. Many types of ID systems are available today, such as passive infrared (PIR) motion detection systems, photoelectric beam systems, vibration sensor systems, and others [15]. ID systems have varying levels of quality and complexity. Typically, the more expensive the IDS, the more complex and successful it is.

PIR motion detection systems are common in the security industry due to its relative affordability. A PIR sensor is a sensor that measures infrared light radiating from objects within its proximity and field of view [15]. These detectors can function without needing to create and radiate its own energy.

Photoelectric beam systems work by emitting infrared light beams over an area of relevance. If these beams are obstructed, an object is present in the area of relevance and the user is notified. These systems typically have a relatively high installation cost, and advanced techniques are used to reduce false alarms, including the use of dual beams and complex signal processing methods [15].

Vibration sensor systems, or seismic detectors, are partially mechanical. They rely on vibrations to slightly move unstable mechanical configurations in the device, which modulate the flow of current and ultimately triggers an alarm following advanced signal analysis [15].

One common aspect of ID systems is that they are mostly “blind” sensors. This means that they notify the control room of the presence of a disturbance, but the observation does not include visual information for verification purposes. This typically requires the reaction team to investigate a site to see what the reason for the alarm was, which leads to a high operational cost, especially if the system generates many false alarms. Moreover, without some sort of visual verification, the reaction team cannot be sure what they will encounter, which can result in uncertain, unsafe and stressful confrontations.

CCTV systems provide visual verification and they can be accompanied by an ID system. Therefore, if the ID system detects a disturbance, an operator can log into the CCTV system and attempt to identify the cause of the alarm from another geographic location. Furthermore, recorded scenes can be pulled from the storage system on-site in a further attempt to identify the

reason for an alarm. These systems, however, are expensive relative to ID systems and the large file sizes of the video clips make transferring data over a communication medium timely and costly.

A more cost-effective system overcoming the visual aspect that IDS lacks is an ID system accompanied by a basic snapshot intrusion detection (SID) system. A basic SID system takes a few snapshots at the moment an ID system detects an anomaly. This greatly assists the operators in the control room since they are more likely to gain certainty on the reason the IDS triggered an alarm. These basic SID systems are slightly more expensive than basic ID systems as cameras and additional complexity features, however, it is much less expensive than traditional, basic CCTV systems.

Loosely integrated control rooms serving a large number of sites critically depend on automated detection because of their reactive nature. If an event occurs which triggers an alarm, the event can be either a true positive (TP) or a false positive (FP). A true positive (an incident) is when an alarm is triggered and there is indeed unfavourable activity, while a false positive (a false alarm) is when an alarm is triggered and there is no malicious activity on-site. False positives are commonly caused by pests, ill-disciplined users triggering alarms, or other elements such as strong winds, air conditioners, moving plants and other environmental disturbances. False negativity (FN) is when there is indeed unfavourable activity but no alarm is triggered and true negativity (TN) is when there is no malicious activity and no alarm is triggered [16].

3.3 Human factors

3.3.1 Control room related factors

Operators serve as key functional units in control rooms, as they are required to make decisions regarding how events should be handled. Therefore, relevant human factors must be researched as humans form part of the conventional “AS-IS” control room systems. Human error is present in all settings where humans interact [1], including control rooms. Monitoring shortcomings may be equipment-related (camera position, maximum tilt, zoom functions, etc.). In any event, this is not the only contributing factor [17].

Control room operators performing surveillance are responsible for handling large volumes of (mostly repetitive) information. There are typically more cameras and sensors than operators in both loosely and tightly integrated security control rooms. The nature of these control room

settings requires operators to rotate through, or select cameras or sensors in a predefined pattern or prioritised sequence, which may lead to operators potentially missing a threat. Even if a direct threat is not missed, the situation awareness of a specific site may be disrupted, affecting the situational judgement of an event [18].

Recent work showed that the amount of visual information that needs to be processed by surveillance operators who are proactively monitoring scenes is directly related to substandard detection performance [19]. A challenge of proactively determining suspicious behaviour is that it depends on multiple factors, such as the location of the behaviour (which may have had historical malicious events), and the expected context of the area or event being monitored [11]. For instance, a group of people jogging in a public park may be less suspicious than groups of people running in an airport. This, however, is more applicable to tightly integrated systems than loosely integrated systems due to its proactive nature.

If an input device on-site produces many false alarms, operators tend to become desensitised to alarms. This may result in the operators ignoring an alarm thinking it is most likely a false alarm and potentially overlooking a threat. On the other hand, operators may become overconfident in these systems, creating a false sense of security. This leads the operators to think that all threats and issues will be identified by the technology, which is not necessarily the case.

Many operators practise intuition in the decision-making process contrary to only using analytical methods [20]. Intuitive decision-making takes place when decisions are made partly on “hunches” and feelings and not according to text-book facts and details. Intuition is known to form subconsciously with experience in a specific field and some operators report it as having a “sixth sense” [21].

Control rooms are typically populated by multiple operators sharing physical space, which may cause distractions. These distractions may cause an operator to temporarily disengage from monitoring to focus on something else, potentially missing a threat, as events will continue to unfold while the operator is distracted. Following a distraction, time is needed for reconfiguration and to recover concentration. Also, studies have found that the longer the attention is turned away from monitoring, the more effort it typically requires to regain concentration [22].

One study argues that when humans perceive deviant sounds, the short-term memory is affected and attention is diverted away from the focus area [23]. On the other hand, another study found

that higher levels of concentration may block out some peripheral distractions [24]. One study suggests that operators may be more vulnerable to distractions as the cognitive load increases [25].

Prolonged concentration times are well-known to decrease alertness, and one view is that operators “switch off” to save costly mental resources and energy for activities requiring more effort at a later time. The task of proactive surveillance requires high levels of attention, but with the low occurrence rate of threats, resulting in a phenomenon called “perceptual blindness”. Perceptual blindness in control rooms occur when an operator fails to perceive events unfolding in plain sight, purely due to a lack of attention. This phenomenon is evident when information about events is reactively reviewed, since large numbers of false alarms are present relative to incidents.

3.3.2 Psychomotor learning

Fundamentally, control room operators must learn tasks related to event management and execute them accordingly when needed. This is commonly done through a physical interface such as a computer, which makes the process of interpretation and management fall naturally within the psychomotor domain. Therefore, psychomotor learning is chosen to be further evaluated in this section.

Psychomotor learning is the relationship between cognitive functions and physical movement. Examples of this learning include driving a car or playing a musical instrument. It should be noted that psychomotor learning is not limited to only physical activities such as the aforementioned examples, but includes many forms of cognitive interaction with the physical environment.

Simpson [26] proposed the following levels of psychomotor learning:

1. Perception;
2. Set;
3. Guided response;
4. Mechanism;
5. Complex overt response;
6. Adaption;
7. Origination.

The *perception* level is based on the ability to guide activity through sensory cues. In the control room setting, it would typically be the ability to perceive visual information and audio from input devices. The emphasis of this level is the ability to interpret non-verbal cues and act accordingly in an effective manner. The *set* level can be translated to “the readiness to act”. The evaluation of this level is primarily based on the ability of an entity to predetermine how it is going to respond in various situations. These sets are typically guided by emotional, mental, and physical sets.

The *guided response* level is commonly referred to as a group of the early stages of learning a complex skill. These stages include imitation and trial and error, and examples in control rooms include learning how to classify objects as hazardous or not malicious. The *mechanism* level is the “intermediate” stage in learning a complex skill. An entity competent in this level can perform complex responses confidently and proficiently. Examples include a person driving a car and using a personal computer in such a manner that it seems natural.

The *complex overt response* is the level referring to quick, accurate, and highly coordinated performance requiring minimal energy. This level has been described as subconsciously knowing what result will be produced from some action as it is being carried out. The successor of the complex overt response level is the *adaptation level*. At this level, the entity is expected to alter responses based on special requirements. In other words, requirements not necessarily defined previously.

The final level defined by Simpson in psychomotor learning is the *origination* level, and the main outcome of importance in this level is creativity. Here, the entity is expected to come forth with new and creative designs. The main consideration of this level is constructing a new set of patterns around a novel concept or theory. Effectively constructing a high-quality research publication through the interpretation of existing literature and the development of new concepts is an example of this.

3.4 Technology and industry 4.0 methods

3.4.1 Video scene analysis

Video scene analysis is further researched as security control rooms use visual data such as CCTV footage and images to identify the cause of an alarm. This technology is considered relevant to the security control room environment and it is important to provide a brief overview of

video scene analysis as it may have a significant influence on the future configuration of resources in the overall security control room system.

Video scene analysis is a method used for the autonomous recognition and tracking of objects in monitored scenes. The technological advances in this field are significant, and robust object detection is receiving attention. Mustafah, *et al.*, defines robust object detection as: “the problem of locating an object of interest in an image in the presence of uncontrolled lighting, complex background, and variations of appearance and orientation such as scale and rotation [4]”. Given sufficient image quality, robust object detection has a relatively high success rate.

Video scene analysis is the process of recognising and analysing humans and objects from live-streamed or recorded video scenes, in an attempt to recognise human action, classify activities, and interpret scenes [5]. Relatively unsophisticated scene analysis can easily be accomplished with modern technology through intelligent automation.

Robust object detection and video scene analysis can collaborate to perform tasks such as the elimination of sections in video clips where no change in a scene is detected, or emphasis on sections where humans are detected with intrusion tools. Furthermore, scenes can be automatically analysed to intelligently determine if alarms should be sounded or not on the fly. Both scene analysis and object detection are widely available and are relatively inexpensive. Furthermore, open-source versions can be obtained online and adapted to fit many settings with minimal effort and expenses.

In the security environment, there have been many success stories on automated scene analysis, including automated number plate recognition (ANPR) and vehicular traffic monitoring [27]. Both of these accomplishments rely on the detection of some physical characteristic which can be defined by mathematics or physics, whether it is the recognition of a shape or the velocity of an object.

3.4.2 Artificial intelligence (AI)

Artificial intelligence in a broad sense can be defined as intelligence demonstrated by machines, unlike natural intelligence shown by humans and animals [28]. More specifically, a focus of AI is to mimic the cognitive activities of humans in various settings, such as learning and problem-solving [29]. AI is considered relevant to this research, since it has evolved immensely in the past decade, and there are many areas where AI may be applicable for candidate “TO-BE” models.

As already mentioned, many progressions have been made in AI over the recent decades, and table 1 illustrates a comparison of humans and the fields of AI-based on cognitive intelligence, emotional intelligence, social intelligence, and artistic creativity.

Table 1: Comparison of humans to various AI systems adapted from [37]

	Expert systems	Analytical AI	Human-inspired AI	Humanised AI	Human beings
Cognitive intelligence	No	Yes	Yes	Yes	Yes
Emotional intelligence	No	No	Yes	Yes	Yes
Social intelligence	No	No	No	Yes	Yes
Artistic creativity	No	No	No	No	Yes
Supervised learning, unsupervised learning, reinforcement learning					

Analytical AI only has cognitive intelligence characteristics. These systems learn from historical data to inform future decisions. Examples include fraud detection systems in corporate environments and image recognition systems. Human-inspired AI has similar cognitive abilities to analytical AI, but with the addition of emotional intelligence. These systems cannot physically experience emotions, but they can be trained to recognise emotions such as joy and anger through learning. Humanised AI will show competencies of cognitive, emotional, and social intelligence. It should be noted that these systems do not yet exist at the date of this research. Humanised AI would be self-conscious and self-aware within its environment [30].

Table 2: Examples of areas of application taken from [30]

	Analytical AI	Human-inspired AI	Humanised AI
Universities	Virtual teaching assistants able to answer student questions and tailor reactions to individual data	AI-based career services able to identify emotions to improve interview techniques of students	Robo-teachers animating a student group by acting as moderator and sparring partners
Corporations	Robo-advisors leveraging automation and AI algorithms to manage client portfolios	Stores identifying unhappy shoppers via facial recognition at checkouts to trigger remedial actions	Virtual agents dealing with customer complaints and addressing concerns of unhappy customers
Governments	Automation systems to set the brightness of streetlights based on traffic and pedestrian movements	Virtual army recruiters interviewing and selecting candidates based on emotional cues	AI systems able to psychologically train soldiers before entering a war zone

Table 2 showcases examples of the areas of applications for the three types of AI in universities, corporations, and governments. In these categories, AI can achieve multiple tasks at various complexity levels, which can be expressed through the psychomotor learning levels proposed by Simpson [26]. All the AI levels in table 1 can effortlessly adhere to the perception level of psychomotor learning since they can collect and have data ready for further interpretation. The set level can also be achieved by all the AI levels in table 1, since it is programmed to decide on a response based on its findings through the perception level.

Again, all the AI levels can adhere to the guided response level proposed by Simpson [26], as physical changes can be prompted after a decision has been made on how it should respond. Many AI research topics in the past decade have been at the mechanism level, such as studies of self-driving cars. Human-inspired AI is largely able to achieve the mechanism level. Many of the functions of the complex overt response level such as speed and accuracy can be accomplished by human-inspired AI. However, it does not meet the standard of low energy consumption, since high levels of energy are required for human-inspired AI systems.

Human-inspired AI is outperformed by humans on the adaption level since humans can subconsciously identify the intention of first-of-a-kind incidents much better than human-inspired AI. In the future, humanised AI should be able to achieve this level of learning once it has been developed, but this is merely speculation as it does not exist yet. In the loosely integrated control room setting, the origination level is not required to manage events with efficacy. The adaption level, however, is of importance in this research, as this is required in the control room as new *modi operandi* are frequently observed. This level is the point where humans are differentiated from the AI options available at the time of this research.

A key aspect that artificial intelligence (AI) lacks, is behavioural analysis. It is extremely hard for AI to make sense of human behaviour and intention, especially in a dynamically changing environment. On the other hand, complex activities which do not require such a deep behavioural understanding can be pre-programmed into a system [27]. Furthermore, it is important to note that the intention of AI is not necessarily to replace a human but to aid the human to achieve certain goals.

3.4.3 Augmented cognition

A section of literature is conducted on augmented cognition since it considers the collaboration of modern technology and humans in a system. Humans in a system have both pros and cons, as mentioned previously. Even so, augmented cognition will aid in enhancing the advantages of having humans in the system. Socio-technical systems, including semi-automated systems such as augmented cognition, work at their best when participants are mutually predictable, responsive to one another's input, and able to communicate their intentions in a way the other parties can clearly understand [31].

For many years, the augmentation of human capability and capacity for the increase of operational performance has been a popular topic. Augmented cognition is a field of study that focusses on neuroscience, cognitive science, and human-machine interaction to create closed-loop systems that can measure human information processing (HIP) and act accordingly in real-time. These closed-loop architectures are defined by employing neurophysiological sensors that measure operators' cognitive activity. Mitigating responses to the activity are prompted through an interface such as a computer screen. Typical examples of HIP variables of interest include cognitive workload, situation awareness, and alertness. Electro-encephalography (EEG) is a method used for measuring the electrical activity of the brain (brain waves). It is the chosen method for measuring cognitive functions, and these systems are becoming increasingly comfortable, portable, non-intrusive, and affordable [32].

Other options for measuring cognitive activity have been available for more than a decade. These include oculomotor indices, which measures eye movement such as pupil dilations and prolonged gazing. Fuchs, *et al.*, [32] mentions that dynamic display mitigations employed through cognitive measurements must consider relevant trade-offs, such as a cost-benefit trade-off. For example, dynamic display mitigation may shift an operator's focus to a higher priority event but this, in effect, creates an attention "spotlight" reducing the situational awareness in other areas. Fuchs further postulates that there are two main categories of augmented cognition, namely:

1. The measurement of general cognitive levels and their changes over time;
2. The evaluation of immediate cognitive responses to specific events.

These approaches are elaborated upon in Table 3 below.

Table 3: Comparison of augmented cognition categories taken from [32]

Approach 1	Approach 2
Considers when physiological sensors indicate a problem. Accounts for the general physiological state. Applicable where task models are not feasible. Mitigation targets the symptom.	Potential to consider when, where and how to mitigate problems. Indicates the physiological response to pre-defined events. Applicable only to well-defined, procedural tasks. Mitigation can be context-sensitive and target the cause.

Fuchs [32] mentions that the impacts of augmented cognition can be theorised in the control room and there is significant reason to believe that augmented cognition may reduce cognitive load on operators, increase the speed and effectiveness of event management, and reduce error rates in control rooms. However, Fuchs [32] mentions that further investigation is required before it can be deployed in an operational setting.

3.4.4 AI costing

Since additions to the “TO-BE” candidate systems are expected in the form of AI, the cost of these systems must be taken into account. The cost of AI – that is, the hardware and software aspects – tends to increase as the complexity of the decision-making tasks increase. In some cases, bespoke software and hardware solutions are designed and implemented. A bespoke solution is when the hardware is purchased and software is specifically developed and maintained for a business. Advantages of bespoke software solutions include [33]:

- The software matches the niche needs of the company;
- Customisation and the ability to rapidly adapt to company needs;
- Ownership of the data captured, prepared and analysed.

Some deficiencies of bespoke software solutions include:

- High installation costs, as expensive infrastructure must be purchased and upgraded periodically [33];
- High maintenance costs, as expensive specialists need to be hired permanently;
- The virtual impossibility of reselling infrastructure and software after use [33];
- The risk of theft and damage, which remain the responsibility of the business.

Bespoke solutions are typically used by large companies such as Google and Facebook since the volumes of data and the niches of the companies justify these solutions. Also, some of these large companies need to have ownership of data to an extent, since many of their services (and therefore, income streams) are built on data.

One initiative that overcomes some of the shortfalls of bespoke software solutions, and that may be more suitable for small or medium companies, is software as a service (SaaS). SaaS is a software licensing and delivery model in which software is hosted centrally, typically from a remote

location. The cloud is commonly used as a communication medium between the business and the centrally located software. Some of the advantages of SaaS include:

- No or low direct hardware and infrastructure costs [34];
- System upgrades and maintenance are not the responsibility of the user, and it is executed seamlessly [34];
- Pay-as-you-go options [35];
- The hardware is decentralised, and the risk of theft and damage is not the user's responsibility [35];
- Software is customisable to a certain extent and sufficient for most operations [35].

The disadvantages of SaaS include:

- Responsiveness degradation over networks with poor bandwidth and latency characteristics [36];
- Some compromises on configuration and functionality [37].

3.4.5 Tiny AI

Tiny AI is an emerging field and limited literature is available on this topic. It is currently researched in some industries, particularly the health industry to assist nurses in their daily tasks. Although tiny AI is a relatively new field of research, its applicability may be significant and a section of literature is therefore conducted on it. Tiny AI is receiving attention as it aims to overcome typical AI shortfalls including:

- A large amount of data is required to perform machine learning tasks;
- AI is energy-inefficient and it uses an abundance of energy to perform tasks relative to the amount of energy that humans require to perform the same tasks.

De Ketelaere [38] mentioned at the 2020 digital health summit that about 20% of energy wastage related to AI is due to sending data between edge devices and processing centres. To overcome this, Tiny AI aims to receive and process data on the edge and to make informative, AI-driven decisions on the edge. With Tiny AI devices, significant processing power is expected from small pieces of hardware; therefore it must be energy-efficient. [38]

With this technology, complex decisions must be made with much less data, which requires smarter technology, data usage, and algorithms. De Ketelaere [38] emphasises that instead of having machines learn AI from scratch, previously used algorithms should be adapted smartly to be less resource-intensive.

De Ketelaere [38] mentioned that as of the year 2020, Tiny AI chips have been produced that can track vital signs, observe gestures, and classify activities in a contactless manner through radar. This is particularly significant in the healthcare industry, since cameras may be invasive of privacy. A similar form of Tiny AI is already evident in modern camera systems equipped with analytic capability, as these use different implementations of pattern recognition for scene analysis and anomaly detection.

3.5 Computing in networks

A control room system consists of a network of entities such as technological devices and humans. Therefore, a section of literature is included about common computing methods in networks. There are two popular processing methodologies in network systems, namely *centralised* and *distributed* computing.

A centralised computing system can be defined as a network of devices of which an overwhelming amount of, or all, the processing is done at a central location [39]. An example of this is a mainframe server connected to many client computers. A loosely integrated security control room can be compared to a centralised computing system since data is gained from multiple sites and processed centrally at a single control room. Figure 11 contains an illustration of a centralised computing system.

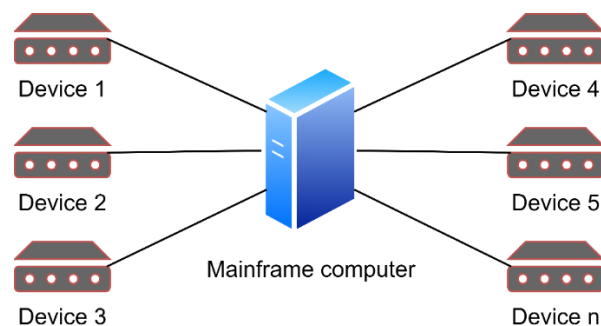


Figure 11: Animation of a centralised computing system

A distributed computing system can be defined as a network of devices that are all able to process sections of data. Therefore, the processing is not only done at a central location but over various devices in the system. Figure 12 contains an illustration of a distributed computing system.

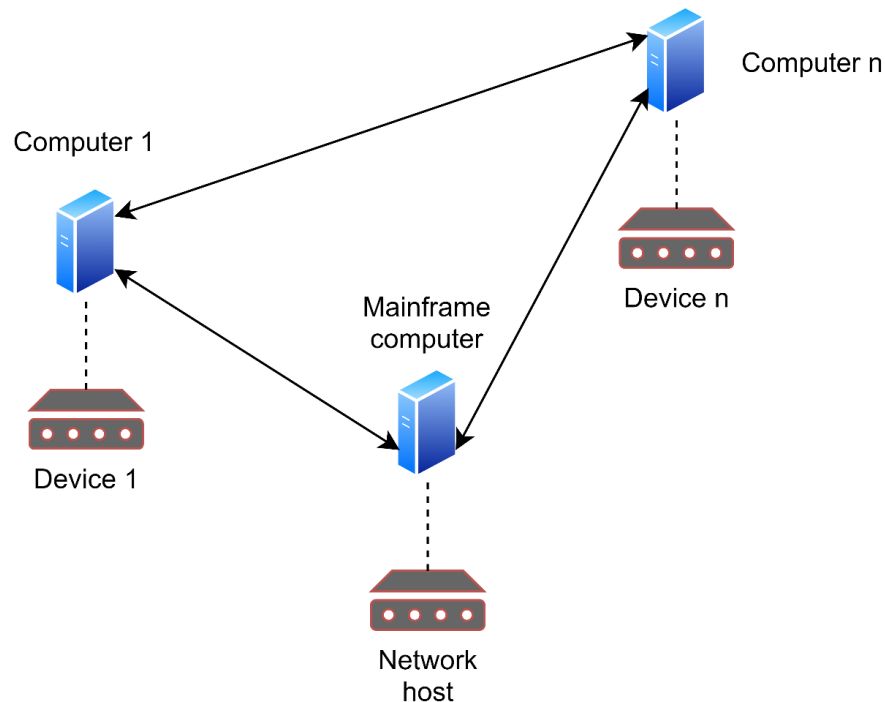


Figure 12: Animation of a distributed computing system

Neither centralised nor distributed computing methods are strictly bound by geographic location and processing can be done with either method in both loosely and tightly integrated settings.

3.6 Signal-to-noise ratio

A ratio commonly used in communication systems that may apply directly to this analysis is the signal-to-noise ratio. This ratio indicates how much signal energy is contained in a digital symbol relative to noise present in a noisy communications channel. A symbol is a combination of bits, modulated in such a way that the symbol carries digital information in an analogue waveform, where the bits are extracted from a symbol through demodulation and decoding. When the signal energy (in a symbol) is high relative to the channel's noise energy, the symbol is easily recognised from a set of possible symbols, and correct information is easily retrieved.

Thus, a decision is made based on the waveform of the symbol received as different symbols will be transmitted over a channel, and a high signal-to-noise ratio gives a high level of confidence in

Page | 31

the decision [40]. In recent research publications, this ratio has also been informally used and lightly remodelled, such as the spam-to-content ratio in online discussion forms [40, 41]. It is thus used as a symbolic expression referring to the ratio of relevant or favourable data to irrelevant or unfavourable data.

3.7 Information and data fusion

Information fusion is the task of joining information from multiple sources into a refined section of information used for decision-making [42]. Similar to information fusion, data fusion can be defined as the collective use of information from multiple sources to assist in the overall understanding of a phenomenon [43]. Information and data fusion are further evaluated in the following section since forms of both information and data fusion take place in control room systems.

Information and data fusion are both relevant in control room systems, since functional units process information from various sources to gain certainty on an event that triggered an alarm, and ultimately form a decision on how to manage it. In other words, patches of data and information are fused and filtered to eventually form a “yes” or a “no” to the question: “Is the event an incident?”. Functional units inside of the control room such as operators may interface with the data and provide their knowledge and thoughts to reduce uncertainty and to shape a decision from all the available information.

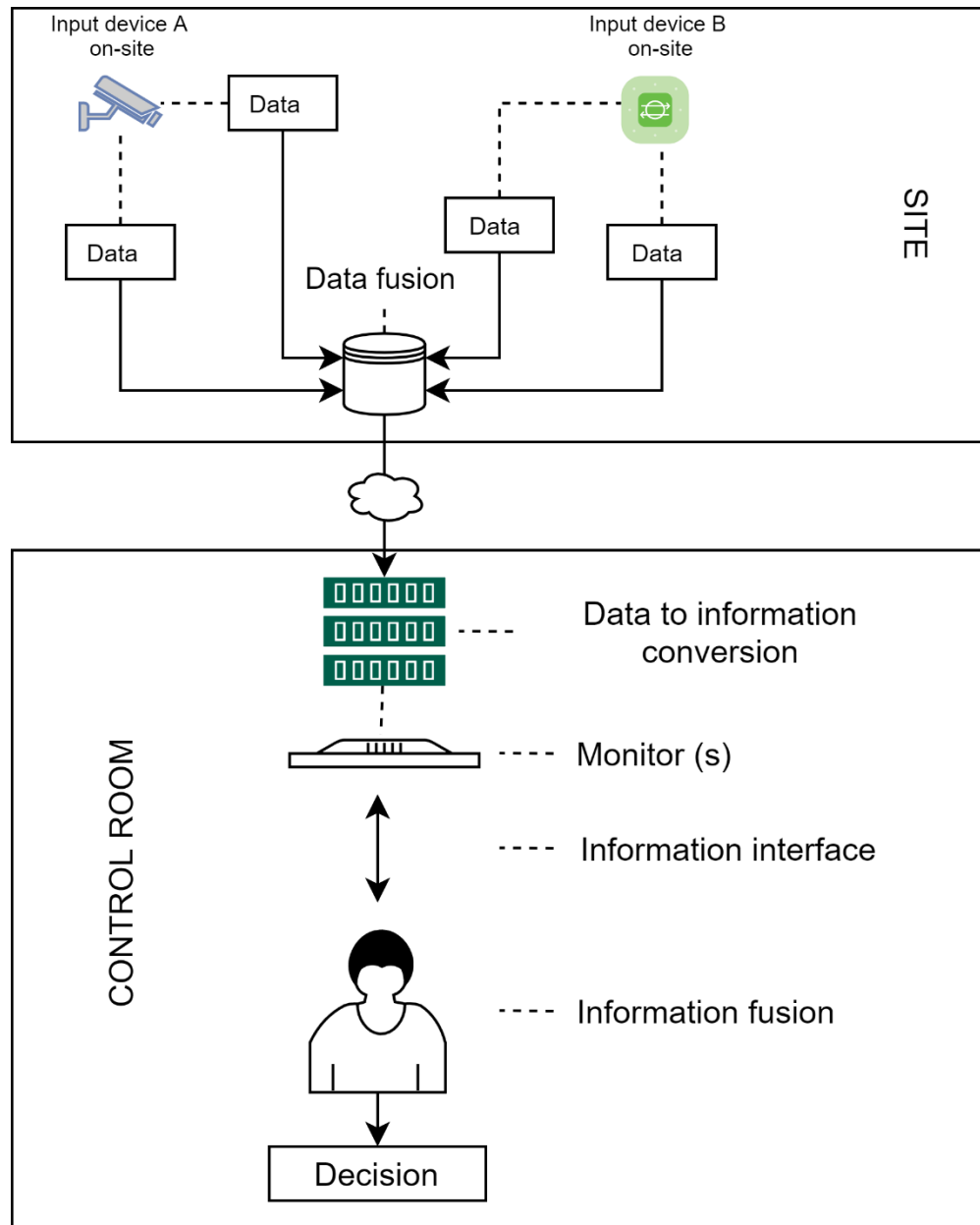


Figure 13: Illustration of information fusion in the control room

Figure 13 illustrates the concepts of information and data fusion in a control room system. Data is gained from various input devices on-site and data fusion can commence depending on the devices and technology available on-site. It is then stored on-site and pushed to the control room, where it is converted to information inside of the control room with automated processes. The operator can then interface with the current information in addition to the available historical information, perform a measure of information fusion, gain certainty, and ultimately make a decision regarding the cause of an alarm.

3.8 Systems engineering

3.8.1 Cognitive systems

The definition of a cognitive system is widely recognised as a system that produces “intelligent action”, in other words, its behaviour is goal-oriented and directed, based on the current knowledge it possesses. Moreover, a cognitive system can adapt to situations and view problems in multiple ways [44]. A slightly modified definition of a cognitive system is proposed as: “a system that can modify its behaviour based on experience to achieve specific anti-entropic ends”[45].

A joint cognitive system is the combination of two or more cognitive systems working together to achieve a specific goal. Humans and intelligent technology systems are both cognitive systems to a certain extent. The collaboration of humans and machines may be considered joint cognitive systems because of the interaction between thinking-humans and “thinking”-machines.

3.8.2 Cognitive systems engineering

A common engineering approach to designing effective socio-technical systems is cognitive systems engineering (CSE). CSE is widely expressed as “A design discipline that uses analyses of work to inform the design of process and technology for human-system integration” [46] and “a design philosophy that advances a broad system design perspective employing modelling concepts from engineering, psychology, cognitive science, information science, and computer science, emphasising human cognitive processes in system design” [47].

CSE is researched in this section since the collaboration of humans and intelligent technological systems will be experimented with. The main principle of CSE is that sociotechnical systems need to be designed, analysed and evaluated in terms of a cognitive system. The consideration of human-and-machine factors in a system has a critical effect on the output of the system as a whole. A recognised goal of CSE is to provide a creator of human-machine interfaces with a realistic model of how humans are expected to function in operational settings [44].

A common error in the design of sociotechnical systems includes the assumption that humans follow the same decision-making process as an idealised rational decision-maker. Humans tend to follow a psycho-logical decision-making process rather than a purely logical decision-making process. In a socio-technical system, an operator should be primarily viewed as a person, not merely as an information processor [44, 48]. Also, one should keep in mind that humans perceive information in a psycho-physical way, as opposed to a purely physical way.

The virtue of CSE is that sociotechnical systems must be conceptualised as adaptive, and systems, where humans and technology collaborate, should be designed as a joint cognitive system to ensure that all the relevant factors of the system are included. In a general sense, different operational tasks require different views of a system's process and the level of abstraction of a task is typically influenced by the field of attention associated with that task [49].

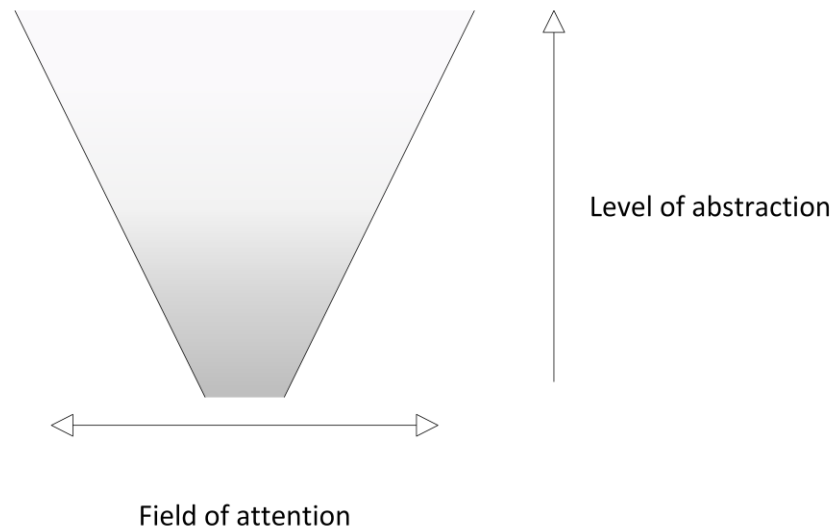


Figure 14: Field of attention versus the level of abstraction adapted from [49]

Figure 14 illustrates the level of abstraction increasing accordingly as the field of required attention of a functional unit broadens. The effectiveness of cognitive entities is expected to increase as the level of abstraction decreases. Humans are known to excel relative to AI in environments where the field of attention is wide and the level of abstraction is high [30]. This is similar to figure 15, originally presented by Jiang, et al., [50] which illustrates the level of complexity based on two driving factors, namely *level of abstraction* and *orientation requirement*.

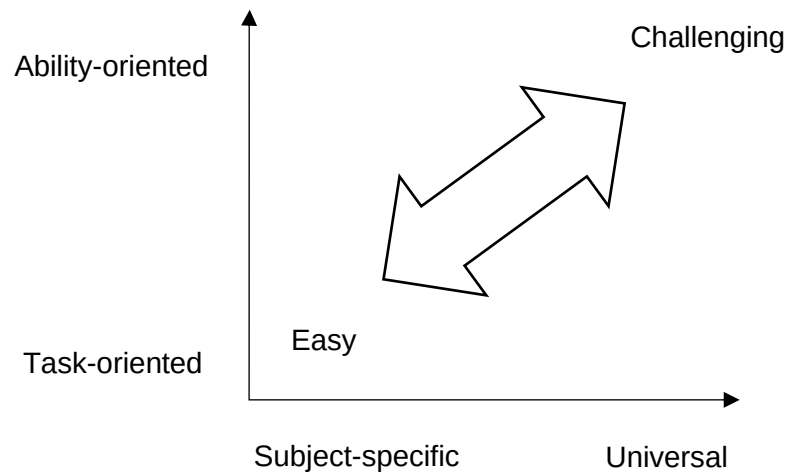


Figure 15: The driving factors of complexity taken from [50]

Furthermore, decision-making in abstract environments is relatively effortless for humans and many researchers in the field of AI are intrigued by this. Humans are also considered very energy-efficient relative to AI.

3.9 Risk terminology

3.9.1 Terminology

Risk is included as an area of focus for this research, since various risks are present in control rooms. These risks include the risk of a site and the perceived risk of an event that triggered an alarm. The term “risk” possesses multiple definitions, and it is a concept that applies to many fields of study and the professional world. Some of the definitions of risk deemed relevant in this research include:

- The “effect of uncertainty on objectives” [51];
- “An unwanted event that may or may not occur” [52];
- “A combination of the probability of occurrence of harm and the severity of that harm” [53];
- “A measure of exposure to loss at a level of uncertainty” [1].

The mathematical relationship for risk in many fields of study is recognised as:

$$Risk = Impact \times Probability \quad (1)$$

This expression can be used to quantify risk, should the probability of an event and the impact thereof be known.

Aven [54] mentions that risk can be divided into 3 regions:

1. Intolerable region: The risk is considered very high and is therefore intolerable;
2. Intermediate region: The risk is in the intermediate region where it can be mitigated;
3. Tolerable region: The risk is considered very low and is therefore negligible.

Risk management is a term used to describe the process of weighing alternatives by assessing their associated risks and if required, selecting and implementing an appropriate mitigation control [55].

3.9.2 Qualitative methods

Qualitative risk methods identify elements of risk by using descriptive terms for specified scenarios or events [1]. There are no quantitative factors associated in cases where risks are evaluated in a purely qualitative manner, and this is a method commonly used in settings where no data is available or as a first-level tool to discuss and illustrate risks based on experience or insightful facts. Figure 16 illustrates a common qualitative risk matrix.

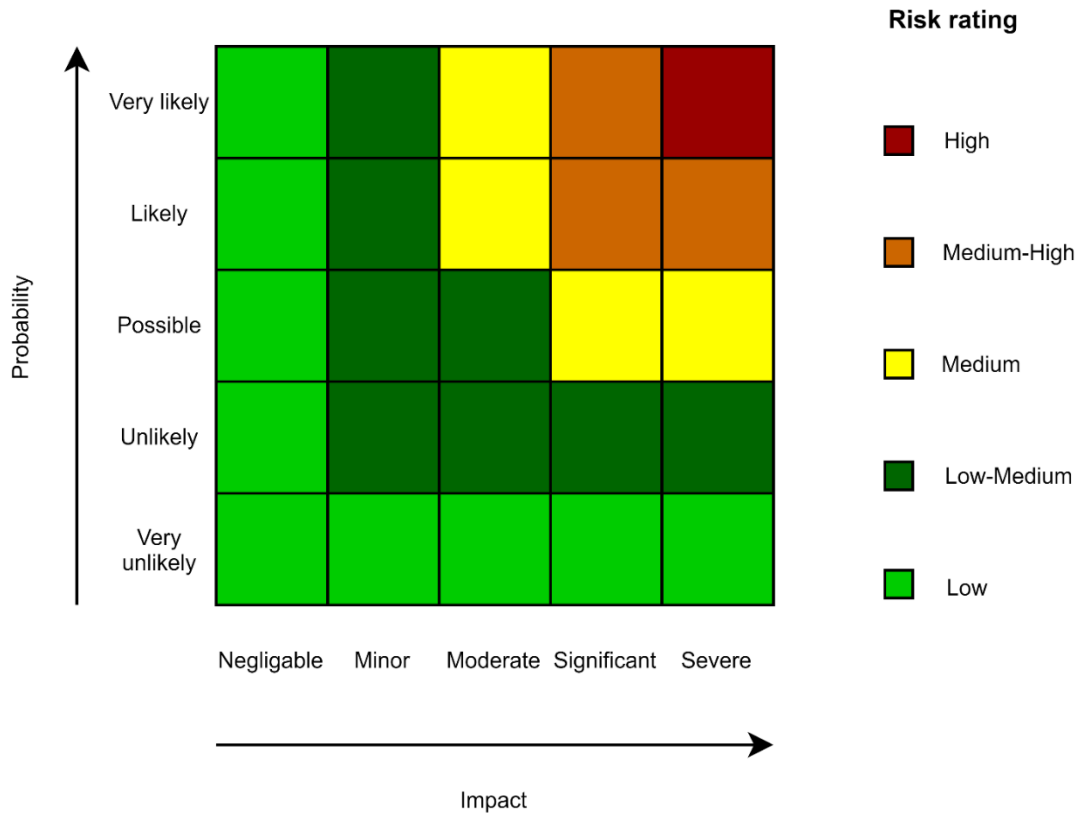


Figure 16: Qualitative risk matrix adapted from[1, 56]

Qualitative measures have numerous shortfalls compared to quantitative initiatives, including [1]:

- It is imprecise;
- A vague justification of weightings is unavoidable when comparing the impact of events;
- It is difficult to compare events directly.

3.9.3 Quantitative methods

Quantitative measures address many of the features lacking in qualitative initiatives. These measures are, however, critically dependent on accurate data, which is not always available – especially in complex and random environments. Numeric outcomes of models cannot be compared directly if there is doubt about the accuracy of the data or if assumptions are made. Control room systems are complex and they function in the presence of humans. Humans, both in the control room and on-site, cannot be perfectly simulated, as many variables are present and humans are unique. This is why purely quantitative methods cannot be used in this research, where a joint cognitive approach is followed. It will therefore not be investigated further.

3.9.4 Semi-quantitative methods

Some of the shortfalls of qualitative and quantitative measures can be addressed by semi-quantitative measures. These measures do not assign actual magnitudes to risk events, but a numerical factor is assigned to categorise the risk of an event. Semi-quantitative measures lack magnitude accuracy, but this can be largely overcome by comparing the numerical factors on a relativistic basis, and not their absolute measures.

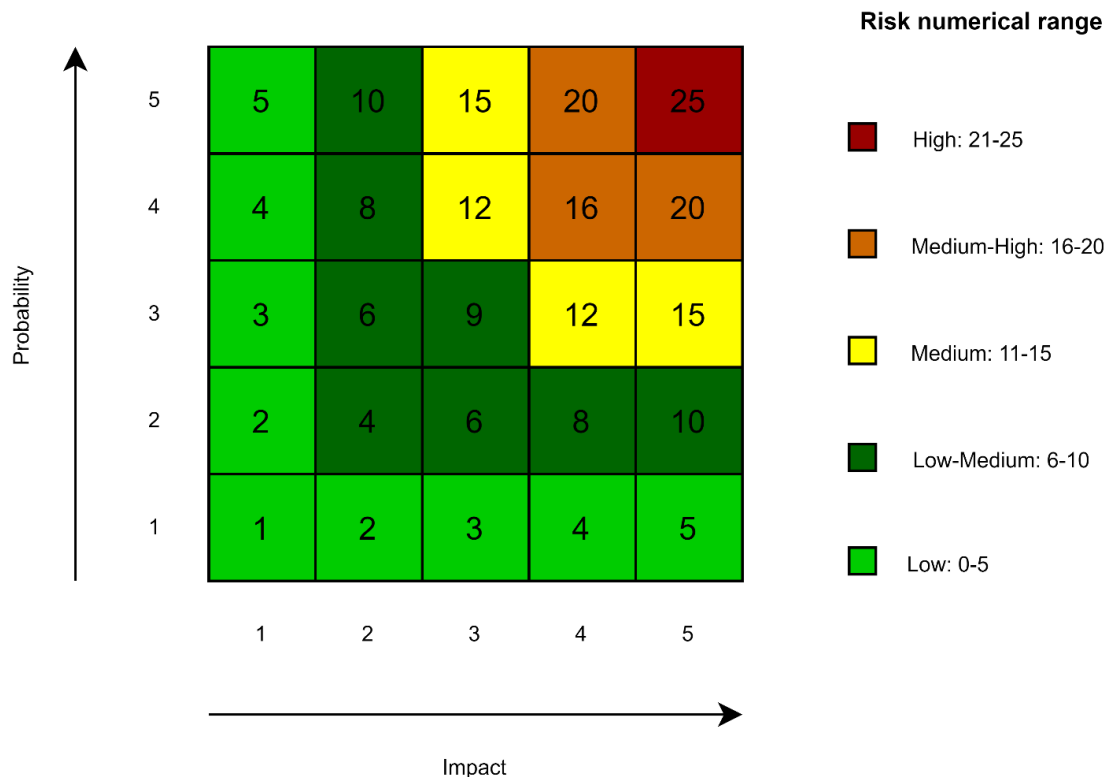


Figure 17: Semi-quantitative risk matrix adapted from [1, 56]

Figure 17 illustrates a semi-quantitative risk matrix. The numerical values in this figure are not actual magnitudes, but rather a factor used for the classification of risk. This risk-approach is the most applicable for this research opposed to purely qualitative methods (not factual) and quantitative methods (impractical for complex, abstract environments where data is lacking).

3.10 Scales of measurement

This section is included in the literature study to evaluate trusted methods of measuring and comparing outcomes of scientific studies and to determine a method applicable to this research.

Stevens [57] performed a study comparing various scales of scientific measurement. He argued that measurements exist in a variety of forms and that the scales of measurements can be classified based on certain characteristics. He defined these classes in his research, which considered empirical operations, mathematical group structures, and permissible statistics.

Table 4: Scales of measurement adapted from [57]

Scale	Basic empirical operations	Mathematical group structure	Permissible statistics
Nominal	Determination of equality	Permutation group	• Number of cases; • Mode; • Contingency correlation.
Ordinal	Determination of greater or less	Isotonic group	• Median; • Percentiles.
Interval	Determination of equality of intervals or differences	General linear group	• Mean; • Standard deviation; • Rank-order correlation; • Product-moment correlation.
Ratio	Determination of equality of ratios	Similarity group	• Coefficient of variation.

Table 4 contains the classes of the scales of measurement presented by Stevens [57]. The following section elaborates on these scales to identify a suitable measurement scale for this research.

3.10.1 Nominal scale

Typically, two types of nominal assignments are distinguished, namely the *numbering of individuals* and the *numbering of classes*, where all the individuals in a class are assigned the same numeral. This scale is considered a primitive form of measurement, and many will naturally argue that it is not a quality measurement scale, as the naming of individuals and classes are quite arbitrary. [57]

3.10.2 Ordinal scale

This scale arose from the operation of rank-ordering. A classic example of an ordinal scale is the scale ranking the hardness of materials [57]. Other examples include scales for the quality of a manufactured product and scales of personality traits. Ordinal scales are widely used in psychology and are mostly qualitative in nature, resulting in a lack of rigour in precise, quantitative scientific studies. [57]

3.10.3 Interval scale

The interval scale is typically used for purely quantitative measurements and comparisons, and almost all the statistical measures apply to this scale. In the application of this scale, the zero-point is merely a matter of convention or convenience. An example of this is the two scales of temperature, namely Centigrade and Fahrenheit. [57]

3.10.4 Ratio scale

These scales are commonly used in scientific studies and are possible when the following four relations are present:

- Equality;
- Rank-order;
- Equality of intervals;
- Equality of ratios.

Once such a scale is defined, its numerical values may be adjusted by multiplying it with any constant. The ratio scale is defined towards addressing the question: “What are the rules, if any, under which numerals are assigned?” [57]. Unfortunately, a consistent set of rules does not exist as the applicable areas of measure are vast, diverse, and ever-growing.

Any scale, sensory or physical, may be subject to bias, low precision, restricted generality, and many other factors. Stevens [57] mentions that scientific studies are relative and practical and that no scale used by mortals is perfectly free of their taint. Hence, a relativistic approach in the form of ratio scales is most suitable for this research, since the artefact will be comparative in nature.

3.11 Decision trust

The major decision that functional units must make, is whether an incident had actually taken place or if an alarm was signalled falsely. This is because incorrect decisions can, over time, lead to misdirection and a significant wastage of resources. The certainty about the cause of an event is crucial in determining whether to respond to an event or not, as wrongfully responding to a false alarm will result in monetary loss, and wrongfully dismissing a true positive may lead to the incident *escalating*. Therefore, a method for decision-making that takes risk and certainty into account must be included in the literature study.

Jøsang and Presti [58] presented an approach for analysing investment options based on a relying client's risk attitude and the probability of a team producing a successful outcome for specified investment options. The term "decision trust" is recognised as the relying client's trust in the team to produce a positive outcome. Mathematically, the decision trust can be expressed as:

$$\text{For } p < p_D : T = \frac{p - p_D}{p_D} \quad (2)$$

$$\text{For } p = p_D : T = 0 \quad (3)$$

$$\text{For } p > p_D : T = \frac{p - p_D}{1 - p_D} \quad (4)$$

where:

$$T = \text{Decision trust} \quad (5)$$

$$p = \text{Probability of the team correctly predicting the outcome of an investment option} \quad (6)$$

$$p_D = \text{Cut - off probability} \quad (7)$$

It should be noted that the cut-off probability is directly proportional to the relying client's risk attitude. If the relying client has a risk-averse attitude, the cut-off probability would be higher. On the other hand, the cut-off probability would be lower if the relying client has a risk-taking attitude.

Only when the decision trust is a positive value, will the relying client agree to undertake the investment option, as the client then trusts the team for an option in a given context. If the decision-trust value equals zero, the client is indecisive on trusting the team for an option in a given context. Finally, if the decision trust is a negative value, the client does not trust the team to produce a positive outcome. If the decision-trust is a negative value, however, trust can be gained through:

1. A change in the client's risk attitude;
2. An increase in the probability of the team correctly predicting the outcome by adding countermeasures, deferring risk, or re-computing the decision trust with more or better metrics.

Although this concept is based on economic studies, it applies to the control room environment since functional units are counted on to process events correctly. Aven [54] mentions that probability is a way of measuring uncertainty. This raises the questions of how certainty influences the risk perception in the event handling process and how to quantify this phenomenon in the simulation environment. This question is further discussed in Chapter 4.

3.12 Simulation modelling

3.12.1 Simulation software

This study aims to construct an artefact – in the form of a simulation model – that is representative of the event management functionality of a control room system. Simulations provide a virtually risk-free environment in which the designer can observe the consequences of the design changes of a model. There are many simulation software packages available with the ability to simulate operations from the physical world and display them visually. These software packages provide an accurate prediction of what can be expected to happen in real-world systems when elements of the system must be changed or adapted.

Researchers have compared simulation software tools [1, 59] on criteria similar to what is required in this research, and it is evident that many software packages possess the ability to effectively simulate and evaluate complex problems similar to a loosely integrated security control room. The Simio software package is chosen as it is a validated, widely-used simulation tool, as confirmed by researchers [1, 60, 61].

3.12.2 Finite-state machines

A finite-state machine (FSM), also known as a finite-state automaton among other terms, is a model of behaviour composed of a finite number of states, transitions between those states, and actions [62]. This research topic is included in the literature study, since an event can be in a finite number of states over its lifetime, and these states need to be defined to ensure that a practical artefact is created. A state represents a behavioural node of a system which continues to execute its specified definition until a trigger signals the transition to another state [62]. FSMs are defined by their states, the triggers that cause transitions, and to which states the transitions will be.

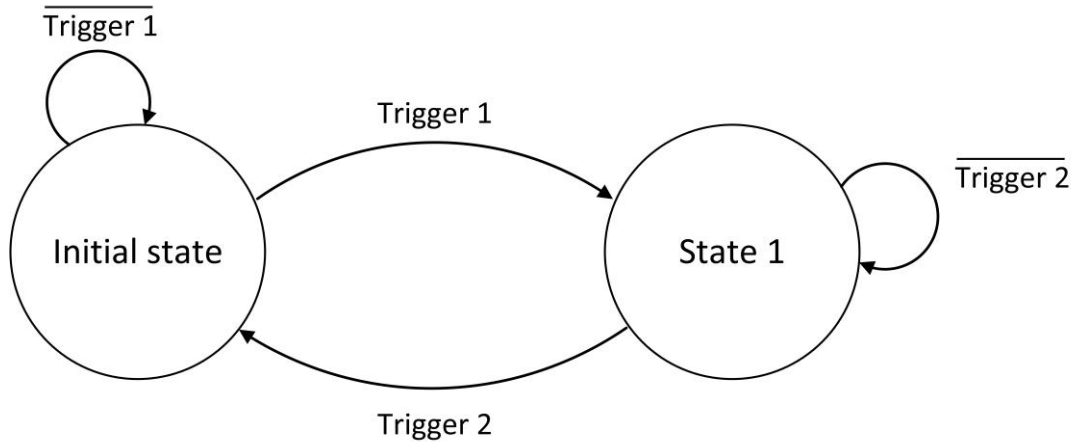


Figure 18: Generic FSM

There can be any finite number of states in an FSM and events may act as triggers - which results in transitions between states. FSMs are typically used in design automation environments. It has, however, also been used as a tool in many different industries at both a high-and-low level [1]. An FSM describes the entire environment of interest, at the level of interest, to aid in the understanding of practically any system. The line above the trigger in figure 18 indicates that that specific trigger had not yet occurred, and the system will remain in its current state until a trigger is executed.

3.12.3 Monte Carlo Simulations

Many operational settings, including control room systems, are directly influenced by random events. This randomness makes it virtually impossible to reproduce determinant values in the simulation environment. Nevertheless, estimations of the randomness must be considered in the simulation model for it to be reasonably representative of the physical world. The Monte Carlo method is a tool that seeks to make sense of this randomness and it is a method commonly used to provide realistic *estimations* in experiments.

There is no exact definition for the Monte Carlo simulations, although some researchers have endeavoured to define it. Anderson *et al.* define Monte Carlo simulations as simulations which use random variables to estimate an expectation by a sample average [63]. Romlay *et al.* state that Monte Carlo simulations are stochastic approaches for modelling phenomenon with significant uncertainty in inputs [64]. Grimson announced in a lecture at MIT that the Monte Carlo method is a composition of the idea that a random sample drawn, will, over time, give the same characteristics as the population [65].

In Monte Carlo simulations, probability distribution ranges are defined for variables which impact the system, yet of which the exact values are unknown. These probability distributions contain real values of which the actual value is likely to transpire in. Random values are produced within these ranges and output samples are generated. This is done repeatedly and reasonable estimations are produced as outcomes in experiments. If sufficiently long run time is chosen for the experiment, accurate estimations outputs are produced. Some advantages for Monte Carlo simulations include:

- Quantitative probabilistic analysis in process design [66, 67];
- Sensitivity analysis of influencing factors [66, 67];
- Graphical results [67];
- Correlation on inputs [67];
- Scenario analysis [67].

The Monte Carlo simulations, therefore, do not only provide relatively accurate output estimates, but it is also possible to determine how likely the occurrences of outcomes are. It is also possible to model the independent relationships between input variables [67]. The Monte Carlo method is important in this research since control room systems (especially loosely integrated control room systems) deal with randomness that, over time, is descriptive of the nature of a control room's operations.

3.13 RVM part one

This section includes the first part of the RVM of this research, ranging from the research need to the concept solutions. The research challenges are individually validated by sources, which, in turn, validates the research problem. All the literature topics covered in chapter 3 contributed to either research challenges or concept solutions and the umbrella terms for these literature sections indicates this in the RVM shown in figure 19 accordingly.

Research need: Determine the influence of intelligent technologies on conventional control room

Research efforts have been managed ineffectively in the past	↓				
Industry observations		↓	↓		↓
Industry data				↓	
Source Challenges Literature focus areas	Uncertainty regarding how to manage research with quality and efficacy	The functional and informational dynamics of conventional control room systems are not well-defined	The interactions between people and technology in control rooms are not entirely clear	No performance data is available on the impact of alterations to a control room system	No standardised norm is defined to compare the outputs of experiments
Research methodologies	↑ ↓				
Control room systems		↑ ↓	↑ ↓	↑	
Human factors		↓	↑ ↓		
Technology and industry 4.0 methods			↑ ↓	↓	
Computing in networks		↑ ↓			
Systems engineering			↑ ↓	↓	
Risk					↑ ↓
Simulation modelling				↓	↑ ↓
Umbrella literature focus areas Research concept solutions	Follow the QRM methodology to manage literature and the DSR and ADR methodologies to create an artefact	Perform a system analysis on the dynamics of a real-world control room system	Follow a systems engineering approach and define the system from a holistic perspective	Create a simulation model of the real world control room system ("AS-IS") and perform experiments ("TO-BE")	Follow a relativistic approach to ensure that the only changes impacting the outputs are those brought by system alterations

Figure 19: RVM part one of this research

3.14 Conclusion

This chapter contained a literature study and a theory summary of concepts that are relevant to this research. Control room systems over three industries were evaluated and it was found that event management is a common and important attribute of control rooms in these industries. The process of event management starts at an event being reported and it ends at improvement proposals, however, only the steps of the event management process which occur while an incident can escalate is considered to be on the critical path.

The real-world system under evaluation was chosen to be a loosely integrated security control room system. Technological systems which are common in security control room systems were analysed to identify what industry 4.0 technologies may be viable options for candidate “TO-BE” systems. Video scene analysis and robust object detection were identified as viable industry 4.0 methods, since the main decision-making data in security control rooms are in the form of visuals such as video footage or images.

Humans conventionally form part of control room systems and it was confirmed from literature that the presence of humans carry both pros and cons in control room systems. Negative aspects include cognitive bias and human error, while positive aspects include being good at classifying “first-of-a-kind” incidents and analysing vague scenarios with high rates of success. The decision-making ability of humans can be presented by the levels of psychomotor learning. Since AI mimics human intelligence through learning, the levels of psychomotor learning can act as a benchmark to directly compare AI with humans on a decision-making level. This will guide how some variables will change in the simulation environment in the experiments in chapter 5.

Literature research was conducted on risk, since risks are ever-present in control room systems. A method for simulating decision-making was needed that considers risk and uncertainty. It was found that a semi-quantitative risk approach is most applicable to this research, and the decision trust framework was identified as the method to be used for including risk and uncertainty in simulations.

Chapter 4: System modelling

4.1 Overview

Literature topics that address research challenges and concept solutions were identified in Chapter 3. The next step toward the completion of the RVM is to identify and synthesise the concept solutions into a valid artefact. This chapter provides a detailed analysis of how the literature topics address the concept solutions. Furthermore, a methodology is proposed at the end of this chapter which is used to integrate the concept solutions into a valid artefact, and it has been developed explicitly for this research.

4.2 System trade-offs

A trade-off is a situational decision that involves losing one department to gain other departments in return [68]. Trade-offs are present in many systems, and it is ever-present in control room systems. The following section elaborates on the typical trade-offs arising in these systems.

4.2.1 Trade-off triangle

This concept has been specifically developed for this research through observation and intuitive reasoning, to ensure that all the main forces influencing event management in the control room setting are defined and understood.

The longer an incident is processed by the control room, the greater the chance of the *incident escalating*. The escalation of incidents can be minimised by responding to every event, but this is not financially viable, since many false alarms are produced by the input devices on sites. These two factors, namely the time an event spends in the system, and the cost of handling the event are in direct trade-off and will be discussed below.

If more certainty is gained in a shorter period, an event can be responded to faster, which will lead to an overall lower incident escalation time – since the event may be an incident. Therefore, three factors are identified in the trade-off, namely:

- The cost of handling an event;
- The certainty about what caused the event;

- The time the event spends in the system.

These three factors all influence each other; hence the *trade-off triangle* is defined and shown in figure 20.

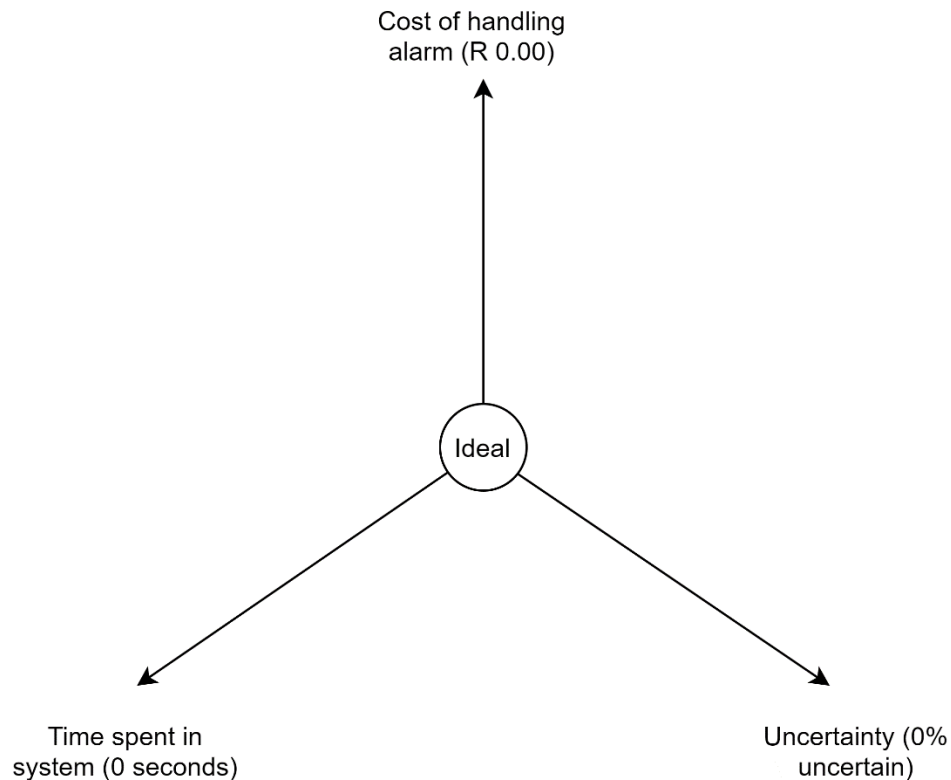


Figure 20: Trade-off triangle

Note that the lengths of the arrows are not drawn to scale. This figure illustrates an “ideal” scenario, where a perfect balance is found between the cost of handling an event, the time an event spends in the system, and the level of uncertainty the control room has about the event’s cause. If this ideal balance is altered in the direction of any of the three arrows, the corresponding trade-off would be one or both of the other arrows. Consider the examples in the following section that illustrate this point more clearly.

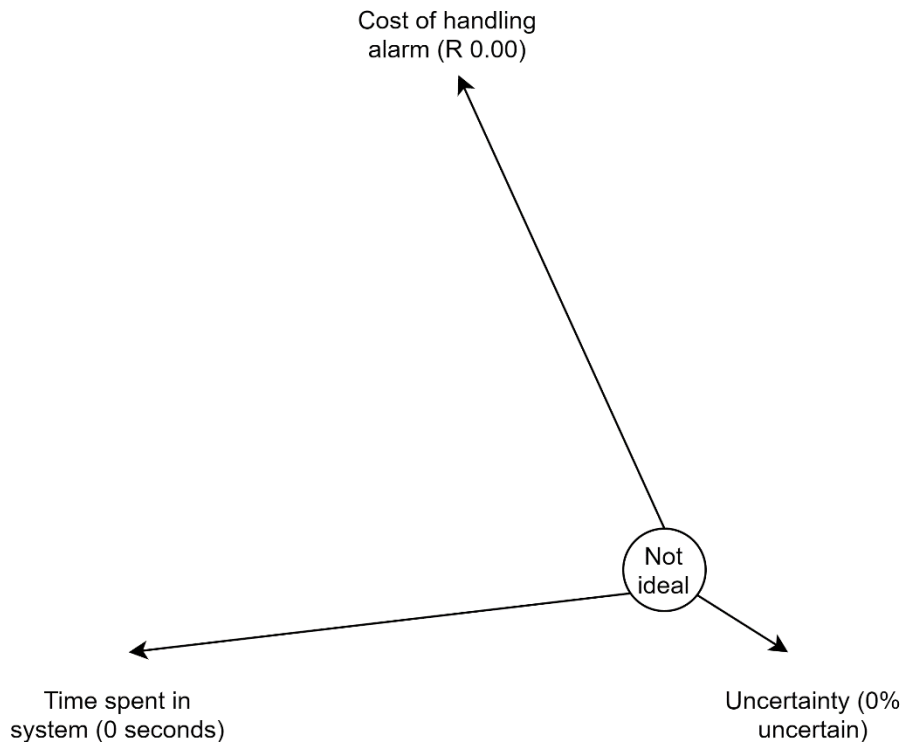


Figure 21: Trade-off to have more certainty

Figure 21 illustrates a scenario where less uncertainty about an alarm's cause is desired. For the uncertainty to be lower, a combination of the time an event spends in the system and the cost of handling the event shall be negatively influenced. Therefore, a trade-off must be made by either *spending more time* in the system (which may result in the escalation of an incident if the event is indeed an incident) by:

- Contacting personnel on-site to obtain more decision support information;
- Acquiring more alarm information from technology on the site.

Or increases in expenditure, such as:

- Sending reaction teams under low certainty – this will result in monetary losses reacting to false positives, where no one had initially been in danger;
- Spending more money on operator training for decision making under uncertainty;
- Installing more expensive systems to provide more alarm information.

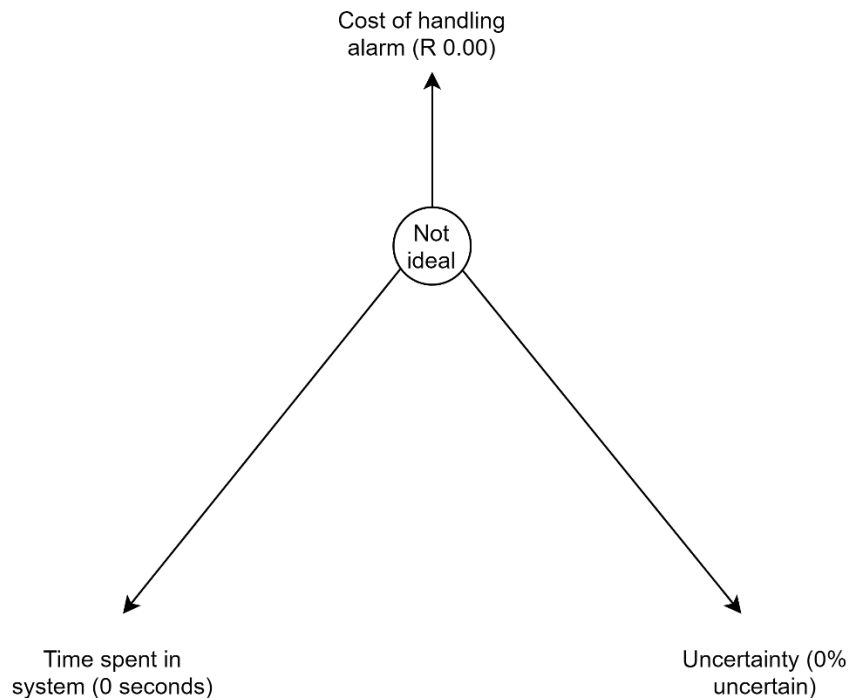


Figure 22: Trade-off to have a lower cost

Consider the second example of the trade-off triangle shown in figure 22 where a lower cost of handling an event is desired. To decrease the cost of handling an event, a trade-off must be made by either increasing the time the event spends within the system – which may lead to an incident escalating if the event is indeed an incident - or the control room will have a higher level of uncertainty regarding the cause of the event (through cheaper input devices) or a combination of both.

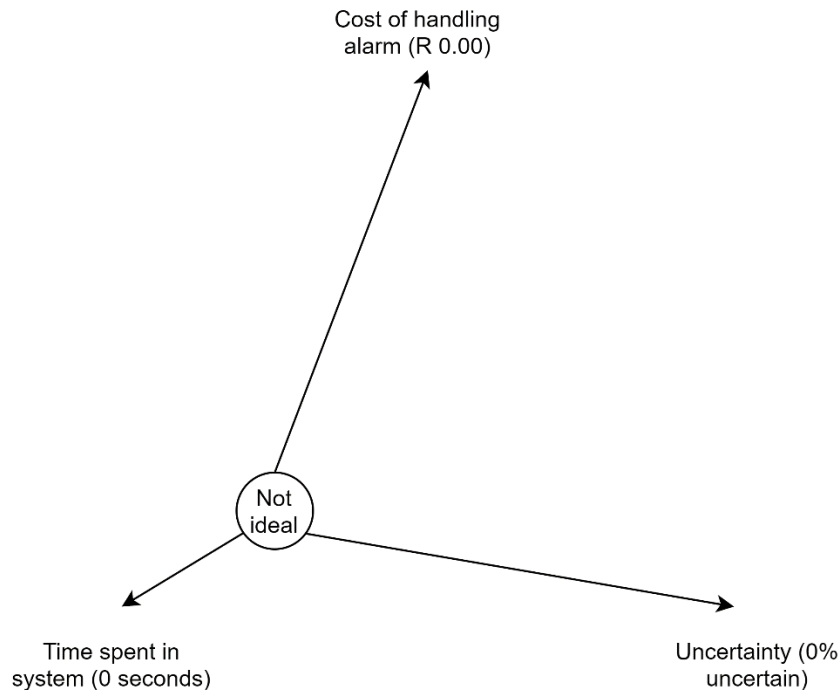


Figure 23: Trade-off to spend less time processing event

In figure 23, the third example of the trade-off triangle is portrayed where it is desirable for the event to spend very little time in the system. To have the control room spend less time processing an event (and to potentially avert incident escalation), a trade-off must be made by either spending more money on handling the event (through more expensive input devices), or by accepting a higher level of uncertainty of the event's cause (which may lead to incorrect responding and resource wastage), or a combination of both.

4.2.2 The model trade-off

The trade-off triangle in the previous section illustrated that each seemingly favourable goal will result in a trade-off of other favourable goals. Also, the trade-off triangle is qualitative in nature, which cannot be used directly in the simulation model but effectively serves to visualise the trade-offs. The following section provides the model trade-off, which effectively is a semi-quantitative implementation of the trade-off triangle.

The trade-off triangle illustrates that the certainty of an event's cause influences both the time and the costs aspects associated with managing an event. The amount of certainty, however, is not a value which provides much insight on the operations of a control room on its own. Monetary

expenditure and incident escalation time, however, are descriptive underlying factors of the efficacy of a control room's operations.

The certainty about an event's cause plays a major role in the management of events. Nevertheless, the control room cannot react to an event based on certainty alone, as some sites are considered to be higher risk than others, and an attack on those sites will have a higher impact. Therefore, the risk attitude of the control room cannot be identical toward events from sites of varying risk factors. It is therefore important to categorise events based on risk impact and to prioritise events accordingly.

Each site monitored by a loosely integrated control room has a predetermined residual site risk. The residual risk of the site is based on the consideration of the environmental risk (the site may be in a dangerous area and therefore more prone to incidents), the site risk (the site may contain high quantities of cash, or many lives are at stake), and the mitigations put in place to counteract these risks (such as physical barriers, electronic technology, security procedures and others).

Each event must, therefore, be assigned a perceived risk score. This is not the actual risk score of the event, but rather a function of the known residual site risk of the site the event occurred on, and the certainty the control room operator has about the event's cause. This perceived risk score is based on observation and it directly influences the perceived probability of the event being a true positive. The term *perceived* is emphasised, as in some cases, an event can be incorrectly interpreted by the control room to be the opposite of the actual, underlying event.

The perceived probability value will change as the certainty of the event's cause changes. More specifically, the perceived probability of the event being an incident will increase as certainty is gained that the event is indeed an incident. Also, the perceived probability of the event being an incident will decrease as the certainty that the event is a false alarm increase. Figure 24 contains an analysis of the model trade-off adapted from the trade-off triangle, as implemented in a model. The main trade-off is the trade-off between (i) the time an incident is allowed to escalate, and (ii) the variable and fixed costs associated.

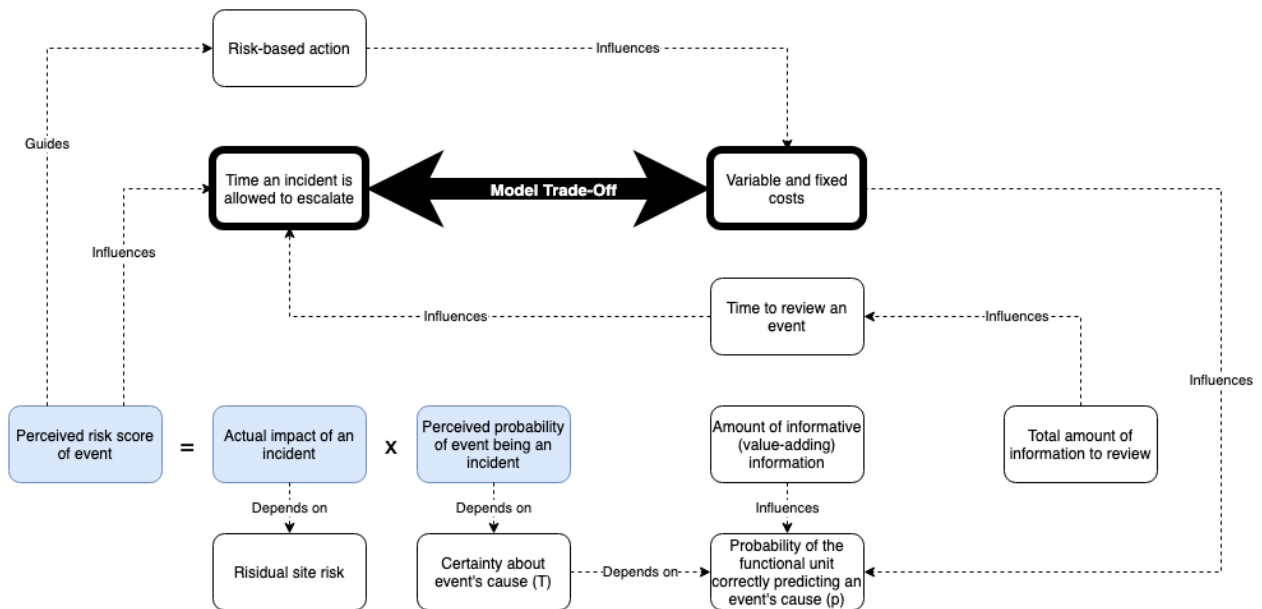


Figure 24: Analysis of the model trade-off

The perceived risk score of an event is dependent on the actual impact that a true incident may have on the site, and the perceived probability of the event being an incident. These two factors are influenced by the actual known residual risk of a site, and the certainty the operator has about what caused the alarm. The latter factor is dependent on both the amount of informative information (and the way it is presented) and expenditure related to operator training.

The perceived risk score directly influences the time an event spends in the system, since an event is only actioned when it is in either the tolerable or intolerable region, and incidents may escalate while the perceived risk of an event is in the undecided region. Moreover, the perceived risk score of an event guides how the event will be handled, which in return influences the variable capital expenditure.

The total amount of associated event information to review directly influences the time to process an event, since more information must be processed and more data must be sent over the communication medium – resulting in additional delays. These processing and transfer delays directly impact the time an incident is not under control, since the event will continue to unfold while information about it is being processed.

Jøsang and Presti [58] presented a method for describing the trust a party has in a team of investors to choose a correct investment option. This trust value is based on the probability of the

team correctly choosing an investment option, and the risk attitude the client has. Consider the adjusted version for the control room setting:

$$p_{fu} = \frac{i_i}{i_R} \quad (8)$$

where:

$$p_{fu} = \text{probability that the functional unit will correctly identify the alarm's cause} \quad (9)$$

$$i_i = \text{amount of informative information available to the functional unit} \quad (10)$$

$$i_R = \text{amount of informative information required by the current functional unit} \quad (11)$$

It should be noted that i_R will depend on the ability of a functional unit (i.e. human, software algorithm, or the like) to interpret the informative data. The contributing factors are the knowledge and experience of such a functional unit, site history, and other factors contributing to the ability of a functional unit to make an informed decision.

The main goal of the simulation models in this research is the management of risk by iteratively evaluating events as more information becomes available, and categorising it accordingly. The categorisation of events will be done through the perceived risk score mentioned earlier, which ultimately guides the control room on how to handle an event. The perceived risk score of an event is referred to as “ r ” in this research. The three categories of risk identified for the simulation models are:

1. Intolerable region:

$$r > a, \text{ where } a \text{ is the threshold for the intolerable region;}$$

2. Tolerable region:

$$r < b, \text{ where } b \text{ is the threshold for the tolerable region;}$$

3. Undecided region:

$$\text{if } (b \leq r \text{ and event perceived as FP}) \text{ or } (r \leq a \text{ and event perceived as TP}).$$

If the r of an event is in the intolerable region, the task force team shall be dispatched. After the response, the event is investigated to identify the underlying causes, or reason, for the event. If the r of an event is in the tolerable region, the response team shall not be dispatched, and the event will be discarded and considered a false alarm. An investigation will follow to identify the cause of the false alarm and mitigations will be put in place to reduce the frequency of similar false alarms. However, if the r of an event is in the undecided region, the event will be reviewed until it is either in the tolerable or intolerable region, as the event must be either an incident or a false alarm, and there is no “grey area” in the security control room setting. Consider the following expression for the perceived risk score of an event:

$$r = I \times P \quad (12)$$

where:

$$P = \text{the perceived probability of an event being an incident} \quad (13)$$

$$P = p_{fu}, \quad \text{if the event is perceived as an incident} \quad (14)$$

$$P = 1 - p_{fu}, \quad \text{if the event is perceived as a false alarm} \quad (15)$$

$$I = \text{the potential impact of an incident on a given site based on the residual site risk} \quad (16)$$

Table 5 contains a summary of the sequential action that will take place for an event based on the r -value of the event.

Table 5: Risk categories and their corresponding actions

r – value	Action 1	Action 2
$r > a$	Dispatch task force	Investigate why the event occurred
$(b \leq r \ \&\& \text{event perceived as FP}) $ $(r \leq a \ \&\& \text{event perceived as TP})$	Further evaluation of the event	Recalculate r value
$r < b$	Investigate why the event occurred	-

Events are evaluated and certainty is gained until the control room is confident in the decision to either respond to an event or dismiss it as a false alarm. In many cases, the control room is not certain about the event's cause, even after revision, since some lower-quality input devices are less informative than others or limited data, may be captured on the event that caused the alarm. Figure 25 contains an illustration of the iterative risk evaluation used in this research.

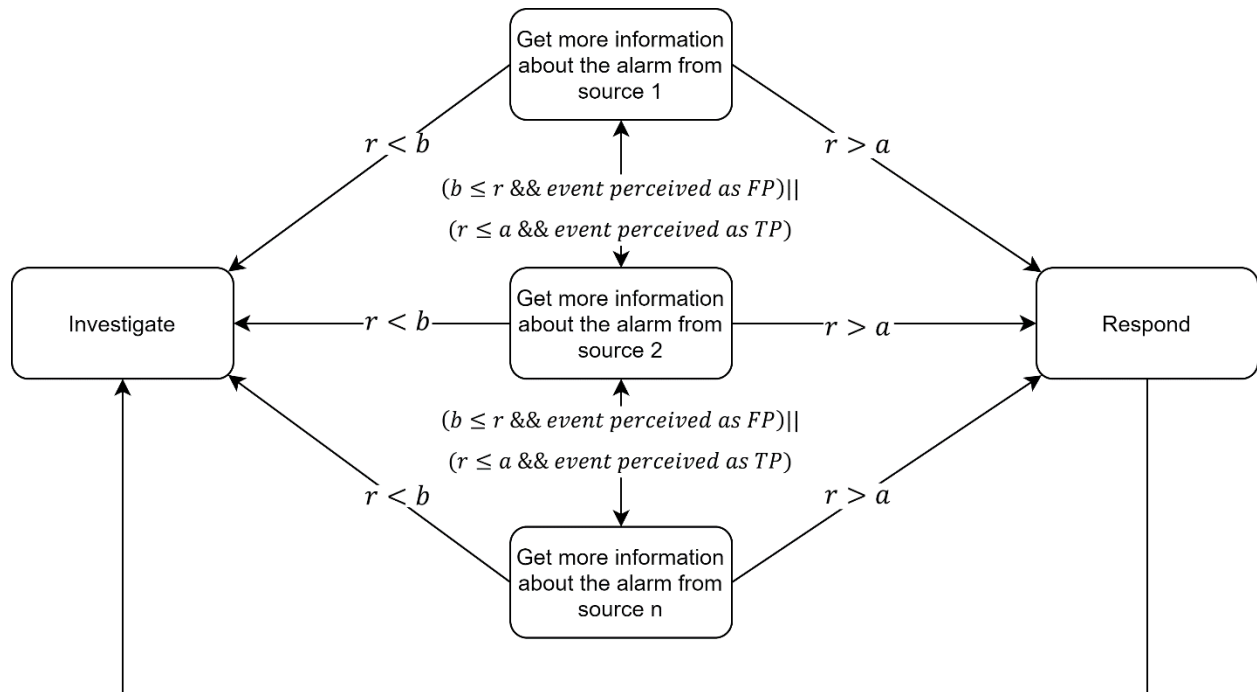


Figure 25: Iterative risk evaluation

The sources mentioned in the iterative risk evaluation figure may be other functional units (such as supervisors) in the control room, SOP's suggestions, or the available input devices on the site of interest.

4.3 The bin-theory

The bin-theory was developed specifically for this research as a tool to evaluate and alter the flow of data in the simulation models. Input devices are devices that are located on monitored sites that provide a control room with decision-making data. A journal article resulted from this research and was published in the special edition of the South African Journal of Industrial Engineering (SAJIE) [69]. Hence, large sections of text in this section and the remainder of chapter 4 directly correspond with the journal article. Copies of the email of acceptance and the article can be found in Appendix C and Appendix D respectively.

The total data obtained from input devices consists of informative event data, referred to as “event indicators” in this research, as well as noise, which is recorded data that contributes no value toward the decision-making of an event’s cause. Event indicators are informative in the sense that they provide information that helps a control room determine why an event was generated. Consequently, event indicators contribute to the certainty that the control room has about an event’s underlying cause.

A bin is a term used in this research to describe the total data pulled from an input device in a set period. In practice, the sizes of bins are rarely the same. For example, if multiple sections of footage (bins) are drawn from a CCTV system on-site over time, the video sections may consist of a different number of frames. Also, the number of event indicators would typically be different in every bin, since the events recorded at the sites are random and unique. The result is that every bin will embody distinct densities of informative data, and each bin will contribute to a distinct amount of certainty.

A practical example of the information density of a bin follows. Consider a video clip with a duration of five seconds. If the video contains evidence of a person breaking and entering, it would be of higher information density than a clip of five seconds only containing a glimpse of an object looking like a limb of a person in a scene. The functional units within the control room would be able to call the first video an actual incident with more certainty than the second video, and more

information may be required to determine the cause of the event in the second video, which will result in the event staying in the system for longer.

Also, if too little information is provided for the functional units in the control room to evaluate the cause of the event, the functional units will need to acquire additional information from the site to increase their certainty about the event's cause, which will cause a potential incident to stay in the system for longer. It is therefore advantageous to have an input device on-site that can provide sufficient data as quickly as possible that can be evaluated efficiently by the control room's functional units.

It seems that by increasing the density of the information available about the event would result in a larger amount of valuable information reviewed in a similar amount of time. This will result in increased certainty per timeframe, resulting in the event being reviewed more quickly. An input device providing either limited informative information or an excess amount of noise will result in a potential true positive staying in the system for longer than needed - as a revision by the functional units will take longer. Figure 26 contains the model trade-off with emphasis placed on the density of informative information in bins.

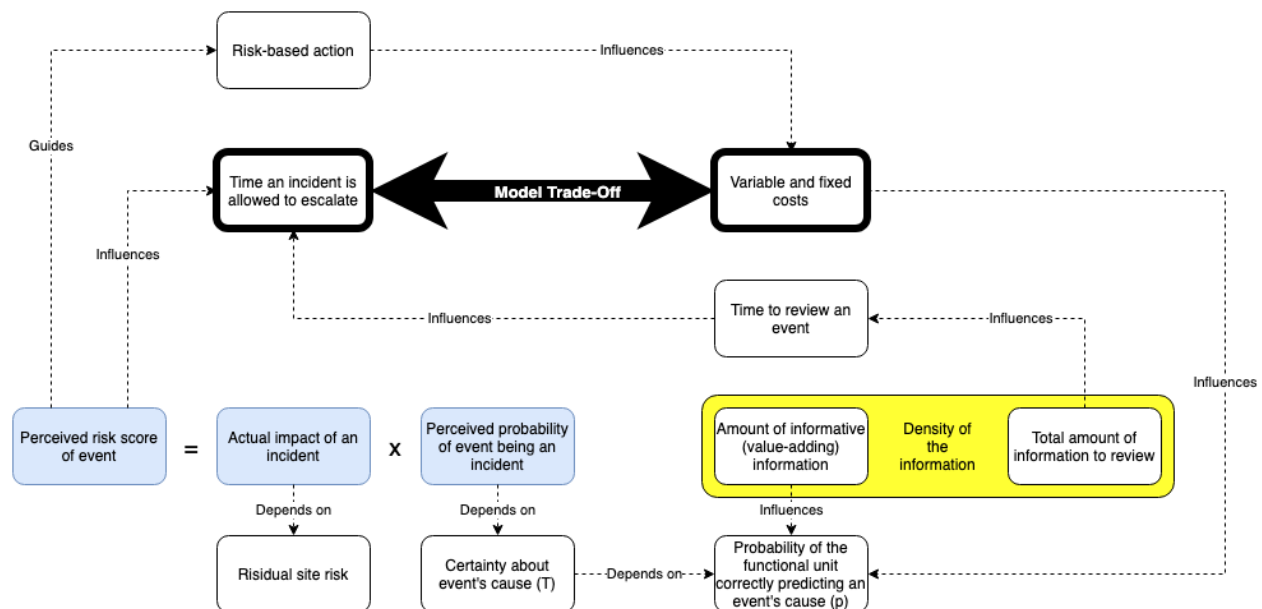


Figure 26: Density of informative information in bins emphasised in the model trade-off

By considering the definition of a bin and the model trade-off, it is clear that in the control room setting event indicators are favourable and noise is unfavourable. This is because only event

indicators contribute to effective decision-making. It is therefore advantageous to obtain high indicator-to-noise ratios in bins, as more certainty about an event's cause is gained in the same timeframe if bins are more informative. Similar to the signal-to-noise ratio, in the case of data sent across the channels between distributed sites and the control room, some data does not carry actual information and may be considered noise. Thus, the information-to-noise ratio of a section of data is defined as the ratio of informative data to noise in the section of data.

$$\text{Information density} = \frac{(\text{Valuable information})}{(\text{Valuable information}) + (\text{Non - valuable information})} \quad (17)$$

The density of data can therefore be changed by either increasing the amount of valuable information, or decreasing the amount of non-valuable information, or a combination of both, thus:

$$\begin{aligned} f(n) &= \text{information density of bin } n \\ &= \frac{(\text{Number of event indicators in bin } n)}{(\text{Number of event indicators in bin } n) + (\text{Number of noise indicators in bin } n)} \end{aligned} \quad (18)$$

The number of event indicators may be the number of informative frames in the case of a CCTV system, the number of informative data packets in the case of intrusion detection systems (IDS), percentages, or any other unit, as long as the units of event indicators and the units of noise are of the same type. The units will then cancel out and the resulting density of informative data would be a dimensionless, real value.

A *perfect input device* is the term used in this research for an input device that consistently produces a bin that consists of 100% event indicators, and therefore 0% noise. An example of this would be a video clip where 100% of the video clip aids in certainty about the event's cause. Devices producing bins of 100% event indicators consistently do not exist at the time of this research, but this hypothetical device is used for calculation purposes. The density of event indicators of such a device is thus one (1), or 100%.

In this research, a *perfect functional unit* is considered to be a functional unit that correctly and consistently interprets 100% of a bin. These functional units do not exist either, as human error is ever-present in operators, and AI currently lacks perception and the ability to accurately determine intentions. In this context, the combination of a perfect input device and a perfect functional unit will result in the perfect functional unit to be 100% certain about the event's cause with the first

bin pulled from the perfect input device, given that the bin is of sufficient size for the perfect functional unit to comprehend the context of the event. Consider the more elaborated version of the aforementioned p_{fu} in the contexts of the bin approach:

$$p_{fu}(n) = \frac{i_i(n)}{i_R(n)} \quad (19)$$

where:

$$\text{For } p < p_D: T = \frac{p - p_D}{p_D} \quad (20)$$

$$p_{fu}(n) = \quad (21)$$

probability of the current functional unit correctly declaring the event's cause by bin n.

$$i_i(n) = \text{cumulative amount of valuable information available by bin } n. \quad (22)$$

$$i_R(n) = \text{amount of informative information required for the current functional unit} \quad (23)$$

to be 100% certain about an event's cause.

The cumulative amount of informative information by *bin n* would then be the sum of all the available informative information gained by the bins up until *bin n*. Consider the following expression:

$$i_i(n) = \sum_1^k f(n) \quad (24)$$

where:

$$f(1) + f(2) + \dots + f(k-1) + f(k) \leq 1$$

The variable k represents the total number of bins required to gain enough certainty to classify the risk of an event. This value will naturally differ between the investigations of events, as the densities of the bins are random, and different numbers of bins would be required to investigate each event. In the case of a perfect input device, k will be 1, as only one bin is required for a perfect functional unit to be 100% certain about an event's cause since it is assumed to be of sufficient size for the perfect functional unit to understand the context of the event.

The rudimentary concept of the Monte Carlo theorem is to use randomness to solve problems by generating an acceptably accurate estimation from a sufficient number of simulation runs. From historical industry data, it is possible to identify the probability distribution ranges in which both the number of event indicators and the bin-size are likely to materialise for each input device. Therefore, given that the precedent ranges are identified for all the input device types in a control room setting, random samples within these ranges, packed inside of bins, would be a reasonable estimation of the efficacy of the input device system over time. Moreover, the intrinsic functionalities of the input devices installed on all the loosely integrated sites, will, over time, along with the inherent operations of the control room, be illustrative of the control room's nature.

With the bin approach, it is possible to both simulate the short-term randomness – which will be different each day – and the long term emerging estimate of what this randomness implies. As a result, the rate at which certainty is gained by a control room would be different for every event, and some events will be resolved quicker by the control room than others.

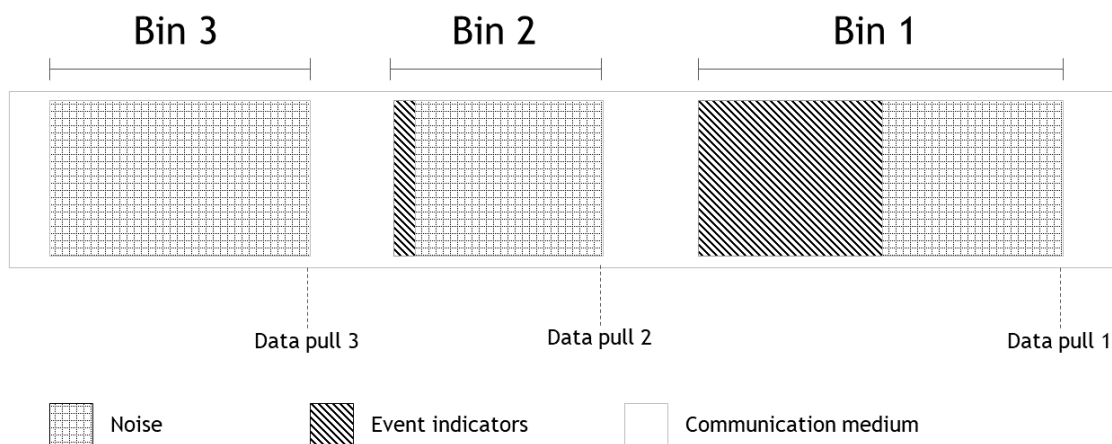


Figure 27: Bin illustration

Figure 27 illustrates the bin-concept for a scenario where data is obtained from a site three times in different instances. The bins are of varying sizes since different amounts of data are typically obtained. The bins are transmitted over a channel from the site to the control room. The density of informative data inside bins of various sizes is dependent on the indicator-to-noise ratio.

Bin 1 contains around 50% event indicators and it is the most significant contributor to certainty out of the three bins. The second bin contains a lower indicator-to-noise ratio than the first. Nevertheless, it marginally contributed to the certainty that the control room has about the event's cause. The third bin exclusively contains noise and contributes nothing toward the certainty that operators have on the cause of the event.

In line with decision theory in a data channel, with fewer event indicators and more noise, the chance of making an incorrect decision is high, more event indicators are required, and more time is spent on obtaining such indicators. This is undesirable, and one would want an Industry 4.0 technology to provide more event indicators and less noise, hence being more informative. Informativity is thus defined in this research as the information-to-noise ratio per timeframe, where a highly informative technology will provide a relatively large amount of valuable information in a short period, with little or no noise.

Due to the loosely integrated nature of the security control room setting and the vast number of sites served, events that arrive at the control room come from a wide array of geographic locations. Many sites have areas more sensitive than others; this may be where valuable items are stored in the case of a security control room setting, or in the case of a traffic control room setting, an area on the street where accidents are prone to occur. If an alarm originated at a sensitive area after hours, it is responded to as quickly as possible and no revision is done inside of the control room before field workers are dispatched.

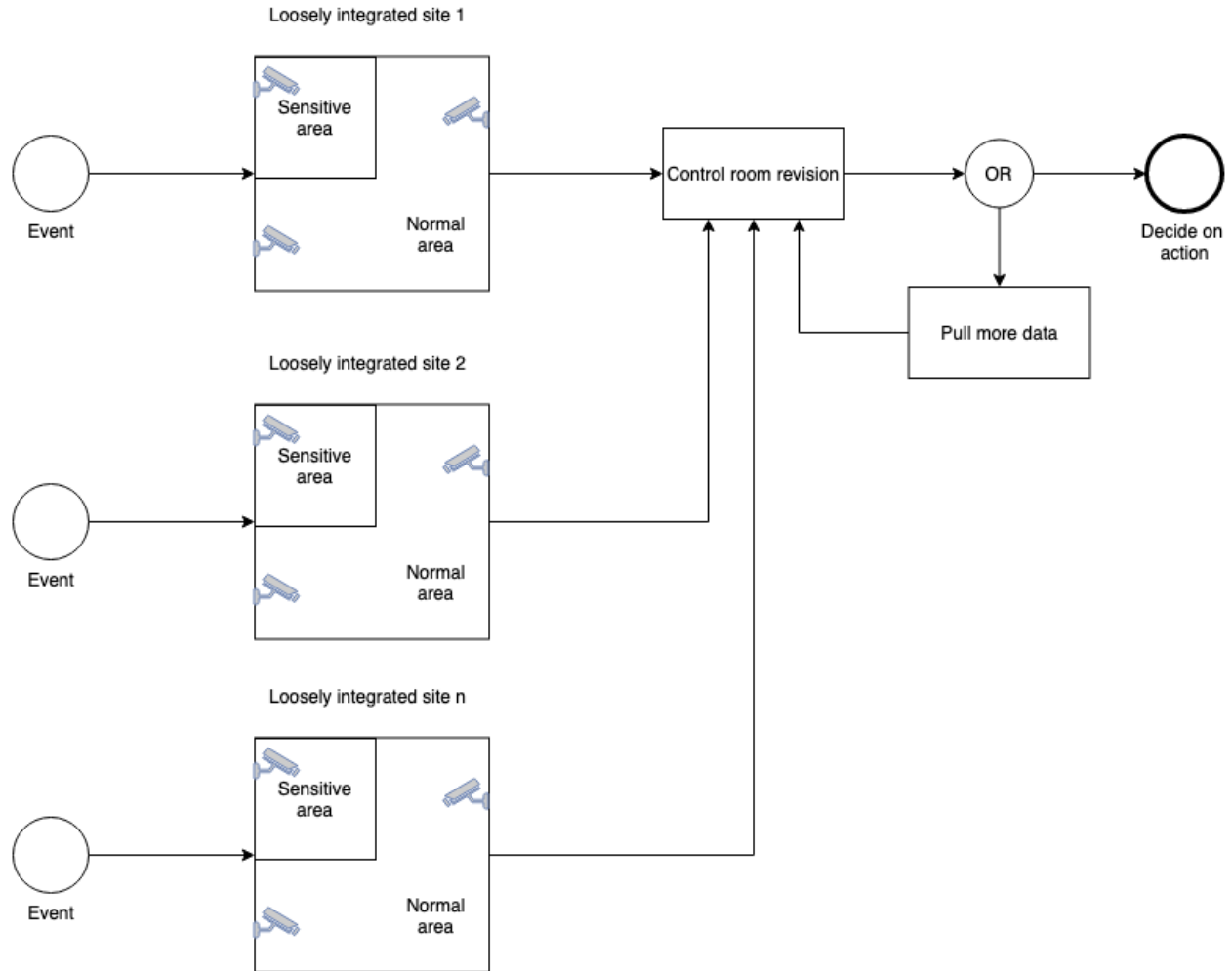


Figure 28: Sensitive and normal areas of a loosely integrated security control room

4.4 Analysis and modelling process

The process used to develop and compare models is presented as a flowchart in the following section. Due to the semi-quantitative nature of this research, the methodology was developed to ensure that results emerge which can be compared in a *relativistic* manner. The significance of a relativistic comparison is that given the same inputs, minor faults in data accuracy and parameter estimation are largely alleviated [1]. Note should be taken that a comparison must be made between a *current* loosely integrated control room setting and a *projected* loosely integrated control room setting, which is *relativistic* in nature.

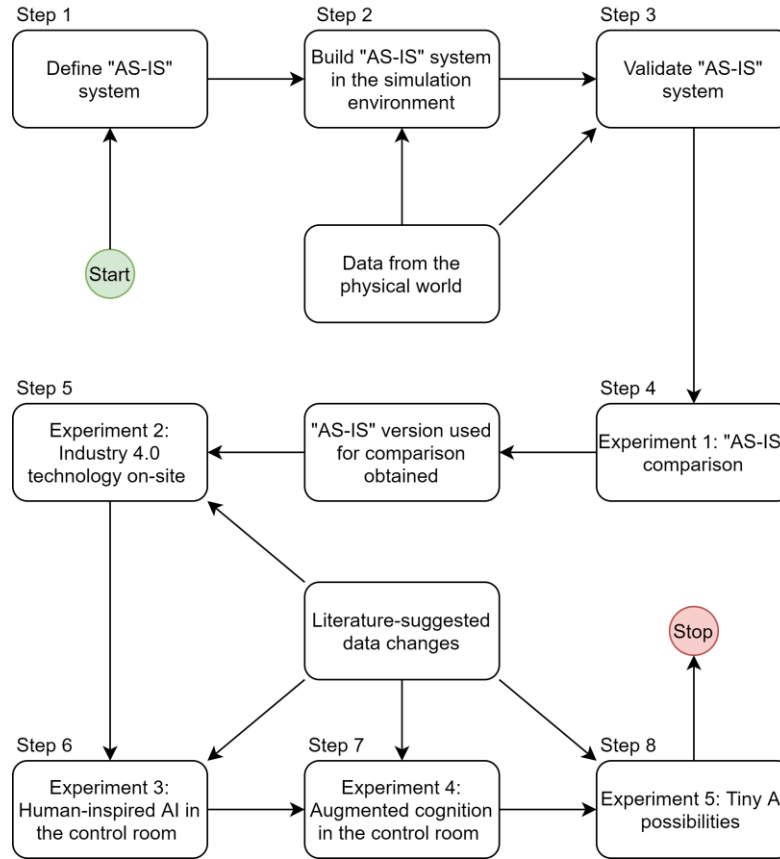


Figure 29: Flowchart of the analysis and modelling process

The flowchart for the analysis and modelling process is illustrated in figure 29. Steps 1 through 3 will be done in chapter 4 and the remainder of the steps (experiments) will be conducted separately in chapter 5. The following section describes the flowchart of the investigation methodology.

The generalised “AS-IS” model’s operational architecture - specifically the event response process - will be defined through observations of the physical loosely integrated security control room. Historical data from a real-world control room will be used to build the simulation model of the “AS-IS” system and to validate it.

Event-related logic, such as routing logic and stack-handling logic vary between control rooms and there is no standardised, “cookie-cutter”, event-related logic in control rooms. Experiment 1 will be conducted to analyse event-related logic. It is, however, impractical to consider all the event routing options ever created, since it is usually tailored for the specific control room system. Rather, typical routing options in control rooms are considered and experimented with within the

simulation model. From this analysis, an event-related logic system will be identified and implemented in the simulation model, which will stay unchanged throughout all experiments to ensure that a good event-related logic system is used and that no bias is present between investigations. The model will be considered representative of a loosely integrated security control room in the industry after experiment 1 is successfully conducted and the system is validated with industry data. By this point, any alterations to variables in the model will indicate what may happen in the physical environment should these variables be altered.

This research focusses on the entire control room system, not solely on the control room. Hence, experiment 2 will consider the impact of industry 4.0 technologies on the input devices on-site, with no changes to the control room itself. The bin-concept will be portrayed in this experiment to conceptualise the impact intelligent technologies on-site may have on the entire system. This experiment will materialise in the form of a sensitivity analysis. Experiment 3 will focus purely on the control room, and no alterations will be made on the sites. In this experiment, the impact of human-inspired AI on the system's operations will be investigated. This experiment will transpire in the form of a literature-inspired sensitivity analysis.

Experiment 4 will consider the augmentation of humans in the control room. An analysis will be done to conceptualise the effect that augmented cognition may have on the control room system, and this experiment will also transpire in the form of a literature-inspired sensitivity analysis. Changes will be made to functional units inside of the control room. No further changes will be made to the other parts of the system in experiment 4. Finally, an experiment will be done by considering Tiny AI in the control room system. Very little literature is available on Tiny AI, however, it seems to be relevant and suitable in the control room setting. Therefore, a rather speculative analysis will be done in experiment 5 to provoke future researchers to perform in-depth studies on Tiny AI when more literature is available. The changes will primarily be made at the sites in this experiment.

4.5 The “AS-IS” system

4.5.1 Step 1: Define the “AS-IS” system

It was mentioned in Chapter 3 that loosely integrated control rooms serving a large number of sites are critically dependent on alarms since the emphasis of these control rooms is on reaction. Nevertheless, the proactive factor cannot be entirely excluded, as it is a notable factor in a security control room. Although the task of abnormality detection is mostly performed by the input devices

Page | 67

on-site, individuals can also contact a site before, during or after an incident, and these individuals cannot be excluded from the control room system.

Staff are on-site during business hours, and this is the only time they can be contacted to provide the control room with clarity on the remote on-site events. After hours, the control room must identify the cause of an alarm without any physical presence on-site. If a staff member informs the control room about an attack, the perceived risk factor would immediately be pushed into the intolerable region and the event will be responded to. It is therefore assumed that an event can be raised by either detection devices (reactive) or staff (proactive or reactive).

The number of expected events may differ between business and after hours depending on the control room setting. Historically, however, data confirmed that, in the setting evaluated in this research, no significant difference was found regarding the number of events during business hours and after hours. Therefore, for this research, the number of events to be simulated would be uniform over all the hours of the day.

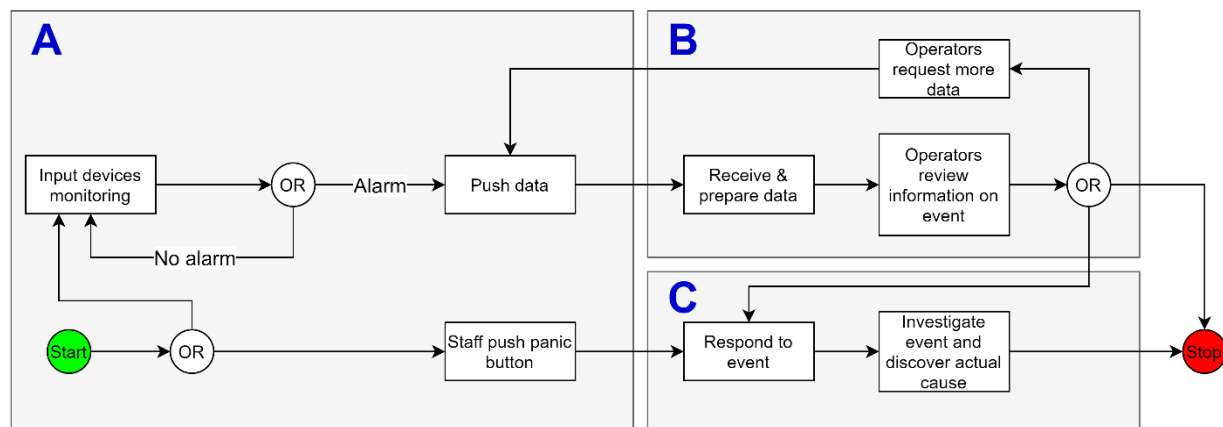


Figure 30: Derived event management flowchart for the loosely integrated security control room setting

The operational flow of a loosely integrated security control room system can be divided into three sections (A, B, and C) as shown in figure 30, namely:

- A. A site or sites;
- B. A Control room;
- C. The field workers.

If a monitoring device signals an alarm, data about the event that caused the alarm is pushed over a digital communication medium to the control room. The data is converted into information and once ready, sent to a functional unit based on a predetermined routing logic. The routing logic

differs between control rooms. However, two popular routing options are used to send information about the event to functional units. These include a *random routing* approach and a *balanced resource utilisation* approach [70]. The random routing approach routes information about the event to a random functional unit in the control room. The balanced resource utilisation approach navigates information about the event to the functional unit with the least number of events waiting for its attention, thereby balancing the processing power of the functional units. Once information about an event arrives at a functional unit, the information is processed and mainly guided by standard operating procedures (SOPs).

When an alarm is signalled by an input device during business hours, it is typically “staff not following procedures” which results in an alarm being triggered accidentally. This was found when previous analyses were conducted. Furthermore, panic buttons are installed on-site and if one is pushed, the reaction team is sent out to the site immediately, bypassing control room revision. SOPs typically differ between control rooms and are set up to suit a specific control room niche. Nevertheless, there is an overlapping of some of the main SOP-functions of various loosely integrated security control rooms. Figure 31 contains a simple, generic SOP which was derived from actual, more detailed security control room SOPs.

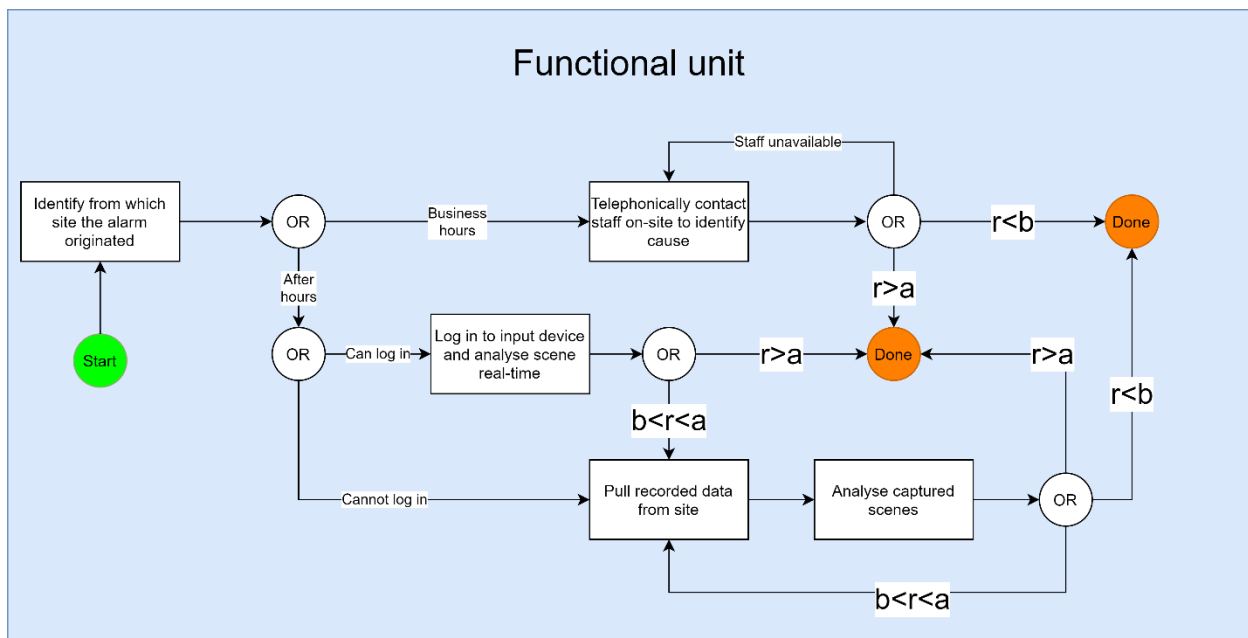


Figure 31: Generic alarm-handling SOP for a functional unit.

In the “AS-IS” model, human operators are considered the functional units. The task of identifying from which site an alarm generated is already partially automated, as it is not unique, fairly

simplistic and repetitive. In practice, when an alarm is triggered, the operator can, with little delay, view the alarm on-screen. It is then actioned and information is displayed regarding which site the alarm was triggered on, and in which area a specific alarm had been triggered. Alarms are frequently triggered, resulting in data about events from various geographic locations arriving at the control room. The operators can shuffle through the alarms routed to them – now waiting on their action stacks - and view details about them.

If an event materialises during business hours, the operator contacts staff on-site to determine whether it is a false alarm or an actual incident. If the staff on-site are unavailable, the attempt to contact them telephonically is reiterated. If a sufficient amount of time has passed, or if the operator notes suspicious behaviour when a staff member is indeed reached, the perceived risk score is considered intolerable and the task force is dispatched. However, if the staff on-site confirms a false alarm and no suspicious behaviour is recognised by the operator, the event is dismissed as a false alarm.

If an event occurs after hours, staff are typically not on-site and reaching them telephonically would be of no decision-supporting value. Therefore, after assessing where an alarm occurred, the operator identifies which devices are available on-site. If a device is available with live streaming such as CCTV, it is logged into and the scene is analysed in real-time. This stage is susceptible to the impact of interruptions, and distractions may cause an operator to miss a potentially determinant scene. Furthermore, if many alarms are waiting on the stack of an operator, the live streaming is delayed at the crucial moments on-site. This is where prioritisation stack handling comes into play.

To reiterate, prioritisation stack handling is an element on which control rooms have different opinions. Therefore, in the “AS-IS” model, two popular stack handling options will be included, namely *first in first out (FIFO)*, and *fast-tracking* an alarm by priority. FIFO is when the alarms are processed in order of arrival [71]. In other words, if alarm one arrived at the control room before alarm two, alarm one will be processed first.

In the case of no live-streaming devices installed on-site, or if live-streaming was available but didn't contribute to enough certainty to be able to determine the cause of the event, recorded data around the time of the event is pulled. The data pulled from the site must now be analysed by the operator similarly to how the live streaming is analysed. If more certainty is required to identify the cause of the event, more information is pulled. This, however, results in the event spending more

time in the system than needed, potentially contributing to incident escalation if the event is an incident. If a set amount of time has passed, and the cause of the event had not been identified, it is responded to.

If the event is perceived intolerable, the task force is dispatched to the site where the event has occurred. The event is then further investigated to identify what its cause has been, to update the business intelligence for future use. Report data is also updated to represent proof of what happened on the site, to aid in further prosecution and close-out. The detailed investigation process is not considered in the simulation model, as it is not on the critical path of averting incident escalation.

An in-depth cognitive analysis will not be done on operators in this research. Nevertheless, due to the semi-quantitative nature of this research, numerical values will be assigned to operators to account for the impact of different levels of operator ability. Table 6 shows the classes of operators and their associated factors.

Table 6: Volatility table based on the operator class

Operator risk level	Operator class	The relative amount of information needed (i_R)	Average bin processing time in a triangular setup	$p_{fu}(n)$
High	1	0.95	$bs * tn * \frac{1}{1 - i_R}$	$\frac{i_i(n)}{i_R}$
Medium	3	0.65	$bs * tn * \frac{1}{1 - i_R}$	$\frac{i_i(n)}{i_R}$
Low	5	0.25	$bs * tn * \frac{1}{1 - i_R}$	$\frac{i_i(n)}{i_R}$

Note that:

$$bs = \text{bin size in the form of items in a chosen unit} \quad (25)$$

$$tn = \text{time needed for a perfect functional unit to revise a single item in the bin} \quad (26)$$

Therefore, the model takes into account that riskier operators with a lower level of ability will have a lower probability of correctly identifying the cause of an alarm by bin n . Also, riskier operators with less experience and a lower level of knowledge and ability will take longer to process bins. Besides, the size of the bin will impact the time it takes for the functional unit to process a specific bin type.

Figure 32 showcases the architecture of a typical site (A), and a control room (B). It should be noted that the number and scale of elements such as input devices and operators are for illustration purposes only. The following discussion defines the real-world model from which the abstracted model was derived – this is done to validate the functional definition of the abstracted model as applied in simulations.

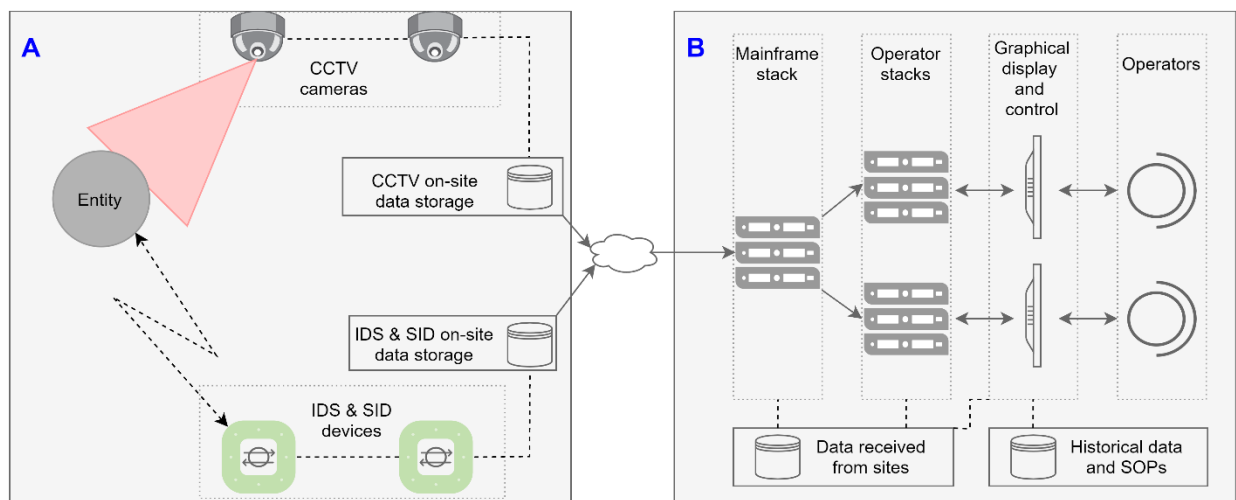


Figure 32: Architecture of a loosely integrated security control room system

Finite state machines (FSMs) are effective when abstracting a real-world model for simulation purposes. An FSM for the simulation model is defined and displayed in figure 33 to illustrate the finite number of stages an event can be in during its lifespan in the control room system. This will partially guide the construction of the model in the simulation environment.

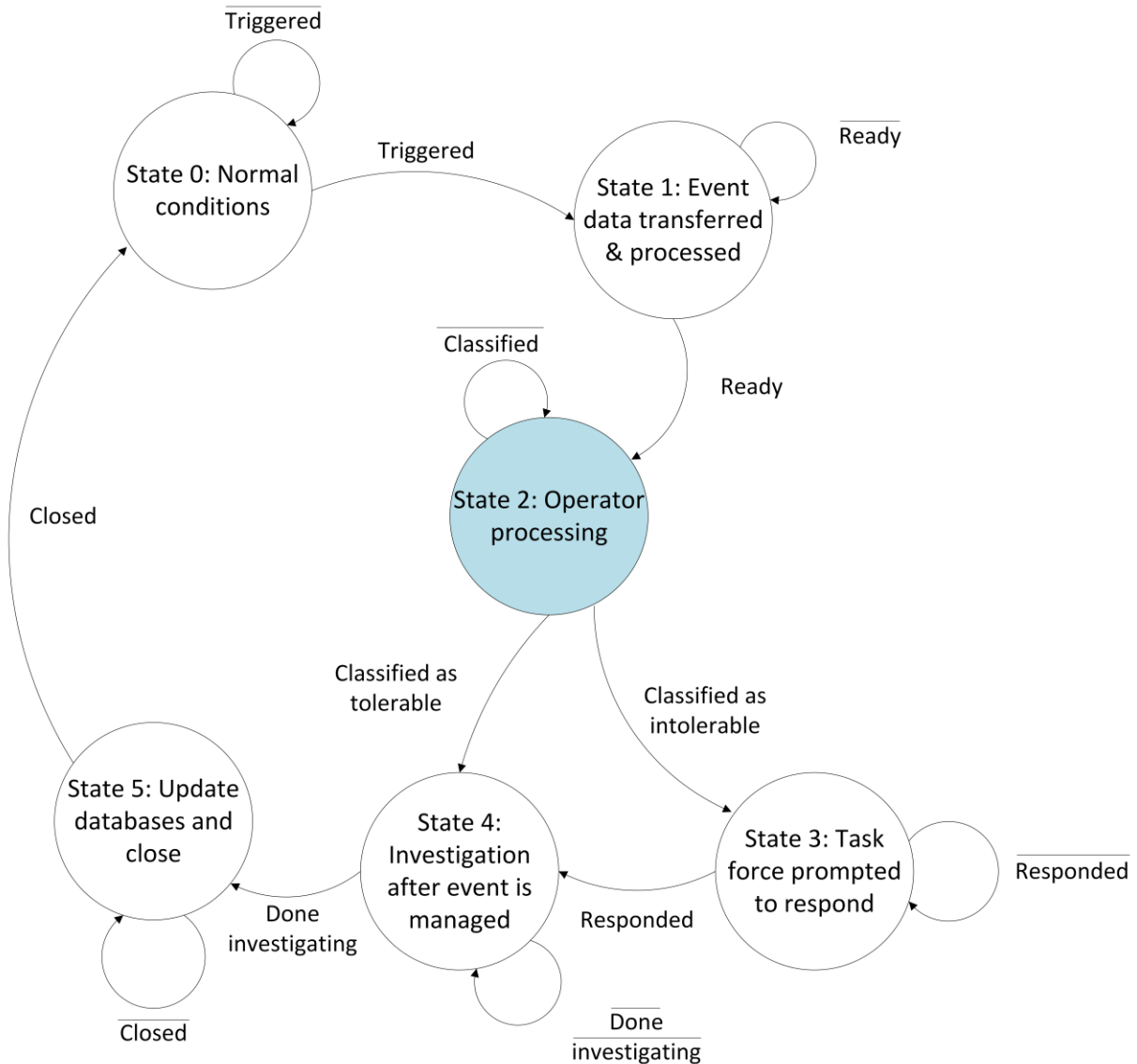


Figure 33: Finite state machine for the attention of alarms

State 0: The site is monitored until an input device or staff on-site triggers an alarm. In this state, the event had not occurred yet and an alarm had not yet been triggered. The alarm remains in this state until an event occurs, which results in an alarm being triggered and the alarm commencing to State 1 of the FSM.

State 1: An alarm is triggered by an event and data moves over the communication medium which is decoded at the control room into a format that the functional units understand. The alarm stays in this state of decoding until it is converted into information and ready for an operator to view. This generally happens very quickly.

State 2: The alarm is now on the stack of the operator, where it is pulled with predetermined stack-handling logic. When the alarm finally has the attention of the operator, the generic functional unit SOP presented in figure 31 is followed. It is in this state of processing and gaining more information that the alarm stays until it is perceived to be either a tolerable or an intolerable risk.

State 3: If the risk of the event is perceived to be intolerable, the task force team is dispatched and the attention of the alarm had moved from a processing state to a reaction state.

State 4: The attention of the alarm now shifts to the investigation of what caused it in the first place, and why it was allowed to happen, as precautions to avert false alarms and incidents are regularly implemented and improved. It should be noted that this happens after the event had been processed by the operators and action of some sort (reacting or ignoring) had taken place.

State 5: The databases are updated with what has been unveiled in the investigation of the event. When this is completed, the alarm is closed and it exits the system.

It is important to note that in the simulation environment, many alarms are active, and these alarms can be in any of the five states during the simulation run. Moreover, the time alarms spend in the various states will be unique, since both the events and the data available on the events are unique.

4.5.2 Step 2: Build the “AS-IS” system in the simulation environment

In step 1, both the layout of the control room and the operational states of events had been elucidated. It is now needed to translate the defined “AS-IS” system into the simulation environment for validation and experimentation purposes.

Due to the complex nature of a loosely integrated control room, a mechanism is needed to keep track of many events and their aspects simultaneously. This is achieved by defining two distinct event types (referred to as *entities* in SIMIO), namely True Positives and False Positives. Incidents are represented by True Positives and false alarms are represented by False Positives.

At the sources, clones of both True Positives and False Positives are created and they flow through the system where definitions in the systems influence their flow and associated variables. State variables and many other properties can be allocated to each of the event types, which is then inherited by the clones of the event types. This permits each clone of an event type to possess these properties, which can contain unique values. By creating clones of the two event

types, it is possible to keep track of any property of any event that occurs on any site throughout its entire life cycle. Figure 34 illustrates the two event types used in the simulation model.



Figure 34: Event types

An important state variable assigned to both of the event types is “certainty”. This variable is representative of the certainty an operator has about the cause of an event, and it is based on the *perception* of an operator. Thus, in the simulation environment, an event may be interpreted correctly or incorrectly, and only once an event is investigated after a decision has been made, will it be apparent whether it was interpreted correctly or not. For instance, an actual incident may be perceived as an incident, or it may be interpreted incorrectly as a false alarm. Moreover, an actual false alarm may be correctly perceived as a false alarm, or it may be incorrectly perceived as an incident. This approach ensures that the simulation model accounts for events such as false negatives, which are actual incidents incorrectly interpreted as false alarms.

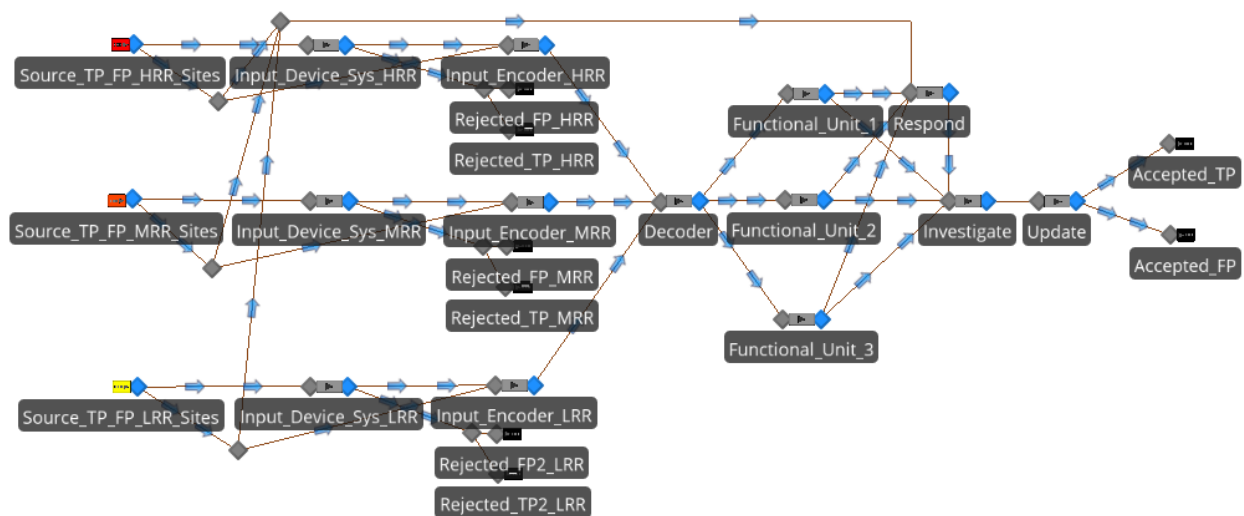


Figure 35: Loosely integrated security control room system SIMIO model

Figure 35 shows a screenshot of the actual loosely integrated security control room in the SIMIO simulation environment. The following section elaborates on what happens in the simulation

model and it will be compared throughout with occurrences in the real-world as partial validation. All the sites served by the generic control room are representative of either a low, a medium, or a high residual risk class. Each of the three sources in the model represents a residual risk class, and the number of events originating at each source is scaled to match the number of sites represented in a source.

The number of sites served by control rooms differs since clients come and go and the scales of operations vary between companies. It would be impractical to simulate a large, real-world control room exactly as it is in the real-world as a large number of operators and sites will have to be included in the model. The simulation model was scaled, with no functional or performance loss, so that three operators are included in the control room serving 2000 sites in total. The ratio of operators per site was obtained from a real-world control room configuration.

Due to the uniqueness of sites, it is difficult to classify sites in a specific residual risk category. Many factors influence the residual risk of the site such as the geographic location. Geographic location, however, is debatable too. For example, a site inside of a shopping mall would naturally be of lower risk than a site just outside of the same shopping mall. Also, some of the sites are randomly targeted more frequently than others, since a syndicate may operate in a certain area temporarily. Actual field data provided reasonable estimations of ratios, with estimated percentages of residual site risks obtained from a real-world, functional control as follows:

- Approximately 40% low residual risk;
- Approximately 10% medium residual risk;
- Approximately 50% high residual risk.

Therefore, the events originating at roughly 800 low residual risk sites, 200 medium residual risk sites, and 1000 high residual risk sites are simulated by the three sources. These events are then handled by the three functional units inside of the control room. This ensures that a realistic number of events is generated at the relevant residual risk sites, without the need to create each of the 2000 sites individually. All events have a state variable attached describing from which residual risk site the event had originated. The number of events occurring annually varies. For this research, events are stochastically created to be either a True Positive or a False Positive based on historical data.

Table 7: Residual site risk classes

Site residual risk level	Class	Expected impact class (I): $\frac{5}{Class}$	r
High	1	$\frac{5}{1}$	$I \times P$
Medium	3	$\frac{5}{3}$	$I \times P$
Low	5	$\frac{5}{5}$	$I \times P$

Table 7 showcases the semi-quantitative residual risk levels of sites. In the model, sites with a larger residual risk are expected to have a greater impact should an incident occur on that site. Also, the perceived risk factor will be larger for the same certainty of an event's cause for these sites (from the perspective of an operator) and the same probability of the operator correctly declaring the event's cause (from the perspective of the managers of the control room).

If it is "after hours" in the simulation model, the events occurring flows toward an input device system on the site on which it had originated. The logical length of the path between a source and an input device system is zero since an event is only an event once it has been detected, and it is only detected once it had happened. Therefore, even though there is a visual starting point and a detection point of an event in the simulation environment, the event occurrence and event detection are virtually simultaneous. For example, consider a window breaking, the event is the window breaking and the detection of the event may be an input device recognising the sound of glass shattering.

If the simulation model detects that the date and time in the model are corresponding with the predefined business hours, an event may either be a panic button pushed, a robbery, or a staff member that accidentally triggered an alarm. In the case of a panic button, the events flow directly to the *respond* task. However, if an alarm is triggered, the control room will have to review the event. Panic buttons are sometimes pushed accidentally, and although scarce, this is accounted for. If an alarm is triggered during business hours, it is typically in the morning and late afternoon

when staff arrive on-site or leave for home. It can, however, be a robbery and a panic button may not have been reached in time, which is why the control room must confirm with staff on-site.

The input device systems on-site may accept or reject events. More specifically, it may detect an event and notify the control room, or it may not detect an event and the control room will not be notified. It is advantageous if the input device system detects an incident, as the control room will be notified and hopefully perceive the event as an incident. Also, it is favourable if a false alarm is rejected by the input device system since it strains the resources in the control room if it is accepted. However, if an incident is rejected by the detection device, the control room is not notified and the event will escalate indefinitely.

From historical data, it is found that, on average, merely 0.3% of events detected by input devices and sent to the control room are incidents. Therefore, the overwhelming majority of events arriving at the control room are indeed false positives at 99.7%. If the same quality equipment is assumed over all the sites, the number of false alarms would be similar over sites of varying residual risk. It is, however, a fact that higher residual risk sites are more prone to incidents than lower residual risk sites. To compensate for this fact in the simulation model, high, medium, and low residual risk sites are assumed to produce 0.5%, 0.3%, and 0.1% incidents respectively.

In the timeframe of a year, the control room in question experienced 1 678 508 events. Approximately 41000 of these events were manually induced for testing purposes, and will therefore not be included in the analysis, as the operators are informed about these events and the cause of the alarm needn't be determined. This number is scaled to an average of 223 745 events per year for the simulation model to ensure that the number of events managed by the three operators in the model are realistic and comparable to the physical world. Therefore, events will arrive at the control room at an average of one event every 2.35 minutes. Events, however, are unique and will not necessarily arrive at the control room every 2.35 minutes. Rather, the average time over long simulation runs should regress toward an average event arrival time of 2.35 minutes.

Since it is considered that the number of sites over varying residual risks is not the same – the three sources cannot produce events at the same frequency. Of the 223 745 events that arrive at the control room, approximately 111 873 is expected to originate on high-risk sites, 22 375 is expected to originate on medium residual risk sites, and 89 498 is expected to originate on low residual risk sites. These values are obtained through the weights of sites indicated earlier and

translate to one event arriving at the control room every 0.426 minutes on average. More specifically, events will arrive at the control room every 0.07833 minutes (4.7 seconds), 0.39167 minutes (23.5 seconds), and 0.08617 minutes (5.17 seconds) from the high, medium, and low residual risk sites on average, respectively.

At the input devices in the simulation model, 100% of the false alarms generated at the sources will be accepted. This is because a false alarm is only a false alarm if it has indeed been detected by the input device. The same is not true for an incident, as an incident may be detected or missed. Therefore, an estimated acceptance weight by the input devices of 99% is assigned for incidents, as incidents are rarely missed.

The number of expected events arriving at the control room cannot be the same as the number of events occurring on-site, since some incidents are missed. This is compensated for in the model to ensure that at least 99% of the incidents generated at the sources in the model equals the approximate numbers recorded at the control room.

The sensitive areas of the site are commonly higher risk and they are often surrounded by more physical barriers than lower-risk areas. Therefore, alarms are less frequent in these areas as opposed to lower-risk areas. Sites of higher residual risk do experience more attacks in sensitive areas relative to sites of lower residual risk, not only because more attacks are present, but because more treasury is typically available on these sites. The percentages of events occurring in sensitive areas of the sites in the simulation model are:

- Approximately 5% for low residual risk sites;
- Approximately 7.5% for medium residual risk sites;
- Approximately 10% for high residual risk sites.

Due to the uniform nature of the sources in the simulation environment, an assumption is made that the same input device systems are installed on all the sites of a given residual risk level. The input device systems on a site can be one of many different systems. For simplicity and practicality reasons, three common input device systems are identified and implemented in the model, namely:

- A basic, high-quality intrusion detection system (IDS) that provides no form of visualisation;
- A basic, high-quality IDS combined with a basic, non-intelligent CCTV system;

- A basic, high-quality IDS combined with basic snapshot intrusion detection (SID). Snapshot intrusion detection works by taking a few snapshots at the moment of anomaly detection.

Also, it is assumed that the ID system initially triggers an alarm and all the input device systems have the same quality IDS triggering alarms. The cost to acquire and install an input device system typically varies, as the quality of systems and labour costs are not uniform. Costs shown here were recorded at the time of conducting this research, and actual costs may be different at a later point in time. Currently, a high-quality IDS and CCTV system combination on an average-size site is estimated to cost about R200 000 including installation costs. A high-quality IDS is estimated to cost around R50 000 and an SID and IDS combination cost around R60 000. Recurring monthly costs assumed in the model include a monitoring fee of R400 per site and maintenance cost of 7.5% of the installation and system costs.

If an input device detects an event in the simulation model, a Monte Carlo informativity sample is created by randomly generating a bin-size and several event indicators within their respective probability distributions. This results in randomly distributed information-to-noise ratios in the bins sent to the control room from the sites every time an event is detected or if more data is pulled. This ensures that the unique and random nature of events is taken into account in the simulation model.

The units of the bin sizes of the combination of IDS and SID and the combination of IDS and CCTV are both measured in frames. The frames or “snapshots” an IDS and SID combination generates are naturally unique and numbers can range from one to one hundred snapshots depending on the activities of attackers on site. It is, however, more common for the IDS and SID combination to produce a lower number of frames than CCTV systems. Therefore, a triangular distribution is implemented in the model with the values (1,6,100) as the number of frames. It should be noted that the first value is the minimum, the second value is the mean, and the third value is the maximum.

The range of event indicators is also unique. With non-intelligent devices, it is difficult to obtain a high number of event indicators. For the IDS and SID combination, a uniform percentage between 10% and 20% is simulated as event indicators for every event.

Since the bin-sizes for IDS and CCTV combinations are unique, it also follows a triangular distribution to ensure outliers are accounted for. The size of each bin would be larger for the IDS and CCTV combination than that of the IDS and SID combination as single photo-frames (IDS and SID) are compared to many frames (IDS and CCTV) in video format. The triangular values for the IDS and CCTV combination are, therefore (100, 150, 300). The IDS and CCTV combination typically has a lower fraction of event indicators per bin, and therefore the percentage range of event indicators for each bin is 5%-10%.

The basic IDS produces no form of snapshot intrusion detection and primarily functions by sending “blind” alarm signals to the control room. It is almost impossible to determine whether an alarm is an incident or a false alarm based on these signals alone. Where these signals have originated may suggest the movement of an object from one area to the next, which may indicate activity and movement on-site. Nevertheless, in general, control room operators cannot have complete certainty on what caused the event if only ID systems are installed on-site.

Thousands of signals may be received from a site for a given event, and the signal bin-size for the basic IDS in the simulation model is assumed to be of a uniform distribution between 1000 and 2000 signals. Also, since these systems are far less informative than IDS and SID combinations and IDS and CCTV combinations, an event indicator range of 0.1%-0.2% is chosen.

South Africa faces many challenges which directly influence the control room system, such as unstable electricity supply and network speed limitations. In this research, however, it is assumed that a stable electricity supply and good network speeds are present, to ensure that the results from this research are not skewed to only fit a South African context but to apply to a broader range of countries.

The accepted bins of information on the events are then encoded on-site and sent to the control room, each containing random densities of value-adding information. The event then flows over the communication medium to the control room where it is decoded into understandable terms for the revision of the functional units. The section between the encoders and the decoder in figure 35 is illustrative of the communication medium between the decentralised sites and the control room. This medium is typically the cloud or a cellular network.

When an abnormality is detected and an alarm is signalled in the simulation model, the first batch of valuable information on the given event - $i_i(1)$ - is sent to the control room. This is saved as a

state variable allocated to the event, which is then sent to a functional unit (in the case of the “AS-IS” model, an operator) by following predetermined routing logic.

When an event arrives at a functional unit in the simulation model, it interprets the available information about the event. The probability that the operator will correctly interpret the available information is subject to the cognitive ability and experience of an operator, as well as the information available on the event. The certainty that the control room has about the event’s cause is therefore determined by both the *amount of valuable information*, and the *ability of the functional unit*.

The functional unit follows a prescribed SOP to determine the cause of the event. SOPs are also highly detailed in practice, as they refer to specific units within the input device system. In the simulation model, the SOP is more generalised, but still sufficiently representative of the generic control room setting. In the physical world, it is critically important to follow a detailed SOP, however, in the simulation model (for relative comparison), it is assumed that a detailed SOP is followed which advises the functional unit on what to look for and how to look for it.

It is therefore not necessary to construct the entire, detailed SOP in the abstracted, generalised simulation model when it is accepted that these detailed tasks are executed in the generic SOP, and the influencing factors associated with these tasks are accounted for. It is therefore considered that the bins which are randomly generated are received from a carefully considered input device by following detailed SOP-task instructions, and associated processing and times are included. To accomplish this in the simulation environment, a processing logic flowchart had to be developed for the functional units. The processing logic flowchart follows in figure 36.

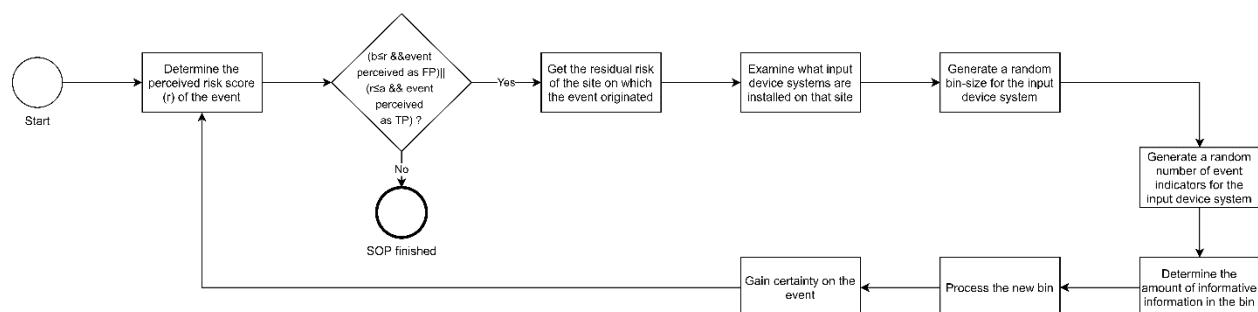


Figure 36: Functional unit processing logic flowchart

Firstly, the risk score (r) is determined once an event arrives at the functional unit in the simulation model. If r is in the undecided region, that is, the control room is not certain about the event’s

cause yet, the site from which the event originated is obtained. This is done by extracting the string “origin”-property from the event. The model then determines which input device systems are implemented on that site. With this knowledge, the random, realistic bin size is generated for the respective input device system on that site together with a random number of event indicators. With these variables, the density of value-adding information in the bin is determined. In the case of determining an estimation of the long-term efficacy of an input device, the bins needn’t be representative of the same event. The random density-samples will then over time provide the bin-density characteristic of the input device type it was drawn from.

The functional unit then interprets the bin to gain more certainty about the event’s cause. If the r -value of the event is still uncertain, the process is repeated, otherwise, the SOP is considered finished. This process is considered the simulation equivalent of a functional unit processing an event and pulling more data to decide on how to handle the event.

In some instances, not enough certainty is gained by the operators on the event that caused an alarm for a decision to be made on whether to respond or not. Nevertheless, the event cannot be left unattended and after a specified in-system allowable time, the event is responded to anyway. For the simulation model, based on control room data, the allowable time in the system is set to 30 minutes. Therefore, if the cause of an alarm is uncertain after 30 minutes, the task force is dispatched regardless of certainty.

If an incident is not detected by the input devices, the incident will in most cases escalate to the maximum possible damage. Therefore, a maximum escalation time is defined and added to the total escalation time in the simulation for all incidents missed by the input devices. In the simulation model, the maximum escalation time is set to one hour. In other words, if one hour has passed since an incident arrives on the site, the maximum possible damage is assumed to occur on the site.

The event is now categorised as either a tolerable or intolerable risk. Recall that both incidents and false alarms can be considered tolerable or intolerable, as it depends on the functional unit’s interpretation of the event. From the functional unit blocks in the SIMIO layout in figure 35, events in the simulation model considered intolerable move to the “Respond” processing block and events in the simulation model considered tolerable move directly to the “Investigate” processing block.

In the simulation model, a basic IDS is assumed to have the lowest percentage of correctly interpreted alarms, since there is no way to visually verify what the causes of alarms are. Therefore, the percentage of events correctly interpreted by the operators in the control room is set to 50%.

An IDS and CCTV combination will have a higher percentage of correctly interpreted alarms than the basic IDS, as a visual factor is included. However, as there are delays to receive bins (and therefore event indicators), some actions may be missed. In the simulation model, the percentage of events correctly interpreted for an IDS and CCTV combination is set to 85%.

Since the IDS and SID combination provides snapshot intrusion detection at the moment an event triggered an alarm, the cause of the event is more likely to be identified than the latter two systems. Thus the percentage of events correctly interpreted for the IDS and SID combination in the simulation model is set to 90%.

The percentages correctly interpreted are informed by control room classification and based on control room experience. The 50%-value for the basic IDS is considered an optimistic upper limit and the 90%-value for the IDS and SID combination is considered an optimistic lower limit. The 85%-value of the IDS and CCTV combination is considered an optimistic upper limit between the limits of the basic IDS and IDS and SID combination.

Responding to an event has financial implications, such as active working hours and travel costs of the workforce. In practice, the workforce can be either a third party company or a division of the parent company of the control room, or a combination of both. For practicality, the financial impact of responding to an event is determined in terms of *kilometres travelled* and *hours worked*. If a false alarm is incorrectly perceived as an incident, the task force will respond unnecessarily, wasting resources such as time, money and energy. However, if an incident is incorrectly perceived as a false alarm, the event is not responded to and an escalation of the event occurs, which has financial and non-tangible implications such as serious injury and death.

Taskforce units are mobile and they roam the general area of the sites they are allocated to respond to, and it is thus not practical to predict with precision how far the unit will travel to respond to an event. Also, due to the uniqueness of events, it is not practical to predict exactly how long the services of the task force will be required. Therefore, it is not feasible to assign exact values to the distance travelled and the time spent on a site. Thus, probability distributions are created

and random values are generated within these ranges every time a unit is prompted to respond. This creates realistic short-term randomness in the model together with good longer-term estimations. The distance a unit is expected to travel when responding is between 15km and 45km.

Physical barriers are one of the main causes of site-inspection delays by the task force, and the physical inspection time is estimated to be between 10 and 25 minutes on-site. Both the distance travelled and inspection time is randomly generated as a uniform distribution between these ranges. It is important to realise that there are not an unlimited number of task force units available, and their services may become *saturated*. It is therefore particularly important that false alarms are not responded to frequently, as the task force units may not be available to respond to actual incidents.

In the Simio simulation environment, it is possible to create *response variables*. These variables are defined to capture a specified output value of importance in the simulation environment. The two main response variables defined are also the two main trade-offs for the model, namely *incident escalation time* and *costs*. These response variables are the most important in the relativistic comparison between simulation models.

After responding to the event or not responding to it, some sort of investigation takes place. The time required to complete an investigation is also random due to the uniqueness of events. This investigation and database updating phases may take weeks to complete, and it is not on the critical path of incident escalation and it will therefore not be investigated in-depth in this research, since the scope of this research is only the management of events while its cause is uncertain.

4.5.3 Step 3: “AS-IS” model validation

To validate the simulation model and results, simulation runs were executed and the findings were compared with real-world data. Moreover, the functional flow and architecture of the simulated models were compared to the real-world model for verification purposes. The input data used in the simulation model were obtained from recorded real-world data and verified by industry experts.

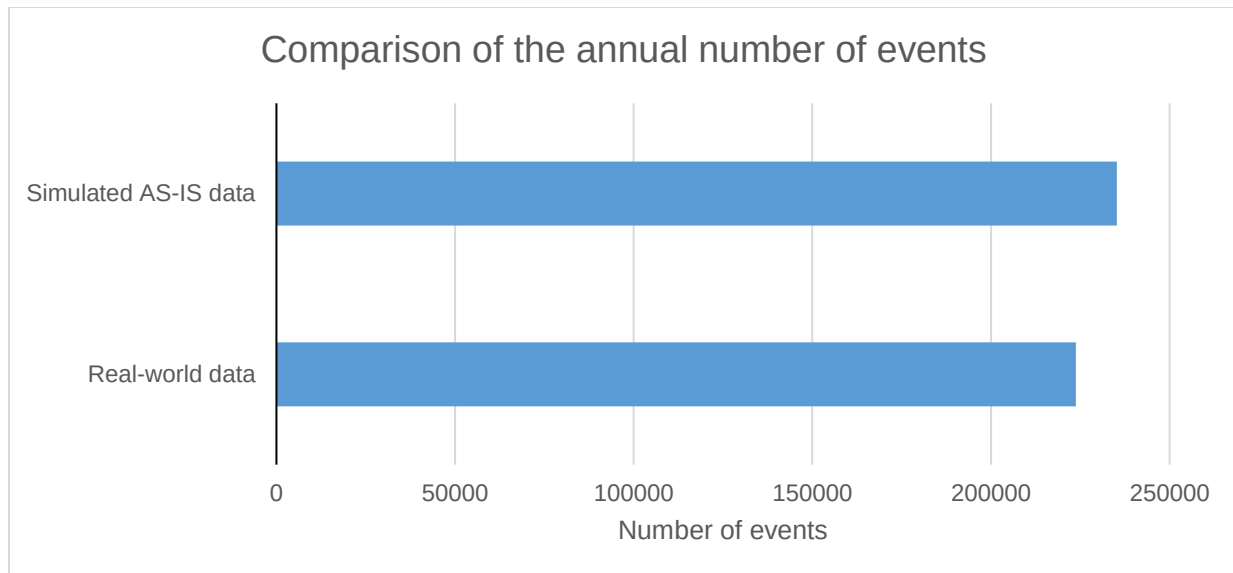


Figure 37: Comparison of the annual number of events for model validation

The number of events for the year 2019 of the physical world for a real-world control room is compared in figure 37 to the number of events ultimately generated by the simulation model in the timeframe of one year. As mentioned before, the actual number of events in the physical world was scaled to be representative of a control room with three operators. The number of events generated by the simulation model was slightly over 95% accurate relative to the number of events experienced in 2019 by the real-world control room. It should be noted that the number of events experienced in the physical world varies annually, and the above comparison was found reasonably representative of real-world numbers.

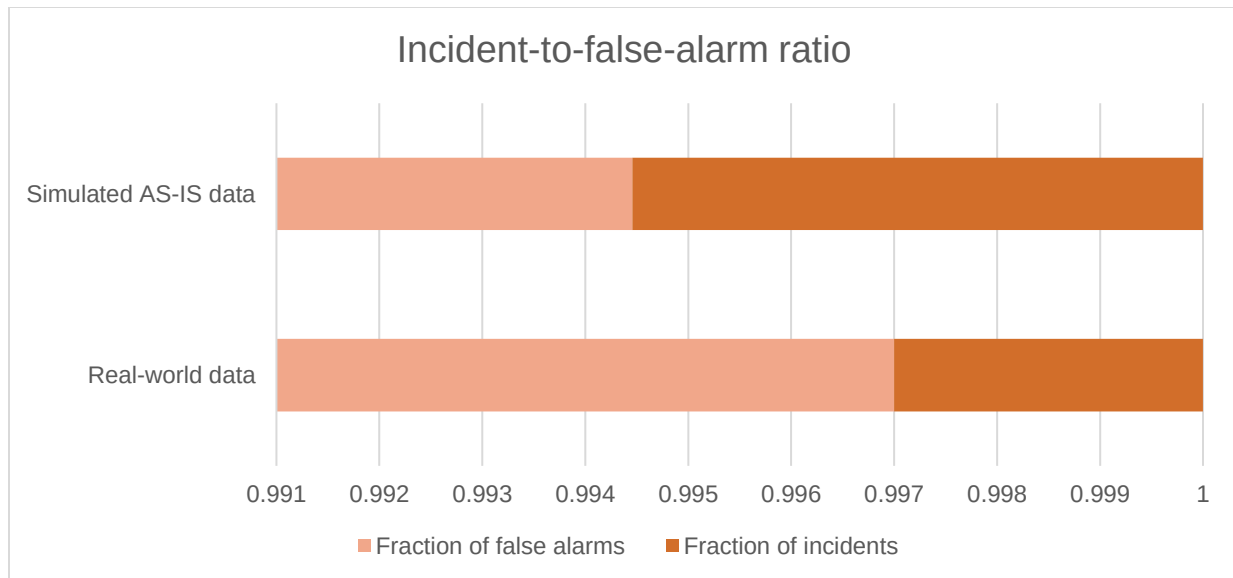


Figure 38: Comparison of the incident-to-false-alarm ratios for model validation

The ratio of incidents relative to false alarms is compared in Figure 38. Note that the horizontal range was limited (i.e., magnified) to show the correspondence between the real-world and the simulated results. From the graph, it is evident that the simulation model compares favourably with real-world data for the incident-to-false-alarm ratio.

It is noted, as with most modelling challenges, that the simulation model will always be an estimation of the real world, as minor variations are always present. However, the goal of this research is to compare a contemporary model with a prospective model in a *relativistic* way, which limits the impact of these small variances. With this relativistic approach, simulated output variables of interest are compared between simulated models, and results will show an improvement, or not.

4.6 RVM part two

The first part of the RVM matrix was shown at the end of chapter 3. That section covered the validation of the research problem together with how the literature contributed to either research challenges or concept solutions. This section of the RVM – part 2 – illustrates how the analysis and modelling process developed in this research validates the “AS-IS” simulation model. The second part of the RVM is shown in figure 39.

Validation process of the "AS-IS" model	Research concept solutions Literature and analysis and modelling process	Follow the QRM methodology to manage literature and the DSR and ADR methodologies to create an artefact	Perform a system analysis on the dynamics of a real-world control room system	Follow a systems engineering approach and define the system from a holistic perspective	Create a simulation model of the real world control room system ("AS-IS") and perform experiments ("TO-BE")	Follow a relativistic approach to ensure that the only changes impacting the outputs are those brought by system alterations
	QRM, DSR and ADR	↑				
	Step 1: Define "AS-IS" system		↑	↑		
	Step 2: Build "AS-IS" system				↑	
	Step 3: Validate "AS-IS" system				↑	

Figure 39:RVM part two – The validation of the “AS-IS” simulation model

4.7 Conclusion

This chapter provided an analysis of the trade-offs present in conventional security control rooms. The main model trade-offs that consider risk factors and data were defined in this chapter. The bin-theory was developed and included in this chapter as a tool for managing and monitoring the flow of event-related information in the simulation environment. This chapter presented a flowchart representing the investigation methodology of the experiments to be conducted in chapter 5. Chapter 4 concluded with the second part of the RVM for this research.

The validation of the simulation model of the “AS-IS” system is of importance since experiments on the simulation model will only be meaningful once it has been validated. The “AS-IS” simulation model had been validated in this chapter the following ways (as a combination of measures):

1. The simulation model was derived from a real-world control room system, and was purposefully designed to be functionally and architecturally similar – this was verified against the real-world functions and thus serves as functional verification;
2. The sequence of task executions of the simulation model also corresponds with the task execution sequence of a control room in the real-world – this verifies functional logic in a process flow;
3. Actual historical data from a real-world loosely integrated security control room system was included in the simulation model – this was verified by an industry expert and confirmed to be accurate;

4. In terms of performance measures, the number of events flowing through the simulation model was verified to be sufficiently similar to the real-world data (over 95% relative to measured 2019 numbers);
5. Finally, the ratio of incidents to false alarms corresponds 99.75% with the 2019 ratio of incidents to false alarms in the physical control room.

Therefore, any changes to the variables of the “AS-IS” simulation model in the simulation environment will give a strong indication of what can be expected in the physical world – should these particular variables change.

Chapter 5: Experimental analysis

5.1 Overview

This chapter contains the application of the experiments illustrated in the analysis and modelling process presented in Chapter 4. An “AS-IS” generic model was defined in chapter 4 and shaped with emphasis on the most important function of a loosely integrated control room – effective event management. The experiments conducted in this chapter will be done on the “AS-IS” model defined in chapter 4. The variable-changes of these experiments will be inspired by literature, and it will act as a form of validation on the “TO-BE” models.

5.1.1 Step 4: Experiment 1 - “AS-IS” event logic comparison

As previously mentioned, there are popular routing options that control rooms use to navigate events to the stacks of the functional units in the control room. These include sending events randomly to functional units and sending events to the functional unit with the lowest number of events waiting on its stack. There are many other routing options used in control rooms, however, they are not considered in this research since it would be setting-specific.

Other than the routing logic to the stacks of the functional units, events are processed from the stack in a predetermined manner. Many control rooms adopt a first-in-first-out (FIFO) strategy where events are handled by the function unit in the order that they arrive in. However, in some settings, events may be prioritised by many pre-established factors which are not identical in all control room settings. The two prioritisation logic approaches used in the simulation include FIFO and the fast-tracking of events from higher residual risk sites.

Experiment 1 will determine which combination of the defined routing logic, prioritisation logic and input device systems perform the best cooperatively in the simulation environment. This is done to identify the best combination of a conventional “AS-IS” system within the constraints of the model. In this experiment, every combination of routing logic, prioritisation logic and input device system must be simulated over a long period of operational time for all the residual risk site-groups. For this experiment, “average” operators are considered as functional units, with a score of 3 out of 5. This score may not be perfectly representative of the actual abilities of the operators in the control room, however, the simulation results will still be valid since these values are the same over all the scenarios. Moreover, the aim of experiment 1 is merely to gain insights on which

combination of routing logic, prioritisation logic and input device system is the best representative of the “AS-IS” system.

One of the prioritisation logic options is to fast-track an alarm based on its priority. What is considered to be a higher priority alarm is not uniform over control rooms. For this simulation model, the priority of an alarm is over-simplified and considered directly proportional to the residual risk of the site it originated on. In other words, an alarm originating on a medium residual risk site will have priority over an alarm originating on a low residual risk site. Also, an alarm originating on a high residual risk site will have priority over alarms originating on both low and medium residual risk sites.

Appendix A contains all the possible combinations – portrayed as scenarios - for the “AS-IS” candidate models under evaluation in experiment 1. A total of 108 scenarios were defined in the simulation framework for experiment and each scenario was run for 30 iterations over a long time (in this case 5 years).

Table 8: Top 10 scenarios based on the incident escalation factor

The output of experiment 1								
Ranking	Scenario	Routing logic	Prioritisation logic	Input device system on LRR	Input device system on MRR	Input device system on HRR	Incident escalation factor	Response efficiency factor
1	32	Random	Fast track	IDS + SID	IDS + SID	IDS + SID	3.34	0.18
2	84	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + SID	3.35	0.18
3	6	Random	FIFO	IDS + SID	IDS + SID	IDS + SID	3.36	0.19
4	58	Lowest on stack	FIFO	IDS + SID	IDS + SID	IDS + SID	3.37	0.18
5	103	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + CCTV	3.52	0.16
6	51	Random	Fast track	IDS + SID	IDS + SID	IDS + CCTV	3.54	0.16
7	25	Random	FIFO	IDS + SID	IDS + SID	IDS + CCTV	3.61	0.16
8	53	Random	Fast track	IDS + SID	IDS + CCTV	IDS + SID	4.04	0.18
9	79	Lowest on stack	FIFO	IDS + SID	IDS + CCTV	IDS + SID	4.05	0.18
10	27	Random	FIFO	IDS + SID	IDS + CCTV	IDS + SID	4.07	0.18

Considering the top 10 scenarios based on the incident escalation factor in table 8, it is notable that there is not a significant difference in system response if the routing and prioritisation logic is

changed. These results, however, may be considerably different if a more detailed, company-specific prioritisation logic is implemented. For the purposes and scope of this research, however, this will not be considered. Furthermore, the results may be much different if the ratio of sites relative to operators in the control room increases significantly. However, an in-depth robustness study will not be done in this research as it is not within the scope of this project.

An important finding of experiment 1 is that the four systems that produced the lowest incident escalation factor were indeed the systems containing an IDS and SID combination on all the sites. The bar chart in figure 40 compares the incident escalation and response efficiency factors of the best performing scenarios of each of the following combinations:

- IDS and SID combinations on all the sites;
- IDS and CCTV combinations on all the sites;
- IDS on all the sites.

In the simulation model, the amount of time incidents escalated during the experiment is determined by recording the time each *actual* incidents spends in the system. The time actual false alarms spend in the system does not contribute to this value, since there it is not a malicious event. If an incident is completely missed or misinterpreted as a false alarm, the maximum escalation time is added, which is the estimated amount of time needed for an incident to escalate to its peak. The maximum possible incident escalation time in the experiment is determined by multiplying the number of incidents generated by the model with the maximum escalation time.

The factors showcased in Figure 40 are determined by the following equations:

$$\begin{aligned} & \text{Incident escalation factor} & (27) \\ & = \frac{\text{Total time incidents escalated during the experiment}}{\text{Maximum possible incident escalation time in the experiment}} \times 10 \end{aligned}$$

$$\begin{aligned} & \text{Response efficiency factor} & (28) \\ & = \frac{\text{Number of responses given the event was indeed an incident in the experiment}}{\text{Total number of responses in the experiment}} \times 10 \end{aligned}$$

A factor-approach is used to compensate for the randomness in each experimental run. For example, the amount of time an incident escalates cannot be compared directly between

experiments, as a different number of events may be present in the experimental runs. The experiments must be run for a sufficient amount of time and at multiple iterations to ensure that the randomly generated values provide reasonable and consistent estimations. Therefore, the experiments were simulated over a period of five years, and each of these experiments is repeated 30 times to obtain good averages.

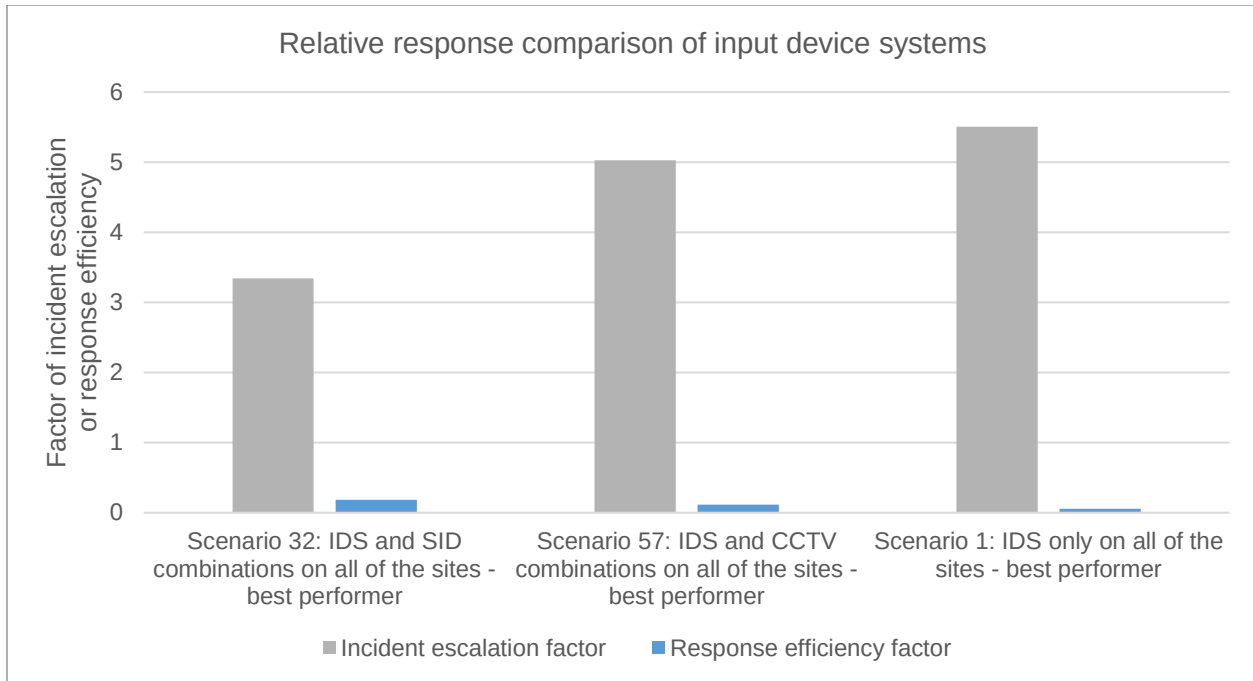


Figure 40: Comparison of the best performers of each input device system

Clearly, the IDS and SID combination is the best input device system as it achieved both the lowest incident escalation factor and the highest response efficiency factor. The IDS and CCTV combination had a higher incident escalation factor and a lower response efficiency factor than the IDS and SID combination. The worst performing input device system is the basic IDS, as the incident escalation factor is higher than the latter two systems. This is because basic ID systems provide no form of visual verification which leads to uncertainty and ineffective response.

The IDS and SID combination has the highest level of informativity since the bins it produces are relatively small in size with a high density of informative information. The IDS and CCTV combination has a lower level of informativity relative to the IDS and SID combination since the bin-sizes are larger and the density of informative information is lower. Although the response efficiency factor is slightly better for some input device systems than others, the change is relatively small. The reason for this is because the same quality ID system is assumed for all the

input device systems – meaning that more or less the same number of false alarms are still making it to the control room, regardless of the system on-site.

Table 9: Top 10 scenarios based on the response efficiency

The output of experiment 1								
Ranking	Scenario	Routing logic	Prioritisation logic	Input device system on LRR	Input device system on MRR	Input device system on HRR	Incident escalation factor	Response efficiency factor
1	6	Random	FIFO	IDS + SID	IDS + SID	IDS + SID	3.36	0.1869
2	84	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + SID	3.35	0.1848
3	58	Lowest on stack	FIFO	IDS + SID	IDS + SID	IDS + SID	3.37	0.1846
4	32	Random	Fast track	IDS + SID	IDS + SID	IDS + SID	3.34	0.1833
5	79	Lowest on stack	FIFO	IDS + SID	IDS + CCTV	IDS + SID	4.05	0.1772
6	27	Random	FIFO	IDS + SID	IDS + CCTV	IDS + SID	4.07	0.1758
7	53	Random	Fast track	IDS + SID	IDS + CCTV	IDS + SID	4.04	0.1758
8	105	Lowest on stack	Fast track	IDS + SID	IDS + CCTV	IDS + SID	4.08	0.1733
9	103	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + CCTV	3.52	0.1595
10	25	Random	FIFO	IDS + SID	IDS + SID	IDS + CCTV	3.61	0.1588

Table 9 contains the top 10 scenarios based on response efficiency. The IDS and SID combinations were proven best once again in all the scenarios (top 4) where IDS and SID combinations were selected to be on all the sites. Moreover, the following best scenarios were those where the IDS and SID combinations were placed on the low and high residual risk sites and the CCTV and IDS combinations on the medium residual risk sites. This is since the CCTV and IDS combinations are the second-best of the three input device systems evaluated in this research, and it is placed on the sites with the lowest expected event volumes – namely the medium residual risk sites.

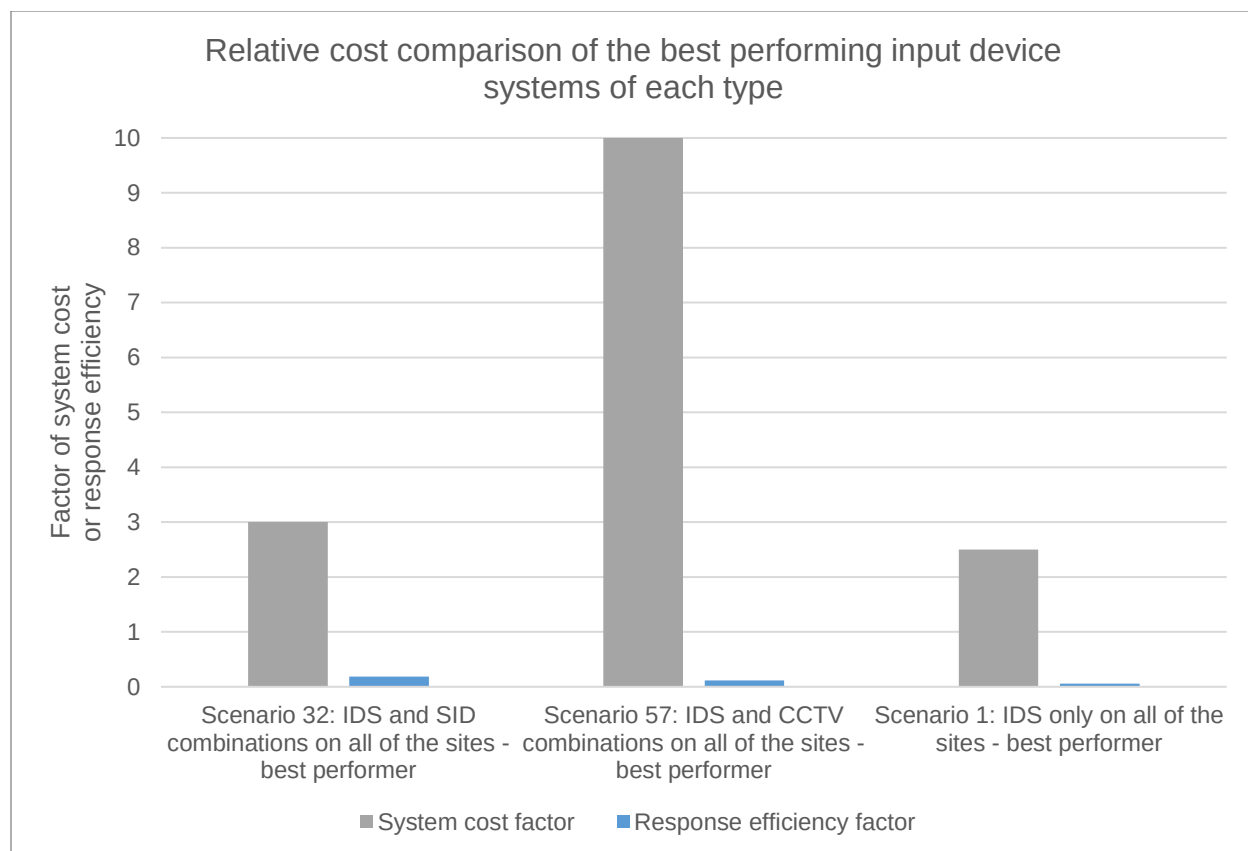


Figure 41: Cost comparison of the input device systems

Figure 41 contains a bar chart comparing the relative cost of input device systems. These costs are illustrations of the actual system costs announced in chapter 3, and these cost factors are representative of both the once-off system installation cost and the ongoing monthly maintenance costs. The basic IDS is the most cost-effective of the three input device systems used in the comparison and companies tend to select these non-informative systems for its cost-effectiveness. The IDS and CCTV combination is relatively expensive compared to the other two input device systems.

In the case of this experiment, an increase in the cost of the input device system does not mean an increase in operational effectiveness. An IDS and CCTV combination is trusted by clients and often blindly selected as these clients may think that this combination is the best as it is the most expensive. The large installation and maintenance costs do not justify the IDS and CCTV combination to be the best option for the event management of loosely integrated security control rooms. The IDS and SID combination not only proved to be the best combination through incident

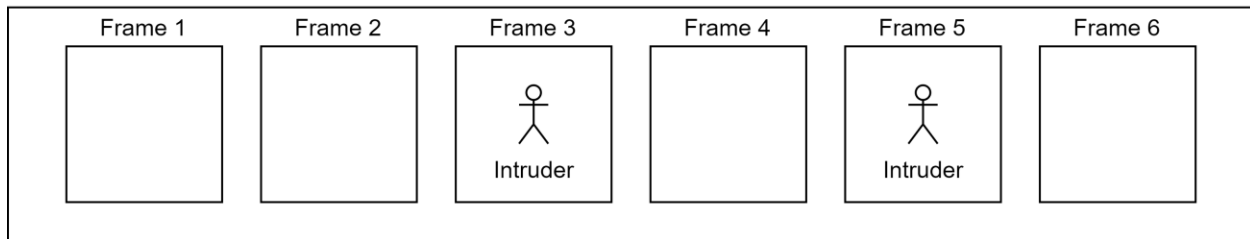
escalation and response efficiency, but it is also much less expensive than conventional IDS and CCTV combinations.

5.1.2 Step 5: Experiment 2 - Industry 4.0 technology on-site

Experiment 1 compared three basic input device systems based on the estimated amount of incident escalation time and the fixed and variable costs associated. It was evident that an increase in the density of valuable information in bins - by only considering the average densities of valuable information of the three input device systems - will result in an informed decision to be made quicker, which results in a lower incident escalation time, and a lower variable cost over time. The fundamental method of increasing the density of informative information is to increase the number of event indicators per bin or decrease the bin-sizes.

Object detection and scene analysis software are cost-effective methods that may result in an increase in informativity through increased information density in bins. This can be accomplished by complimenting the already installed visually informative input devices such as CCTV and SID with inexpensive or open-source software on-site. This software can analyse a scene and eliminate sections which are likely to be irrelevant or “noise”, or emphasise the exact location of where the object was detected. In the simulation model, object detection and scene analysis software will effectively decrease the bin size through noise elimination.

Untreated bin



Treated bin

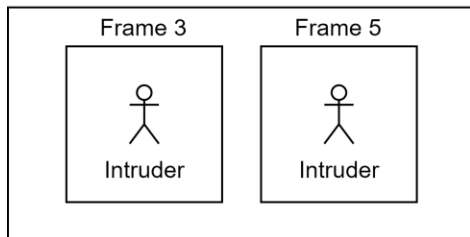


Figure 42: Bins before and after being treated by video scene analysis on-site

Figure 42 showcases an over-simplified illustration of how a bin changes when it is treated with video scene analysis and object detection on-site. The bin, containing visual data in the form of frames, is analysed, noise is rejected, and the new bin contains mostly event indicators. Experiment 2 assumes the same control room and functional units as Experiment 1, with the addition of scene analysis software installed on CCTV and SID units on the sites. Therefore, the parameters to change from Experiment 1 to Experiment 2 include a reduced minimum and maximum bin-size with a similar number of event indicators. The number of events occurring on the sites and all the other variables will stay the same, to ensure that the only factors impacting the output variables are those directly impacted by the intelligent scene analysis software.

To illustrate the impact of Industry 4.0 technologies on a control room's operations, a relativistic comparison of basic CCTV systems installed on all the sites ("AS-IS") and basic CCTV systems with the addition of scene analysis ("TO-BE") is performed. The control room component of the "TO-BE" system thus stays unchanged and the only change from the "AS-IS" system is the addition of automated scene analysis installed on the input devices on the sites served by the control room.

The impact of this technology is simulated with Simio software by altering the conventional "AS-IS" simulation model by decreasing the amount of noise in bins and lowering the average number

of false alarms accepted by the input device. It is very important to note that the quality of the ID system is not improved and the number of false alarms created will not decrease, only the number of false alarms accepted to be sent to the control room will decrease. The rest of the model, including the rate at which events occur, stays unchanged to ensure that the only variables changing, are the ones directly influenced by the industry 4.0 technologies.

It is difficult to predict exactly how much the relevant variables will change after these technologies have been implemented since the technology currently available is of varying quality. It is, however, a fact that certain variables will change if automated scene analysis is implemented. The impact thereof on the output variables can, however, be illustrated by performing a basic sensitivity analysis or a “what-if” analysis.

For example, assume that variable A is known to be larger if a specific functional unit change is made. Then, variable A will be increased with interval-percentages inside of the simulation model, to conceptualise the impact on the output variable (by analysing trends) as a result of an increase to variable A. Table 9 contains the “what-if” alterations that will be made to variables to simulate the impact of automated scene analysis in the control room system.

Table 10: “What-if” alterations for the “AS-IS” transition to the “TO-BE” candidate with video scene analysis

Experiment 2, sub-experiment:	Average noise change in bins in the “TO-BE” candidate	The average change of the acceptance rate of false alarms in the system of the “TO-BE” candidate	The average change in the number of event indicators in bins in the “TO-BE” candidate
I	-20%	-10%	0%
II	-40%	-20%	0%
III	-60%	-30%	0%
IV	-80%	-40%	0%

The number of event indicators will not reduce in bins, as only noise is reduced by the automated scene analysis. Also, the technology does not change the physical event occurring on-site, it rather manipulates the recorded data before sending it to the control room. A cost analysis, when using distributed processing as opposed to processing all signals in a control room, was not done in this case as hardware with processing ability has already been installed on sites, and open-source software can be obtained and implemented. The results of experiment 2 are showcased in figure 43.

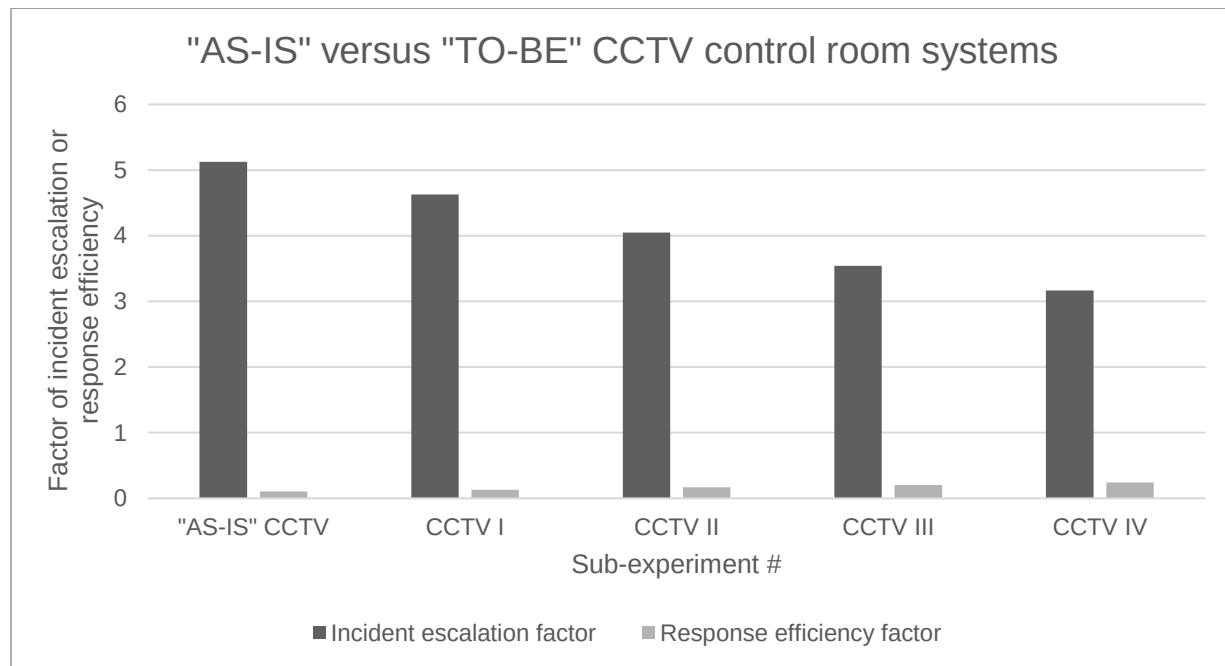


Figure 43: The Impact of industry 4.0 technology on conventional CCTV systems

Since a bin consists of noise and event indicators, the information-to-noise ratios of bins increase when noise is reduced (effectively, the size of the bin may also reduce if noise is eliminated). Therefore, to illustrate the impact of scene analysis in the system, the average amount of noise in bins is reduced by 20% for each sub-experiment. In effect, smaller bins are transferred over the communication medium between the site and the control room as the amount of noise reduces, resulting in the operators gaining quicker access to the information available on what caused the event. Due to the reduced size of the bin and the semi-distributed processing nature of this “TO-BE” model, the time required for an operator to review the bin also decreases. Furthermore, fewer false alarms are present inside of control rooms which results in lower congestion levels.

A similar phenomenon can be seen in figure 44 where the industry 4.0 technologies are applied to snapshot intrusion detection (SID) devices. The bin-sizes of conventional SID systems are much smaller than those of CCTV systems (due to the nature of static images vs CCTV footage) and it should thus be evident that conventional SID systems are more effective in the loosely integrated security setting than conventional CCTV systems.

Trends in improvement are evident when Industry 4.0 methods are used in both of these input device systems. Conventional SID systems, however, outperform conventional CCTV systems since SID systems typically produce bins with better indicator-to-noise ratios (and therefore a higher level of informativity) than CCTV systems. This is since SID systems take snapshots at the moment when an intrusion is detected (a few, highly indicative image frames) as opposed to transmitting large amounts of uninformative data, as is the case with CCTV systems (hundreds of uninformative image frames). However, Industry 4.0 methods applied to SID systems will still filter out unwanted snapshots and provide slightly smaller bin-sizes than conventional SID systems, hence the relative improvement.

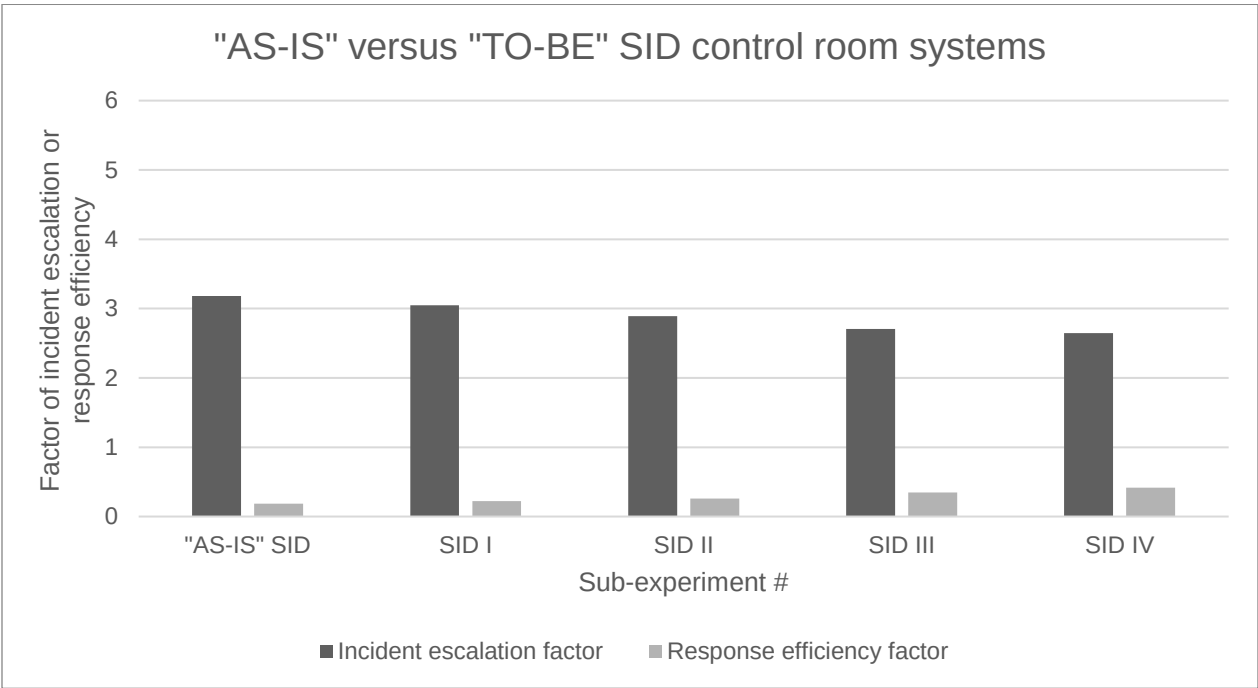


Figure 44: The Impact of industry 4.0 technology on conventional SID systems

Although exact values for the “AS-IS” to “TO-BE” transition had not been identified, the sensitivity analyses proved that a reduction in noise at the sites monitored by a loosely integrated control

room is likely to result in a lower incident escalation factor and better response efficiency. Also, input devices producing bins with high information-to-noise ratios have high levels of informativity.

Another important goal of the control room is to lower the overall operational expenditure (or resource wastage, in the case of this research). In this simulation model, operational expenditure is difficult to measure, since many arbitrary costs such as salaries and fuel prices are present. Therefore, operational expenditure is compared on a relativistic basis by considering *hours worked* and *kilometres driven*. More specifically, a factor-comparison is made based on *hours wasted* and *kilometres wasted*. The two wastage factors are determined by the following equations:

$$\text{Wasted hours factor} = \frac{\text{Wasted hours responding to false alarms in the experiment}}{\text{Total responding hours in the experiment}} \times 10 \quad (29)$$

$$\begin{aligned} \text{Wasted kilometres factor} \\ = \frac{\text{Kilometres wasted responding to false alarms in the experiment}}{\text{Total kilometres driven in the experiment}} \times 10 \end{aligned} \quad (30)$$

The kilometres wasted responding to false alarms in the experiment is determined by randomly generating a kilometre-value within the expected kilometre-range every time the task force is incorrectly prompted to respond (the cases where the events are false alarms). The total kilometres driven in the experiment value is determined by summing all the kilometres driven when responding. This includes the response actions to both incidents and false alarms.

The wasted hours responding to false alarms in the experiment is determined by calculating the time it takes to drive the randomly generated distance every time the event is incorrectly responded to, as well as a randomly generated site-investigation time. Figure 45 contains an illustration of the waste present in both the “AS-IS” and “TO-BE” systems.

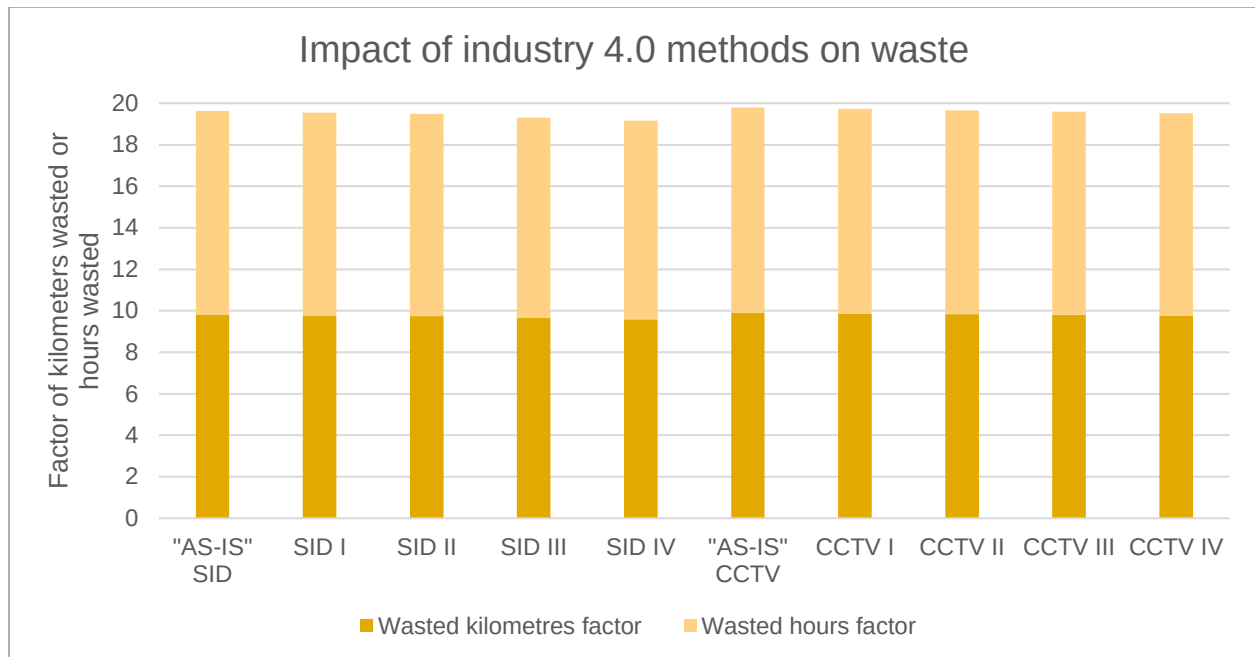


Figure 45: Observations in waste reduction

Figure 45 shows that, conventionally, significant waste is evident in operations. This is mostly due to a large number of false alarms relative to incidents that occur on sites, where false alarms are often incorrectly interpreted as incidents. Also, a major reason for wastage is alarm signals of which the cause is uncertain, but for which, a reaction team is sent to a site anyway.

Overall, a less-pronounced improvement is observed regarding wastage when industry 4.0 methods are implemented in both the CCTV and SID control room systems. A small decrease in both kilometres and hours wasted was noticed. Hence, although not the main consideration, an increase in the speed of event handling and a reduction in false alarms resulted in a minor improvement in wastage.

To re-iterate, the reason for insignificant changes in resource wastage is because the same quality ID systems are simulated – resulting in similar numbers of false alarms created. This experiment assumed a similar reduction in the acceptance rate of false alarms in the steps of the sensitivity analyses, however, large numbers of false alarms were still sent to the control room.

5.1.3 Step 6: Experiment 3 - Human-inspired AI in the control room

Experiment 3 is set up to observe the economic and operational impact of alterations to the functional units inside of the control room in the form of human-inspired AI. This experiment builds

onto experiment 2, and the only parameters to change in this experiment are the ones directly impacted if a transition is made from a human operator to human-inspired AI. No further variables are changed and the automated scene analysis stays implemented in the experiments to follow. Following a priori approach, the literature outlines three major parameters that will change if changes are made to a functional unit, namely:

1. The time required for the functional unit to analyse and process an event's data;
2. The fraction of events correctly interpreted by the functional unit;
3. The operational costs associated with the functional unit.

In the loosely integrated security control room environment, the functional units are expected to perform the levels presented by Simpson [26] up until the *adaption* level since origination is not required in control room environments. Human-inspired AI can perform all Simpson's levels with efficacy up until the adaption level, where it is outperformed by humans since it is not on par with first-of-a-kind incidents. It can, however, perform the adaption level to a certain extent. Nevertheless, AI is much quicker at event revision than humans if the same, stable communication medium is assumed.

A relevant advantage of AI over humans in the control room settings is that AI is not constrained by cognitive biases such as desensitisation toward alarms as most humans are. Human error is therefore considered in the form of cognitive biases (such as desensitisation) and often results in dismissing an alarm as a false alarm when it is indeed an incident.

Humans have varying cognitive ability and levels of desensitisation, and the intelligent technology available is of varying quality. These two factors may both decrease the percentage of events correctly classified in systems considering humans or AI as the functional units inside of the control room. Nevertheless, it is commonly known that, at the time of this research, humans still perform better in decision loops for complex assets. Therefore, in this research, it is assumed that the percentage of events correctly classified is higher when humans are selected as functional units inside of the control room, as opposed to AI.

AI, on the other hand, processes the information available on an alarm much quicker than humans. This is a major advantage that cannot be ignored, as quicker event management is an attractive candidate "TO-BE" model consideration. Although it is not practical to identify values for the variables in the model that will be descriptive of all the control room systems, values must still

be chosen as model inputs to conceptualise the impact of changes to these variables. These values are chosen on a relative basis to the other variables and the choices of values are based solely on literature suggestions.

Table 11: Sensitivity analysis of the virtual control room “TO-BE” candidate

Experiment 3: “TO-BE” virtual control room sub-experiment	Simulated change in percentage events correctly classified	Simulated change in event processing speed	Simulated change in the number of event indicators detected as a percentage of total event indicators
I	-80%	+20%	+20%
II	-60%	+40%	+40%
III	-40%	+60%	+60%
IV	-20%	+80%	+80%
V	0%	+100%	+100%

In table 11, the percentage changes are indicated if a functional unit change is made from an operator as the functional unit to a human-inspired AI functional unit in the form of a “virtual” control room. In this experiment, no humans form part of the decision-making process of an alarm’s cause. The following section elaborates why the values were chosen to change as they were. From the literature, it is known that the percentage of events correctly classified will decrease if this change is made since first-of-a-kind incidents cannot be classified by human-inspired AI with as much efficacy as humans. It can, however, complete many of the tasks and an increase of 20% per sub-experiment is chosen for this variable in the simulation environment.

The speed at which events are processed will increase with a virtual functional unit inside of the control room since none of the delays between interfaces present in control rooms with operators is present with human-inspired AI as the functional unit. There are also no distractions to the

functional unit and the time to revise the event is therefore increased with 20% per sub-experiment.

Although event indicators may be present in a bin, not all them are necessarily detected by the functional unit. This may be due to cognitive fixation, getting distracted in the control room, and other functional-unit-specific factors. A human-inspired AI option will not experience these human-unique factors, and although event indicators are interpreted with less efficacy, they are more frequently identified. Therefore, if a functional unit transition is made from a human to human-inspired AI, the number of event indicators *present* are *detected* more frequently. This is simulated by increasing the number of event indicators by 20% per sub-experiment in the simulation environment.

Other than the expected operational changes - resulting in alterations to the functional units within the control room - fixed and variable costs must also be considered. Naturally, a bespoke AI solution would be much more expensive in terms of fixed and variable costs than a human operator in an operational sense.

At the time of this research, SaaS options are available that can process the events of a loosely integrated security control room at \$1 per 1000 decisions (or \$1 per 1000 event “calls”) [72]. It is assumed that the current salary of an operator in South Africa to be in the range of R6000 per month for an 8-hour daily shift and that three shifts occurs in a day. Therefore, three operator salaries must be paid for operators to fill the position of one functional unit in the control room, which equates to R18000 per month per model representation of a functional unit. In an eight-hour shift, operators make around 220 calls, resulting in about 660 calls per functional unit per 24-hour day.

The cost per 1000 calls for operators in the position of a functional unit would therefore be approximately \$1.66. With the exchange rate at the time of this research, this translates to approximately R27.30 per 1000 calls. In the model, a cost per call is specified, and the abovementioned results in approximately R0.016 per call for the virtual SaaS AI approach, and R0.026 per call for the “AS-IS” approach where humans are functional units.

For the sensitivity analyses of experiment 3, it is important to note that the same response (output) variables are considered as in experiment 2, with the addition of *operational cost* in the form of *cost per event managed*. Since the IDS and SID combination was previously declared the best

system in the security control room systems out of the three tested, it is the chosen system for experiment 3.

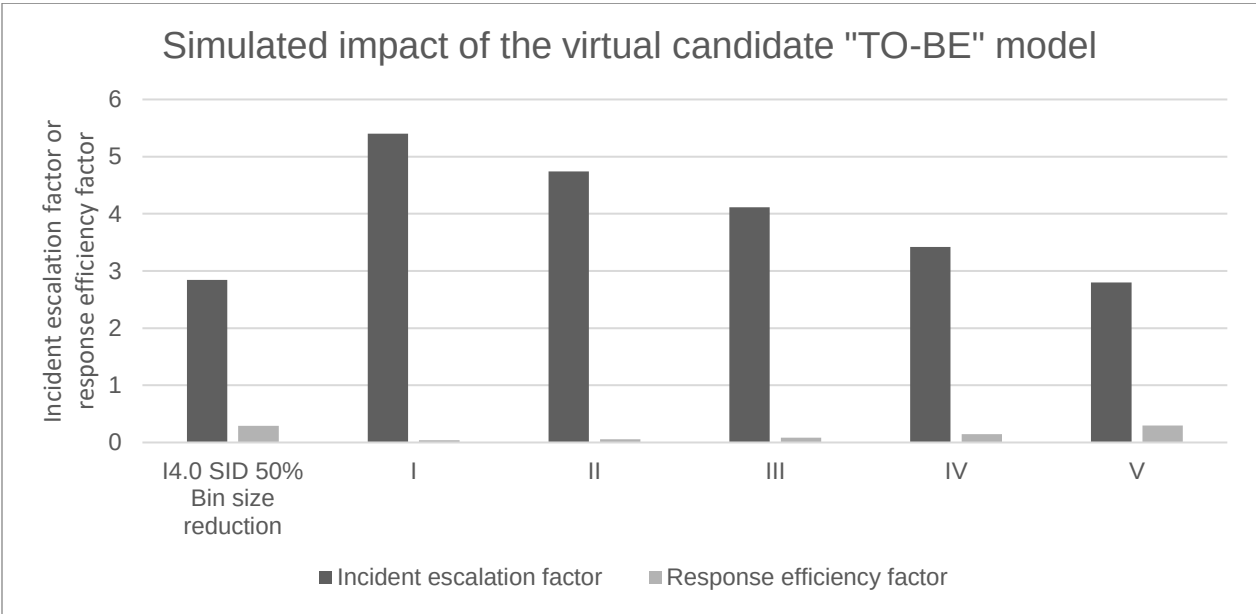


Figure 46: Impact on the system if a functional unit transition is made from a human to human-inspired AI

Figure 46 illustrates the outputs of the simulation model when the functional units of the control room are virtual, pay-as-you-go SaaS technology. Slightly higher levels of the incident escalation factor were observed relative to the experiment with human selected as the functional units. Therefore, although a gradual increase in the speed of event management was present, even a slight decrease in the percentage of events correctly classified overwhelmed these advantages.

The increase in the incident escalation factor is not immense and shouldn't be overemphasised, and the operational cost advantages that SaaS provides cannot be ignored. On an operational level, it is much more cost-effective to perform event management in the cloud through SaaS on a pay-as-you-go level. This finding is even more relevant in some countries where control room operators earn much larger salaries than those in South Africa since the cost of the SaaS services are similar worldwide.

As seen in sub-experiment V, if the virtual control room can identify first-of-a-kind incidents with the same accuracy as humans in the future, with higher speeds and no cognitive biases, human operators will be outperformed. Nevertheless, humanised AI such as this does not yet exist, and a completely automated loosely integrated security control room is not expected to materialise

soon. Even when the technology becomes available, it will take time to gain trust and transition to completely humanised AI.

Furthermore, with a SaaS approach, no infrastructure maintenance or physical, dedicated buildings are required. This translates to a significant cost advantage over traditional control room settings. These are notable advantages, however, the scope of this research will only consider major operational expenditure in the form of resource wastage and maintenance. The cost of real estate and upgrades to hardware (i.e. equipment depreciation and replacement) and software (such as licenses and software upgrades) in the control room will not be considered.

5.1.4 Step 7: Experiment 4 - Augmented cognition in the control room

Another “TO-BE” candidate system is a control room where human operators are supported with augmented cognition. This system will allow first-of-a-kind incidents to be detected more frequently since humans are still in the decision-making loop, which will result in a higher percentage of events correctly interpreted than AI. Furthermore, an augmented cognition system will reduce the number of events incorrectly classified by humans due to cognitive biases such as desensitisation and fatigue.

Similar to experiment 2 and 3, it is not sensible to predict with exactly how much the processing speed or percentage of the event correctly classified will change when the operator inside of the control room is assisted with augmentation technology. This is since the cognitive ability of humans and the quality of intelligent technology both vary.

In chapter 3, literature was conducted on the work of Fuchs, *et al.*, [32] regarding augmented cognition. It was mentioned that there are good prospects regarding changes of operator error rates and operator overload which would cause an increase in the speeds events are managed. For the experiment, these prospects are simulated – not to confirm the study of Fuchs [32] - but to simulate the impact on the control system should these prospects materialise.

Table 12: Sensitivity analysis of the augmented control room "TO-BE" candidate

"TO-BE" augmented control room sub-experiment #	Simulated change in percentage events correctly classified	Simulated change in event processing speed	Simulated change in the number of event indicators detected as a percentage of total event indicators
I	+2.5%	+10%	+20%
II	+5%	+20%	+40%
III	+7.5%	+30%	+60%
IV	+10%	+40%	+80%

In table 12, the percentage changes are indicated if a functional unit change is made from an operator as the functional unit to an operator complimented with augmented cognition technology. Similar to the functional unit transition from a human to human-inspired AI in experiment 3, the proceeding section elaborates on the selection of variable changes in table 12.

In experiment 4, the percentage of events correctly classified will increase since human interpretation would still be present, and first-of-a-kind incidents will be correctly identified more frequently. Therefore, the percentage of events correctly classified is selected to be the highest for all the simulation candidates so far, with an increase of 2.5% per sub-experiment run. The reason for the low percentage increase per sub-experiment is because under conventional conditions, the percentage of events correctly interpreted is quite high, and a large increase in this value will result in a value larger than 100% correctly interpreted, which is illogical.

For the transition from a human to an augmented human, the bin-processing-speed is expected to increase since specific operators are chosen in real-time based on their brain activity. An augmented operator, however, is expected to be more timeous in the task of processing bins than the human-inspired AI, since the interface between a human and machine is still present. Therefore, when the functional unit transition is made from an operator to an augmented operator, an increase of 10% per sub-experiment is selected, to ensure that events are processed faster

than the human-only option, and slower than the 20% increase per sub experiment of the transition from a human functional unit to human-inspired AI. Figure 47 illustrates the outcomes of the sensitivity analysis.

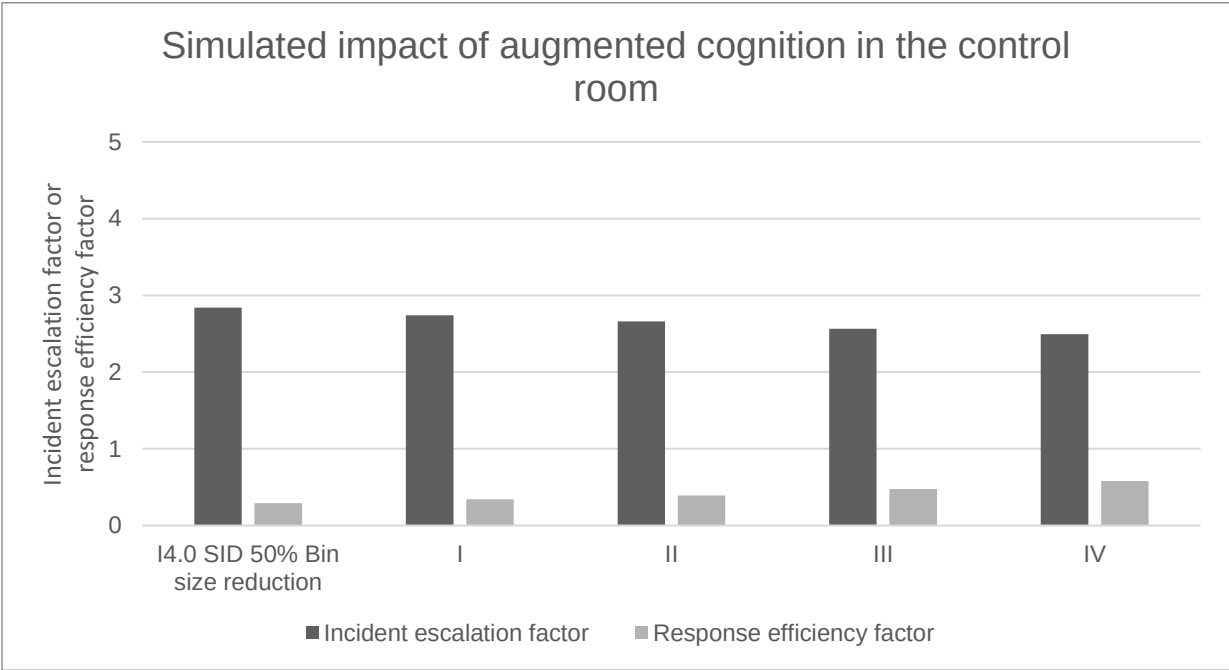


Figure 47: Impact on the system if a functional unit transition is made from a human to an augmented human

When the event management process of operators is augmented through decision support, it was found that the incident escalation factor decreased. This is due to an increased percentage of events correctly interpreted, a quicker event management time, and a larger percentage of event indicators detected as a percentage of total event indicators. This candidate “TO-BE” option achieved the lowest incident escalation factor and the highest response efficiency so far.

An augmented cognition setup would be more expensive than both a pay-as-you-go SaaS virtual control room, and operators as the functional unit. This is since operator salaries must still be paid with the addition of fixed and variable costs associated with an augmented cognition system. Nevertheless, augmented cognition does not improve the response efficiency and only slight improvements in the incident escalation factor are observed. Therefore, the focus of the analyses must shift toward other areas in the control room system, and a detailed cost analysis will not be conducted on augmented cognition.

5.1.5 Step 8: Experiment 5 - Tiny AI possibilities

The experiments up until this point illustrated an important finding: By improving only the control room will not result in significant improvement in terms of response efficiency and therefore resource wastage. The focus must now shift other areas in the control room system, and the logical areas are the sites served by the control room. The experiment done on Tiny AI below is a hypothetical “thought” experiment and not a physical experiment with confirmed data. However, it is included in the spirit of defining new research and inspiring creative thought. Having defined the purpose of this experiment, it is instructive, though, to know that the validated Simio model is adapted to provide a reference for proposed adjustments.

Tiny AI refers to AI with scaled-down hardware which focusses energy and algorithm efficiency. This field of research is still in its infancy and little academic literature is available on this topic at the time of this research. Tiny AI devices have already been implemented in the healthcare setting with great success. At the time of this research, this technology has not yet been fully tested in control room systems, however, its capabilities seem to be extremely relevant to control room settings as this principle is implemented in a reduced form by using video analytics (confirming the potential).

Should Tiny AI be implemented in the control room system, primary control room decision-making functionality would effectively move to the edge devices on the sites. It is common knowledge that tightly integrated control rooms are the best way of managing the events on-site; however, it has not previously been financially viable to construct an entire control room for a single site in many instances - hence the existence of loosely integrated systems. With Tiny AI, this cost will be significantly lower as physical structures needn't be built and the bidirectional data sending over a distance will be reduced significantly. Moreover, the control room would never be overwhelmed since only the events from a single site is managed per tiny AI device, also located on-site.

The implementation of tiny AI would result in the transition of advanced analysis such as data fusion and information fusion to the edge device systems on-site. This will result in bins being sent over to a control room with not only noise removed through video scene analysis and object detection, but with a more advanced analysis including:

- Pattern recognition;
- Analytics;
- Site history;

- Behavioural intelligence;
- Modus operandi.

In other words, many of the detailed operator-functions will be transferred to the site, and only a high-level decision would be required by a human being. From the virtual control room experiment, it was clear that humans should not be entirely excluded in the decision-making process. Nevertheless, a distinct advantage of the SaaS control room was that there is no physical infrastructure that requires capital expenditure. The experiment in this section aims to include these findings since they are known to be advantageous. Figure 48 illustrates the proposed tiny-AI-setup.

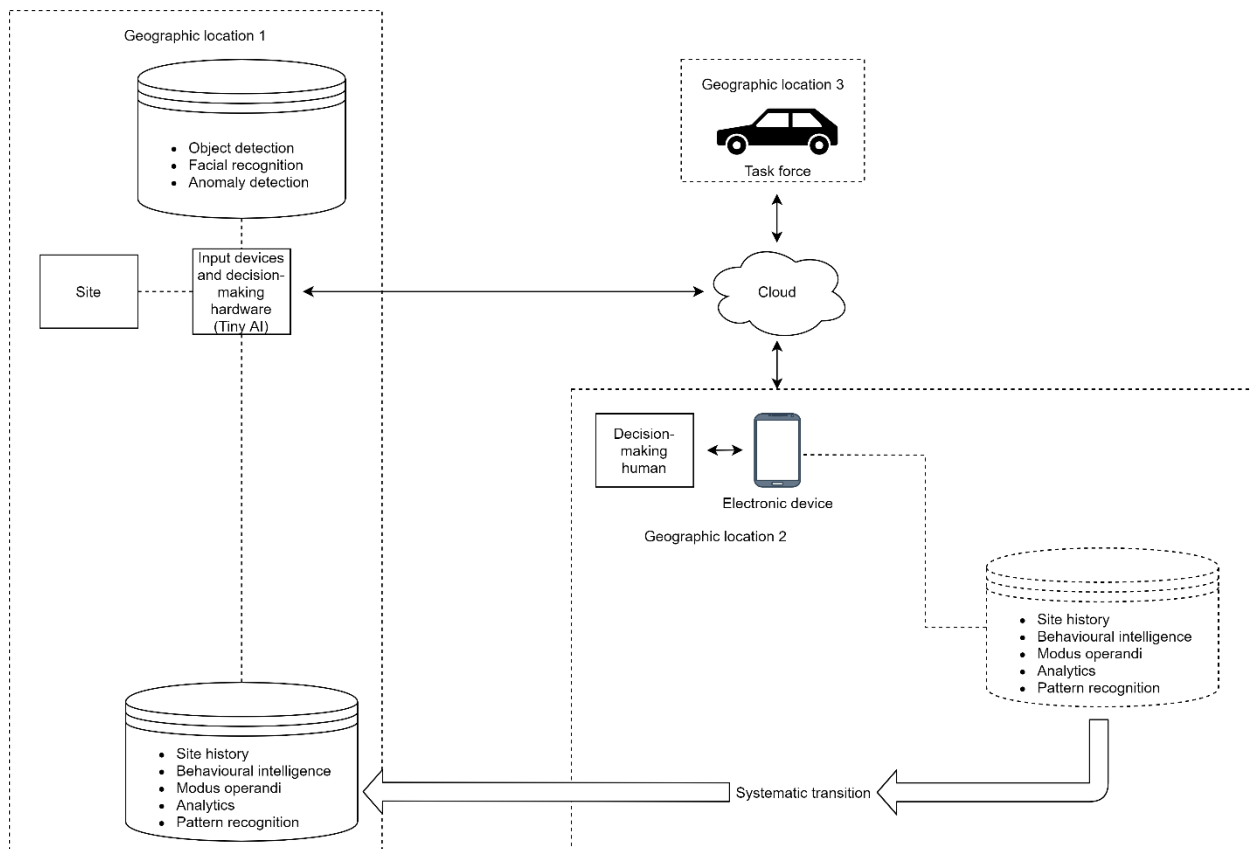


Figure 48: Tiny-AI-setup

With the setup shown in figure 48, the human is still “in-the-loop” without the need for a physical control room, however, the role of the human will change. For this research, the site history, behavioural intelligence, analytics, pattern recognition and modi operandi will be referred to as the umbrella-term “container”. The core thought-process behind this “TO-BE” candidate is that

the container that is conventionally used centrally in a control room will systematically move to the sites. This means that many of the conventional operator-functions will be done on-site, which will enable the tiny AI devices on-site to make decisions of higher quality on-site, resulting in:

- A lower number of false alarms;
- An increase in the number of event indicators detected as a percentage of total event indicators;
- An increase in the number of events correctly classified;
- An increase in the event-processing and data transfer speeds;
- An increase in fixed costs, since additional hardware and software acquisitions, must be made.

The new role of the human will be to classify or label events on a high-level, as opposed to the conventional in-depth analysis of the event through information fusion. This will result in a continual relearning / retraining of the tiny AI system on-site. Automated cross-training of the sites can occur where applicable, ensuring that lessons learnt on one site that may apply to others are taken into consideration. Therefore, the system would be adaptive in nature, where site-specific intelligence is considered together with system intelligence.

Similar to the previous experiments, it is not practical to assume specific values since the quality of technology varies and it is a dynamic and random system. Hence, a sensitivity analysis is conducted with slight increments in each of the variables expected to change with the addition of tiny AI to identify trends.

Table 13: Sensitivity analysis of the tiny AI experiments

"TO-BE" Tiny AI control room sub- experiment #	Simulated change in percentage events correctly classified	Simulated change in event processing and data- transfer speeds	Simulated change in the number of event indicators detected on- site as a percentage of total event indicators	Simulated change in TP/FP ratio	Simulated change in event creation rate
I	-80%	+100%	+10%	+10%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
II	-60%	+200%	+20%	+20%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
III	-40%	+300%	+30%	+30%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
IV	-20%	+400%	+40%	+40%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
V	+0%	+500%	+50%	+50%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
VI	+2%	+600%	+60%	+60%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
VII	+4%	+700%	+70%	+70%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
VIII	+6%	+800%	+80%	+80%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
IX	+8%	+900%	+90%	+90%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$
X	+10%	+1000%	+100%	+100%	$\frac{\text{Number of anticipated events over all sites}}{\text{Number of actual sites}}$

Table 13 illustrates the values used in the sensitivity analyses and the following section describes why these values were chosen. The simulated change in the percentage of events correctly classified will increase with an increase in the quality of the analysis on-site. This value is

systematically increased until it reaches its maximum value in sub-experiment X. Furthermore, the time it takes the human to process an event will decrease significantly, since only a final, high-level “call” will be made. This is because the human will not analyse the site history, behavioural intelligence etc. since this is done on-site by the tiny AI. Also, large amounts of data are not transferred to another geographic location, effectively reducing the data transfer times. An increase of 100% per sub-experiment is selected since less time will be required for the human to review the event, and lower amounts of data will be transferred to other geographic locations as the sub-experiments progress.

The simulated change in the number of event indicators detected on-site as a percentage of the total possible event indicators will increase since the quality of the analysis on-site increases, and this variable is selected to increase with 10% per sub-experiment. Finally, the number of events that are truly false positives that signal alarms will decrease due to the increased quality of the analysis on-site. This will effectively increase the ratio of true positives (incidents) relative to false alarms and it is chosen to increase with 10% per sub-experiment. It is emphasised that this change results in a lower number of false alarms triggered in the first place, as opposed to rejecting false alarms which are triggered. This is of importance since rejecting triggered alarms, in the control room or on-site, was found to not have a significant impact on the response efficiency and therefore resource wastage.

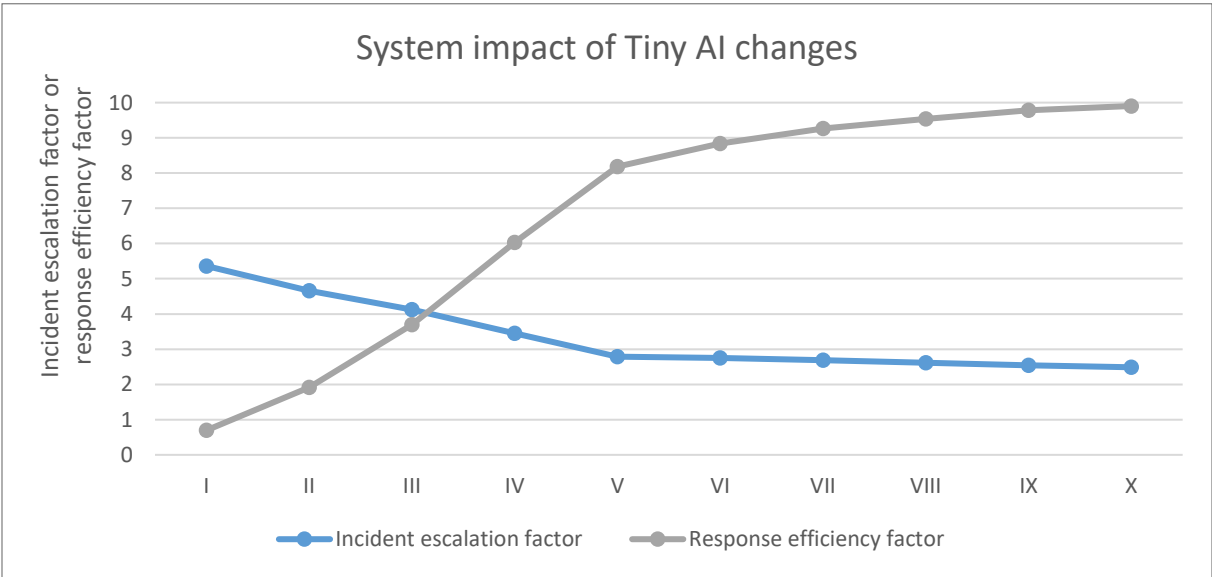


Figure 49: Simulated impact of the Tiny AI sensitivity analysis

Figure 49 showcases the impact of the Tiny AI sensitivity analysis on both the incident escalation and response efficiency factors. The incident escalation factor will decrease and the response efficiency factor will increase when events are reviewed by tiny AI on-site with a systematic transition of the contents of the container from the control room to the site. Figure 50 illustrates the changes in resource wastage when the sensitivity analysis is conducted.

The resource wastage will decrease significantly when the containers are systematically moved to the sites. The decrease in resource wastage is significant relative to the previous experiments since the previous experiments assumed that only ID systems signal alarms, with no additional intelligence, triggered alarms which resulted in many false alarms. Managing false alarms at various parts of the system will be to no significant avail if large numbers of false alarms are still present.

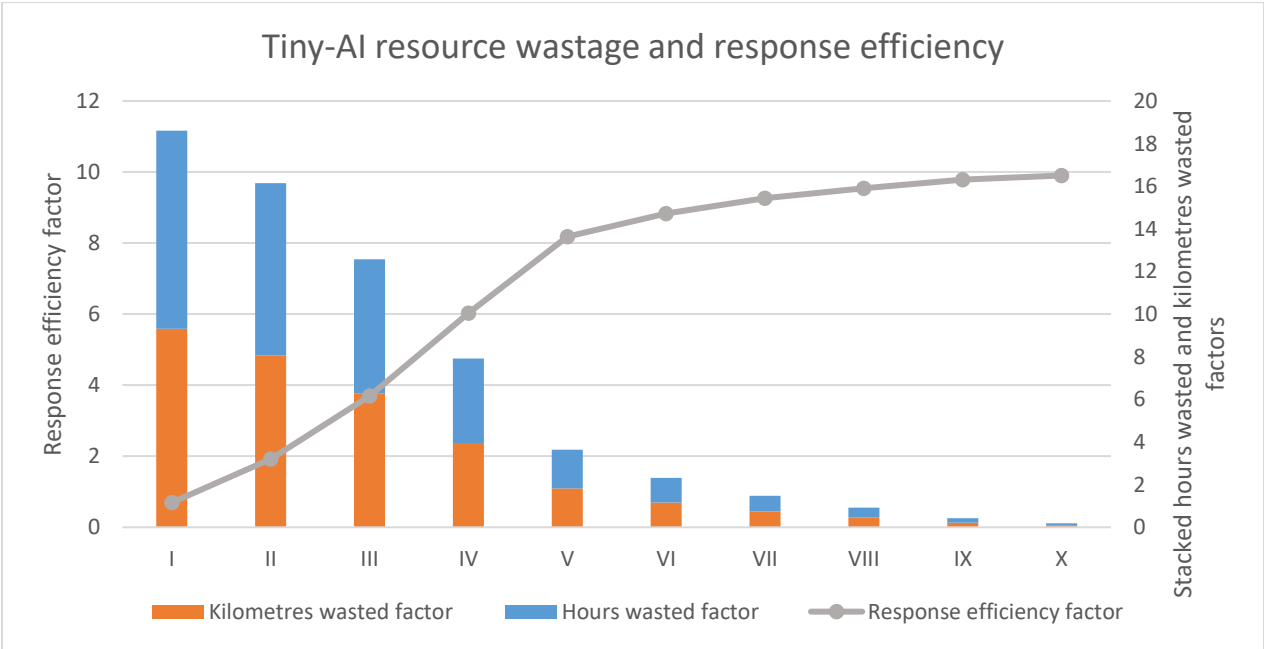


Figure 50: Simulated change in resource wastage and response efficiency with the implementation of tiny AI

To date, limited research has been done on the cost of tiny AI. Researchers have analysed and benchmarked ultra-low power, resource-constrained machine learning systems [73]. A detailed cost analysis is thus not sensible at this point in time, but it is reasonable to assume that the initial capital layout will be higher than current system, with savings in operating cost to provide a return on investment potentially over a number of years. In the future, as the costs of hardware and

algorithms fall, it may be more attractive to consider such an initial expense based on cost-performance.

5.2 Conclusion

This chapter contained the experiment of the “TO-BE” candidate models conducted on the validated “AS-IS” simulation model. Changes were made to the system at two key areas, namely (i) on the loosely integrated sites and (ii) inside of the control room with the focus of improving the event management functionality of the control room system concerning the incident escalation and response efficiency output factors. This chapter did not contain an exhaustive list of experiments, and many other “TO-BE” candidate models could have been identified and simulated. It was never the goal, however, to simulate a fully comprehensive list of experiments, as the main goal was to raise insights about the control room system and what is expected to happen when some variables change. The following insights were gained in this chapter:

- The human element should not be excluded from the control room system. Humans must still be included at a high-level decision-making position, to largely exclude human error and cognitive biases on lower levels and include a quick, exception-based revision at a higher level.
- High-quality decisions on whether an alarm must be signalled or not should be made on-site, to decrease the number of false alarms and therefore the amount of resource wastage. This must be done as opposed to signalling many false alarms and attempting to manage them.
- Candidate “TO-BE” alterations to the decision-making in the control room system such as augmented cognition may decrease the incident escalation factor to sufficiently low levels. However, to reduce operational expenditure, the number of false positives and the depth of the decision made by a human must be reduced.

Research concept solutions Literature and analysis and modelling process	Follow the QRM methodology to manage literature and the DSR and ADR methodologies to create an artefact	Perform a system analysis on the dynamics of a real-world control room system	Follow a systems engineering approach and define the system from a holistic perspective	Create a simulation model of the real world control room system ("AS-IS") and perform experiments ("TO-BE")	Follow a relativistic approach to ensure that the only changes impacting the outputs are those brought by system alterations
Step 4: Experiment 1 - "AS-IS" comparison				↑	↑
Step 5: Experiment 2 - Industry 4.0 technology on-site				↑	↑
Step 6: Experiment 3 - Human-inspired AI in the control room				↑	↑
Step 7: Experiment 4 - Augmented cognition in the control room				↑	↑
Step 8: Experiment 5 - Tiny AI possibilities				↑	↑

Figure 51: RVM Matrix part 3 - Experiments

Figure 51 contains the third part of the RVM matrix for this research and it illustrates how the experiments contributed to the concept solutions. The complete RVM matrix presenting the compilation of the three RVM matrices will be shown in chapter 6.

Chapter 6: Conclusion

6.1 Research summary

This research aimed to analyse, model, and evaluate the main function of control rooms - namely event management. A generalised, loosely integrated security control room system was chosen to be the real-world setting of focus. Simulation modelling efforts were conducted to discover sections in current control room systems where industry 4.0 technologies may improve the efficacy of event management and decrease the time incidents are not under control.

The bin-approach was defined and used in this research as a measure of the informativity of input devices located on the sites in the control room system. It was found that the control room system responded favourably to a decrease in the amount of noise in bins received from the sites, as the time incidents are not under control were found to decrease. This is since data about the events that trigger alarms are partially processed at the sites, resulting in a quicker transmission of the relevant data of the communication medium and a quicker revision by the functional units in the control room. Although a reduction in incident escalation was found with a decrease in the noise of bins through automated video scene analysis and robust object detection on-site, significant resource wastage was still present.

After the possible advantages of industry 4.0 technologies were identified and proved to be valuable contributors to effective event management, another area of the system – the control room – was analysed. Bespoke technologies were deemed not financially feasible and the virtual candidate “TO-BE” model was simulated by considering a pay-as-you-go option through SaaS. It was found that a virtual, cloud-based control room with no humans in the system performed slightly worse than the “AS-IS” control room in the simulation environment in terms of incident escalation. This is mostly because first-of-a-kind incidents cannot be detected by AI with as much efficacy as humans at the time of this research. Nevertheless, its advantages related to long-term operational expenditure and scalability were found to be notable.

Another “TO-BE” candidate model included operators assisted in the form of augmented cognition was investigated. The experiment was conducted in the form of a sensitivity analysis which considered a current control room system integrated with augmented cognition hardware and software. This experiment aimed to emphasise the advantageous human factors in the control

Page | 118

room. This “TO-BE” candidate was found to manage events with the highest degree of efficacy in loosely integrated control room settings, given that the same quality ID system remains on-site. On the other hand, it was notably the most expensive option in the loosely integrated experiments as both operators and bespoke hardware and software is required. Significant resource wastage was still present, and it became clear that the focus areas for improvement in the control room system needed to shift.

Thus, experiments were conducted where the “container” – defined in this research as an umbrella term for pattern recognition, analytics, behavioural intelligence, modi operandi and site history – was systematically transferred from the decentralised control room to the sites. This resulted in higher-quality decisions being made on-site which in turn resulted in fewer false alarms being generated. A reduction in false alarms was found to result in a significant decrease in resource wastage compared to filtering out large numbers of false alarms generated.

This research was conducted to determine the question: Can currently available industry 4.0 technologies improve conventional control room operations? The answer to this question was proven to be yes on multiple instances in this research.

6.2 Validation

In chapter 4 and 5, the modelling and experimentation processes were explained. This section contains the piece-wise validation of the artefact, namely the simulation model and the experiments conducted on it. A work breakdown structure (WBS) of the modelling and experimentation processes is shown in figure 52 to revise what was done and the sequence it was done in. The detailed, actual processes which are defined in the Simio simulation environment can be found with descriptions in Appendix B.

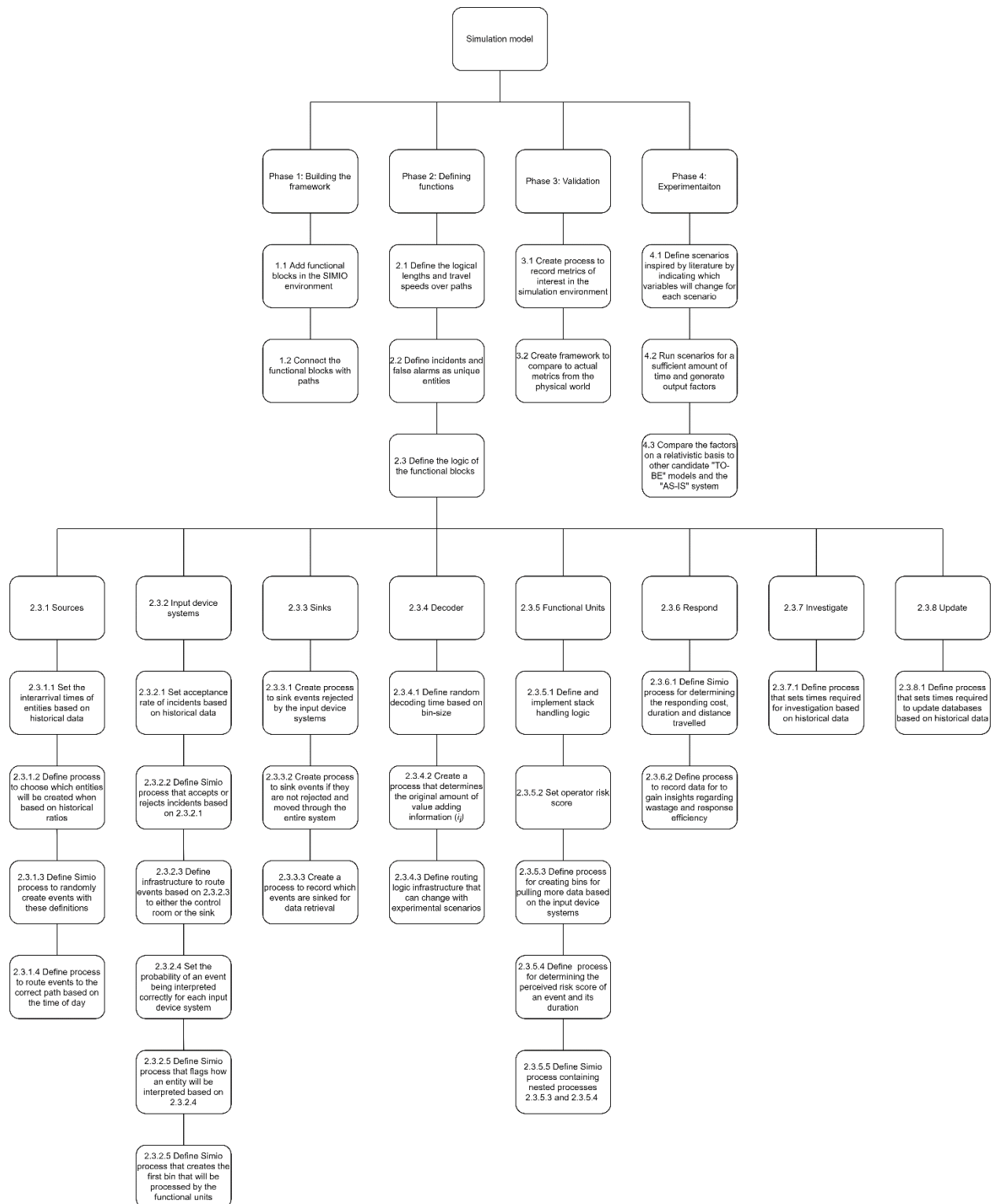


Figure 52: Work breakdown structure

To recapitulate, the “AS-IS” simulation model was validated in the following ways (as a combination of measures):

1. The simulation model was derived from a real-world control room system, and was designed to be functionally and architecturally similar — this was verified against the real-world functions, and this served as a functional verification.
2. The sequence of task executions of the simulation model also corresponded with the task execution sequence of a control room in the real-world — this verified the functional logic in a process flow.
3. Actual historical data from a real-world, loosely integrated security control room system was included in the simulation model — this was verified by an industry expert and confirmed to be accurate.
4. In terms of performance, the number of events flowing through the simulation model was verified to be sufficiently similar to the real-world data (more than 95% accurate relative to the measured 2019 total), as illustrated in chapter 4.
5. Finally, the ratio of incidents to false alarms was 99.75 per cent accurate, compared with the 2019 ratio of incidents to false alarms in the physical control room, shown in chapter 4.

Figure 53 below illustrates the complete RVM for this research.

Research need: Determine the influence of intelligent technologies on conventional control room					
Research efforts have been managed ineffectively in the past	↓				
Industry observations		↓	↓		↓
Industry data				↓	
Sources					
Research challenges	Uncertainty regarding how to manage research with quality and efficacy	The functional and informational dynamics of conventional control room systems are not well-defined	The interactions between people and technology in control rooms are not entirely clear	No performance data is available on the impact of alterations to a control room system	No standardised norm is defined to compare the outputs of experiments
Literature focus areas					
Research methodologies	↑ ↓				
Control room systems		↑ ↓	↑ ↓	↑	
Human factors		↓	↑ ↓		
Technology and industry 4.0 methods			↑ ↓	↓	
Computing in networks		↑ ↓			
Systems engineering			↑ ↓	↓	
Risk					↑ ↓
Simulation modelling				↓	↑ ↓
Literature focus areas					
Research concept solutions	Follow the QRM methodology to manage literature and the DSR and ADR methodologies to create an artefact	Perform a system analysis on the dynamics of a real-world control room system	Follow a systems engineering approach and define the system from a holistic perspective	Create a simulation model of the real world control room system ("AS-IS") and perform experiments ("TO-BE")	Follow a relativistic approach to ensure that the only changes impacting the outputs are those brought by system alterations
Literature + analysis and modelling process					
QRM, DSR and ADR	↑				
Step 1: Define "AS-IS" system		↑	↑		
Step 2: Build "AS-IS" system				↑	
Step 3: Validate "AS-IS" system				↑	
Step 4: Experiment 1 - "AS-IS" comparison				↑	↑
Step 5: Experiment 2 - Industry 4.0 technology on-site				↑	↑
Step 6: Experiment 3 - Human-inspired AI in the control room				↑	↑
Step 7: Experiment 4 - Augmented cognition in the control room				↑	↑
Step 8: Experiment 5 - Tiny AI possibilities				↑	↑

Figure 53: Complete RVM

The validation of “TO-BE” cannot be done similarly to the “AS-IS” validation. This is because the “AS-IS” simulation model was compared to actual industry data and performance measures. This type of comparison and validation can only be done with the “TO-BE” models if the simulation models are translated to systems in the physical world – which is not done in this research. Therefore, a weaker form of validation is done on the “TO-BE” models in the following ways (as a combination of measures):

1. Reputable literature provoked the changes of the majority of the variables for every scenario.
2. The findings were never meant to be absolute. Rather, sensitivity analyses were conducted which established *trends* when the variables – recommended by literature – are changed.
3. Multiple different “TO-BE” scenarios revealed similar conclusions. One of these conclusions is the finding that the focus should be to not signal many false alarms in the first place as opposed to managing many false alarms at various points in the system. The insignificant changes in the response efficiency factor, and therefore the resource wastage, confirmed this.

6.3 Recommendations for future research and notable remarks

It should be noted that the simulation insights in this research were obtained through sensitivity analyses which were inspired by literature. The study was not fully comprehensive and it was done out of a “what-if”, semi-quantitative point of view, since inconsistencies in control room operations, technological quality, and human cognitive ability made a purely quantitative study impractical. Also, “TO-BE” candidates were not implemented in the physical world, and it is recommended that future, more specialised studies implement “TO-BE” findings in control room systems, for stronger validation of prospective solutions.

In this research, routing options and stack handling measures were implemented in the model, but analysed rather superficially, since routing options vary between control rooms and a single setting cannot be descriptive of all the control rooms in a given industry. It was found that only minor fluctuations in output variables were present when these measures were altered. This research was conducted to construct a generalised event management system of control room systems. Nevertheless, it is recommended that detailed routing options and stack-logic are considered based on the specific setting the analysis will commence in, since a specific industry may be more susceptible to fluctuations in outputs due to routing options.

Future research efforts should focus on intelligent technologies that can decrease the number of false positives originating in the first place, and that keeps a human in the system at a high-level.

Therefore, the findings in this research contribute to the fifth industrial revolution, or industry 5.0, since it is found that, at the time of this research, humans and industry 4.0 technology complement each other and they perform better combined than separated. This finding is made based on the currently available technology, should humanised AI become available, it is recommended that it is compared to a scenario where the strengths of humans and AI are in cooperation.

Appendix A

Table 14: Combinations of possible "Best 'AS-IS'" models

Experiment 1					
Scenario	Routing logic	Prioritisation logic	Input device system on LRR	Input device system on MRR	Input device system on HRR
1	Lowest on stack	FIFO	IDS	IDS	IDS
2	Random	FIFO	IDS	IDS	IDS
3	Lowest on stack	Fast track	IDS	IDS	IDS
4	Random	Fast track	IDS	IDS	IDS
5	Random	FIFO	IDS + CCTV	IDS + CCTV	IDS + CCTV
6	Random	FIFO	IDS + SID	IDS + SID	IDS + SID
7	Random	FIFO	IDS	IDS + CCTV	IDS + SID
8	Random	FIFO	IDS + SID	IDS	IDS + CCTV
9	Random	FIFO	IDS + CCTV	IDS + SID	IDS
10	Random	FIFO	IDS	IDS + SID	IDS + CCTV
11	Random	FIFO	IDS + CCTV	IDS	IDS + SID
12	Random	FIFO	IDS + SID	IDS + CCTV	IDS
13	Random	FIFO	IDS	IDS	IDS + CCTV
14	Random	FIFO	IDS + CCTV	IDS	IDS
15	Random	FIFO	IDS	IDS + CCTV	IDS
16	Random	FIFO	IDS	IDS	IDS + SID
17	Random	FIFO	IDS + SID	IDS	IDS
18	Random	FIFO	IDS	IDS + SID	IDS
19	Random	FIFO	IDS + CCTV	IDS + CCTV	IDS + SID
20	Random	FIFO	IDS + SID	IDS + CCTV	IDS + CCTV
21	Random	FIFO	IDS + CCTV	IDS + SID	IDS + CCTV
22	Random	FIFO	IDS + CCTV	IDS + CCTV	IDS
23	Random	FIFO	IDS	IDS + CCTV	IDS + CCTV
24	Random	FIFO	IDS + CCTV	IDS	IDS + CCTV
25	Random	FIFO	IDS + SID	IDS + SID	IDS + CCTV
26	Random	FIFO	IDS + CCTV	IDS + SID	IDS + SID
27	Random	FIFO	IDS + SID	IDS + CCTV	IDS + SID
28	Random	FIFO	IDS + SID	IDS + SID	IDS
29	Random	FIFO	IDS	IDS + SID	IDS + SID
30	Random	FIFO	IDS + SID	IDS	IDS + SID
31	Random	Fast track	IDS + CCTV	IDS + CCTV	IDS + CCTV
32	Random	Fast track	IDS + SID	IDS + SID	IDS + SID

33	Random	Fast track	IDS	IDS + CCTV	IDS + SID
34	Random	Fast track	IDS + SID	IDS	IDS + CCTV
35	Random	Fast track	IDS + CCTV	IDS + SID	IDS
36	Random	Fast track	IDS	IDS + SID	IDS + CCTV
37	Random	Fast track	IDS + CCTV	IDS	IDS + SID
38	Random	Fast track	IDS + SID	IDS + CCTV	IDS
39	Random	Fast track	IDS	IDS	IDS + CCTV
40	Random	Fast track	IDS + CCTV	IDS	IDS
41	Random	Fast track	IDS	IDS + CCTV	IDS
42	Random	Fast track	IDS	IDS	IDS + SID
43	Random	Fast track	IDS + SID	IDS	IDS
44	Random	Fast track	IDS	IDS + SID	IDS
45	Random	Fast track	IDS + CCTV	IDS + CCTV	IDS + SID
46	Random	Fast track	IDS + SID	IDS + CCTV	IDS + CCTV
47	Random	Fast track	IDS + CCTV	IDS + SID	IDS + CCTV
48	Random	Fast track	IDS + CCTV	IDS + CCTV	IDS
49	Random	Fast track	IDS	IDS + CCTV	IDS + CCTV
50	Random	Fast track	IDS + CCTV	IDS	IDS + CCTV
51	Random	Fast track	IDS + SID	IDS + SID	IDS + CCTV
52	Random	Fast track	IDS + CCTV	IDS + SID	IDS + SID
53	Random	Fast track	IDS + SID	IDS + CCTV	IDS + SID
54	Random	Fast track	IDS + SID	IDS + SID	IDS
55	Random	Fast track	IDS	IDS + SID	IDS + SID
56	Random	Fast track	IDS + SID	IDS	IDS + SID
57	Lowest on stack	FIFO	IDS + CCTV	IDS + CCTV	IDS + CCTV
58	Lowest on stack	FIFO	IDS + SID	IDS + SID	IDS + SID
59	Lowest on stack	FIFO	IDS	IDS + CCTV	IDS + SID
60	Lowest on stack	FIFO	IDS + SID	IDS	IDS + CCTV
61	Lowest on stack	FIFO	IDS + CCTV	IDS + SID	IDS
62	Lowest on stack	FIFO	IDS	IDS + SID	IDS + CCTV
63	Lowest on stack	FIFO	IDS + CCTV	IDS	IDS + SID
64	Lowest on stack	FIFO	IDS + SID	IDS + CCTV	IDS
65	Lowest on stack	FIFO	IDS	IDS	IDS + CCTV
66	Lowest on stack	FIFO	IDS + CCTV	IDS	IDS
67	Lowest on stack	FIFO	IDS	IDS + CCTV	IDS
68	Lowest on stack	FIFO	IDS	IDS	IDS + SID
69	Lowest on stack	FIFO	IDS + SID	IDS	IDS
70	Lowest on stack	FIFO	IDS	IDS + SID	IDS
71	Lowest on stack	FIFO	IDS + CCTV	IDS + CCTV	IDS + SID

72	Lowest on stack	FIFO	IDS + SID	IDS + CCTV	IDS + CCTV
73	Lowest on stack	FIFO	IDS + CCTV	IDS + SID	IDS + CCTV
74	Lowest on stack	FIFO	IDS + CCTV	IDS + CCTV	IDS
75	Lowest on stack	FIFO	IDS	IDS + CCTV	IDS + CCTV
76	Lowest on stack	FIFO	IDS + CCTV	IDS	IDS + CCTV
77	Lowest on stack	FIFO	IDS + SID	IDS + SID	IDS + CCTV
78	Lowest on stack	FIFO	IDS + CCTV	IDS + SID	IDS + SID
79	Lowest on stack	FIFO	IDS + SID	IDS + CCTV	IDS + SID
80	Lowest on stack	FIFO	IDS + SID	IDS + SID	IDS
81	Lowest on stack	FIFO	IDS	IDS + SID	IDS + SID
82	Lowest on stack	FIFO	IDS + SID	IDS	IDS + SID
83	Lowest on stack	Fast track	IDS + CCTV	IDS + CCTV	IDS + CCTV
84	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + SID
85	Lowest on stack	Fast track	IDS	IDS + CCTV	IDS + SID
86	Lowest on stack	Fast track	IDS + SID	IDS	IDS + CCTV
87	Lowest on stack	Fast track	IDS + CCTV	IDS + SID	IDS
88	Lowest on stack	Fast track	IDS	IDS + SID	IDS + CCTV
89	Lowest on stack	Fast track	IDS + CCTV	IDS	IDS + SID
90	Lowest on stack	Fast track	IDS + SID	IDS + CCTV	IDS
91	Lowest on stack	Fast track	IDS	IDS	IDS + CCTV
92	Lowest on stack	Fast track	IDS + CCTV	IDS	IDS
93	Lowest on stack	Fast track	IDS	IDS + CCTV	IDS
94	Lowest on stack	Fast track	IDS	IDS	IDS + SID
95	Lowest on stack	Fast track	IDS + SID	IDS	IDS
96	Lowest on stack	Fast track	IDS	IDS + SID	IDS
97	Lowest on stack	Fast track	IDS + CCTV	IDS + CCTV	IDS + SID
98	Lowest on stack	Fast track	IDS + SID	IDS + CCTV	IDS + CCTV
99	Lowest on stack	Fast track	IDS + CCTV	IDS + SID	IDS + CCTV
100	Lowest on stack	Fast track	IDS + CCTV	IDS + CCTV	IDS
101	Lowest on stack	Fast track	IDS	IDS + CCTV	IDS + CCTV
102	Lowest on stack	Fast track	IDS + CCTV	IDS	IDS + CCTV
103	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS + CCTV
104	Lowest on stack	Fast track	IDS + CCTV	IDS + SID	IDS + SID
105	Lowest on stack	Fast track	IDS + SID	IDS + CCTV	IDS + SID
106	Lowest on stack	Fast track	IDS + SID	IDS + SID	IDS
107	Lowest on stack	Fast track	IDS	IDS + SID	IDS + SID
108	Lowest on stack	Fast track	IDS + SID	IDS	IDS + SID

Appendix B

In this appendix, the detailed processes used in the Simio simulation environment are shown and elaborated on.

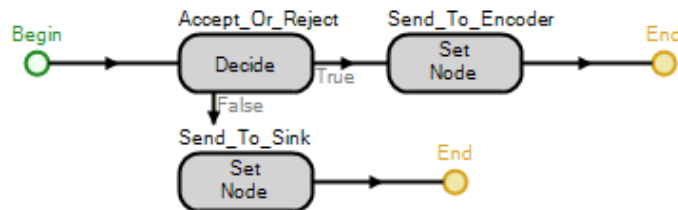


Figure 54: Process for accepting or rejecting an event

Figure 54 showcases the process that the ID system on-site follows for accepting or rejecting an event. This framework accepts incidents and false alarms at a rate similar to the actual industry data to ensure that the rate and ratio at which incidents and false alarms arrive at the control room are realistic. Three such processes are defined and implemented for the high, medium and low residual risk sites. Figure 55 below illustrates the process defined to determine the maximum possible cost of input device systems in the control room system. This is done to determine the cost-ratios of each scenario to compare them on a relativistic basis.

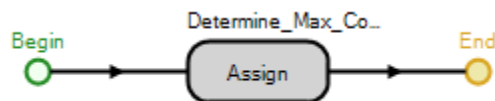


Figure 55: Maximum cost allocation

Figure 56 shows the process used to define events as either incidents or false alarms based on historical data. This process only defines the type of event - the creation rates of events are defined at the sources.

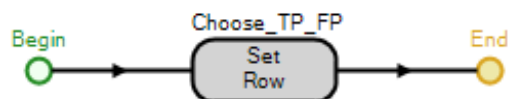


Figure 56: Event creation process

Figure 57 illustrates the process used in the simulation model to define how an event will be interpreted by the functional units. It should be noted that this is determined in the simulation environment before an event reaches the functional unit, and it is based on historical data. At first, the process determines at which site the event occurred and what the residual risk of that site is. Next, the probability of the event being interpreted correctly is determined by considering the type of input device system installed on the site at which the event generated, and the interpretation accuracy operators had historically with these systems installed on-site. Events are then assigned a variable declaring if it will be interpreted correctly or incorrectly throughout its entire life.

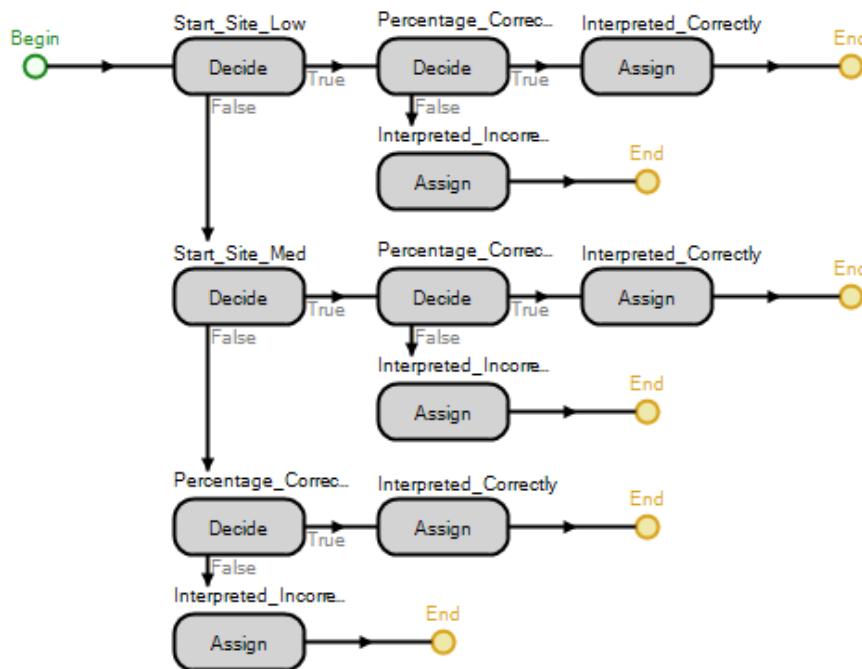


Figure 57: Event interpretation process

Figure 58 below showcases the process used in the simulation environment to create the first bin of data on the event at hand that will be sent to the control room. As mentioned previously, all the alarms are assumed to be signalled by the same quality ID system, except for the tiny AI experiment. Hence, an IDS bin of random size (within the defined ranges) is created. A random number of event indicators is then generated, also within the defined ranges. The density of value-adding information is then determined and this density is considered a sample value for the Monte Carlo analysis. The i_i value is then chosen to be this Monte Carlo sample for further analysis. Next, the site on which the event originated is determined and it is assigned to either has

originated in a sensitive area or a normal area by considering actual ratios of sensitive and normal areas in historical data.

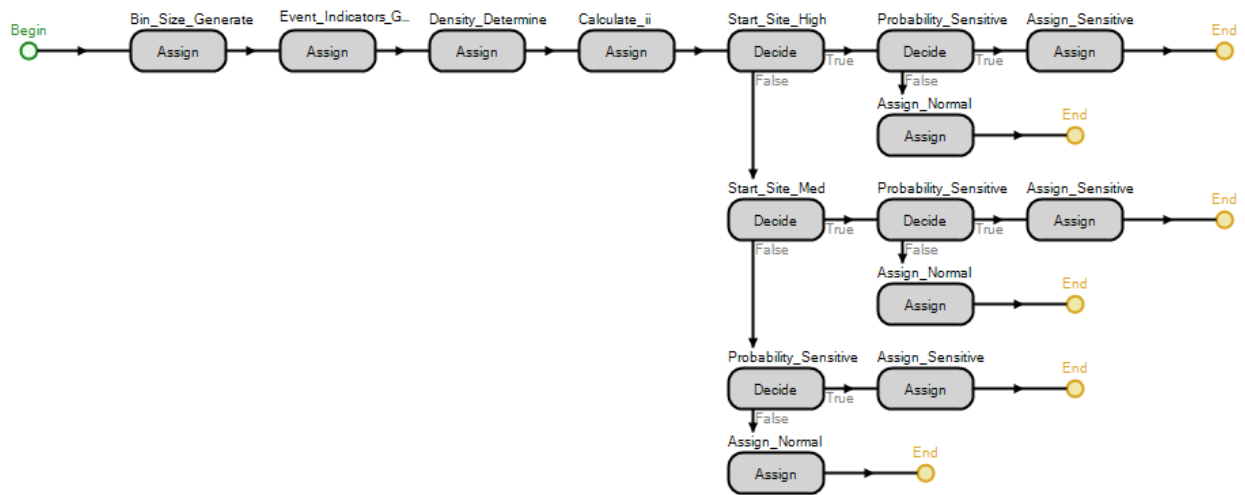


Figure 58: The original bin

Figure 59 shows the process used to determine the i_R value, which is the amount of value-adding information required for the functional unit to be able to decide on an alarm's cause. First, the entity confirms which functional unit is currently busy processing the information available on it. Thereafter, the score of that functional unit is extracted from a table and i_R is determined.

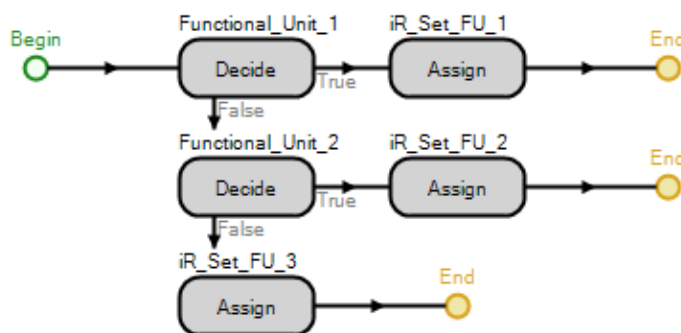


Figure 59: Define the i_R value

Figure 60 showcases the process defined in the Simio environment to determine the perceived risk score (r) of an event. This process is a sub-process of the functional unit processing logic shown in figure 61. Therefore, the processes of figure 60 and figure 61 will be explained concurrently in the following section.

Starting in figure 61, the first step in the functional unit processing logic is to execute the sub-process shown in figure 60. The event is first deemed tolerable or intolerable based on whether (i) it triggered an alarm in a sensitive area or not, or (ii) if it has been in the system for the longest tolerable amount of time or not. If it is deemed tolerable, in other words, if it had not triggered an alarm in a sensitive area nor has it been in the system for an intolerable amount of time, the current certainty is determined with the i_l and i_R values determined earlier.

On the other hand, if it is deemed intolerable, r is immediately set to a value larger than a - the intolerable region threshold. Its “threshold comparable” value is set to c , since it is not comparable to threshold a or b and this will be used later in the processes. It should be noted that c is not a threshold, only a and b are, but the variable must be set to a value other than a or b to make decisions in the following steps. After the r -value is determined, or the event is deemed intolerable, the process shown in figure 60 is exited and the next steps of the process shown in figure 61 will commence.

Figure 60: Process to determine the perceived risk score

Continuing the process shown in figure 61, the entity is tested to see with what threshold it will be compared to. If the “threshold comparable” value is set to c , it is deemed intolerable and the process ends immediately. However, if the “threshold comparable” value is set to a or b , the entity will commence in the process. The r -value of the entity is then extracted to confirm it is still in the undecided region. If the event is either intolerable or tolerable, the process is exited. However, if it is indeed still in the undecided region, the process commences to determine on which site the event occurred. After it is known on which site the alarm occurred, the input devices systems available on those sites are identified.

A random bin-size is generated and it depends on the typical bin-size ranges of the input devices located on the site where the event occurred. A random number of event indicators are generated – also dependent on the typical ranges of event indicators for a given input device system. Next, the density of informative information is determined as a Monte Carlo sample, and the process is delayed to simulate the bin transferring times and the processing times of the functional units. These times are directly proportional to the size of the bin and the type of data. The new i_i -value is calculated and the process is looped back to the beginning, where the process shown in figure 60 is executed again. This will continue until the event is either considered tolerable or intolerable.

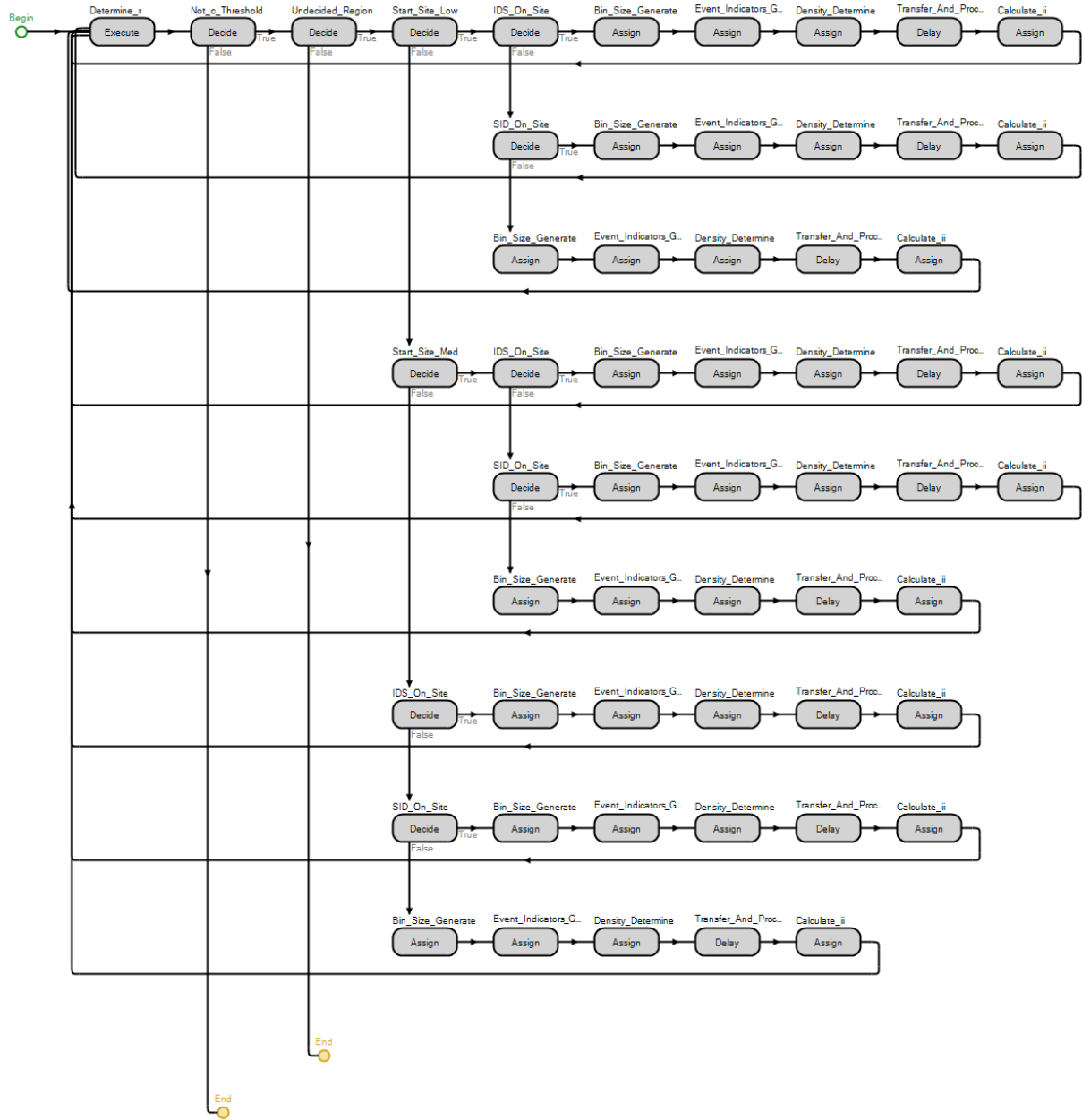


Figure 61: Functional unit processing logic

Appendix C

[SAJIE/2423] Editor Decision: Acceptance  



Dr Teresa Hattingh 29779235@nwu.ac.za [via sun.ac.za](mailto:via@sun.ac.za)
to Johann, me, lynette.pieterse ▾

Thu, Sep 17, 1:54 PM   

Dear authors

Your article "SAJIE31/3 Synthesis and Evaluation of an Industry 4.0 Control Room" has been considered and selected for the special edition, as part of the SAJIE31 conference review process. Your SAJIE article has now been registered in the SAJIE online system and has a new reference number, as shown in the subject line.

The publication fee is now payable. The publication fee is now payable (you do not have to pay submission fees). An invoice will be sent under separate cover with the banking details.

- Publication fee for articles with a South African affiliation: R2250 + 15% VAT
- Publication fee for international articles: USD275 + 15% VAT

Once payment is received, the article will be sent for language editing and final layout. You will be contacted to review the final proof.

Dr Teresa Hattingh
Special Edition Editor

South African Journal of Industrial Engineering
<http://sajie.journals.ac.za>
sajie@saie.co.za

Appendix D

South African Journal of Industrial Engineering November 2020 Vol 31(3) Special Edition, pp 1-12

SYNTHESIS AND EVALUATION OF AN INDUSTRY 4.0 CONTROL ROOM

E.L. Hugo^{1*} & J.E.W. Holm²

ARTICLE INFO	ABSTRACT
Article details Presented at the 31st annual conference of the Southern African Institute for Industrial Engineering (SAIIE), held virtually from 5-7 October 2020. Available online 11 Nov 2020 Contact details * Corresponding author eduan.hugo@gmail.com Author affiliations 1 Department of Industrial Engineering, North-West University, South Africa 2 Department of Electrical & Electronic Engineering, North-West University, South Africa ORCID® identifiers E.L. Hugo https://orcid.org/0000-0001-8685-1890 J.E.W. Holm https://orcid.org/0000-0003-2862-909X DOI https://dx.doi.org/10.7166/31-3-2423	The technological world is ever-evolving, and industries worldwide must match the pace of inevitable change. We are in the midst of the fourth industrial revolution, and many are suggesting that there may be a fifth industrial revolution in sectors where human interaction is critical. Control rooms are important functional units in many industries, which raises the question of the relevance of Industry 4.0 technologies in the modern-day control room system. A focus area of this study includes defining a generalised operational architecture of a real-world control room with event management functionality – the ‘AS-IS’ model. The impact of intelligent technologies on typical control room operations is modelled holistically (‘TO-BE’), and compared with contemporary control rooms to unearth design considerations for future control room development. OPSOMMING Die tegnologiese wêreld ontwikkel voortdurend en industrieë wêreldwyd moet aanpas by die tempo van verandering. Die mensdom is in die middel van ’n vierde industriële rewolusie gewikkel en daar is sprake van ’n vyfde rewolusie in sektore waar menslike interaksie krities is. Beheerkamers vorm ’n belangrike funksionele element van baie industrieë, wat die vraag na vore bring oor die toepaslikheid van Industrie 4.0 tegnologie in ’n moderne beheerkamerstelsel. Die fokus van hierdie studie sluit die definisie van ’n veralgemeende bedryfsargitektuur van ’n regte-wêreld beheerkamer in, met inagneming van gebeurlikheidsbestuurfunksies - die huidige of ‘AS-IS’ model. Die impak van intelligente tegnologie op ’n tipiese beheerkamer se bedryf word holisties gemodelleer (die toekomstige of ‘TO-BE’ model) en word vergelyk met kontemporêre beheerkamers om die ontwerpsoorwegings van ’n toekomstige beheerkamer te ontgin.

1 INTRODUCTION

Significant technological advancements have been made in recent years, and Industry 4.0 technologies have proven revolutionary in many fields. This paper analyses the effects of Industry 4.0 methods in a control room system through alterations to a simulated ‘AS-IS’ system. If applicable methods and technologies can be identified and proven effective, it may assist the designers of modern control rooms to develop more efficacious systems in the future.

Control rooms are used in various industries, including nuclear power generation, traffic control, and private security [1]. Although these industries are explicitly unique, the fundamental control room function of *event management* is universal. In this analysis, the focus will be on a security control room, as it is the real-world system that is under investigation.

In a security control room, incoming events are typically categorised as either *incidents* or *false alarms*; and it is the task of an operator to classify events as either of these categories. The classification must be done promptly, for if the event is indeed an incident, it may *escalate* and result in material and related intangible losses.

The number of sites served by a control room typically depends on whether the system is loosely or tightly integrated. Tightly integrated systems, such as nuclear power plant systems, serve a single site, whereas

1

loosely integrated systems, such as traffic control or some security settings, serve many sites over various geographic locations simultaneously. The control room of interest, the security control room, is thus an example of a loosely integrated operational system, as opposed to a highly automated tightly integrated system.

Typically, control rooms in a loosely integrated system do not perform high levels of proactive surveillance, but rather monitor reactively. This is natural, since a few operators cannot keep track of real-time phenomena on literally thousands of distributed sites. Therefore, these control rooms act largely on a *reactive* basis, and the focus of control room operators is on events originating at the monitored sites.

2 SUMMARY OF THE LITERATURE AND THEORY

2.1 Event management

Event management is important in the control room environment, as the operational worth of a control room is dependent on its ability to manage events. The most important goal of event management is to restore the system to its normal operating conditions as quickly as possible [2]. This is to ensure that the best possible levels of service are provided, and that minimal downtime is experienced.

Event management, in its abstract form, is similar in control rooms over various industries. In the security control room environment, an important goal is to lower the allowed incident escalation time by reacting timeously to an event. This is not only the case for security control rooms, since incidents in other industries may also escalate over time. Examples include an attack on confidential information in the IT industry, and a road accident in the traffic control industry. The objective, therefore, is to manage events effectively to get incidents under control and arrest escalation.

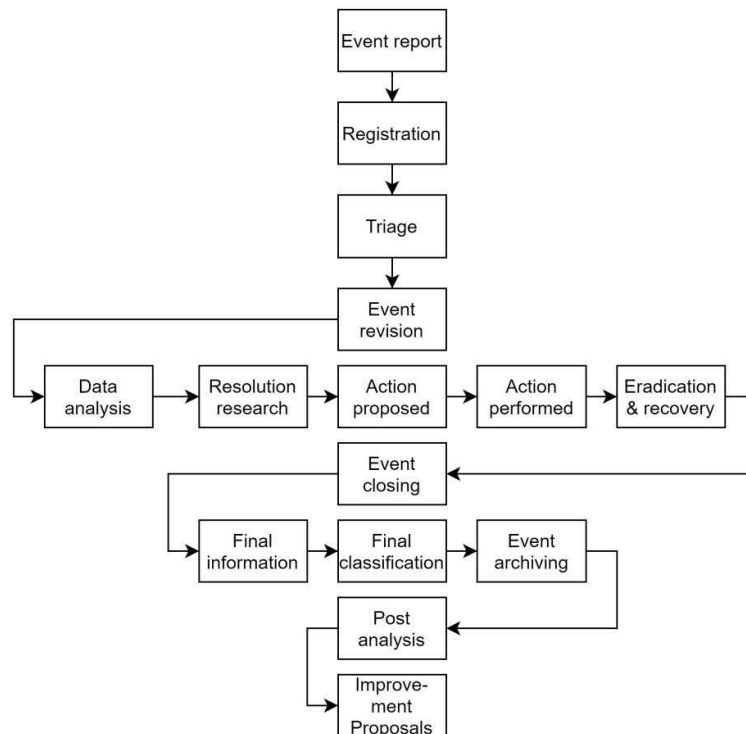


Figure 1: Detailed general event management flowchart, adapted from Maj, Reijers and Stikvoort [3]

The steps in an event management process are shown in the flowchart in Figure 1. After (i) an event has been reported, (ii) a decision is made as to its severity, after which (iii) appropriate action is taken, and

(iv) the event is closed. Should an event be a false alarm, its severity is negligible, and no action is taken at the time. However, in the case of an actual incident, the type of incident will determine the severity, and reaction personnel are dispatched to get the incident under control. The additional steps that are shown above (pertaining to the management of an event over its life cycle) do not directly influence the escalation of incidents, as these steps only occur after the event is under control.

The tasks in the flowchart in Figure 1 are executed using different resources, which will be discussed in the sections to follow. These resources are deployed in a particular 'AS-IS' configuration — the configuration currently employed by the control room system under investigation. The system includes distributed monitoring points (sites) that form part of the analysis, as these sites interface with the main control room and the reactive resources. The 'TO-BE' configuration will take on a different form as new functions are introduced in the form of Industry 4.0 methods.

2.2 Video analysis as an Industry 4.0 method

It is important to provide a brief overview of video analysis, as it has a significant influence on the configuration of resources in the overall security control room system. Video analysis is a method for the autonomous recognition and tracking of objects in monitored scenes. The technological advances in this field are significant, and robust object detection is receiving significant attention. Mustafah and Azman define robust object detection as “the problem of locating an object of interest in an image in the presence of uncontrolled lighting, complex background, and variations of appearance and orientation such as scale and rotation” [4]. Given sufficient image quality, robust object detection has a relatively high success rate. Video scene analysis is the process of recognising and analysing humans and objects from live-streamed or recorded video scenes, in an attempt to recognise human action, classify activities, and interpret scenes [5]. Relatively unsophisticated scene analysis can easily be accomplished with modern technology through intelligent automation.

Robust object detection and scene analysis collaborate to perform tasks — such as eliminating sections in video clips where no change in a scene is detected, or emphasising sections where humans are detected with intrusion tools. Scenes can also be automatically analysed to determine intelligently and ‘on the fly’ whether alarms should be sounded or not. Both scene analysis and object detection are widely available and are relatively inexpensive, and open-source versions can be obtained online and adapted to fit many settings with minimal effort and expense.

2.3 Information-to-noise ratio

A ratio commonly used in communication systems that may apply directly to this analysis is the signal-to-noise ratio, which gives an indication of how much signal energy is contained in a symbol relative to the noise present in a noisy communications channel. When the signal energy is high relative to noise energy, a symbol is easily recognised and information can be retrieved. A decision is then made as to the type of symbol received, and a high signal-to-noise ratio gives a high level of confidence in the decision [6].

In recent research publications, this ratio has also been informally used and lightly remodelled, such as with the *spam-to-content* ratio in online discussion forms [6, 7]. It is thus used as a symbolic expression referring to the ratio of relevant or favourable data to irrelevant or unfavourable data.

Similarly, in the case of data sent across the channels between distributed sites and the control room, some data does not carry actual information and may be considered noise. Thus the information-to-noise ratio of a section of data is defined as the ratio of informative data to noise in a specific section of data.

3 MODEL CONCEPTS

3.1 The bin approach

Input devices are devices that are located on monitored sites that provide a control room with decision-making data. The total data obtained from input devices consists of informative event data, referred to as *event indicators* in this research, and *noise*, which is recorded data that contributes no value toward the identification of an event’s cause. Event indicators are informative, in the sense that they provide information that helps a control room determine why an event was generated. Consequently, event indicators contribute to the certainty that the control room has about an event’s underlying cause.

A *bin* is defined for the purpose of this research as a packet of data provided by equipment on a remote site that contains information about an event. Bins will thus vary in size for different equipment types, and

will contain both event indicators and noise. Furthermore, the number of event indicators would typically be different in every bin, since the events recorded at the sites are *random and unique*. The result is that every bin will embody distinct densities of informative data, and each bin will thus contribute to a distinct amount of certainty.

In the control room setting, event indicators are favourable and noise is unfavourable. This is because only event indicators contribute to effective decision-making. It is advantageous, therefore, to obtain high indicator-to-noise ratios in bins, as more certainty about an event's cause is gained from more informative bins. This is in line with the discussion on information-to-noise, where the informative elements, in this case, are called 'event indicators'.

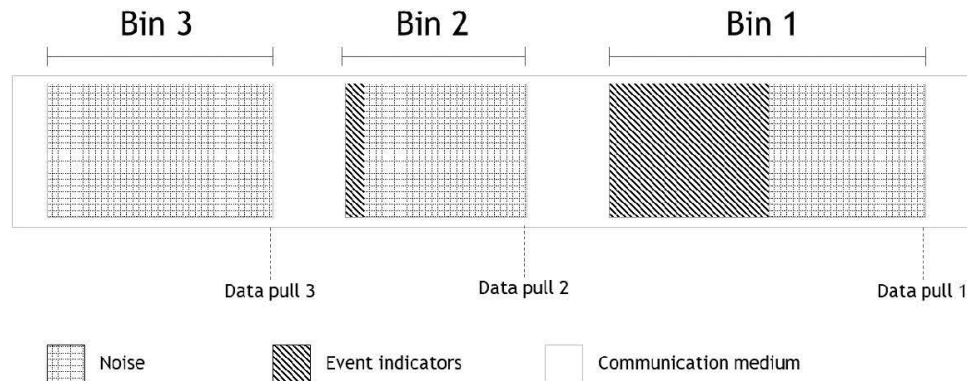


Figure 2: Illustration of the bin concept

Figure 2 illustrates the bin concept for a scenario where data is pulled from a site three times in a row and transmitted over a communication channel from a remote site to the control room. The bins shown in Figure 2 are of varying sizes, to illustrate that data is typically obtained over different timeframes.

Bin 1 contains around 50 per cent event indicators, and of the three bins it is the most significant contributor to certainty. The second bin contains a lower indicator-to-noise ratio than the first. Nevertheless, it contributes marginally to the certainty that the control room has about the event's cause. The third bin exclusively contains noise, and contributes nothing to the certainty that operators have on the cause of the event.

In line with decision theory in a data channel, with fewer event indicators and more noise, the likelihood of making an incorrect decision is high, more event indicators are required, and more time is spent on obtaining such indicators. This is clearly undesirable, and one would want an Industry 4.0 technology to provide more event indicators and less noise, thus being more informative.

Thus the information-to-noise ratio of a bin influences the density of informative data in a bin. Operators will be able to identify the cause of an alarm quicker and with more certainty when an increase in the density of informative data is present in a bin. 'Informativity' is thus defined in this research as the information-to-noise ratio in a bin (over a defined period of time), where highly informative technologies will provide a relatively large amount of valuable information in a short period of time, with little or no noise. In other words, devices with high levels of informativity will consistently provide the control room with bins containing high densities of useful information.

3.2 Simulation modelling

For this research, a detailed model was built with simulation software to represent functionally a loosely integrated security control room. Many simulation software packages have the functional requirements to simulate the event management of a control room system; however, SIMIO® simulation software was the chosen package, since reputable researchers have previously used SIMIO® in systems analysis and design [8, 9]. The next section includes an analysis of the event management of a loosely integrated security control room.

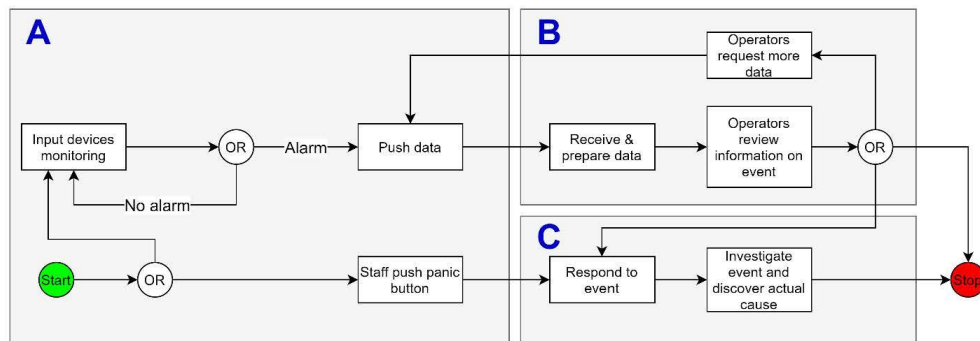


Figure 3: The operational flow of a loosely integrated security control room system

The operational flow of a loosely integrated security control room system can be divided into three sections, A, B, and C, as shown in Figure 3:

- A. The sites
- B. A control room
- C. The field workers

In a real-world setting, a site's personnel are on-site during business hours; they can be contacted to gain more information about the circumstances on site, and so become part of the information provisioning system. After business hours, however, personnel are unavailable, and control room operators must identify the cause of an event remotely by receiving and processing 'bins' of site data. Figure 4 showcases the architecture of a typical site (A) and a control room (B). Note that the number and scale of elements, such as input devices and operators, are for illustration purposes only. The following discussion defines the real-world model from which the abstracted model was derived; this is done to validate the functional definition of the abstracted model as applied in simulations.

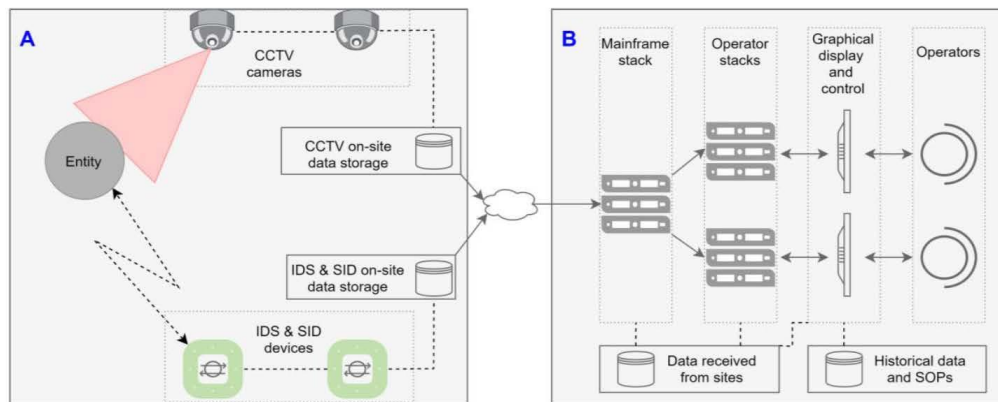


Figure 4: Architecture of a loosely integrated security control room system

The sites contain input devices that generate alarms and store the data on site. Alarms are signalled when entities are identified on site and data is pushed over the cloud to the control room for processing. Similarly, data such as CCTV footage can be pulled from sites to the control room. The control room is then notified about the alarm (event reported), after which a standard operating procedure (SOP) is executed, based on the applicable scenario and severity. The operator then attempts to identify what caused the alarm by processing the available information on the event, and pulling more data as needed from CCTV footage or any other available device that can inform the operators about the activities on site. This is an iterative process, and the operator gradually gains certainty about what has caused the alarm, which then guides the operator on how to manage the event. This is a common scenario in event management, where

information (observation) is iteratively gathered, and its quality is improved in order to define the underlying cause (reality).

If the operator presumes that an alarm is caused by an actual incident, or if the operator is unsure about what caused the alarm, a task force is notified to respond. If the alarm is, in fact, a false alarm, mitigations are implemented to reduce the occurrence of these specific false alarms in the future by changing the site's physical configuration. After responding to an event, an investigation begins to analyse potential new *modi operandi* and other intelligence that will be used to mitigate future attacks (risks).

Risk is an important factor in the event management functionality of a control room, as the risk of an event guides an operator on how to manage and prioritise it. It is important to note that the risk factor that guides an operator in the event management process is not the *actual* risk of an event, but rather the *perceived risk* of an event. Events are therefore managed based on an operator's perception and interpretation – which is formed by the available useful information on the event at the time, and which changes as more information is gained.

The number of operators in security control rooms varies depending on the number of sites that the control room serves. In the simulation model for this analysis, three operators are simulated, together with 2 000 sites of varying risk levels, or classes. Site risks are classified as low, medium, or high risk, depending on factors such as the value of the assets being protected, their geographic location, and the measure of security mitigations implemented at each site. For practicality, these sites are not modelled individually, and three event-generating sources are implemented in the model. The number of events generated in the simulations at these sites is scaled to match those expected from each of the site risk classes (low, medium, or high).

The sources of events at the sites of the simulation model *randomly* create events at reasonable frequencies while considering the historical incident-to-false-alarm ratio. Events are then either detected or missed by the devices on-site, based on the predetermined incident and false alarm *acceptance rates*. As events flow through the system, they are assigned a perceived risk value, which is based on the *perceived probability* that an event is an incident and on the corresponding impact an incident may have on the site where it originated.

The perceived probability of an event being an incident is directly proportional to the certainty that an operator has about what caused an event. Also, the impact an incident may have on a site is derived from the risk class of a site. The perceived risk value of the event therefore changes as operators receive event indicators in bins related to the event. If the perceived risk score of an event surpasses the tolerable or intolerable thresholds, it is managed appropriately. Events may, therefore, be responded to incorrectly, as the risk may be wrongly classified owing to incorrect presumption.

Owing to the randomness of the events that occur on sites, it is imperative that the short-term operations of a control room differ accordingly. Therefore, appropriate probability distribution ranges in which actual values are likely to transpire were chosen for variables – such as bin sizes, number of event indicators, and processing times. Random values were then simulated in these ranges and, given a sufficiently long simulation time, a good estimation of the actual operational performance of the control room emerged, as stated by the Monte Carlo theorem.

3.3 Model validation

To validate the simulation model and the results, simulation runs were executed and compared with real-world data. The functional flow and architecture of the simulated models were also compared with the real-world model for verification purposes. The simulation data was obtained from recorded real-world data and verified by industry experts.

The number of events in the year 2019 for a real-world control room is compared in Figure 5 with the number of events ultimately generated by the simulation model. The actual number of events in the physical world was scaled to be representative of a control room with three operators. The number of events generated by the simulation model was slightly over 95 per cent accurate relative to the number of events experienced in 2019 by the real-world control room. Note that the number of events experienced in the physical world varies annually, and the above comparison was found to be representative of real-world numbers.

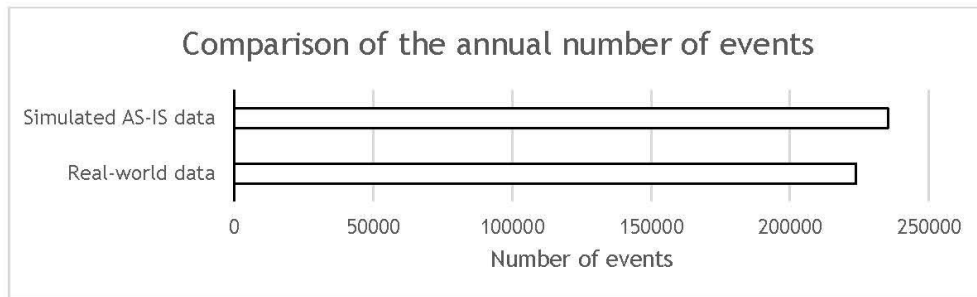


Figure 5: Comparison of the annual number of events for model validation

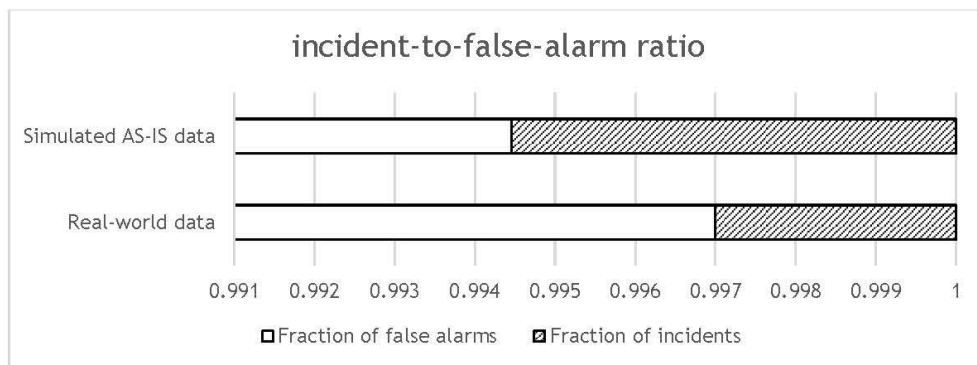


Figure 6: Comparison of the incident-to-false-alarm ratios for model validation

The ratio of incidents relative to false alarms is compared in Figure 6. Note that the horizontal range was limited (i.e., magnified) to show the correspondence between the real-world and the simulated results. From the graph, it is evident that the simulation model compares favourably with real-world data for the incident-to-false-alarm ratio.

It is noted, as with most modelling challenges, that the simulation model will always be an estimation of the real world, as minor variations are always present. However, the goal of this research is to compare a contemporary model with a prospective model in a *relativistic* way, which limits the impact of these small variances. With this relativistic approach, simulated output variables of interest are compared between simulated models, and results will show an improvement, or not. The same assumptions were used in all simulation models.

The validation of the simulation model was important, and it was validated in the following way (as a combination of measures):

1. The simulation model was derived from a real-world control room system, and was designed to be functionally and architecturally similar – this was verified against the real-world functions, and this served as a functional verification.
2. The sequence of task executions of the simulation model also corresponded with the task execution sequence of a control room in the real-world – this verified the functional logic in a process flow.
3. Actual historical data from a real-world, loosely integrated security control room system was included in the simulation model – this was verified by an industry expert and confirmed to be accurate.
4. In terms of performance, the number of events flowing through the simulation model was verified to be sufficiently similar to the real-world data (more than 95% accurate relative to the measured 2019 total), as shown in Figure 5 above.
5. Finally, the ratio of incidents to false alarms was 99.75 per cent accurate, compared with the 2019 ratio of incidents to false alarms in the physical control room, shown in Figure 6.

4 FINDINGS

The influence of technologies such as robust object detection and automated scene analysis can be simulated by employing the bin concept in the SIMIO® environment. These technologies, in effect, eliminate noise levels on the site where an event occurs, which essentially improves the information-to-noise ratio of the bin and reduces its overall size. Events can also be filtered with object detection, and typical events that cause false alarms can be identified and automatically ignored on site, potentially averting the arrival of many false alarms at the control room. This changes the functionality of the overall control room system, as discussed below.

To illustrate the impact of Industry 4.0 technologies on a control room's operations, a relativistic comparison of a basic CCTV control room system ('AS-IS') and an intelligent CCTV control room system ('TO-BE') was performed. The 'TO-BE' system was thus the 'AS-IS' system, with the addition of robust object detection and automated scene analysis on the input devices on all of the sites served by the control room.

The impact of these technologies was simulated by altering the conventional, validated 'AS-IS' simulation model by decreasing the amount of noise in the bins and lowering the average number of non-malicious events triggering false alarms. The rest of the model, including the rate at which events occur, stayed unchanged to ensure that the only variables to change were the ones directly influenced by the Industry 4.0 technologies.

It is difficult to predict exactly how much the relevant variables will change after these technologies have been implemented, as the currently available technology is of varying quality. The impact of these technologies can, however, be illustrated by performing a basic sensitivity analysis, or a 'what-if' analysis. Table 1 portrays how the variables of interest would change in the sensitivity analysis.

Table 1: 'What-if' alterations for the 'AS-IS' to the 'TO-BE' transition

Experiment #	Average noise change in 'TO-BE'	Average acceptance rate of false alarms change in 'TO-BE'	Average change in the number of event indicators in 'TO-BE'
I	-25%	-50%	0%
II	-50%	-50%	0%

The number of event indicators will not reduce in the bins, since only noise is expected to reduce with the addition of Industry 4.0 technology. Also, the technology does not change the physical event occurring on site; rather, it manipulates the recorded data before sending it over the communication medium to the control room.

A cost analysis when using distributed processing as opposed to processing all signals in a control room was not done in this case, as hardware with processing ability had already been installed on the sites, and open-source software can be obtained and implemented.

4.1 Effectiveness

In the simulation model, the number of time incidents escalated during the experiment was determined by recording the time each *actual* incident spent in the system. The time that actual false alarms spend in the system does not contribute to this value, since there they are not malicious events. If an incident is completely missed or misinterpreted as a false alarm, the maximum escalation time, which is the estimated amount of time needed for an incident to escalate to its peak, is added. The maximum possible incident escalation time in the experiment was determined by multiplying the number of incidents generated by the model by the maximum escalation time.

The factors showcased in Figure 7 are determined by the following equations:

$$\text{Incident escalation factor} = \frac{\text{Total time incidents escalated during the experiment}}{\text{Maximum possible incident escalation time in the experiment}} \times 10 \quad (1)$$

$$\text{Response efficiency factor} = \frac{\text{Number of responses and event was indeed an incident in the experiment}}{\text{Total number of responses in the experiment}} \times 10 \quad (2)$$

A factor approach is used to compensate for the randomness in each experimental run. For example, the amount of time an incident escalates cannot be compared directly between experiments, as a different number of events may be present in the experimental runs.

The experiments must be run over a sufficiently long period of time, and through multiple iterations, to ensure that the randomly generated values provide reasonable and consistent estimations. Therefore, the experiments were run over a period of five years, and each of these experiments was repeated 30 times to obtain good averages. With the changes in Table 1 implemented as individual scenarios, the results obtained are shown in Figure 7.

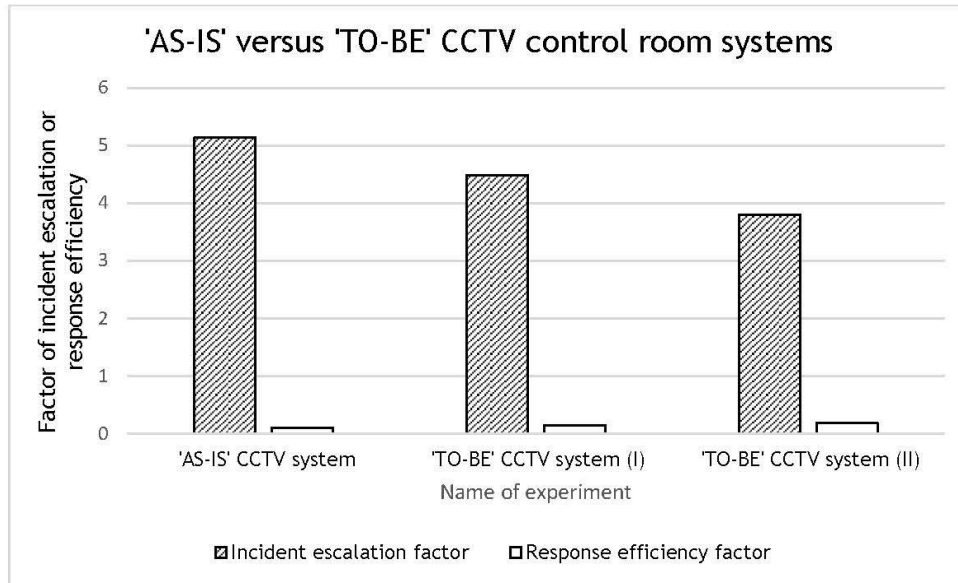


Figure 7: The impact of Industry 4.0 technology on conventional CCTV systems

Since a bin consists of noise and event indicators, the information-to-noise ratios of bins increase when noise is reduced (effectively, the size of the bin may also reduce if noise is eliminated). In effect, smaller bins are transferred over the communication medium between the site and the control room, giving the operators quicker access to the available information on what caused the event (increased confidence). Owing to the reduced size of the bin and the semi-distributed processing nature of this 'TO-BE' model, the time required for an operator to review the bin also decreases. Furthermore, fewer false alarms are present, which results in a less congested control room.

A similar phenomenon can be seen in Figure 8, when the Industry 4.0 technologies are applied to snapshot intrusion detection (SID) devices. These devices are typically intrusion detection devices coupled with image-capturing functionality that provide additional decision-support information in the form of visuals (as opposed to simple detection signals). The bin sizes of conventional SID systems are much smaller than those of CCTV systems (owing to the nature of static images vs CCTV footage), and it should thus be evident that conventional SID systems are more effective in the loosely integrated security setting than are conventional CCTV systems.

Trends in improvement are evident when Industry 4.0 methods are used in both input device systems. Conventional SID systems, however, outperform conventional CCTV systems, since SID systems typically produce bins with better indicator-to-noise ratios (and therefore a higher level of informativity) than CCTV systems. This is because SID systems take snapshots at the moment when an intrusion is detected (a few, highly indicative image frames), as opposed to transmitting large amounts of uninformative data, as is the case with CCTV systems (hundreds of uninformative image frames). However, Industry 4.0 methods in SID systems will still filter out unwanted snapshots, and provide slightly smaller bin sizes than conventional SID systems — hence the relative improvement.

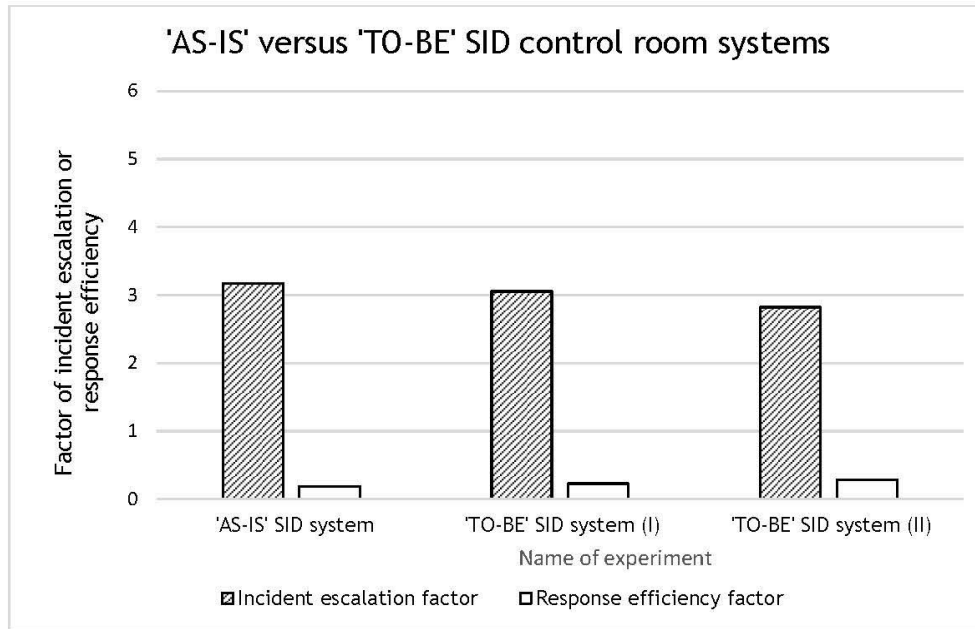


Figure 8: The impact of Industry 4.0 technology on conventional SID systems

Although exact values for the 'AS-IS' to the 'TO-BE' transition had not been identified, the sensitivity or 'what-if' analysis proved that a reduction in noise at the sites monitored by a loosely integrated control room is likely to result in a lower incident escalation factor and better response efficiency. Also, input devices producing bins with high information-to-noise ratios offer high levels of informativity.

4.2 Wastage

Another important goal of the control room is to lower the overall operational expenditure (or wastage, in this case) of reactive forces. In this simulation model, operational expenditure is difficult to measure, since many arbitrary costs such as salaries and fuel prices are present. Therefore, operational expenditure is compared on a relativistic basis by considering *hours worked* and *kilometres driven*. More specifically, a factor-comparison is made based on hours *wasted* and kilometres *wasted*. The two wastage factors are determined by the following equations:

$$\text{Wasted kilometres factor} = \frac{\text{Kilometres wasted responding to false alarms in the experiment}}{\text{Total kilometres driven in the experiment}} \times 10 \quad (3)$$

$$\text{Wasted hours factor} = \frac{\text{Wasted hours responding to false alarms in the experiment}}{\text{Total responding hours in the experiment}} \times 10 \quad (4)$$

The value for 'kilometres wasted responding to false alarms in the experiment' is determined by randomly generating a kilometre value within the expected range every time the task force is incorrectly prompted to respond – in the cases where the events are false alarms. The 'total kilometres driven in the experiment' value is determined by summing all of the kilometres driven when responding. This includes the response actions to both incidents and false alarms.

The value for 'wasted hours responding to false alarms in the experiment' is determined by calculating the time it takes to drive the randomly generated distance every time the event is incorrectly responded to, as well as a randomly generated site-investigation time. Figure 9 contains an illustration of the waste present in both the 'AS-IS' and the 'TO-BE' systems.

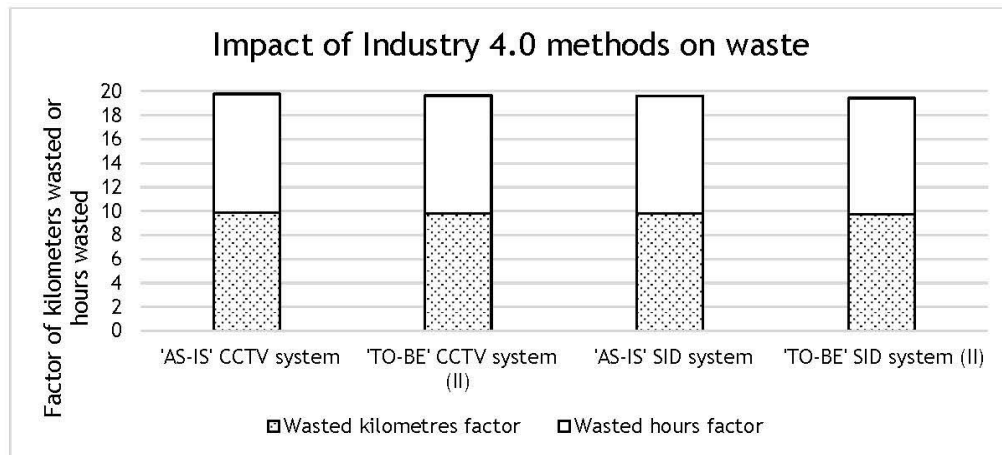


Figure 9: Observations in waste reduction

From Figure 9, it is evident that, in the leftmost ('AS-IS') column, significant waste is evident in operations. This is mostly due to a large number of false alarms relative to incidents that occur on sites, where false alarms are often incorrectly interpreted as incidents. Also, a major reason for wastage is alarm signals for which the cause is uncertain, but for which a reaction team is sent to a site anyway.

Overall, a less pronounced improvement is observed for wastage when Industry 4.0 methods are implemented in both the CCTV and the SID control room systems. A small decrease in both kilometres and hours wasted was noticed. Thus, although not the main consideration, an increase in the speed of event handling and a reduction in false alarms resulted in a minor improvement in wastage.

5 CONCLUSION

In this article we analysed the effects of Industry 4.0 methods on a control room system, with the purpose of (a) defining a context for in-depth research, and (b) demonstrating the advantages of using video analytics (an Industry 4.0 method) for operational effectiveness. Video analytics were introduced to a simulated operating model – in SIMIO® – that represents the event management functionality of a typical loosely integrated security control room. It was found that, when methods such as robust object detection and automated scene analysis are introduced on distributed sites, the operational effectiveness of the control room improves. The time for incidents to escalate is thus reduced, together with a minor reduction in operational costs, as found from the simulations. The analysis done in this research adds value by providing relative improvement measures.

In addition to introducing a control room system environment, the concepts of 'information-to-noise' and 'informativity' were introduced to define the relative information content of an information packet (or bin) and the amount of value-adding information produced by an input device in a set time period respectively. These concepts were applied in the simulated operating models, and will be used in future research to classify different technologies and methods.

We have thus confirmed that existing loosely integrated control room systems can be improved with Industry 4.0 methods to reduce the amount of noise (non-informative data) arriving at the control room, which would inevitably improve both the rate of event processing by an operator and the information transfer rate over the communication channel. These modern methods may also lower operator workload, as fewer false alarms are sent to the control room, which is ascribed to automated decision-making at remote monitoring sites.

The focus of this study was thus on improving the operational effectiveness of the informativity of technology, with an increase in informativity that resulted in an overall operational improvement in the overall control room system. This study is by no means comprehensive, and is the first step towards modelling a complete environment, which will include both cost and effectiveness elements.

Future research will expand the scope of this research, and will include the following:

- Cost analysis – This research considered open-source methods that effectively illustrated that a reduction in noise at distributed sites would improve the operational effectiveness of the control room. An area where future research might contribute is an in-depth cost analysis of commercial software and related technologies when applied in this context.
- Control room in-depth analysis – The impact of the collective improvements of both the control room and the Industry 4.0 methods on site will be analysed in an integrated way by investigating the effects of specific changes on the control room functions and resources.
- Form, fit, and function – Reflecting on this research, it is evident that the configuration change of a control room system, specifically relating to form, fit, and function, results in functional changes. (AI-enhanced tasks, such as decision-making, may be relocated from humans to machines.) These changes will result in changes to resources (humans, machines, and software) and their relative interfaces. These could be analysed.

In summary, it is evident that the introduction of Industry 4.0 methods (and similarly, technology relating to the 4th industrial revolution) improve the performance of control room systems. The framework and results from this research add value to the knowledge base, and future research will use detailed operational analyses to address burning questions relating to both the 4th and the 5th industrial revolutions.

REFERENCES

- [1] Su, R. & Yurcik, W. 2005. *A survey and comparison of human monitoring of complex networks*. University of Illinois at Urbana-Champaign, National Center for Computing Applications (NCSA). Chicago, USA.
- [2] Alam, K.P. & Dhavale, N. 2012. *Data mining tools for integrated complaint management system*. Institute for Development and Research in Banking Technology. Hyderabad, India.
- [3] Maj, M., Reijers, R. & Stikvoort, D. 2010. *Good practice guide for incident management*. European Network and Information Security Agency (ENISA). Heraklion, Greece.
- [4] Mustafah, Y.M. & Azman, A.W. 2012. Out-of-plane rotated object detection using patch feature based classifier. *Procedia Engineering*, 41, pp. 170-174.
- [5] Abbas, Q., Ibrahim, M.E. & Jaffar, M.A. 2018. Video scene analysis: An overview and challenges on deep learning algorithms. *Multimedia Tools and Applications*, 77(16), pp. 20415-20453.
- [6] Alam, S.J., Alam, M.R., Hu, G. & Mehrab, M.Z. 2011. Bit error rate optimization in fiber optic communications. *International Journal of Machine Learning and Computing*, 1(5), pp. 435.
- [7] Wang, B., Zubiaga, A., Liakata, M. & Procter, R. 2015. *Making the most of tweet-inherent features for social spam detection on Twitter*. University of Warwick. Coventry, UK.
- [8] Van der Merwe, G.P.R. 2014. *A risk-based approach to the acquisition of electronic safety equipment for mines*. North-West University. Potchefstroom, South Africa.
- [9] Vik, P., Dias, L., Pereira, G., Oliveira, J. & Abreu, R. 2010. Using Simio for the specification of an integrated automated weighing solution in a cement plant. In *Proceedings of the 2010 Winter Simulation Conference*, Baltimore, USA. IEEE.

References

1. Van der Merwe, G.P.R., *A risk-based approach to the acquisition of electronic safety equipment for mines*. North-West University:2014.
2. Hevner, A.R., et al., *Design science in information systems research*. MIS Quarterly, 2004: p. 75-105.
3. Hevner, A.R., *A three cycle view of design science research*. Scandinavian Journal of Information Systems, 2007. **19**(2): p. 4.
4. Sein, M.K., et al., *Action design research*. MIS Quarterly, 2011: p. 37-56.
5. Mullarkey, M.T. and Hevner, A.R., *An elaborated action design research process model*. European Journal of Information Systems, 2019. **28**(1): p. 6-20.
6. Gregor, S. and Hevner A.R., *Positioning and presenting design science research for maximum impact*. MIS Quarterly, 2013: p. 337-355.
7. Holm, J.E.W. and Van der Merwe, G.P.R., *Quality Research Management Improves Design Research Effectiveness*. South African Journal of Industrial Engineering, 2019. **30**: p. 238-252.
8. Kotek, L., et al., *Impact of microclimate conditions on the control room personnel—case study*. MM Science Journal, 2015. **2015**(03): p. 682-685.
9. Standardization, I.O.f., *ISO 11064*, in *Design of Control Centers – Part 1: Principles for the Design of Control Centers*. 2000.
10. Su, R. and W. Yampaigunurcik, *A Survey and Comparison of Human Monitoring of Complex Networks*. 2005., National Center for Supercomputing, IL.
11. Hodgetts, H.M., et al., *See No Evil: Cognitive Challenges of Security Surveillance and Monitoring*. Journal of Applied Research in Memory and Cognition, 2017. **6**(3): p. 230-243.
12. Hugo, J., et al., *Light Water Reactor Sustainability Program A Reference Plan for Control Room Modernization: Planning and Analysis Phase*. 2013. Idaho National Laboratory (INL).
13. Kelly, M.J., *Preliminary human factors guidelines for traffic management centers*. 1999, United States. Federal Highway Administration.
14. Alam, K.P. and Dhavale,N., *Data Mining Tools for Integrated Complaint Management System*. 2012.

15. Wong, W.K., Loo, C.K. and Lim, W.S., *Omnidirectional Human Intrusion Detection System Using Computer Vision Techniques*. Effective Surveillance for Homeland Security: Balancing Technology and Social Issues, 2013: p. 435-439.
16. Mutemwa, M., Mtsweni, J. andimba, L., *Integrating a Security Operations Centre with an Organization's Existing Procedures, Policies and Information Technology Systems*, in *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. 2018.
17. Voorthuijsen, G.V., et al. *CCTV effectiveness study*. in *Proceedings 39th Annual 2005 International Carnahan Conference on Security Technology*. 2005.
18. Gill, M. and Spriggs, A., *Assessing the impact of CCTV*. Vol. 292. 2005: Home Office Research, Development and Statistics Directorate London.
19. Stainer, M.J., Scott-Brown, K.C. and Tatler, B.W. *On the factors causing processing difficulty of multiple-scene displays*. i-Perception, 2017. **8**(2): p. 2041669516689572.
20. Bryant, D.J., *Classifying simulated air threats with fast and frugal heuristics*. Journal of Behavioral Decision Making, 2007. **20**(1): p. 37-64.
21. Keval, H. and Sasse, M.A., *"Not the Usual Suspects": A study of factors reducing the effectiveness of CCTV*. Security Journal, 2010. **23**(2): p. 134-154.
22. Salvucci, D.D., *On reconstruction of task context after interruption*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2010. Atlanta, Georgia, USA: Association for Computing Machinery. 89–92.
23. Hughes, R.W., Vachon, F. and Jones, D.M., *Disruption of short-term memory by changing and deviant sounds: Support for a duplex-mechanism account of auditory distraction*. Journal of Experimental Psychology: Learning, Memory, and Cognition, 2007. **33**(6): p. 1050.
24. Halin, N., et al., *A shield against distraction*. Journal of Applied Research in Memory and Cognition, 2014. **3**(1): p. 31-36.
25. Lavie, N., *Distracted and confused?: Selective attention under load*. Trends in Cognitive Sciences, 2005. **9**(2): p. 75-82.
26. Simpson, E., *Educational objectives in the psychomotor domain*. Behavioral objectives in curriculum development: Selected readings and bibliography, 1971. **60**(2): p. 1-35.
27. Dee, H.M. and Velastin, S.A., *How close are we to solving the problem of automated visual surveillance?* Machine Vision and Applications, 2008. **19**(5-6): p. 329-343.
28. Schalkoff, R.J., *Artificial intelligence: an engineering approach*. 1990: McGraw-Hill New York.

29. Seshia, S.A., Sadigh, D. and Sastry, S.S. *Towards verified artificial intelligence*. arXiv preprint arXiv:1606.08514, 2016.
30. Kaplan, A. and Haenlein, M., *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*. Business Horizons, 2019. **62**(1): p. 15-25.
31. Klien, G., et al., *Ten challenges for making automation a "team player" in joint human-agent activity*. IEEE Intelligent Systems, 2004. **19**(6): p. 91-95.
32. Fuchs, S., Hale, K.S. and Axelsson, P., *Augmented cognition can increase human performance in the control room*. in *2007 IEEE 8th Human Factors and Power Plants and HPRCT 13th Annual Meeting*. 2007. IEEE.
33. Badpeyma, J., *Analysis of price and entry barriers to bespoke-purpose application markets through static Bayesian game*. Iranian Industrial Economics Studies, 2017. **1**(1): p. 1-12.
34. Lewandowski, J., Salako, A.O. and Garcia-Perez, A., *SaaS enterprise resource planning systems: challenges of their adoption in SMEs*. in *2013 IEEE 10th International Conference on e-Business Engineering*. 2013. IEEE.
35. Kumar, K.K.M., *Software as a service for efficient cloud computing*. Environment, 2014. **7**: p. 10.
36. Atwood, C.A., et al., *Secure Web-Based Access for Productive Supercomputing*. Computing in Science & Engineering, 2016. **18**(1): p. 63-72.
37. Hayashi, E., *Varied Needs for Biological Sample Management*. Applied Clinical Trials, 2016. **25**(10/11): p. 40.
38. De Ketelaere, M. *What's Tiny AI? You'll Want to Know*. in *Digital Health Summit*. 2020. Las Vegas.
39. Pasquier, S., *The cirrostratus platform concepts, architecture and evaluation*. 2009, ETH, Eidgenössische Technische Hochschule Zürich, Department of Computer Science.
40. Alam, S.J., et al., *Bit error rate optimization in fiber optic communications*. International Journal of Machine Learning and Computing, 2011. **1**(5): p. 435.
41. Wang, B., et al., *Making the most of tweet-inherent features for social spam detection on Twitter*. arXiv preprint arXiv:1503.07405, 2015.
42. Mahler, R.P., *Statistical multisource-multitarget information fusion*. 2007: Artech House, Inc.
43. Gros, X., *NDT data fusion*. 1996: Elsevier.

44. Hollnagel, E. and Woods, D.D., *Cognitive systems engineering: New wine in new bottles*. International Journal of Man-Machine Studies, 1983. **18**(6): p. 583-600.
45. Hollnagel, E. and Woods, D.D., *Joint cognitive systems: Foundations of cognitive systems engineering*. 2005: CRC Press.
46. Daniel, H.S., et al., *A Use-Centered Strategy for Designing E-Collaboration Systems*, in *Encyclopedia of E-Collaboration*. 2008, IGI Global: Hershey, PA, USA. p. 673-679.
47. Douglas, G. and Frank, L.G., *Neo-Symbiosis*, in *Encyclopedia of Information Science and Technology, Second Edition*. 2009, IGI Global: Hershey, PA, USA. p. 2773-2777.
48. Janis, I.L. and Mann, L., *Decision-making: A psychological analysis of conflict, choice, and commitment*. 1977: Free press.
49. Goodstein, L. and Rasmussen, J., *The use of man-machine system design criteria in computerized control rooms*. in *Automation for Safety in Shipping and Offshore Petroleum Operations: IFIP/IFAC Symposium*. 1980. North-Holland Publishing Company.
50. Jiang, F., et al., *Artificial intelligence in healthcare: past, present and future*. Stroke and vascular neurology, 2017. **2**(4): p. 230-243.
51. Barafort, B., Mesquida, A.L. and Mas, A., *ISO 31000-based integrated risk management process assessment model for IT organizations*. Journal of Software: Evolution and Process, 2019. **31**(1): p. e1984.
52. Boholm, M., *How do Swedish Government agencies define risk?* Journal of Risk Research, 2019. **22**(6): p. 717-734.
53. Wu, F., Bills, E.L. and Eisner, J., *Advancing Regulatory Science through Comprehensive, Rational Risk Management*. Biomedical instrumentation & technology, 2019. **53**(1): p. 70-74.
54. Aven, T., *Foundations of risk analysis*. 2012: John Wiley & Sons.
55. Elmer, A. *Application of Risk Management in the Marine Transportation System*, in *Conference proceedings 22-Risk Management in the Marine Transportation System*. 2000.
56. Altenbach, T.J., *A comparison of risk assessment techniques from qualitative to quantitative*. 1995, Lawrence Livermore National Lab., CA.
57. Stevens, S.S., *On the theory of scales of measurement*. 1946.
58. Jøsang, A. and Presti, S.L., *Analysing the relationship between risk and trust*, in *International conference on trust management*. 2004. Springer.

59. Pezzotta, G., et al., *Evaluation of discrete event simulation software to design and assess service delivery processes*. Service Supply Chain Systems: A Systems Engineering Approach, 2016. **8**(86): p. 83-100.
60. Zaayman, G. and Innamorato, A., *The application of simio scheduling in industry 4.0*. in *2017 Winter Simulation Conference (WSC)*. 2017. IEEE.
61. Bonetto, A.A., H.P. Castello, and I.R. Wais, *Stream regulation in Argentina, including the superior Paraná and Paraguay rivers*. Regulated Rivers: Research & Management, 1987. **1**(2): p. 129-143.
62. Wang, J., *Handbook of finite state based models and applications*. 2012: CRC Press.
63. Anderson, E.C., Williamson, E.G. and Thompson, E.A., *Monte Carlo evaluation of the likelihood for Ne from temporally spaced samples*. Genetics, 2000. **156**(4): p. 2109-2118.
64. Romlay, F., Ouyang, H. and Nizam, M., *Failure prediction for automotive suspension springs using Gaussian and Monte Carlo method*. International Journal of Vehicle Design, 2011. **55**(1): p. 23-34.
65. Grimson, E., Gutttag, J, Bell, A., *Monte Carlo Simulation*, in *Introduction to Computational Thinking and Data Science*. Fall 2016, Massachusetts Institute of Technology: MIT OpenCourseWare: Cambridge, MA.
66. Bihani, A., *A New Approach to Monte Carlo Simulation of Operations*. Laser, 2014. **20**: p. 0.20.
67. Zarei, A., Harsini, M.N., and Hemmati, H., *Research Journal of Pharmaceutical, Biological and Chemical Sciences*.
68. CAMPUS, E., *Environmental economics and ecosystem valuation—the rationale behind*. 2019.
69. Hugo, E.L. and Holm, J. *Synthesis and evaluation of an industry 4.0 control room*. South African Journal of Industrial Engineering, 2020. **31**(3): p. 1-12.
70. Marinelli, M., *Key requirements for future control room functionality*. 2015.
71. Attiogbé, C., *Modelling and verifying an evolving distributed control system using an event-based approach*. In *International Symposium On Leveraging Applications of Formal Methods, Verification and Validation*. 2014. Springer.
72. Vermaak, N., *Design and synthesis of an image-based object detection system*, in *Engineering*. 2019. North-West University: Potchefstroom. p. 134.
73. Janapa Reffi, V. *Benchmarking Ultra-low Power Machine Learning Systems*, in *tinyML Summit*. 2020. Burlingame, CA: MLPerf.