Tensions between Safety Cases and STAMP – Where do they disagree and who is right?

Daniel Grivicic
Rail Control Systems Australia Pty. Ltd.
Level 8, 136 Exhibition St
Melbourne, 3000, Victoria

daniel.grivicic@railcontrol.com.au

Abstract

Safety engineering faces the dual challenge of creating safety (reducing the risk of harm) and creating assurance (demonstrating that risk is acceptable). Safety Cases grew from the concept that goal-focused, performance-based safety can provide better risk reduction in contrast to safety achieved through prescribed risk controls. Safety Cases use the close association of safety and assurance to drive improvement. Safety Case failures, resulting in system losses, question this tight coupling of safety and assurance. Such failures prompt detractors to challenge whether too much focus on demonstrating safety results in loss due to confirmation bias or complacency. Once such group of critics propose an alternative process, Systems Theoretic Accident Model (STAMP), intended to redirect attention to building safety into a design. Both approaches claim to offer a better solution for system safety. What does it mean for a safety case to be effective? How valid are the criticisms of safety cases? Does STAMP indeed offer an alternative that addresses the criticisms of safety cases? This paper directly compares Safety Cases and STAMP to highlight where they align and by how much they vary. The paper provides a summary of the recent evidence on each side of the debate and suggests ways of application for practitioners.

Keywords: Safety Case, STAMP.

1 Is demonstrating safety a good idea?

Safety engineers are continually faced with the task of balancing tensions between reducing the risk of harm whilst demonstrating that risk is acceptable. Historically, the predominant approach has been the use of Safety Cases, whereas, more recently safety engineering has seen the application of The Systems-Theoretic Accident Model and Processes (STAMP). Each method has its advantages and disadvantages, and both offer unique approaches to safety.

Specifically, the advantages of Safety Cases include that they are a structured process used to support claims of safety and, being performance based provide flexibility. Safety Cases need to prove through evidence that they will achieve their claimed level of safety.

Conversely, disadvantages of Safety Cases include that they encourage cognitive bias and are applied retrospectively. These disadvantages have directly resulted in the incorrect application of safety which has resulted in catastrophic failure.

Considering the above, alternative approaches to Safety Cases have evolved: notably, STAMP. This novel approach to systems safety has distinct advantages over Safety Cases. Specifically, STAMP provides continual tuning of safety through feedback control. Furthermore, STAMP facilitates a 'safety in design' approach, which has not been the focus of Safety Cases.

With the model only being recently developed, only a few disadvantages of STAMP have been elucidated in the literature. These include limited validation of its processes, as well as, limited guidance for its application. Over time and with broader application, specific disadvantages pertaining to STAMP may be forthcoming.

This literature review will describe and provide backgrounds to Safety Cases and STAMP respectively; it will also highlight their advantages and disadvantages. The review will consider the requirements for an effective Safety Case and associated criticisms. Lastly, the author will discuss if STAMP can offer a useful alternative to Safety Cases.

2 Approaches to demonstrate safety: Safety Cases and STAMP

2.1 Safety Cases

2.1.1 What is a Safety Case?

A Safety Case is the amalgamation of requirements, argument and evidence presented in an auditable format to assure a system is safe (Kelly, 2018). The Safety Case, typically presented as a report, "should present a clear, comprehensive and defensible argument that a system is acceptably safe to operate within a particular context" (Kelly, 1998). While presented as a report a Safety Case is not a static document and should help the organisation narrate clear safety requirements over the system's lifecycle (Kelly, 2018).

Within some industries, for example, a Major Hazard Facility (MHF), a Safety Case is a legal requirement. Used for regulation, a Safety Case will be utilised to detect risks and associated hazards, explain control methods, and detail the management system used for safeguarding

(Commonwealth of Australia, 2018). Being legislated, the regulator will oversee the operator's use of the Safety Case and all documentation produced will be reviewed by a competent group assigned by the Regulator.

As there are many types and formats of Safety Cases (Squair, 2016), a single definition of a Safety Case is not easily presented (Leveson, 2011c).

2.1.2 Evolution of Safety Cases

To improve the efficiency of the Watt steam engine, Evans and Trevethick utilised high pressure (above atmospheric) steam to power their advanced engine designs (Warburton, 1981). Watt's engine was inherently safe, and he steadfastly protested the use of the more efficient, yet significantly more dangerous high-pressure engines. Hundreds of deaths and injuries occurred from exploding high-pressure boilers on steamboats, in plants and locomotives (Leveson, 1992). Reacting to these failures, responsible operators of high-pressure steam devices formed learned societies in England (Manchester Steam User's Association – 1855) (Warburton, 1981) and later in Germany (Bavarian Steam Boiler Inspection Association – 1870) (TUV-Sud, 2017) to provide technical inspection services that provided a voluntary licence to operate these devices safely. Refer to the timeline in Figure 1.

Similarly, legislation was developed in 1858 for the new public railway system in England that required technical safety inspections by Her Majesty's Railway Inspectorate before a public railroad could operate. Thus, the concept of a licence to operate, issued by an overseer, was created (Railways Archive, 2005).

Technical inspections (to prescriptive requirements) provided significant safety improvement (Stromeyer, 1898). However, prescriptive requirements did not provide industry the flexibility that was often required (Wilkinson, 2002). The United Kingdom (UK) Factories Act, from the early 1900's, in part, recognised this and incorporated requirements to ensure that "Every dangerous part of machinery shall be securely fenced" (Wilkinson, 2002), and thus specified a performance-based or goal-setting requirement.

Societal expectations, concerning safety, also matured with a turning point in the field of tort law. A judgment from the Court of Appeal in the case of Edwards v National Coal Board, 1949, resulted in the concept of "Reasonably Practicable" becoming a legal requirement. A calculation was now required to determine if the amount of risk reduction was reasonable, considering all the factors involved to mitigate the risk (Wilkinson, 2002).

Safety requirements for major hazards thus progressed from the need to satisfy a standards-based assessment to a societal drive for the achievement of reasonably practicable goal based safety. The first such application of this requirement was in the UK nuclear industry. To obtain an operating licence, the early UK nuclear industry required reactor operators to develop an operating report or Safety Case (Wilkinson 2002), (Kelly 2018). It follows that the Safety Case concept was used in the transition from a prescriptive safety regulatory environment to a performance-based one and provided an evolutionary way to create and assure safety (Wilkinson 2002).

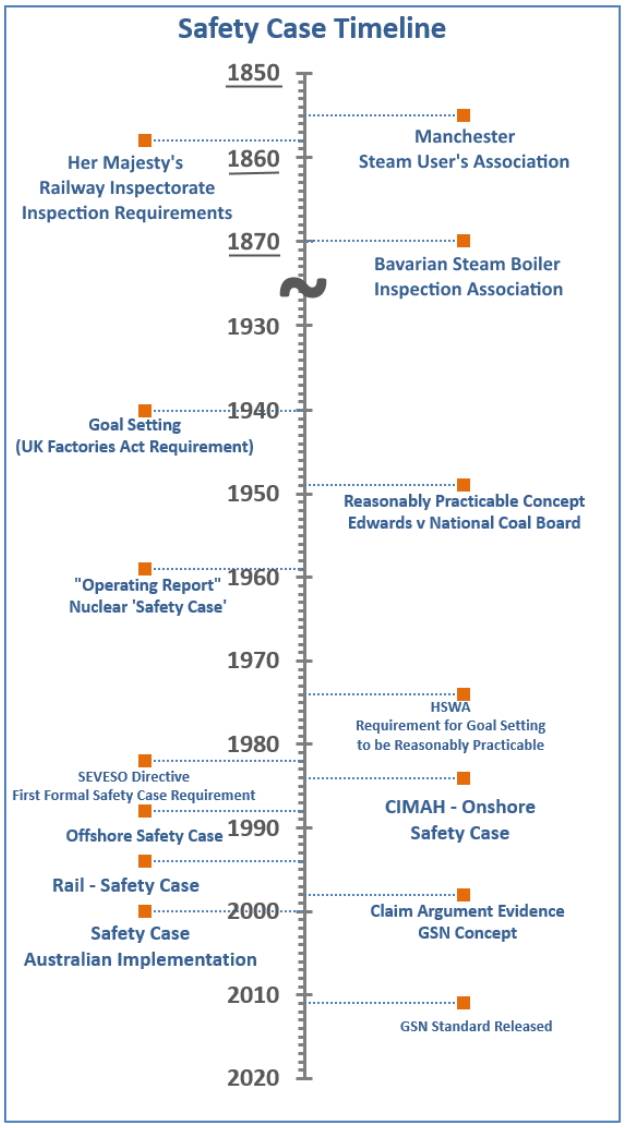

Figure 1 - Safety Case Timeline

The Robens Report (Health and Safety Executive, 2014), reviewing the state of workplace health and safety in the UK resulted in the Health and Safety at Work Act (HSWA) in 1974. The Act directed companies in the UK to reduce the risk of harm to a level that was As Low as is Reasonably Practicable (ALARP) (Haddon-Cave, 2009). Prior to the HSWA, ALARP was not formally legislated. Several MHF catastrophes occurred in Europe in the mid-1970's with the Seveso disaster and its resultant European directive, leading to the development of regulations in the UK to prevent similar major industrial events from occurring (Wilkinson, 2002). In the UK, the broader concept of a Safety Case was first legislated with the introduction of the Control of Industrial Major Accident

Hazards (CIMAH) Regulations in 1984 (Kelly, 2018). The growth of Safety Cases, whether legislated or not, is a required process for creating safety within the UK (Kelly 2018).

Safety Cases were initially limited to onshore major hazard facilities through CIMAH. Progressively, offshore requirements were included after recommendation by Cullen (2009) following the Piper Alpha disaster and were introduced into the legislative requirements for rail after the Clapham Junction collision (Kelly, 2018). The same conceptual foundation of presenting and communicating argument, for a Safety Case, is applied across all domains.

It is unfortunate that disaster triggers a fundamental shift in safety thought. The trigger for the introduction of Safety Cases into Australia was the Esso Longford explosion in 1998, with Safety Cases legislated in 2000 (Cooke & Shears, 2003).

Through broad use and ongoing research, Safety Case theory has also matured along with its wider application. Kelly (1998) introduced the concept of Goal Structuring Notation (GSN). GSN is a graphical representation of a Claim, Argument and Evidence (CAE) that form the requirements of all modern Safety Cases. CAE is how Toulmin's argument theory (from 1959) is used and applied to the structure of Safety Cases (Kelly, 1998).

2.1.3 Benefits of Safety Cases

The history above has shown that since their introduction, in the 1960's as a safety management tool, Safety Cases have been widely applied. Their application has also been extensively researched and benefits found in many areas. Safety Cases have been applied to and benefited:

1) Companies
2) Public
3) Regulators

Companies

When correctly used, Safety Cases can provide companies with an in-depth understanding of their safety risk exposure by detailing how well risk is being managed and where risk improvements are required (Kelly, 2018).

As Leong, Kelly and Alexander (2017) suggest, an organisation should use a Safety Case as a process to understand the safety systems it has in place, ensure that these systems function and revisit the safety argument regularly to ensure that an appropriate level of safety is being maintained.

In many situations, Safety Cases are legislative requirements (Cooke & Shears, 2003). A significant benefit for organisations that use Safety Cases is that they will meet their statutory requirements.

Public

Informing the public about risk is a vital outcome of a Safety Case (Maguire, 2006). Safety Cases that educate the public are made available by an MHF (Mobil Oil Australia, 2012) and offer clear insight into the organisation.

Although not always made public (Sujan et al., 2016), knowing that a Safety Case is available, the community find additional benefit by understanding what an organisation that requires a Safety Case does. While the contents of a Safety Case may not be directly accessed by the community, it is disseminated for the community's benefit by interested organisations, for example, the local council (Hobson's Bay, 2016). The Safety Case will outline the amount of risk the public is exposed to and what the organisation that develops the Safety Case considers to be acceptable. Corporate social responsibility is also reflected in the Safety Case with the public directly benefiting from such disclosure (Mobil Oil Australia, 2012).

Regulators

Regulators are tasked with ensuring the safety and well-being of workers and the public. In performing these tasks, regulators are required to obtain clear and concise safety information from industry (Hopkins, 2007). Importantly, presenting and challenging an argument is a fundamental concept of Safety Cases (Kelly, 2018) that can assist the regulator in their function. Additionally, well-formed argument within a Safety Case could spark further questioning or close enquiry (Habli et al., 2015) that could give more assistance (by the regulator) to an operator.

2.1.4 Criticisms of Safety Cases

A significant and lasting criticism of Safety Cases was delivered by the independent government report into the Nimrod disaster chaired by Haddon-Cave (The Review). The Hawker Siddeley Nimrod was a Royal Air Force patrol aircraft. Developed from a de Haviland comet of the 1950's, the Nimrod was first flown in 1969. In 2002, new regulations established by the UK Ministry of Defence required the development of a Safety Case for military aircraft and this requirement was applied to the Nimrod.

The Review discovered that, as required, a retrospective Safety Case was developed for an existing military aircraft, with reasonably safe service history. There was little evidence, in The Review, of a thorough safety investigation being performed. Significant reliance was placed on the aircraft's solid safety reputation which was directly reflected in the poorly developed Safety Case. Haddon-Cave (2009) wrote that the Nimrod Safety Case was "a story of complacency…[because] the system was safe anyway".

The criticism by Haddon-Cave of Safety Cases is also put forward by Leveson (2011c) in that 'cognitive bias' leading to 'group think' results in flawed safety analysis and that:

> "…some industries that have adopted a Safety Case and goal-based approaches have experienced much higher accident rates, such as offshore oil exploration and production." (Leveson, 2011c p.8)

The criticism by Haddon-Cave and Leveson is shared evidently by others. Eriksson (2004) created a retrospective Safety Case based on a rail collision that occurred in the year 2000 at Asta, Norway. Discoveries from the exercise suggested paralleling of The Report in that development and actioning of retrospective Safety Cases is difficult, and errors are likely. Additionally, information was difficult to find, and assumptions were required. Similar system-based observations were made by Cullen (1991). It follows that the proper application of a Safety Case is one which is integrated into the system and not retrospectively applied (Hobbs, 2016) for compliance.

The term 'Safety Case' is broad and covers many different methods all of which can claim to be a Safety Case (Kelly, 2018). Cognitive bias can be found in more than one of these different Safety Case methods. The CENELEC standard for rail signalling EN50126 requires the development of a Safety Case (Kelly, 2003). The Safety Case needs to meet the requirements of the standard, which has been developed by domain experts. Compliance with any "EN" or European Norm, is a requirement of European law. The possible mistake for a Safety Case is to simply follow the assumed inherently safe standard. Interestingly, Fulfilling the requirements of a standard does not necessarily result in a safe outcome (Dekker, 2018), yet it would not be unreasonable for the creator or the acceptor of the Safety Case to think it does. Cognitive bias can, therefore, occur in unsuspecting ways.

The proper understanding of Safety Case requirements is important and is frequently overlooked due to the perceived simplicity of the task (Kelly, 2018). A significant failing of the Safety Case process is that in many circumstances it is not challenged (Sujan et al., 2016). A Safety Case report is developed and a reviewed for quality (Kelly, 2018). The failure that then surfaces is that if the Safety Case is challenged by the system, failure will occur as the robustness of the argument has not been previously tested.

A final, novel, observation of safety case failures that may help explain why an initially good idea has regressed is an observation suggested by Squair (2016). Squair suggests that safety arguments have progressively become gerund, with the argument having no action.

2.2 Systems Theoretic Accident Model and Processes (STAMP)

2.2.1 What is STAMP?

STAMP is a systems engineering based model, developed by Leveson, that is used to understand safety. It leverages feedback and control design (Leveson, 2004) to provide information on the current state and potential drift of safety within a system (Waterson & Chung, 2010).

Leveson (2004), claims that system safety is a control rather than a component failure problem, citing examples where software control has failed leading to disaster. Additionally, Leveson argues that preventing component failures is a futile safety exercise. However, placing appropriate constraints within the system based on its design will ensure safety. Subsequently, all aspects of the system's design (physical, organisational and social) need to be appropriately constrained for safety to be guaranteed.

Constraints are one of three elements of a STAMP model; the other two are a hierarchical control structure and an accurate process model (Leveson 2011b) - Figure 2.

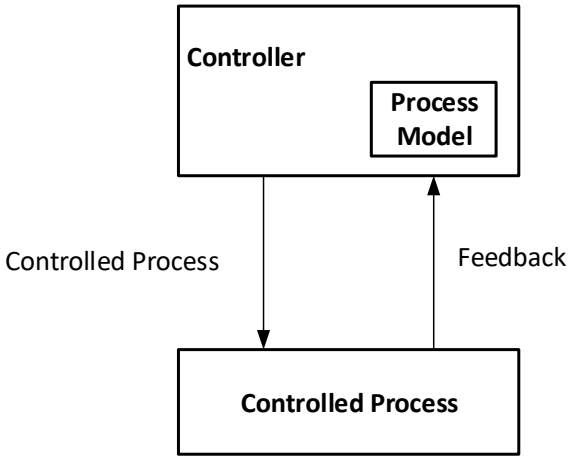

Figure 2 - STAMP Model (Leveson, 2011b)

Within a hierarchical structure, a feedback control loop is embedded. Upper levels control lower ones through imposed constraints (Johnson, 2006). The performance measure of the limitations is made through returning feedback where safety can be realised by how closely the constraints are met (Leveson, 2011b).

For the control system to function, a model of the ideal process is required. This model is developed through a clear understanding of requirements. The system's requirements are used directly during operation to monitor and ensure safety.

2.2.2 Evolution of STAMP

During the Cold War, the increasing complexity of all engineering disciplines required updated thinking. The fly-fix-fly approach typically used when developing novel products were not suitable to the development of nuclear arms (Leveson, 2011b). The discipline of systems engineering evolved in the 1940's with advancements made during the rocket age of the 1950's. Subsequently, the specialist area of systems safety was created for the Minuteman missile program through guidance developed in 1961 (Stephans & Stephenson, 2004) – refer to Figure 3.

The concept of systems thinking was applied by Rasmussen (1997) to the area of safety. Rasmussen identified that to demonstrate safety within a complex sociotechnical system, a non-linear systems-centric approach was required. Rasmussen (1997) proposed that a layered and interactive technique be applied to the safety problem. Within this envelope, all actors shared the responsibility for the implementation of a safe system.

Behaviour within a complex system is an emergent property (Dekker, 2011). The unpredictability of emergent engineered systems where engineers do not have a good understanding can lead to unsafe states (Johnson, 2006). Complex systems, where the whole is not the sum of its parts, need to be treated differently.

Fault Tree Analysis (FTA) was developed in 1962 to assess component failures for the Minuteman missile program. FTA is a linear component interaction tool, that will answer the component interaction problem but not the complex question of overall system safety. FTA will struggle when attempting to understand emergence within a system (Johnson, 2006).

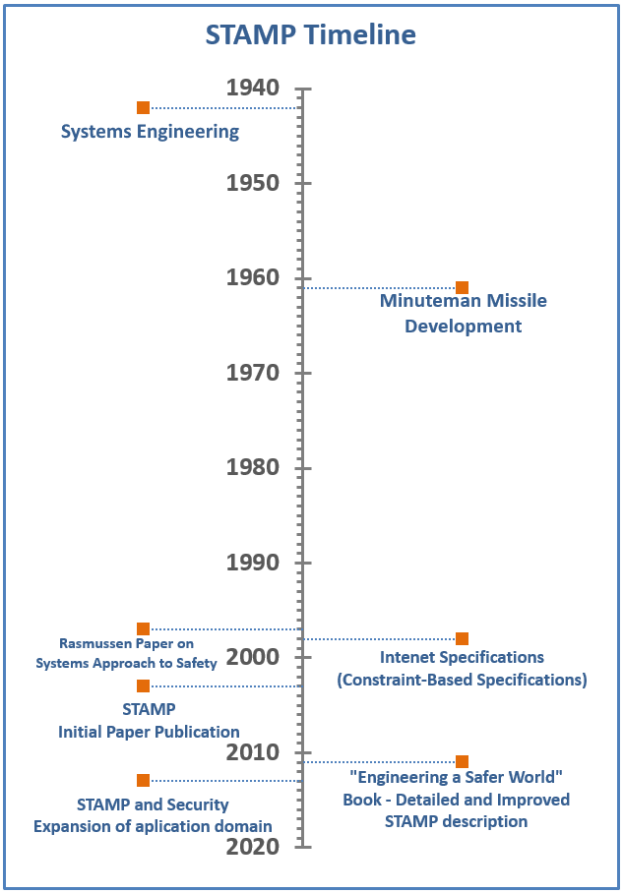

Figure 3 - STAMP Timeline

When developing systems, an important step are the requirement specifications, which detail what will be achieved when the system is realised. Leveson (2011b) theorised that both knowing what and equally importantly why something (development path, subsequent changes) was performed should be documented. Leveson developed the method of Intent Specifications in 1998 to detail this why and what requirement.

Drawing on the ideas of Rasmussen and combining Intent Specifications with engineering systems theory, Leveson, in 2003, proposed that the current systems safety practices while slightly improved were still heavily based on the processes used during the Cold War. At that time when control systems were still in their infancy and suited to tools such as FTA. A true systems approach to safety in design should be adopted, with STAMP being the result.

Research into STAMP, primarily by Leveson or her students, slowly increased the core knowledge available (Underwood & Waterson, 2012). Progressively, the theory on which STAMP is based has been applied in complementary areas, such as accident investigation and security. In 2011, a book on STAMP was released which provided solid foundation material on the theory (Leveson, 2011b).

STAMP is a new safety theory, being realised in 2003, with wider application knowledge developed in 2011 (Leveson, 2011b). The domains to which STAMP is applied has grown through adoption and application by researchers internal and external to the core group at the Massachusetts Institute of Technology.

2.2.3 Benefits of STAMP

The benefits of STAMP discussed in Leveson's (2004) original paper presented references to case studies where STAMP was applied retrospectively. In all the case studies, advantages and resultant benefits of STAMP were claimed. The benefits outlined are based on these case studies. STAMP can provide benefit to the following groups:

1) Companies
2) Regulators
3) Public

<u>Companies</u>

When an accident occurs, the usual response from an organisation is to perform a root cause analysis to determine who or what is to blame and subsequently eliminate that element (Leveson, 2011b). The STAMP approach does not accept that any single event is the cause of an accident. It will probe deeply into the interactions that take place within the elements of the system, both physical and interpretational (Leveson, 2011b). STAMP argues that merely removing the bad apple will not prevent a similar event from reoccurring. The cause lies in an understanding of the complex control relationships that exist within workplaces (Leveson, 2011b).

STAMP claims that it can better understand accidents, which can lead to the reduction or the elimination of future similar events. Using STAMP to better understand a

system's interactions will also reduce other failures that could lead to disaster (Leveson, 2011b).

The proper management of security is an increasing requirement for the management of safety. STAMP has shown that its model can be extended for the use in security management (Young & Leveson, 2014).

Regulators

The public relies on the regulator to be the overseer of safety (Commonwealth of Australia, 2018). To be an overseer, or to have a better understanding of a safety problem, regulators must be able to analyse safety information to which they have access. Most regulators do not have the time nor the tools available to understand all aspects of a presented problem (Quinlan, 2014).

Having a methodology available that can provide an overall understanding of a safety problem is invaluable (Leveson, 2011b). STAMP claims to be the tool that can give the regulator insight into the safety of a system. The use of STAMP as a tool that provides insight for the regulator was provided through the Walkerton case study (Leveson, 2011b).

Public

The public interacts with systems over which they have little direct safety control (Dekker, 2011). The public exists at the 'sharp end' of safety and is directly affected should failures occur. Rasmussen (1997) identified and STAMP (Leveson, 2011b) extended the idea that safety is a sociotechnical problem, where competitive constraints may play a part in systems failures. STAMP therefore directly acknowledges that the public are impacted by system decisions and how they are affected must be included in any analysis. (Cranyon 2013)

2.2.4 Criticisms of STAMP

STAMP was presented as a superior method that is used to assess and understand safety (Leveson, 2004). The introductory paper detailed many ways in which current methods were lacking, with the solution being STAMP. Like other methods before it, STAMP presented an idea without evidence (Reason, Hollnagel, Paries, 2006). In contrast to STAMP, methods such as the "Swiss Cheese" model were presented as an idea, rather than claiming that they are better (Reason, Hollnagel, Paries, 2006). Interestingly, STAMP, claims it is better method yet provides no evidence to support this (Underwood, & Waterson, 2012).

Since the initial release of STAMP, further expanding research (such as STAMP in security) has occurred (Leveson 2011b), (Young & Leveson, 2014). What has not been determined is if STAMP works (Underwood, & Waterson, 2012). A study by Waterson & Chung (2010) questioned the reliability of STAMP by asking whether parallel independent STAMP analysis have similar results.

The criticisms of the STAMP model could be related to its immaturity, having only been released in 2004 and more formally through a book published in 2011. As a method, it is not well known and still not widely used (Underwood & Waterson, 2013).

3 Tensions between Safety Cases and STAMP

3.1 Debates

Over many years, the concept of a safety case crystallised through the assistance of several progressive catalysts. The initial use of a Safety Case was in a safety critical industry. Over approximately sixty years, Safety Cases have matured and been accepted as the most suitable tool for understanding and management of safety critical industries (Kelly, 2018).

Systems engineering and more recently systems safety, on which STAMP is based, also has a history. The history of STAMP is somewhat shorter than Safety Cases with emergent properties related to safety being significantly discussed only recently (late 1990's). STAMP entered into the domain with significant fanfare. STAMP's developer argued that Safety Cases, through their design and use, are far from state of the art (Leveson, 2011b) with the suggestion that the method is unsuitable for state of the art projects. STAMP offers a more modern approach.

The author was not able to understand why STAMP took such an aggressive approach towards Safety Cases (Leveson, 2011b) to claim legitimacy. The aggressive stance taken by STAMP has not helped. Underwood & Waterson (2013) revealed evidence, that since its debut in 2003 it is still not well known. Underwood & Waterson also found that fault tree analysis – a task that was typically undertaken in a Safety Case (and dismissed by Leveson) is better known and used by significantly more safety practitioners than STAMP. From a safety research perspective, the results were similar, with STAMP being less well known and used than fault trees. Communication and training within the systems-based models require improvement (Underwood & Waterson 2013). This result was reiterated by another study by Underwood, Waterson, & Braithwaite (2016). Mailing list archives (University of York, 2012) also reveal passionate debate regarding STAMP's benefits.

Was such an aggressive stance required? Safety Cases being process driven embrace external help. STAMP being a model can legitimately share the space and provide benefit. Safety Case supporters argued their ground without any direct attack on STAMP, in one case openly welcoming STAMP (Leong, 2017) as a method that could support Safety Cases in some way and in another (Greenwell & Knight, 2007) showing that STAMP could just slot in. The legitimacy question is one STAMP has created on its own. Could the slow and limited uptake of STAMP and similar complexity-based analysis methods simply be out of place due to difficulty in implementation? (Roelen, Lin & Hale, 2011)

Claims by critics of Safety Cases will point to the spectacular failures of systems assured by Safety Cases (Leveson, 2011c). However, as Safety Cases are legislated in the Commonwealth (and no legislative support of their removal found), with few significant disasters reported, it is essential to consider the 'Safety II' (focus on what goes right rather than wrong) approach and understand what Safety Cases are doing right (Hollnagel, 2014).

While STAMP claims to be a superior choice for the creation of safety there is no evidence that it is as research has not been performed to determine whether STAMP works (Underwood, & Waterson, 2012). A significant number of assessments presented in STAMP's literature are retrospective (Leveson, 2011a). In support of the legitimacy debate surrounding STAMP, a study by Waterson & Chung (2010) raised additional concerns. Could the "my method is better" stance of STAMP create cognitive bias within its domain?

One aspect of the debate between Safety Cases and STAMP is currently very one sided. STAMP does not create safety. STAMP sets itself up to failure in this regard by dismissing requirements for quantitative assessment (Leveson, 2011b). The partial argument STAMP puts forward in this regard is that quantitative calculations are the domain of component failure and safety is not simply measured by component failure when a systems approach is observed (Leveson, 2011b).

Safety Cases through their evidence requirement (Kelly 2018) seek quantitative assessment as their use in assurance requires this. Quantitative assessments as suggested by Habli (2015) would less likely be contested as the mathematics does not lie (Downer, 2013). Quantitative assessments, therefore, provide sound evidence that an appropriate level of safety has been achieved. STAMP simply does not currently offer this.

3.2 Can inter-theory support be found?

Both Safety Cases and STAMP want to create safety. The methods achieve safety in different ways. However, there are a few areas where support for each method can be found.

Within safety, there is a need for a narrative (Rae, 2015). Both Safety Cases and STAMP fundamentally try to provide a story. For Safety Cases, Kelly (2018) suggests that a Safety Case Report (the document) is not as useful as a Safety Case (the narrative). Leveson (2011b) also discusses that story is essential and the STAMP process tells a story specific to what is currently happening through its inherent feedback.

A process similar to a Safety Case is found within STAMP; Intent Specifications. Intent Specifications explain what and why requirements were selected and are developed to assist engineers understand the system, through a structured approach (Weiss, 2003). Safety Cases are like Intent Specification when used appropriately (Johnson, 2004).

While a bitter divide does exist between STAMP and Safety Cases, there is common ground to bring the parties together over coffee (or perhaps tea).

4 Future Considerations

The catastrophic failures of systems under the watch of Safety Cases have repeatedly been brought to the attention of safety practitioners. While failures have occurred, the failure has not been due to the structure of a Safety Case; it has been to the improper application (Haddon-Cave, 2009).

Detractors of Safety Cases should consider the number of safety cases that are working rather than focus on the few that have failed. Such an idea is supported by the Safety II view where the focus is on what goes right rather than what goes wrong. Significantly more evidence is available into what goes right as adverse events due to Safety Case failures are front page news and seldom appear.

Is it possible to consider STAMP as an alternative to Safety Cases? The evidence found in this literature review is not supportive as each approach is different. STAMP is a systems-based model; however, Safety Cases are processes (Greenwell & Knight, 2007). While there is the possibility of overlap and collaboration (Greenwell & Knight, 2007), (Leong et. Al., 2017) Safety Cases are required to meet specific legislative needs to which STAMP cannot comply (ExxonMobil, 2012). As such, the Safety Case process is currently the only way of creating and assuring safety for areas of significant risk.

The development of a Safety Case typically occurs late in a system's lifecycle (Stålhane & Myklebust, 2016). Such late development occurs to ensure that appropriate knowledge regarding the system has been gathered. STAMP is a method that builds safety from a system's initial development. It follows that system safety through a Safety Case struggles initially and when STAMP is used, the argument of safety is lost.

STAMP was created, however, Safety Cases evolved. As Safety Cases were well known at the introduction of STAMP, thought into how STAMP could be initially presented to practitioners should have been considered. Engineers are not good marketers. A recent change in STAMP's position towards Safety Cases has been observed: "Does not imply what previously done is wrong and new approach correct" (Leveson, 2018).

5 Conclusion

Since their inception within the domain of nuclear assurance, the application areas of Safety Cases have grown extensively. As a tool for the creation and assurance of safety they are very suitable. Failures of Safety Cases should prompt safety practitioners to try to understand causes and drive improvement. Practitioners should not try to look for alternatives. In the literature reviewed no evidence was found that Safety Cases no longer meet their intended requirements and thus need replacement.

The alternative systems safety method – STAMP is still immature and requires further research. In its current form STAMP cannot replace a Safety Case as while it creates safety it does not demonstrate it. Demonstration of safety is a fundamental requirement of a Safety Case.

Safety Cases struggle to build safety into design. Can STAMP methods be used to support a Safety Case that is created earlier in a systems design rather than later?

6 References

Commonwealth of Australia. (2018). What is a safety case. Retrieved March 01, 2018, from https://www.nopsema.gov.au/safety/safety-case/what-is-a-safety-case/

Cooke, G., & Sheers, R. (2003). SAFETY CASE IMPLEMENTATION – AN AUSTRALIAN REGULATOR'S EXPERIENCE. *IChemE Symposium Series No. 149*, 605-617. Retrieved April 10, 2018, from http://www.icheme.org/communities/subject_groups/safety and loss prevention/resources/hazards archive//~/media/Documents/Subject Groups/Safety_Loss_Prevention/Hazards Archive/XVII/XVII-Paper-47.pdf

Cullen, L. (1991). *The public inquiry into the Piper Apha Disaster*. London: HMSO.

Dekker, S. (2018). *The safety anarchist: Relying on human expertise and innovation, reducing bureaucracy and compliance*. Abingdon, Oxon: Routledge.

Dekker, S. W. (2011). Systems thinking 1.0 and systems thinking 2.0: Complexity science and a new conception of "cause.". *Aviation in focus: An international aeronautical journal, 2*(2), 21-39.

Downer, J. (2013). Disowning Fukushima: Managing the credibility of nuclear reliability assessment in the wake of disaster. *Regulation & Governance*. doi:10.1111/rego.12029

Edwards v National Coal Board (Court of Appeal December 31, 1949).

Eriksson, L. (2004). Using Formal Methods in a Retrospective Safety Case. *Lecture Notes in Computer Science Computer Safety, Reliability, and Security*, 31-44. doi:10.1007/978-3-540-30138-7_4

Greenwell, W. S., & Kinght, J. C. (2007). Framing analysis of software failure with safety cases. Retrieved from https://www.researchgate.net/publication/228341586_Framing_analysis_of_software_failure_with_safety_cases

Habli, I., Kelly, T., Macnish, K., Megone, C., Nicholson, M., & Rae, A. (2015). The ethics of acceptable safety . *23rd Safety-critical Systems Symposium*. doi: 10.13140/2.1.2977.5043

Haddon-Cave, C. (2009). *The Nimrod Review: An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006* (Rep.). London: The Stationery Office.

Health and Safety Executive. (2014, July 25). The Robens Report. Retrieved April 28, 2018, from http://www.hse.gov.uk/aboutus/40/robens-report.htm

Hollnagel, E. (2014). *Safety-I and safety-II: The past and future of safety management*. Farnham: Ashgate.

Hobbs, C. (2016). *Embedded software development for safety-critical systems*. Boca Raton (FL): CRC Press.

Hobsons Bay City Council. (2018). Emergency Management. Retrieved April 28, 2018, from http://www.hobsonsbay.vic.gov.au/Community/Emergency-Management

Hopkins, A. (2007). Beyond Compliance Monitoring: New Strategies for Safety Regulators. *Law & Policy,29*(2), 210-225. doi:10.1111/j.1467-9930.2007.00253.x

HSE. (2003). *Out of control: why controls system go wrong and how to prevent failure*. Sudbury: HSE Books.

Johnson, C. (2004, October 8). Forensic Software Engineering: Are Software Failures Symptomatic of Systemic Problems? Retrieved February 27, 2018, from http://www.dcs.gla.ac.uk/~johnson/papers/Safety_Science/forensic.html

Kelly, T. P. (1998). *Arguing safety - A systematic approach to managing safety cases* (Unpublished master's thesis). University of York.

Kelly, T. (2018). Safety Cases. In *Handbook of Safety Principles*. West Sussex: Wiley.

Kelly, T. P. (2003). Managing Complex Safety Cases. *Current Issues in Safety-Critical Systems*, 99-115. doi:10.1007/978-1-4471-0653-1_6

Leong, C., Kelly, T., & Alexander, R. (2017). Incorporating Epistemic Uncertainty into the Safety Assurance of Socio-Technical Systems. *Electronic Proceedings in Theoretical Computer Science, 259*, 56-71. doi:10.4204/eptcs.259.7

Leveson, N. (1992). High-pressure steam engines and computer software. *International Conference on Software Engineering*. doi:10.1109/icse.1992.753485

Leveson, N. (2011c). The Use of Safety Cases in Certification and Regulation . *Journal of system safety, 47*(6).

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science, 42*(4), 237-270. doi:10.1016/s0925-7535(03)00047-x

Leveson, N. (2011b). *Engineering a safer world: systems thinking applied to safety*. Cambridge, MA: The

MIT Press.

Leveson, N. G. (2011c). Applying systems thinking to analyze and learn from events. *Safety Science, 49*(1), 55-64. doi:10.1016/j.ssci.2009.12.021

MAGUIRE, R. (2006). *SAFETY CASES AND SAFETY REPORTS: Meaning, motivation and management*. S.l.: CRC PRESS.

ExxonMobil. (2012). *Mobil Altona Refinery Safety Case Summary* [Brochure]. Author. Retrieved May 1, 2018, from http://www.exxonmobil.com.au/en-au/company/news-and-updates/publications/publications-overview

Mobil Oil Australia. (2012). *Mobil Yarraville Terminal Safety Case Summary 2013-2017* [Pamphlet]. Melbourne: Mobil Oil Australia.

Quinlan, M. (2014). *Ten pathways to death and disaster: Learning from fatal incidents in mines and other high hazard workplaces*. Annandale, N.S.W.: The Federation Press.

Rae, A. (2015). Tales of disaster: the role of accident storytelling in safety teaching. *Cognition, Technology & Work, 18*(1), 1-10. doi:10.1007/s10111-015-0341-3

Railways Archive. (2005, July 24). The First Requirements of the Inspecting Officers of Railways. Retrieved April 21, 2018, from http://www.railwaysarchive.co.uk/docsummary.php?docID=161

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2-3), 183-213. doi:10.1016/s0925-7535(97)00052-0

Reason, J., Hollnagel, E., & Paries, J. (2006). Revisiting the "Swiss Cheese" Model of Accidents. *EEC Technical/Scientific Report No. 2006-017*.

Roelen, A., Lin, P., & Hale, A. (2011). Accident models and organisational factors in air transport: The need for multi-method models. *Safety Science,49*(1), 5-10. doi:10.1016/j.ssci.2010.01.022

Salmon, P. M., Cornelissen, M., & Trotter, M. J. (2012). Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science, 50*(4), 1158-1170. doi:10.1016/j.ssci.2011.11.009

Simpson, R. (2017). *Formalised responsibility modelling for automated socio-technical systems analysis* (Unpublished master's thesis). University of Glasgow. Retrieved March 4, 2018, from http://theses.gla.ac.uk/8495/1/2017simpsonphd.pdf

Squair, M. (2016, June 16). M12 Safety Cases and Arguments V1.4. Retrieved March 01, 2018, from https://criticaluncertainties.com/m12-safety-cases-and-arguments-v1-4/

Stephans, R. A., & Stephenson, J. (2004). *System safety for the 21st century: The updated and revised edition of System safety 2000*. Hoboken, NJ: Wiley-Interscience.

Stromeyer, C. E. (1898). *Memorandum by chief engineer presented at the annual meeting of the general body of the members* (Publication). Manchester: The Manchester steam users' association.

Stålhane, T., & Myklebust, T. (2016). The Agile Safety Case. *Lecture Notes in Computer Science Computer Safety, Reliability, and Security*, 5-16. doi:10.1007/978-3-319-45480-1_1

Sujan, M. A., Habli, I., Kelly, T. P., Pozzi, S., & Johnson, C. W. (2016). Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. *Safety Science, 84*, 181-189. doi:10.1016/j.ssci.2015.12.021

TUV Sud. (2017, April 27). Part I: 1866 – 1900. Retrieved April 28, 2018, from https://www.tuv-sud.com/about-tuev-sued/history/part-1-1866-1900

Underwood, P., & Waterson, P. (2012). A critical review of the stamp, fram and accimap systemic accident analysis models. In *Advances in human aspects of road and rail transportation*. Boca Raton: CRC Press.

Underwood, P., & Waterson, P. (2013). Systemic accident analysis: Examining the gap between research and practice. *Accident Analysis & Prevention, 55*, 154-164. doi:10.1016/j.aap.2013.02.041

Underwood, P., Waterson, P., & Braithwaite, G. (2016). 'Accident investigation in the wild' – A small-scale, field-based evaluation of the STAMP method for accident analysis. *Safety Science, 82*, 129-143. doi:10.1016/j.ssci.2015.08.014

University of York. (2012). Safety-Critical Mailing List Archive. Retrieved from https://www.cs.york.ac.uk/hise/safety-critical-archive/

Warburton, R. (1981). A history of the development of the steam boiler, with particular reference to its use in the electricity supply industry (Unpublished master's thesis). Loughborough University. Retrieved from https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/10498/1/Thesis-1981-Warburton.pdf

Waterson, P., & Chung, P. (2010). Investigating the potential to simulate hospital-based infection outbreaks using the stamp architecture. *5th IET International Conference on System Safety 2010*. doi:10.1049/cp.2010.0829

Weiss, K. A., Ong, E. C., & Leveson, N. G. (2003). 5.1.1 Reusable Specification Components for Model-Based System-Engineering. *INCOSE International Symposium, 13*(1), 108-120. doi:10.1002/j.2334-5837.2003.tb02604.x

Wilkinson, P. (2002). *Safety cases: success or failure?* (Rep.). Retrieved https://openresearch-repository.anu.edu.au/handle/1885/41698

Young, W., & Leveson, N. G. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM*,*57*(2), 31-35. doi:10.1145/2556938