URN in place of GSN - Design Rationale versus Assurance Argument

Ray Feodoroff
MSc Safety, Risk and Reliability Engineering (Heriot Watt)

Abstract

Goal Structured Notation (GSN) is a recognized means to couch validation arguments. Proponents of GSN have proposed moving GSN from the validation role into earlier aspects of a project lifecycle, as a Design Rationale capture mechanism.

If there is an argument for a graphical notation for assurance argument to be used in the Design Rationale space, then the converse can be true. That is, a graphical Design Rationale notation may potentially be used in the assurance argument space.

User Requirements Notation (URN) is a mature graphical notation which supports goal oriented requirement elicitation, specification and rationale capture. URN includes goal refinement and evaluation strategies. Therefore, URN could potentially support assurance argumentation in a fashion that would allow Design Rationale to act as an argumentation component in a Safety Case without the need for re-articulation in GSN.

Keywords: User Requirements Notation; Goal Requirement Language; Goal Refinement; Use Case Maps; Causal Logic; Semi-Formal Method; Formal Method; Goal Structured Notation; Problem Frames; Sequent Calculus; Design Decisions; Decision Support; Design Rationale, Justification; Phased Safety Case; Assurance Case; Intent Specification.

1 Introduction

This paper is an attempt to balance forces set in motion by Nancy Leveson (2002a), who has called upon the work by Jens Rasmussen, for the purposes of using Goal Oriented thinking as the basis for Design Rationale capture in Intent Specifications. This idea by Leveson (2011) is in friendly competition with the idea of Safety Cases which are recorded as Arguments, often using the Goal Structured Notation (GSN) proposed by Kelly (1998). GSN based arguments have previously sat in the qualification phase of a project rather than driving the design. To better inject safety into system design many authors, including Kelly, have proposed phased safety cases. This phasing of safety cases tends, however, to make fuzzy the distinction between Argument and Rationale. Leveson's notion of Rationale, for example, might be taken as the first temporal slice of Argument since Rationale is aimed to occur within the design cycle and also within the design artefacts. The corollary of this is the HSE terminology for its model of Phased Safety Cases by Bishop, Bloomfield and Froome (2001), each slice being called a ***Justification***. Justification is one use of Argument. The other use of Argument is Explanation. As a juxtaposition, two aspects of Goal Orientated approaches are Intention and Refinement which are tools for planning and problem solving.

A starting proposition then is that Intention is actually to Refinement what Justification is to Explanation, and that Justification is simply an analogue of Intention (or vice versa). If so, then temporal slices of argument over Preliminary, Architectural and Implementation Justification may be better expressed in an Intentional Notation (looking forwards) rather than a Justification Notation (looking backwards). It may also make sense that the notation allows one to argue in an ***Argumentation Terrain*** that speaks in terms of first class architectural concerns (problems, requirements, features, aspects, and tactics).

The often third party, posthumous nature of Assurance Case generation may also work against temporal or phased Safety Cases, both because of the dynamic nature of the design process, and the lethargy of the third-party-assurance-argument-authoring model. Certainly, the idea of injecting safety (or indeed other quality attributes) into the system life cycle as early as possible is favoured.

To discount the temporal aspect, the term Justification, is adopted in this paper as it acts as a term that arbitrates between the Design Rationale and Safety Argument camps as it is agnostic of when in the system lifecycle the claim is made.

Design Rationale as Justification during Preliminary, Architectural and Implementation phases is of special interest here. For the earliest Justifications the problem is potentially addressed by using an approach closer to the semantics of graphical specification and design notations.

Rather than invent a new approach to Design Rationale capture, as many authors have attempted, the search should be to use appropriate modelling heuristics atop a current graphical specification and design notation that might act in place of GSN as a Justification (and as an Explanation). The proposition is that that notation is User Requirements Notation (URN) which is Goal Oriented by design and as Leveson recommends. URN also has Actor/Agent oriented aspects to the notation. Allocating goals to Actors/Agents facilitates capturing the ***Argument for the Act of Design***, through the power of ***Allocation***, which meets Leveson's aspirations for Rationale within the design cycle and within the design artefacts. URN also, treats elements of the ***Argumentation Terrain*** as first class members of its lexicon, syntax and semantics. URN, conveniently, has philosophical roots back to Jens Rasmussen's ideas which are recommended by Leveson.

The ideas behind goal orientated notations, however, have previously been discounted by the GSN community. So, with the prompting of Leveson, a revisiting of the GSN critiques of goal orientation is warranted. Also included will be critiques from other quarters that, when reconsidered, provide evidence of the breadth and depth URN brings to ***Argument for the Act of Design*** over the ***Argumentation Terrain***, and as an embeddable argument within design artefacts.

Heading 2 will discuss the problems with Design Rationale.

Heading 3 will look at the notion of *'means-end'* and the potential for *'cascading constraints'* that set the *'context'* for each phase of a phased assurance case which is then to be captured in a graphical Design Rationale notation.

Heading 4 will look at the argument for URN via revisiting critiques of its ancestors.

Heading 5 will look at the notion of the ***Toulmin Breakpoint*** to argue that "Argument over Calculi" is likely nugatory as the Toulmin Model was, according to Toulmin, designed for use where Calculi were not available. URN is thus argued to be an embodiment of semi-formal Causal Calculus and also a potential means to express a semi-formal Sequent Calculus when certain modelling heuristics are applied.

Heading 6 will conclude with the assertion that URN is a viable means to express Justification of attainment of Assurance goals, in the earlier project phases at least, for the purpose of phased Assurance Cases. Doing so by looking backwards up the chain of reason or the Explanation over the goal refinement into requirements and into architecture.

2 The Problems with Design Rationale

2.1 Leveson versus Toulmin

Leveson (2011), in a criticism of Safety Cases, has pointed out that Safety Engineers need to focus on proving that a system is unsafe, rather than safe per se. More specifically, Leveson suggests that System Engineers *'have already created arguments for why their design is safe'*, and thus Safety Engineers should therefore use the opposite mindset from that of developers.

There appears then a presumption that System Engineers, and even Software Engineers, are generally providing *'argument'* that the system is safe simply through delivering normal engineering artefacts. The so-called *'argument'* provided, it is suggested, is likely to be more *'intuition'* in most cases. Toulmin (2003) makes the following point in the update of his seminal work "The Uses of Argument":

> *The contrast between the philosophical and non-philosophical uses of the term 'intuition' can be brought out by returning to the notion of 'grounds' ... very often someone's claim to know that so-and-so must be rejected if he can produce no grounds ... [p. 224]*

2.2 Leveson versus Burge

Examining Leveson's idea that System Engineers have *'created arguments'*, let's take *'argument'* to mean formally structured and grounded propositions leading to conclusions. Burge (2005) notes that Design Rationale (or our propositions) differs from design documentation because it captures the reasoning behind the Design Decisions (or our conclusions). Often design documentation will likely only contain Design Decisions. This makes design documentation, the normal output of System Engineering, somewhat less than an *'argument'*. In fact, whilst there may be a list of explicit design decisions, many potentially subtly important decisions are more often implicitly reflected in the actual design outcomes without reasoning attached.

This *'argument'*, if it exists, should thus be part of the Design Rationale behind System Engineering Design Decisions. The *'argument'* should include the reasons why the decisions are apt to meet assurance or other goals that have been identified for the system. Burge, however, points out that:

1. The capture of Design Rationale itself is problematic.
2. Recording all decisions, including those overturned, is time consuming and expensive.
3. The more intrusive the capture process, the more resistance to using it.
4. Design Rationale capture is expendable when it comes up against project milestones.

Therefore, where System/Software Engineer provided Design Rationale is absent (regardless of the reason for the absence), then no *'grounds'* for *'argument'* has been provided.

2.3 Leveson versus Rasmussen

When describing Intent Specifications, Leveson (2002a) states:

> *Intent specifications are hierarchical abstractions based on why (design rationale) as well as what and how. ... The organization of the specification results in a record of the progression of design rationale from high-level requirements to component requirements and designs.*

If one takes snap-shots of an Intent Specification, as the system design evolves; it is likely meeting the intent of a phased Justification. The term Intent comes from the Cognitive Science notion of Goal Intention, which comprises Attainment, Maintenance, Cessation, and Avoidance as the four targets of Goal Satisfiability.

The advantage of the Intent Specification would then appear to be that the third-party-assurance-argument-authoring model is avoided. However, if none of the issues Burge raises are addressed then no *'grounds'* for *'argument'* will be provided.

Leveson (2002a) suggests the way to capture the *'why'* is through Abstraction Hierarchy (AH) and *'means-end'* relationships. AH is a concept that comes from the Cognitive Sciences but especially from Jens Rasmussen - a leader in Cognitive Science and especially around Cognitive Work Analysis (CWA). Leveson (2002b), vouching for Rasmussen's work, states:

> *Intent specifications apply means-ends abstractions to system specifications… Viewing a system from a high level of abstraction is not limited to a means–ends hierarchy, of course. Most hierarchies allow one to observe systems at a less detailed level. The difference is that the means–ends hierarchy is explicitly goal-oriented and thus assists goal-oriented problem solving.*

A problem for Leveson's suggestion arises when observations by CWA practitioners are taken into account. Naikar, Hopcroft, & Moylan (2005), when discussing Work Domain Analysis (WDA), state:

> *A point that is sometimes not appreciated about WDA, and about CWA in general, is that constraints are modelled in terms of categories – as opposed to*

examples or instances (Rasmussen et al., 1994). Hence, WDA models categories of purposes, values and priorities, functions, and physical resources rather than instances of purposes, values and priorities, functions, and physical resources. [p. 6]

AH in its raw form appears then to sit outside of the design of the actual system, focusing on classification and intention of the problem space. It needs to be morphed into the solution space. As a corollary, Black (2009) notes of Intent Specifications:

Safety-related constraints are defined as system design principles. This approach provides a framework for expressing system safety goals, but does not offer tactics for safety goal decomposition. [p. 19]

Black also notes that:

A disadvantage of formal specification is that non-formalists may be reluctant to use formal requirements, particularly in the early analysis and design stages when creating safety requirements is begun ... [p. 20]

Hence, a semi-formal approach such as URN that is suitable during early analysis and design stages, when creating safety requirements, is a useful aim.

Black goes onto use a formal goal decomposition scheme. However, *'means-end'* and Goal Refinement strategies recommended by Leveson also have lives of their own, away from AH, in semi-formal Goal Oriented Requirements Engineering (GORE) approaches. As assurance models are sliding scales with respect to formality of approach, the use of semi-formal approaches then has wider application than just the lower to medium levels of assurance. Indeed, in the Preliminary and early Architectural phases of projects, the cloud of abstraction will not allow for formal approaches and so semi-formal approaches are more apt until the level of concretisation, of both the problem and the design, reaches that point of flocculation where the solution presents.

3 Means-Ends and Intention

3.1 Leveson versus GORE

Kavakli and Loucopoulos (2004) point out that (citing Rasmussen amongst others):

... research in goal-driven RE has a cognitive basis in psychological research. This research has established much evidence for the influence of goals on human behaviour, and for the use of strategic and goal-driven processes in many kinds of activities that humans perform (Dasgupta, 1994; Rasmussen, Pejtersen, and Goodstein, 1994). [p. 2]

Kavakli and Loucopoulos describe Goal Modelling as a cycle of goal setting, execution and evaluation. These aspects are modelled using a goal based semantics and lexicon that results in *'design artefacts'*. Importantly, Kavakli and Loucopoulos argue that:

... whatever is done during the process, is done in order to identify the means by which the ends stated will be satisfied. [p. 20]

The *'means-ends'* relationship, called upon by Leveson, is thus a core aspect of GORE. Moreover, capturing the reasons behind the goal refinement during goal modelling is capturing its *'why (design rationale)'* – or the Explanation.

3.2 Rasmussen versus GORE

Recall Naikar, Hopcroft, & Moylan (2005) emphasize WDA results in *'constraints… modelled in terms of categories'* as opposed to *'design artefacts'*. The *'means-ends'* relationships of AH, result in *'categories'* as described by Rasmussen Pejtersen and Schmidt (1990) depicted at Figure 1 reproduced from p. 46 of Naikar, Hopcroft, & Moylan (2005). This notion of *'constraints'* and *'categories'* arguably also correlates to the observation of Intent Specifications by Black (2009). Thus a *'tactic for safety goal decomposition'* is still required.

MEANS-ENDS RELATIONS	PROPERTIES REPRESENTED
Purposes and Constraints	Properties necessary and sufficient to establish relations between the performance of the system and the reasons for its design, i.e., the purposes and constraints of its coupling to the environment. *Categories are in terms referring to properties of environment.*
Abstract Functions	Properties necessary and sufficient to establish priorities according to the intention behind design and operation: Topology of flow and accumulation of mass, energy, information, people, monetary value. *Categories in abstract terms, referring neither to system nor environment.*
General Functions	Properties necessary and sufficient to identify the 'functions' which are to be coordinated irrespective of their underlying physical processes. *Categories according to recurrent, familiar input-output relationships.*
Physical Processes and Activities	Properties necessary and sufficient for use of equipment: To adjust operation to match specifications or limits; to predict response to control actions; to maintain and repair equipment. *Categories according to underlying physical processes and equipment.*
Physical Form and Configuration	Properties necessary and sufficient for classification, identification and recognition of particular material objects and their configuration; for navigation in the system. *Categories in terms of objects, their appearance and location.*

Figure 1: Means-Ends relationships of AH

In fact, Ernst, Jamieson and Mylopoulos (2006) have suggested that a synergistic relationship can exist between CWA and GORE approaches. Ernst et al. note that the WDA phase if CWA, where AH is used, is *'solely concerned with context'*. However, during GORE Ernst et al. point out that *'context is provided implicitly, without explicit linkages to later phases of engineering'*.

Ernst et al. go onto suggest that WDA can provide *'cascading constraints'* between project phases, thus anchoring each phase by setting the *'context'* for each developmental phase at the relevant level of abstraction for that phase. Where these phases resemble those proposed by Bishop, Bloomfield and Froome (2001) one might attain *'cascading constraints'* or *'context'* in support of the 5 temporal slices of Assurance argumentation over a system life cycle namely:

1) Preliminary Safety Justification
2) Architectural Safety Justification
3) Implementation Safety Justification
4) Installation Safety Justification
5) Operational Safety Justification

4 URN versus Justification

Goal-oriented Requirement Notation (GRL) is one of the two modelling approaches under User Requirements Notation (URN).

When discussing the synergy between WDA/AH and GORE, Ernst, Jamieson and Mylopoulos (2006) were using a modelling notation called *i** (pronounced i-star). GRL is actually based upon *i** by Yu (1995), which itself was influenced by the earlier goal oriented approach Non-Functional Requirements (NFR) by Mylopoulos, Chung and Nixon (1992).

The argument for using URN as a graphical Justification notation is based upon revisiting critiques of

NFR and *i** from different quarters, as NFR and *i** were both precursors of GRL. NFR being dropped in 1995 by the GORE community with the introduction of *i** and of Agent Orientedness.

4.1 Bate versus *i**

Bate (2008) proposed using Goal Structured Notation (GSN) as a Design Rationale tool for design trade-offs. This likely intrusive approach sits outside the analysis and design space as an additional artefact, which is the same relationship GSN based safety arguments currently have in relation to the system design.

Many of the approaches Bate calls upon to support his Design Rationale capture mechanism using GSN, that are not provided by GSN, are already built into URN, namely:

1) Problem Derivation and Understanding
2) Scenario Based Assessment
3) Decomposition of the Design

One could, in fact, take the procedural heuristic Bate proposes and substitute URN, in doing so spanning:

> *modelling the system, production of Arguments/Justifications or Design Rationale for key objectives and properties, setting of qualitative and quantitative criteria, design evaluation results, scenarios and static analysis of the model.*

Usefully for this paper, Bate makes the claim that the closest approach to the one he proposed was by authors of earlier NFR practices from the 90s. Bate discounts use of those earlier NFR practices, suggesting NFR was a graphical tool for representing requirements only. However, quoting the same 1992 paper referenced by Bate, the aim of the NFR approach proposed by Mylopoulos, Chung and Nixon (1992) was actually:

> *...to develop techniques for justifying design decisions during the software development process ... Design Decisions may affect positively or negatively particular non-functional requirements. These positive and negative dependencies can serve for arguing that a software system indeed meets a certain non-functional requirement... [p. 2]*

Indeed, in the 16 years between the work by Mylopoulos, Chung and Nixon, and its assessment by Bate in 2008, NFR had evolved via Yu (1995) and his work on *i**, and thence onto GRL, including the induction of URN as an International Telecommunication standard as of 2003.

As the paper by Bate is now historical, it thus makes sense to revisit the use of URN for Design Rational Capture (aka Explanation and conversely then Justification) since GRL has long supplanted NFR as an approach.

4.2 Wu versus *i**

Wu (2007), similarly to Bate, submits that NFR (again, a very early precursor to *i** and hence GRL) *'fails to provide an effective mechanism for formulating quality requirements'* and discounts goal oriented approaches. One should note, however, a number of facts:

- Wu included Use Case Maps (UCM) as part of the method proposed in the thesis.
- UCM is the second of the two modelling approaches under URN.
- Amyot[1] was reporting application and research areas related to URN in 2007.

Indeed, it appears the main reference for UCM that Wu cited was the 1995 survey text for the method by Buhr and Casselman (1995). UCM had thus been bedded down for at least 12 years as evidenced by the availability of a survey text. Indeed, 7 years earlier again, Amyot (2001) described the specification of and validation of telecommunication systems using UCM and LOTOS. UCM is actually tooled for transformation into formal notations, something for which GSN is clearly not.

It might be instructive to note then that as of 2008 URN (including GRL and UCM) was the subject of International Telecommunication standards (with the original standard set down in 2003 with updates as late as 2012):

- Z.150 User Requirements Notation (URN) - Language requirements and framework; and
- Z.151 User Requirements Notation (URN) - Language definition.

In Z.151, GRL is covered under Chapter 7 and UCM is covered under Chapter 8. GSN community have since drafted a proposed "standard" in 2011[2].

To counter Wu's assessment of NFR then: the evolution of NFR through *i** into GRL, and the subsequent association of UCM with GRL within URN by 2003, ratified in 2008 and further ratified in 2012, was (and still is) a means to *'provide (an) effective mechanism for formulating quality requirements'*.

Of interest also is the manner Wu uses Bayesian Belief Networks (BBN) for Architectural Decision Making. The simple structure of the BBN proposed by Wu can readily be replicated in GRL for the purposes of supporting Decision Making. Certainly, Mylopoulos, Kolp and Castro (2001) had demonstrated the use of *i** in support of software architecture Design Decisions 7 years earlier. Indeed, Decision Support is primarily the purpose of GRL strategies as discussed by Amyot and Mussbacher (2011).

Similarly, the notion of *'anti-goals'* that Wu presents is accommodated within GRL by negative values of contribution between goals. In fact, anti-goals, in principle, act in the same way as conflicting or competing goals. For example, two positive-goals in GRL may interfere with one another, and one is generally taken to have a negative value of contribution on the other.

As the thesis by Wu is now historical, it thus makes sense to revisit the use of URN for Design Rationale Capture (aka Explanation and conversely then Justification) as GRL has long supplanted NFR as an approach. GRL has also been integrated with UCM which allows for scenario modelling of system goals, and of system behaviours for the purpose of developing Requirements and of Specification.

4.3 Jackson versus Rasmussen

In defense of agent based goal modelling, Zave and Jackson (1996) made the point that with respect to expressiveness in terms of control of actions:

---

[1] See: http://www.site.uottawa.ca/~damyot/pub/

[2] See: http://www.goalstructuringnotation.info

"Agent formalisms [Dardenne et al. 1993; Dubois et al. 1993; Feather 1987; Feather et al. 1991; Jeremaes et al. 1986; Johnson 1988] have all the recommended expressive capabilities."

It might be instructive to note also that Dubois had collaborated with both Yu and Mylopoulos on other references called out by Zave and Jackson.

Jackson (2000), of course, is the instigator behind Problem Frames. Yu and Mylopoulos, of course, were introduced earlier as being instigators behind *i** and NFR.

The premise for Problem Frames and their use in Specification is deceptably simple, as can be seen in Figure 2 below. A Machine works within the context of the Problem World to meet a Requirement. The Requirement is in the User Space. The Specification is on the Machine.

Jackson's Problem Frames, as they sit on the *'machine'*, map into the *'System'* of the taxonomic framework for CWA of Rasmussen Pejtersen and Schmidt (1990) depicted at Figure 3. That is, where available, the lowest level of *'context'* set by CWA would dictate the *'problem world'* against which Problem Frames might be applied. However, since walking over Problem Frames takes one from Requirement to Specification, they do not help setting Goals and nor walking over Goals to Requirements. This melding of the two models arguably spans Justifications 1, 2 and 3 of the HSE model. Some work is still required for the story around Architecture Justifications however.

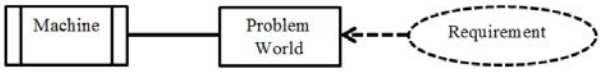


Figure 2: Problem Frame Meta-model

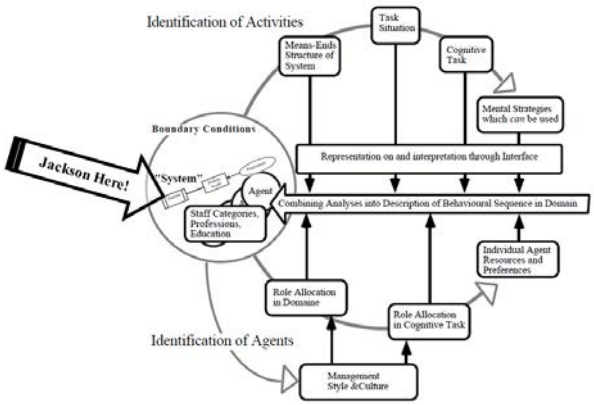


Figure 3: Intersection of Rasmussen and Jackson

Problem Frame "thinking" in GRL (call it ***ProblemFramesque***) might be a means to move heuristically from the *'constraints'* and *'categories'* of the AH, once the Requirements have been derived via goal refinement. Coupled with potential synergies already discussed, between CWA/WDA/AH and GORE, modelling of ***ProblemFramesque*** URN thus potentially provides the goal decomposition required to walk over Preliminary, through Architectural to Implementation Justification – especially as the Problem Frame community use the technique in environments requiring assurance.

4.4 Li versus *i**

In Figure 4 below the Problem Frame pattern – Commanded Behaviour – is re-interpreted by Lencastre, Alves, Melo and Alencar (2006) in *i** at Figure 5.

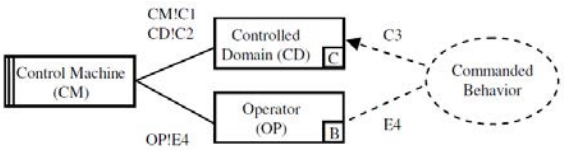


Figure 4: Commanded Behaviour

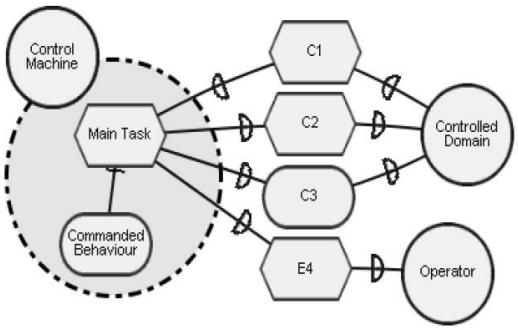


Figure 5: Commanded Behaviour in *i**

The thesis of Li (2007), however, when looking at formalizations for Problem Frames, felt there is a shortcoming of *i** based methods. Li suggests that soft goals are difficult to quantify and as of 2007 *'there is yet to be a systematic way of deriving specifications from requirements in this (i*) approach'*.

Li's criticism was on the perceived problem of quantifying *'soft'* or qualitative goals. The *i** and GRL notations also actually include (so-called) *'hard'* goals which are, by convention, quantitative. The means to quantify *'soft'* goals is via refinement or decomposition to *'hard'* goals which is also the '*wicked problem'* of design. One cannot pan *i** simply because of the nature of the *'wicked problem'*.

Goals of course tend to sit higher than Requirements, and are to be resolved to Requirements. Goals then naturally do not fall through to Requirements without some work. In a similar vein Requirements do not fall through to Specification without some work. Note also that goals Allocated to agents beget Requirements or Specification given semantically one arrives at:

The <Agent> ***shall*** <Attain|Maintain|Avoid|Cease> <Goal>

Expressing *i** models using Problem Frame modelling heuristics might then potentially be the backbone of an approach that is a *'systematic way of deriving specifications from requirements'*. To further support the ideas presented in this paper consider that when generating specifications from Problem Frames, Li proposes two methods, both appealing. The first, a formal method based upon Communicating Sequential Processes (CSP), and a second semi-formal method based on the work of Moffett, Hall, Coombes and McDermid (1996) on ***Causal Logic***. In the second approach, Li goes onto describe progressing "problems" using graph grammars and then Directed Labelled Graphs.

What is interesting about Figure 5 above is that the Tasks and Goals in the *i** model are actually sitting on the edges of the representative Directed Labelled Graph of the associated Problem Frame. This has implications for any UCM associated with the GRL model.

Amyot and Mussbacher (2001) point out that UCM are in fact for specifying *'causal relationships between*

responsibilities[3]*'*. Taking the hint from Li, and looking to Moffett, Hall, Coombes and McDermid (1996) for an explanation of Causal Logic, it is noted that there are four kinds of Causal Relationships shown in Figure 6. The four kinds of Causal Relationships can actually be interpreted in the graphical aspects of UCM as in Figure 7.

Causal Relationship	Activated by	Ended by
Causes	End of causing condition	_
Terminates	End of causing condition	_
Sustains	Start of causing condition	End of causing condition
Prevents	Start of causing condition	End of causing condition

Figure 6: Summary of Causal Relationships

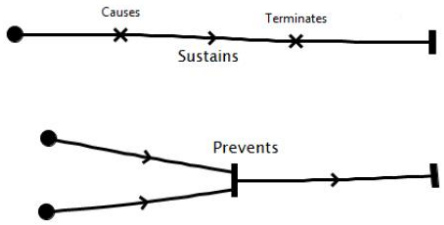


Figure 7: UCM interpretation of Causal Relationships

So, when modelling in GRL, using heuristics from Problem Frame (aka ***ProblemFramesque***) modelling, combined with supporting UCM modelling, one could potentially read across Li's arguments around the use of Causal Logic to support the application of URN as a means to express a semi-formal Specification during Implementation Phase. The URN modelling would act as the Implication Justification. There are certainly examples of UCM being input to formal methods, for example Amyot (2001). This is before one looks for application at the level of Architecture.

In a paper by Hall, Jackson, Laney and Rapanotti (2002) architectural structures are included within the Problem Frame analysis. Hall et al. describe this approach as including: *'architectural structures, services and artifacts'* which presents as an analogue of the notion of Architectural Features. It is also a happy coincidence that Architectural Features (and therefore also Architectural Tactics which will be discussed later in this paper) might be interpreted as *'domain properties'* as described in KAOS. KAOS is the goal oriented approach touched on by Hall et al. when incorporating architecture into the Problem Frame approach.

At the level of abstraction of architecture Amyot (2000) has already described, for example, the manner in which UCM can be used to model the behaviour of Architectural Features. According to Liu, Su, Yin, & Mussbacher (2014), Feature Modelling is now also a first class element in GRL and, with support of an Architectural Feature model in UCM, supports architectural Decision Making. Additionally, GRL can be used at the granularity of both Architectural Patterns as shown by Mussbacher, Amyot & Weiss (2008) and of Architectural Styles as shown by Mylopoulos, Kolp, & Castro (2001).

As a side bar note, Figure 4 and Figure 5 connote the range of interactions of the Control Model defined by Leveson at Figure 8. Hazard analysis obviously would be integral to goal/requirement/specification decomposition. Synergies thus exist between the semantics of the Problem Frame approach, and of the Control Model, both upon which ***ProblemFramesque*** modelling in GRL can leverage. Coupled with the organizational modelling aspects, and especially because of the cognitive science behind it, *i** like modelling has the potential to service the full Systems-Theoretic "thinking".

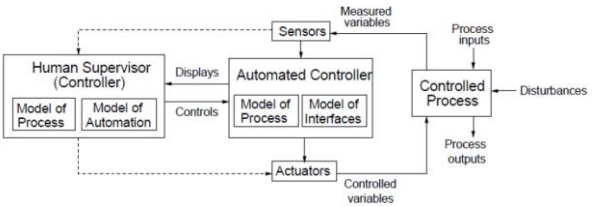


Figure 8: Control Model

Another observation is that the goal "jargon" of *'Attainment'*, *'Maintenance'*, *'Avoidance'*, and *'Cessation'* relates directly to the Causal Logic relationships (Figure 6) as depicted in Table 1.

Goal Oriented	Causal Relationship
Attainment	Causes
Maintenance	Sustains
Avoidance	Prevents
Cessation	Terminates

Table 1: Goal Oriented to Causal Relationships

In GRL there are only *'hard'* and *'soft'* goal types, so the Attainment, Maintenance, Avoidance and Cessation aspect are easily reflected in how the goal is couched or expressed. Thus Goal Oriented based Rationale as expressed in the GRL model can reflect, or can be reflected by, the Causal Logic aspects of the underlying UCM model. Note also that this falls through to the notions of *'liveness'* and *'safety'* in formal approaches. For example, in Linear Temporal Logic (LTL) mapping of *'liveness'* and *'safety'* to goal intentions is at Table 2.

Therefore, when using URN, there is a clear vertical path spanning goals and goal refinement, through Requirements and thence Specification for the Design Rationale based Justification in URN for both Preliminary and Architectural Justification and thence onto seeding Implementation Justification. There is no equivalent mechanism in GSN.

Liveness	Maintain: □(C⇒T) Achieve: C⇒◊T Cease: C⇒◊¬T
Safety	Avoid: □(C⇒¬T)

Table 2: Goal "orientedness" of LTL

As the thesis by Li is now historical, it made sense to revisit the use of URN for Design Rational Capture (aka Justification). This especially if one can model goals, through requirements, through to specifications within the one environment, and including Design Decisions and the supporting Design Rationale around architectural decisions.

[3] Responsibilities in UCM are represented by ⤫.

4.5 Asnar versus *i**

A myriad of authors appear to be converging on a Non Functional Requirement (NFR) model known generally as the Dependability & Security (***D&S***) model by Avižienis, Lapri, Randell and Landwehr (2004) shown in Figure 9 below.

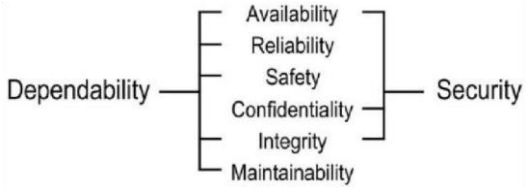


Figure 9: Dependability & Security Attributes

Avizienis et al. (2004) point out that there are four classes of ***Means*** to address three classes of ***Threats*** to a systems quality ***Attributes***, as in Figure 10.

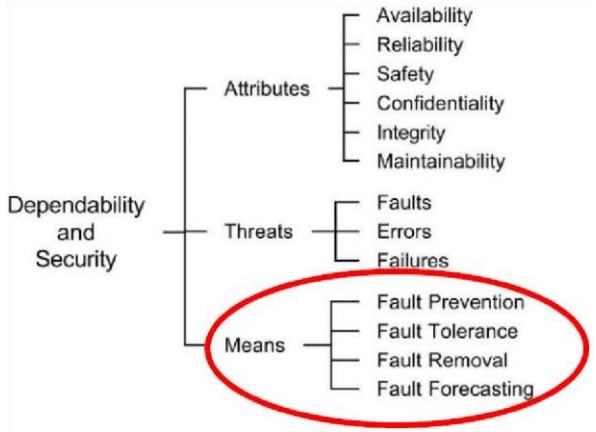


Figure 10: Attributes, Threats and Means

The ***Means*** aspect of the ***D&S*** model connotes the Technical Architecture methods from Carnegie Mellon University (CMU) who formalized the terrain of Technical Architecture in terms of Architectural Tactics according to Bachmann, Bass and Klein (2003). A quantified risk based Decision Support mechanism around the ***D&S*** model would be a candidate for trading off ***Means*** and ultimately ***Attributes*** as part of Architectural Tactic selection.

Usefully, Asnar (2009) has previously proposed a method for risk modelling and trade-off during design. Asnar's approach was based upon Defect Detection and Prevention (DDP), an approach developed at JPL and NASA. Asnar's model is re-interpreted in Goal-oriented Requirement Language (GRL) at Figure 12. Asnar interprets DDP *'objectives'* as *'values'*, *'risks'* as *'events'*, and *'mitigations'* as *'treatments'*. This transformation is likely simply applying Cognitive Science terminology.

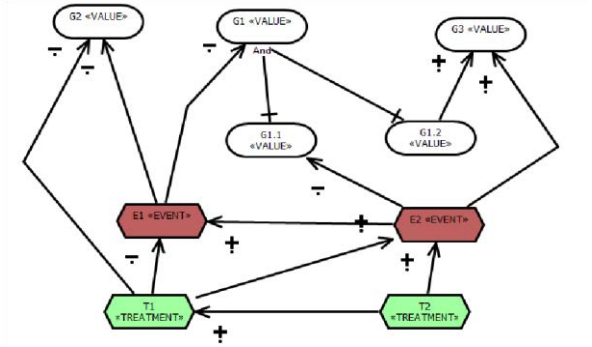


Figure 12: Asnar model interpreted into GRL

Mapping DDP, the *i** based risk modelling approach of Asnar (2009), and the ***D&S*** model of Avižienis et al. (2004) together one arrives at Table 3.

DDP	*i**- Risk	D&S
Objective	Value	Attribute
Risk	Event	Threat
Mitigation	Treatment	Means

Table 3: Concordance mapping

This correlation is not surprising as Dr Algirdas Antanas Avižienis (at least) worked at JPL, the home of DDP. Therefore, the risk based modelling heuristic Asnar proposes can read across to ***D&S***. Therefore, there already exists a quantified risk based Design Decision support method, around the ***D&Sesque*** style model, that can be applied via GRL.

The surprising corollary is, however, when one recalls the discussion around the mapping between Goal Oriented and Causal Logic views – depicted at Table 1 with the update story below at Table 4. That is, despite apparently different paths, multiple authors have "accidently" stumbled into a ***Unification of Intent***. The point being again that Cognitive Science, and indeed Psychology, refers to goal "Attainment", "Maintenance", "Avoidance", and "Cessation" as ***Goal Intention***.

Goal Oriented	Causal Relationship	Means
Attainment	Causes	Forecast faults by use of tactics x, y, z
Maintenance	Sustains	Tolerate Fault by use of tactics x, y, z
Avoidance	Prevents	Prevent Fault by use of tactics x, y, z
Cessation	Terminates	Remove Fault by use of tactics x, y, z

Table 4: Unification of Intent

Therefore, using URN to refine goals through to Requirements, and to Specifications, and into Design Decisions, has the quality that is the ***Intent*** behind so-called ***Intent*** Specifications in the purely Cognitive Science sense. There is, as Black (2009) noted however, no first class goal refinement mechanism laying behind Intent Specifications. URN can bring this first class representation to the front.

Due to the analogue of Intention to Justification URN then can compete with GSN, and indeed other graphical assurance notations, where Justification is taken to be the Argument for Assurance. Thus, using URN in this way would allow key elements of the Assurance Argument to fall out of the *'design artefacts'*. It would also allow argument over Dependability and Security rather than just over Safety – since the trade-off modelling can be between ***Attributes*** as decisions around ***Means*** are occurring. Indeed, an Intent Specification, or an Assurance Argument for that matter, focusing only on one ***Attribute***, would be fragile as any interaction with other ***Attributes*** cannot be, conversely, unmanaged.

5 Toulmin versus GSN

What Strunk and Knight (2008) do for the discussion is to attempt to validate the use of Problem Frames in an argument pattern in GSN. In their paper, which talks about Assurance Cases, Strunk and Knight propose arguing

"Specification correct" by replicating the refinement of Requirement, over Problem Frames, to a Specification in GSN.

It is a particularly interesting juxtaposition because Hall, Mannering and Rapanotti (2007) did point out that Problem Frames are actually (with formalization) a form of Sequent Calculus. Hall, Mannering and Rapanotti describe the form of Sequent Calculus as:

> *...the collection of transformations used form a proof that stands as definitive record of the demonstration (of the transformation) ... [p. 2]*

Of note, when Toulmin (2003) discusses the *'calculus'* of knock-out competitions he says:

> *'What sign will indicate that the calculus of draws is being treated as mathematics and its propositions as mathematical propositions?' The answer is, roughly speaking, that the criteria by which it is decided to accept or reject propositions must no longer involve procedural or other extraneous considerations, but must lie entirely within the calculus. [p. 185]*

What should be taken away from this is that if a formal (perhaps even a semi-formal) *'calculi'* or *'proof'* is adopted, then replicating the argument using procedurally based argumentation notations, such as GSN, is potentially nugatory. For the purposes of this paper this will be referred to as the ***Toulmin Breakpoint***.

This is a strong supporting argument for inclusion of Design Rationale based on appropriate *'calculi'* which is to act as Justification. This is also an impetus for the URN community to continue with efforts to formalize URN.

In defence of GSN, Armstrong and Paynter (2004) discuss the attainment of ***Deductive Closure*** whilst parsing over a GSN based safety argument. Think of Deductive Closure as including qualification of propositions leading to the qualification of a conclusion. So, if Deductive Closure can be applied to GSN then what makes URN a stronger candidate for Rationale Capture and for use in Justifications during the first three project phases?

Firstly, the argument for Deductive Closure over GSN is via Rationale over its nodes and edges when it is used to decompose or refine goals. GRL has the same goal refinement nature as GSN and thus the idea of Deductive Closure can read across to GRL - this is before one applies ***ProblemFramesque*** to GRL (including supporting UCM). As a corollary, the formality of rationale via the natural consequence of step-wise goal refinement over *i** (the precursor to GRL) is demonstrated by Giorgini, Mylopoulos, Nicchiarelli and Sebastiani (2002). Indeed, if the goal refinement of GRL is equivalent to that of GSN then whether or not using URN represents a *'calculi'*, or can create a *'calculi'*, is moot. This is because the argument, as it were, will have already been made during goal refinement and design rationale capture in URN, and through the nature of Goal Intention as an analogue of Justification. In fact, the nature of the example used by Toulmin is sufficiently vague that it could also mean application of an already agreed upon reasoning technique, this is because there is an intuition in the reasoning around knock-out comps that hardly requires formal math.

The real power of GRL, however, is that when one places a Goal "inside" an Actor in GRL, this is an **Act of *Allocation***. The reasoning over the model is thus the ***Argument for the Act of Design***. This comes from Actors existing in GRL, and not in GSN. That is, there is no means to Allocate in GSN.

This is also, in GORE parlance, a ***Stopping Condition***. That is, once the goal is allocated, and is no longer to be refined (at least at that level of abstraction of the system), one has reached the end of the Explanation. Looking back up the Explanation path provides the Justification that the original Assurance goal at the top has been met (up to that point in our temporal slice of Assurance). How would one achieve that in GSN in the absence of Allocation?

Indeed, as GSN is designed as a notation to support classical argumentation, rather than a requirement modelling and specification notation, it likely suffers the problems of classical argumentation, including that of ***Sceptical Regression***. This is the opposite force to that required to solve *'Wicked Problems'*.

The ***ProblemFramesque*** approach, using GRL, in fact offers a domain specific reasoning technique for assurance argument atop the GRL. This is based upon argument provided for the Problem Frame approach from that community. Evidence then is that, unlike GSN, GRL semantics does not constrain the GRL to one interpretation of reasoning practice. For example, if one avoided use of Agents when modelling in GRL one could model in ***GSNesque***. Other alternate reasoning practices can be found, applied to URN, in the literature of that community.

The argument for GSN as a Design Rational capture approach, thus, is weaker because one cannot resolve Goals into Requirements, nor Requirements into Specifications, or into Design Decisions, via *'calculi'* using GSN. In GSN you can only argue, as Strunk and Knight have done, that the application of *'calculi'* is appropriate – call it *"Procedural Argument restates Calculi"*. The GSN based Rationale then likely sits outside of the *'design artefacts'* and then makes it *'intrusive'* – in the manner Burge (2005) warns.

Consider also that the approach by Strunk and Knight (2008) appears to copy the rationale from the Problem Frame analysis into an equivalent GSN model. In fact, the verbatim copying of Rationale is nugatory if one takes the Rationale in the ***ProblemFramesque*** GRL model as the Argument, by applying the ***Toulmin Breakpoint***, and given the notion that the underlying Sequent Calculus forms a *'proof'*.

Note also, the Problem Frame "thinking" must be applied to generate the Rationale to be subsequently moved into the GSN format in the approach by Strunk and Knight – a two-step process. The likely benefit for Strunk and Knight is that there is a dearth of modelling tools for the Problem Frame approach. The Problem Frame model is thus the ***Orator*** and the GSN model is the ***Scribe***.

Revisiting Figure 5 in GRL, one can include GRL *'belief'* annotations which are synonymous to Toulmin's *'grounds'* or *'warrant'*. This is thus one means to capture the Rationale over the model – one can also add meta-data to all nodes and edges of the GRL model. This application of *'reasons'* results in what Hall et al. (2002) describe as *'discharging the Frame Concern'*. The underlying UCM could also help *'outline informally the correctness argument'* documented in the Responsibilities (⇥) littering the causal threads.

Moreover, with the addition of «THREATS» a la Avižienis et al. (2004) or «EVENTS» a la Asnar (2009), one can capture the Rationale for Design Decisions along with the Rationale for Requirement or Specification. The model in Figure 13 thus becomes a Justification in a manner fit for both Architectural and Implementation Justification.

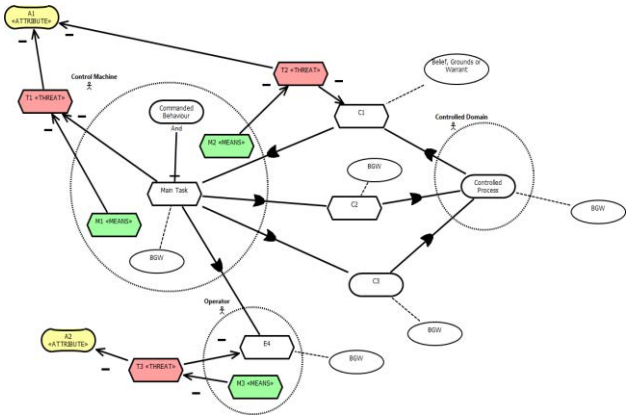


Figure 13: Fully loaded Explanation via annotations

Thus the aim would be to include ***Allocation***, ***Orator*** and ***Scribe*** aspects within the one graphical notation, and for it to act as the Rationale supporting Justification in one location and at one time (earlier rather than later).

URN can thus support Leveson's Intent Specification approach because it embodies the *'means-ends'* or *'why'* that Leveson argues is necessary to refine safety related system goals, as well as acting as a *'design artefact'* in and of itself. As a bonus, URN is already used within organizational modelling, requirement and architecture modelling, implementation modelling (aka Specification), regulatory compliance and so on[4].

6 Conclusion

Revisiting critiques of URN from the GSN community suggests a fair comparison puts URN ahead of GSN as a means to capture Rationale.

Looking at the potential makeup of an ***Argumentation Terrain***, that would support an early Justification in the Rationale, shows that URN is tooled for that purpose by design, the same end cannot be in accommodated in GSN without additional tools and techniques.

If paired with CWA practices GRL based goal modelling could be keyed to temporal phases in system development, and at the level of abstraction appropriate for those phases, to capture the Rationale for refinement, decomposition and allocation of Goals, Requirements and of Specification, and also arguably of Design Decisions over an ***Argumentation Terrain*** of problems, requirements, features, aspects and tactics acting as an ***Argument for the Act of Design.***

Leveraging off the "Toulmin Breakpoint", and including Rationale as a design artefact, URN is argued apt for the level of abstraction for Preliminary and Architectural Justifications without recourse for transcription into another argumentation notation because of the analogue between Intention and Justification.

Once the design moves through the Architectural and into the Implementation Justifications, as the *'wicked problem'* morphs from abstract to concrete, evidence is one can move to formal specifications from both the URN community, and the Problem Frames community, there are certainly synergies therein to investigate.

7 References

Amyot, D. (2000): Use Case Maps as Feature Description Notation. Chapter. Language Constructs for Describing Features. Gilmore & Ryan Ed. Springer, pp. 27-44.

Amyot, D. (2001): Specification and Validation of Telecommunications Systems with Use Case Maps and LOTOS. University of Ottawa, PhD Thesis. Available: http://jucmnav.softwareengineering.ca/ucm/bin/view/UCM/VirLibAmyotPhdThesis

Amyot, D., Mussbacher, G. (2001): Bridging the Requirements/Design Gap in Dynamic Systems with Use Case Maps (UCM). In Proceedings of ICSE 2001 Proceedings of the 23rd International Conference on Software Engineering, pp. 743-744.

Amyot, D., Mussbacher, G. (2011): User Requirements Notation: The First Ten Years, The Next Ten Years. Invited paper, Journal of Software (JSW), Vol. 6, No. 5, Academy Publisher, May 2011, pp. 747-768.

Armstrong, J., Paynter, S. (2004): The Deconstruction of Safety Arguments Through Adversarial Counter-argument. Chapter. Computer Safety, Reliability, and Security Volume 3219 of the series Lecture Notes in Computer Science, pp 3-16.

Asnar, Y. (2009): Requirements Analysis and Risk Assessment for Critical Information Systems. University of Trento. PhD Dissertation. Available: http://disi.unitn.it/~pgiorgio/papers/Yudis-Asnar-Thesis-2009.pdf.

Avižienis, Lapri, Randell and Landwehr (2004): Basic Concepts and Taxonomy of Dependable and Secure Computing. Paper. IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, January-March 2004.

Bachmann, F., Bass, L., Klein, M. (2003): Deriving Architectural Tactics: A Step Toward Methodical Architectural Design (CMU/SEI-2003-TR-004).

Bate, I. (2008): Systematic approaches to understanding and evaluating design trade-offs. Journal of Systems and Software, Volume 81, Issue 8, August 2008, pp 1253–1271.

Bishop, P., Bloomfield, R., Froome, P. (2001): Justifying the use of software of uncertain pedigree (SOUP) in safety-related applications. Whitepaper. Available: http://www.hse.gov.uk/research/crr_pdf/2001/crr01336.pdf

Black, J. (2009): SYSTEM SAFETY AS AN EMERGENT PROPERTY IN COMPOSITE SYSTEMS. PhD Thesis. Available: http://users.ece.cmu.edu/~koopman/thesis/black.pdf

[4] https://www.site.uottawa.ca/~damyot

Buhr, R., Casselman, R. (1996): Use Case Maps for Object-Oriented Systems. Prentice Hall. ISBN-10: 0134565428.

Burge, J. (2005): Software Engineering Using design RATionale. Worchester Polytechnic Institute, PhD Thesis. Available: https://www.wpi.edu/Pubs/ETD/Available/etd-050205-085625/unrestricted/BurgeDissertation.pdf

Ernst, N., Jamieson, G., Mylopoulos, J. (2006): Integrating requirements engineering and cognitive work analysis - A case study. In Proceedings of the Fourth Annual Conference on Systems Engineering Research. Los Angeles: INCOSE.

Giorgini, P., Mylopoulos, J., Nicchiarelli, E., Sebastiani, R. (2002): Formal Reasoning Techniques for Goal Models. Chapter. Journal on Data Semantics I, Volume 2800 of the series Lecture Notes in Computer Science, pp 1-20.

Hall, J., Jackson, M., Laney, R., Rapanotti, L. (2002): Relating Software Requirements and Architectures using Problem Frames. In Proceedings of RE '02 Proceedings of the 10th Anniversary IEEE Joint International Conference on Requirements Engineering, pp. 137-144.

Hall, J., Mannering, D., Rapanotti, L. (2007): Arguing safety with Problem Oriented Software Engineering. In Proceedings 10th IEEE High Assurance Systems Engineering Symposium, HASE '07. 4-16 Nov 2007, pp. 23 – 32.

Jackson, M. (2000): Problem frames: analysing and structuring software development problems. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA. ISBN:0-201-59627-X.

Kavakli, E., Loucopoulos, P. (2004): Goal Driven Requirements Engineering - Evaluation of Current Methods. In: 8th CAiSE/IFIP8.1 Workshop on Evaluation of Modeling Methods in Systems Analysis and Design. EMMSAD.

Kunz, W., Rittel, H. (1970): ISSUES AS ELEMENTS OF INFORMATION SYSTEMS. Working Paper No. 131. Berkeley: Institute of Urban and Regional Development, University of California.

Lencastre, M., Alves, K., R., Melo, Alencar, F. (2006): Analyzing Basic Problem Frames in *i** Context. In Fernanda M. R. Alencar; Juan Sánchez & Vera Werneck, ed., WER, pp. 33-40.

Leveson, N. (2002a): Webpage. Available: http://www.safeware-eng.com/software safety products/Specifications

Leveson, N. (2002b): System Safety Engineering: Back To The Future. Whitepaper. Available: http://sunnyday.mit.edu/book2.pdf

Leveson, N. (2011): The Use of Safety Cases in Certification and Regulation. Journel of System Safety, Vol 47, No. 6.

Li, Z. (2007): Progressing Problems from Requirements to Specifications in Problem Frames. The Open University. PhD Thesis. Available: http://www.scm.keele.ac.uk/staff/z_li/PhD_Thesis.pdf

Liu, Y., Y. Su, Yin, X., Mussbacher, G. (2014): Combined Goal and Feature Model Reasoning with the User Requirements Notation and jUCMNav. 22nd IEEE International Requirements Engineering Conference (RE 2014), Karlskrona, Sweden, August 2014. IEEE CS, pp. 321-322.

Moffett, J., Hall J., Coombes, A., McDermid, J. (1996): A Model for Causal Logic for Requirements Engineering. Article. Requirements Engineering March 1996, Volume 1, Issue 1, pp. 27-46.

Mussbacher, G., Amyot, D., & Weiss, M. (2008). Formalizing Patterns with the User Requirements Notation. In Y. Theng, & H. Duh (Eds.) Ubiquitous Computing: Design, Implementation and Usability (pp. 301-319). Hershey, PA: Information Science Reference. doi:10.4018/978-1-59904-693-8.ch019

Mylopoulos, J., Chung, L., Nixon, B. (1992): Representing and Using Non-Functional Requirements: A Process-Oriented Approach. IEEE Transactions on Software Engineering - Special issue on knowledge representation and reasoning in software development archive, Volume 18 Issue 6, June 1992, pp. 483-497.

Mylopoulos, J., Kolp, M., Castro, J. (2001): UML for Agent-Oriented Software Development: The Tropos Proposal. ≪UML≫ 2001 — The Unified Modeling Language. Modeling Languages, Concepts, and Tools Volume 2185 of the series Lecture Notes in Computer Science pp. 422-441.

Naikar, N., Hopcroft, R., Moylan, A. (2005): Work Domain Analysis: Theoretical Concepts and Methodology. Technical Report. Available: http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/3909/1/DSTO-TR-1665 PR.pdf

Rasmussen, J., Pejtersen, A., Schmidt, K. (1990): Taxonomy for Cognitive Work Analysis. Risø National Laboratory Cognitve Systems Group.

Strunk, E., Knight, J. (2008): The Essential Synthesis of Problem Frames and Assurance Cases. Article. Expert Systems Volume 25, Issue 1, pp. 9–27, February 2008.

Toulmin, S. (2003): The Uses of Argument. Cambridge University Press.

Yu, E. (1995): MODELLING STRATEGIC RELATIONSHIPS FOR PROCESS REENGINEERING. University of Toronto, PhD Thesis. Available: http://ftp.cs.toronto.edu/pub/eric/DKBS-TR-94-6.pdf

Zave, P., Jackson, M. (1996): Four Dark Corners of Requirements Engineering. Whitepaper. Available: http://mcs.open.ac.uk/mj665/papers.html

Process Safety and Personal Safety Need to be Retained in an Integrated Safety Risk Management System

Jim Whiting, Ken Horrigan, & Vanessa Elliott
Soteris Pty Ltd
PO Box 8252, Woolloongabba, QLD Australia 4102
jim@soteris.com.au, ken@soteris.com.au, vanessa@soteris.com.au

Abstract

Legal, moral and financial obligations are an inherent part of managing risks associated with production, transport, storage and use of hazardous substances, chemicals, radiation sources etc. in workplaces called Major Hazards Facilities (MHF). This aspect of safety risk management is often called *Process Safety*.

This paper questions the rationale for the recent trend (IChemE 2013, DuPont 2015, Energy Institute 2015, JCEC 2014) of distinguishing between *Process Safety* and *Personal Safety* or *System Safety*, and *Work Health & Safety* (WHS), to the extent of separating them into 'silos' rather than seeing them as categories of safety risks which can be managed by common principles, frameworks and processes. The arguments for this distinction are usually based on a perceived unbalanced emphasis on personal safety risks and hence a need to refocus on process safety as well.

One important issue is the persistent and erroneous assumption that measures of performance in WHS or Personal Safety as measured by personal injury statistics are valid predictive indicators of performance in managing System or Process safety risks. It should be noted that personal injury statistics, as solely negative, retrospective, lagging and outcome-based measures, lack valid predictive capabilities for personal safety performance.

Process Safety and Personal Safety need not be treated as entirely separated domains of safety risk management. Although specific consequences and controls may vary enough to identify and label them as various categories of risk, the risk management systems approach needs to be universal, consistent and integrated. Positive arguments for an integrated SMS are presented.

Keywords: Process Safety, Personal Safety, System Safety, Work Health & Safety, Integrated Risk Management System

1 Introduction

Many organisations have, or seek to have, a *single integrated safety risk management system* covering the safety of their people, the community, installations, products, assets, brand, and reputation etc. as proposed and recognised by users of Integrated Risk Management Systems standards, such as AS/ISO 31000.

It is argued that some of the results of the investigation of recent major incidents such as *Deepwater Horizon* justify the separation due to an apparent lack of emphasis on *Process Safety*. The *Deepwater Horizon* oil incident in the Gulf of Mexico (Hopkins 2011) highlighted a serious safety cultural disconnect. Hopkins notes that the inquiry held by the U.S. Coast Guard and U.S. Department of Interior found that a management visit to the drilling rig at the time of the well blowout highlighted how senior management had been focused on spills, trips and falls while entirely missing the signs of pending process disaster. The focus of safety for these senior managers, as well for their companies, appeared to be on managing conventional safety hazards as they may impact on individuals personally, not major process safety hazards. These process risks have been proven by all previous high profile, high consequence, low frequency process incidents to be just as, or even more, urgent with respect to risks of harm to individuals. It appears that not only was there a common false belief that 'good' safety performance was indicated by 'good' personal injury statistics, but even worse that personal injury statistics was also indicative and predictive of performance in all categories of safety.

The authors of this paper recognise the benefits of simple categorisation of safety domains but not complete separation into distinct systems which a number of safety professionals are advocating and have adopted. There are increasing numbers of themes in safety literature and conferences distinguishing between two safety risk domains labelled 'personal' and 'process' safety, not just as categories of risks, but entirely separate safety systems, processes, and even responsible personnel.

Separation into standalone systems fails to mitigate undue emphasis on any particular category of safety risks. Safety risks need to be managed – identified, analysed, evaluated and treated – in the same rigorous manner regardless of the origins of some of the risk factors. A design defect in a process component due to an incompetent, distracted, unsupervised, or a misassigned design engineer, is a risk factor which can be involved in causation of a personal injury as well as a process injury (e.g., fire or explosion, production loss or asset/ environmental damage). Risk questions for all scenarios of events, risk factors and outcomes need to be considered together and consistently across all risk events.

There should be no suggestion that completely separate isolated risk assessments by different personnel are required to ask the following separate risk questions

Copyright © 2015, Australian Computer Society, Inc. This paper appeared at the Australian System Safety Conference, Australia. (ASSC 2015), Brisbane 27-29 May 2015. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 169. Ed. Tony Cant. Reproduction for academic, not-for-profit purposes permitted provided this text is included

based on consequences alone:

A. How could the design of safety-critical equipment (e.g. sensors, regulators, valves, etc.) *lead to a safety incident* that harms an operator due to how it is located, installed, operated or/maintained?; and
B. How could the design of safety-critical equipment (e.g. sensors, regulators, valves, etc.) *lead to a major process incident* (e.g., failure, fire, explosion, release or spill leading to major harm) due to how it is located, installed, operated, or maintained?

The proposed separation of risk management approaches, rather than integration of categories, is confusing, inefficient and could lead to safety risk personnel actually missing pertinent safety risk exposures – part of the quoted rationale for introducing the separation.

2 Possible Causes of Inadequate Focus on Process Safety Management (PSM)

To identify and understand the current push to separate safety into silos rather than develop an integrated safety risk management system, refer to Table 1 below, which describes 7 possible reasons for PSM performance deterioration. While all 7 factors are important, b, c, d, and g are highlighted for special mention as particularly relevant to the theme of this paper. If an inadequate focus on PSM with concomitant PSM performance deterioration is identified, then those inadequacies need to be addressed rather than setting up separate safety management systems. Sections 3 to 8 of this paper explain how these inadequacies can be addressed without resorting to separation of the safety management systems.

a)	Regulation sometimes leads to a minimum-cost, compliance-based approach.
b)	Declining worker injury rates may give management a sense of complacency that the risk of process safety incidents must likewise be declining.
c)	PSM may have been implemented as a separate, stand-alone system that was not integrated into the organization's overall management system or as a one-time project instead of an ongoing process.
d)	Audits have focused on symptoms of problems; they have failed to identify underlying causes.
e)	Diminishing resources are devoted to process safety; facilities face increased pressure to achieve short-term financial objectives.
f)	Mergers, acquisitions and divestitures have decreased organizational stability.
g)	Success has led to complacency; the absence of major accidents reduces a company's sense of vulnerability.

Table 1: Possible Causes of PSM Performance Deterioration (AIChE 2007).

3 Addressing the Inadequacies: Clarify Causal Factors, Risk Factors, Root Causes and Consequences to Demonstrate the Similarities Rather than the Differences

Table 1 above indicates that a possible reason for PSM performance deterioration is the separation of PSM from the organisation's overall SMS (refer to point (d) in Table 1). A focus on the differences rather than the similarities can lead to this unnecessary separation.

The causal factors of an incident today are the risk factors of yesterday's risk and as evidenced they were not being managed effectively. The risk factors of today's risk, that are not being managed effectively, will be the causal factors of tomorrow's incident. All safety incidents have causal factors and risk factors which are similar, but may have some different mixtures of types – i.e., systemic, behavioural, physical, equipment, and environmental. There is a common misconception that the causal processes of high severity/low likelihood risks are exactly the same as those of low severity/high likelihood risks (see Manuele 2011 and Section 6 for a discussion on problems with Safety Pyramids & Triangles). This error is used to justify focussing on the more common low severity risks and incidents as a purportedly proactive approach to overall safety. The causes can be similar in nature, however they contribute to different incidents and risks in different sequences, degrees, mixes, and combinations. The differences can justify categorised risk or even differently labelled risk domains, but the overall uniformity in management requirements justifies managing all categories in an integrated safety risk management system, not separate systems. Also, the universal applicability of integrated risk management systems, methods, and tools strongly indicates a unified, consistent approach to all risks. Management of safety risks can benefit from categorisations of the risks based on some chosen characteristics, such as high severity/low likelihood risks or low severity/high likelihood risks but categorisation does not need to lead to actual separation of risk management into PSM and SMS 'silos'.

One of the claimed justifications for separating management of major process risks from other safety risks is the *nature and magnitude of the Consequences* that can involve a MHF. These facilities can have actual incidents and potential risks (e.g., significant fires, explosions, poisoning, toxic harm, etc.) usually affecting large numbers of exposed people, with broad very serious impacts on the assets, the environment and economic wellbeing of an enterprise. The risks are usually regarded as major because they are often high severity, low likelihood risks associated with chemical, nuclear and biological processes moving outside planned process parameters.

The consequences are certainly of a nature which requires an adequate focus on the MHF risks but do not justify a 'siloing' of the personal safety and process safety risk management processes.

Another quoted justification for separation is the *nature and magnitude of the Causal Factors and Risk Factors*, including loss of control and containment associated with operational factors such as high or low pressures, flows, temperatures toxicity or incompatibilities, and inadequate control and mitigation of escalation. These causal and risk factors may require specialist knowledge to assist with the risk analysis and development of risk control measures. As indicated later in this paper, this need is properly addressed through the use of both engineering, security and safety specialists as required.

Lastly, *the nature of the Root Causes* of the Causal Factors and Risk Factors are also used to promote separation**.** Root Causes of process Safety incidents and risks can include inadequate systemic, behavioural and equipment factors involved in defective design, construction, installation, operation, maintenance, modification, change, and decommissioning of a process facility. As indicated earlier in Section 1 of this paper, these root causes can equally lead to both individual and process safety risks.

4 Addressing the Inadequacies: Integrate the Safety Management System (SMS) Rather than Creating Separate SMS or PSM Systems

As stated above in Section 3, Table 1 indicates that a possible reason for PSM performance deterioration is the separation of PSM from the organisation's overall SMS, i.e., lack of integration of the systems.

MHFs and their Regulators recommend that there should be one integrated SMS applied across all Safety Risk domains, yet some organisations continue to utilise distinct systems. While the integrated principle is probably more recognised in Australia and Europe than the USA, the applicability of the principle is the same. All modern SMS models are essentially risk-based and the only differences in application of the SMS to different risk domains are in the Operations and Controls elements of the SMS (see labelled Elements in SMS examples in Appendices 3 and 4).

Occupational Health and Safety Management Systems (OHSMS) have been commonly associated with the management of occupational health and safety in facilities. While the OHSMS for MHF can benefit from the inclusion of some additional categories of risk factors, **the OHSMS structure and applications need not be changed**. The OHSMS can be structurally and functionally the same for all categories of risks. Organisations can ensure that their OHSMS is broad, consistent, comprehensive and integrated. Specific process safety elements are integrated into elements of the one OHSMS without any need for a separate SMS.

Safety Management in the MHF context is the systematic practice of identifying potential for significant harm, assessing the risks, making decisions on appropriate controls, and implementing and monitoring systems and risk control measures to minimise the residual risk to *as low as reasonably practicable* (ALARP).

Table 2 below outlines commonality of characteristics of any Safety Management System ensuring the same risk management approach for any safety risk!
1. Risk Based Focus
The SMS needs to reflect the hazards that are present, and support the actual practices at the facility. An SMS that focuses on the specific requirements for safe operation will ensure that they meet regulatory requirements and manage their risks. An SMS needs to be founded on recognition that there is a potential for minor and major incidents at the facility, and a comprehensive understanding of what may cause or contribute to such incidents. There must be a clear demonstrated commitment to effectively manage and minimise the associated risks. Management and employees need to understand and engage with the SMS. Each operator of a facility needs to implement a workable system appropriate to the particular facility, the identified hazards, the adopted control measures, and the resultant levels of risks.
2. Fitness for Purpose
A key requirement of a SMS is that it be 'fit-for-purpose'. That is, it should be uncomplicated and sufficiently comprehensive to cover the full range of activities at the facility that could have a significant safety impact. **A key factor is the careful integration of the component elements of the system.** The individual elements must be mutually consistent and complement one another as an integrated whole. The SMS should be relevant, realistic and sufficiently clear to be understood by users and reviewers of the system alike.
3. Improvement through Learning and Review:
Errors, deviations and breakdowns in control measures and corresponding parts of the SMS need to be tracked under the SMS, to provide data on the actual safety performance of the facility. Performance standards must be used to facilitate this process and systems should also be in place to learn from the experience of parties external to the operator of the facility.
4. Recognition of Human Factors and Behaviour
When developing systems, procedures and operational controls it is essential that the human factors that contribute to their successes and problems must be fully considered. Just as tasks need to be designed to take into consideration human capabilities and limitations, operators need to take the same consideration in the design, implementation and monitoring of systems and procedures that govern those tasks and make up the overall system. In particular, implementation and maintenance of the SMS must be within the practical capabilities of the workers. The SMS must encompass the varied control measures of the human factors, which influence human actions or inactions involved in the root causes of risk and causal factors. This principle applies to everyone involved with MHF activities whether they are a manager, supervisor, employee, a contractor or a visitor that translates the SMS into real day-to-day risk management.

Table 2: Commonality of Characteristics of any Safety Management Systems – Major or Minor Hazards.

A significant argument for the integration of Process Safety and Personal Safety is the fact that most existing and emerging Safety Management Systems treat each category of the same risk management system and unique operational controls in the same way. All management systems have a framework based on the continual improvement cycle: *Plan, Do, Check, Act*, or their equivalent terminology. Figures 1A to 1E illustrates this universality for SMS Standards AS/NZS 4801:2000, ANSI Z10:2012, the new international SMS standard ISO 45001: 2014, and the international Risk Management System Standard ISO 31000:2009. It would be good management practice for organisations to review their Safety Management Systems to ensure that they are using best practice integrated approaches.

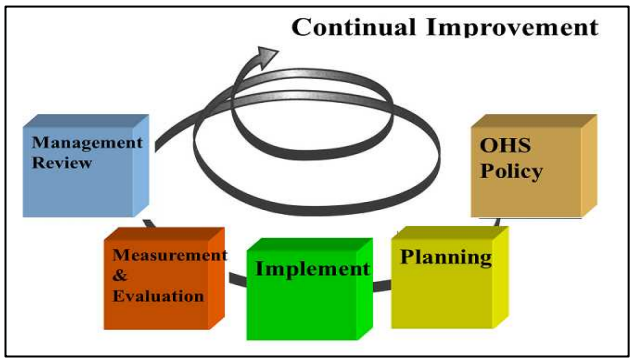


Figure 1A: AS/NZS 4801:2001

It is worth noting that until ANSI Z10:2012 was developed and adopted, the USA did not have a national standard for OHSMS which may be a likely reason for first creating the PSM pseudo management systems shown in Appendix 4.

Additionally, Appendices 3 and 4 demonstrate (without all the sub-detail) that the elements of an integrated SMS cover ALL the Process Safety Management PSM components even if groupings and terminology are not exactly the same.

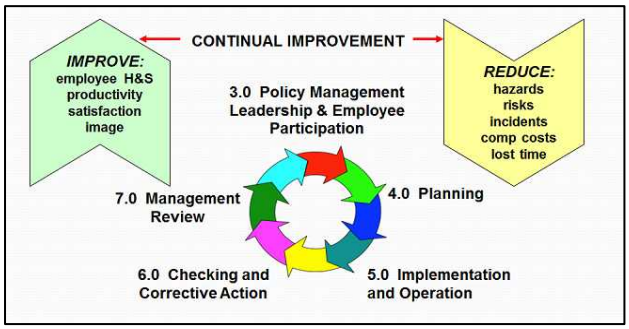


Figure 1B: ANSI Z10:2012

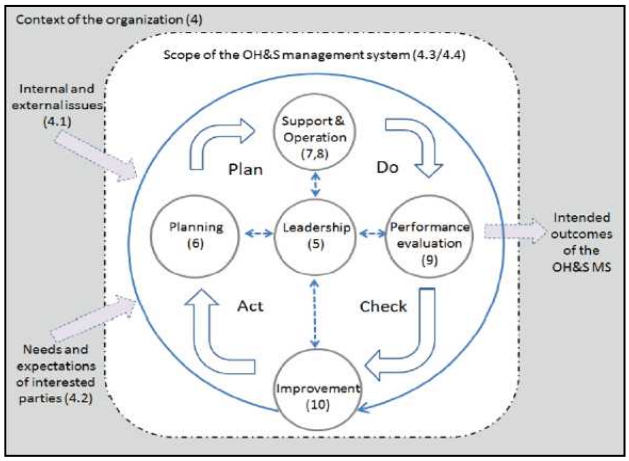


Figure 1C: ISO CD 45001:2014

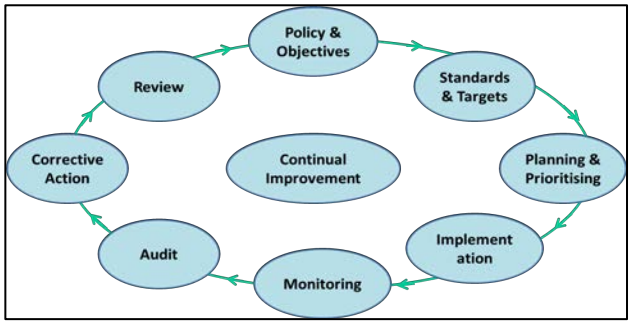


Figure 1D: Generic Elements of a Management System

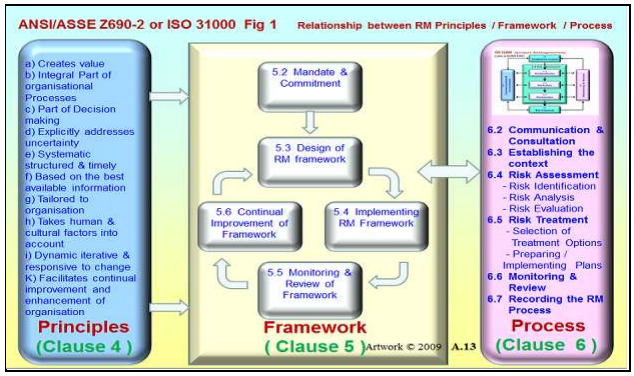


Figure 1E: AS/ISO 31000:2009 Risk Management

An integrated SMS, that can and should also cover PSM, needs to demonstrate that it supports all risk control measures needed for the controls to work effectively. A number of SMS elements need to be functioning effectively to maintain the controls' performance in reducing likelihood and/or consequences of risk factors.

All detailed sub-elements of an integrated SMS can be categorised for different risk types according to the nature and origins of each risk type. For example, in some facilities, sites and organisations there could be categories of safety risks (such as working with hazardous substances, containment integrity, working at heights, exposure to radiation or biological hazards, erection and dismantling of large structures, etc.) requiring specific tools and methods for analysis and control of the risk levels to ALARP. Fortunately, the way those risks are managed can be consistent and universal as shown in Figures 1a to 1e. Applying the integrated SMS can demonstrate all the aspects of each category measures are being managed by SMS elements of a comprehensive system that works together well.

Table 3 shows Extracts from Australian regulatory standards (National Safe Work Australia 2012; Victorian Work Safe 2011; NSW Dept. of Planning 2004, 2011) for major hazards safety. Again, the principle that an integrated SMS should and can cover ALL safety risks is explicit.

Features of successful SMS development and implementation
The following factors are critical to the SMS. The SMS: • Must be **comprehensive** and **integrated** with respect to the adopted control measures. • Should have **sufficient focus on major incident safety**, from planning through to operations. • Must have **performance standards**, which enable the operator to measure the effectiveness of the SMS in ensuring safe operation. • Needs to **cover the whole facility** defined within the Safety Case. • Should reflect the **overall safety culture** and **values** of the facility. It should not be a pure paperwork system divorced from actual behaviours and attitudes of workers.
Core concepts
• The operator of an MHF must establish and implement an SMS, which provides a **comprehensive and integrated** system for the management of all aspects of the adopted risk control measures. • The SMS must be the **primary means** of ensuring safe operation in respect of major hazards, which is achieved by managing and assuring the performance of the adopted control measures. • The SMS should incorporate **processes to identify, select, define, implement, monitor, maintain, review and improve the range of control measures** on which safe

operation depends. Errors, deviations and breakdowns in control measures and corresponding parts of the SMS need to be tracked under the SMS, to provide data on the **actual safety performance of the facility**. Performance standards must be used to facilitate this process. • The SMS should incorporate the **generic management system cycle of planning, implementation, monitoring, corrective action and review**, so that safety is maintained and improved. The SMS should be subject to regular review and improvement.
SMS tests
Is the SMS: • Comprehensive? • Integrated? • Accessible? • Comprehensible? • Documented? • Facility-wide? • Realistic? • Dynamic? • Improving?

Table 3: Principles that an integrated SMS should cover ALL safety risks (Victorian Worksafe 2011)

Figure 1F below shows that the process for management of risks in any safety domain can be structured the same as described in AS/ISO 31000;2009 and ANSI Z690.2:2011. This universal approach satisfies all the OHSMS Standards of Appendices 3 and 4.

Figure 1F: Risk Management process for ALL Risks

5 Addressing the Inadequacies: Develop Appropriate Safety Performance Measurements and Indicators

Table 1 in Section 2 indicates that two other possible reasons for PSM performance deterioration are that declining worker injury rates may give management a sense of complacency that the risk of process safety incidents must likewise be declining, and that success has led to complacency; the absence of major accidents reduces a company's sense of vulnerability (Refer to points (b) and (g) in Table 1). Both are indicative of the inadequacy of the reporting systems to provide a clear understanding of the level of risk in a MHF.

Safety performance measurement is perennially covered topic in the literature. However it is worthwhile highlighting two aspects of safety performance measurement as it relates to arguments for separation of Process Safety and Personal Safety. They are:

1. Measurement with invalid metrics; and
2. Assumption that injury statistics can indicate both Personal and Process Safety Performance.

The authors recognise that many managers continue to inaccurately assume that low injury statistics can also indicate or predict how well risks of process safety incidents are being managed. Operators do recognise when the choice of safety models for measuring safety performance is poor because it usually involves misinterpretations and misunderstandings of the measures being used in the model. For example, the misuse of Heinrich (1980) models using safety triangles and pyramids in choosing safety priorities and Key Performance Indicators (KPIs) is particularly detrimental to establishing, and corrosive to belief in sustaining, a positive safety culture. If workers' safety performance is being measured by confusing or invalid metrics, they certainly cannot believe and engage appropriately. They recognise that having low or even zero Lost Time Injury statistics for any given period is no guarantee that all risks of future incidents are being managed and the organisation's SMS is working well.

Manuele (2011) accurately describes these problems with the Heinrich Model in detail. The most important misunderstanding is the assumption that addressing or focussing safety management on causes of low severity incidents or risks & near misses which are the usual bottom tier of the pyramid, can also simultaneously manage causes of high severity/low frequency/probability incidents/risks at the top of the pyramid. This assumption ignores the fact – which workers readily know – that many of the causes of high severity incidents or risks are NOT the same sequences, mixes and combinations of causes as for lower severity incidents or risks. For example the causes of a plane crash are usually very different to the causes of a baggage handler's back injury. Hence, safety risk management needs to develop and implement risk controls that match the different sequences, mixes and combinations to reduce the risk to ALARP. Each class or category or tier of incident severity can require explicitly different combinations of risk controls to manage their mixes of causes adequately. Performance measures based on how well positive, risk-based, proactive, and prospective controls are being identified, developed and implemented will always provide better predictive assurance than lagging outcome measures of safety performance that are based on historical, reactive, and retrospective injury statistics.

Another serious misinterpretation of Triangle models is that the frequency/severity (f/s) relationship inherent in safety triangles and pyramids is assumed to be true for small sample (N) size. Often ignored is the fact that the linear and log-log plots of f/S graphs are only true for a large sample size (a large N population and for long T time periods). Figures 2A to 2D show that high severity incidents and high severity risks are usually low frequency and low likelihood respectively. The higher the severity the more risk controls or layers of protection have been, or could be ineffective or missing. Simply stated, greater severity outcomes usually require more and/or less likely factors to go wrong and hence, they will be less frequent or likely incidents or risks.

The oversight or ignorance of the importance of sample size (as well as other statistical design elements)

in safety research leads to meaningless comparisons of safety incident results for studies involving small sample sizes. For instance, studies that draw conclusions about safety performance based on a sample size of N = 100 employees on a month-by-month basis (T=1 month) would limit validity or statistical significance in an organisation with 5000 or more employees. There would be much higher confidence in interpretations of variations of incident statistics for large sample sizes, where N=1000 employees and T = 1 year. Trend Analyses and variations need to be analysed within a Statistical Process Control (SPC) context.

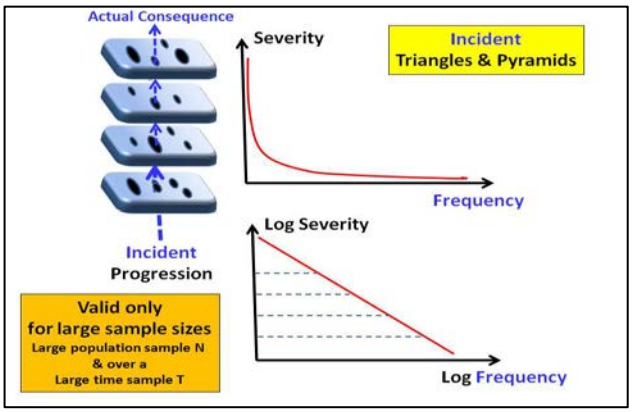


Figure 2A: Large Sample F/S Curves for Incidents

Where invalid research measures have been used in research design, a false interpretation of how any changes in safety programs can be causatively attributed to changes in safety performance seriously undermines belief in those safety programs. Confidence in how well safety is going will be destabilised by using false indicators.

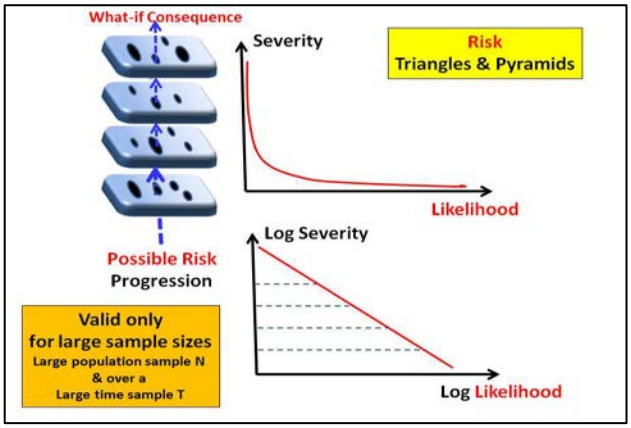


Figure 2B: Large Sample F/S Curves for Risks

For a large sample of *incidents*, the *severity/frequency* plot is inverse – as severity of the *actual incident* increases, *frequency* decreases. A log-log plot straightens out the asymptotic relationship. Also the sketch of the 4 ineffective or missing layers of protection or Swiss cheese *causal factors* shows that the higher the severity, the more layers or controls had to have failed, hence less *frequent* incident progression.

For a large sample of risks, the severity/likelihood plot is inverse – as severity of the what-if risk increases, likelihood decreases. A log-log plot straightens out the asymptotic relationship.

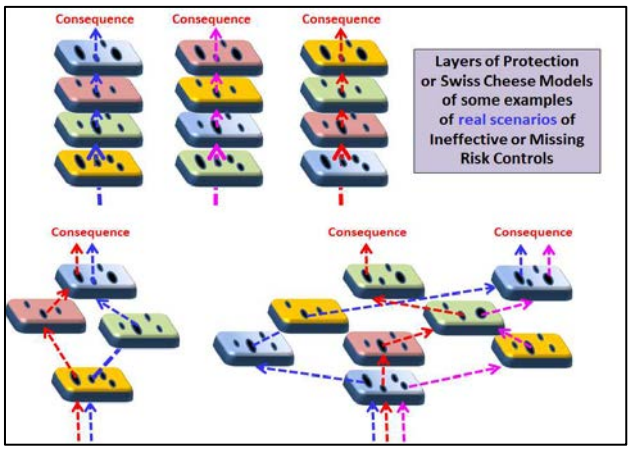


Figure 2C: Layers of Protection and Swiss Cheese models of causation

Also the sketch of the 4 ineffective or missing layers of protection or Swiss cheese risk factors shows that the higher the severity, the more layers or controls would need to fail, hence it is less likely for the risk scenario to escalate or progress to the higher severity. The simplistic linear layers of protection and Swiss Cheese models of causation are not always realistic. Different severities can have similar root causes but in different sequences, mixes and combinations as shown in Figure 2C or even much more complex arrangements.

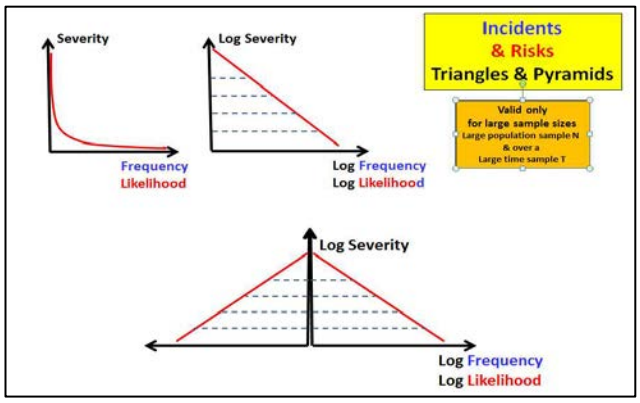


Figure 2D: The ubiquitous Triangle or Pyramid is formed by horizontally mirroring the log/log plot

For the safety triangles and pyramids, it is ALWAYS necessary to clarify if the triangle is for actual incidents or what-if risks NOT a mixture of incidents and risks or even causes as shown in Figure 3.

As previously mentioned, the use of the flawed safety performance measures and incorrect interpretation of these measures does not provide adequate justification for separating Process Safety and Personal Safety into non-communicating, isolated 'silos'. Rather, the process for managing risks of any size can be the same, and common safety performance can be measured in consistent, comprehensive and integrated ways. As stated in the introduction, there is ongoing confusion about what measures are needed to provide best assurance of levels of safety risk management. Personal Injury Statistics are not accurate predictive indicators of how likely a new

incident of variable severity could occur in the future. The American Petroleum Institute API and the US Center for Control of Process Safety CCPS have attempted to categorise Process Safety according to frequency and severity and also risk factors of process incidents in a 4 Tiered triangle as shown in Figure 3 (See Appendix 2 for further discussion).

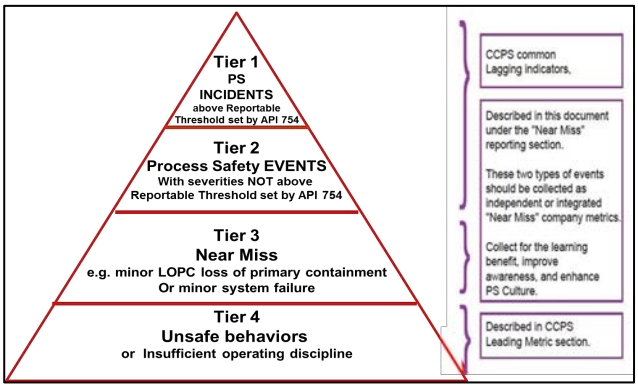


Figure 3: Confusing Process Safety Metric Pyramid
(Adapted from AIChE/CCPS 2011)

There are several concerns with this approach. There is a mixture of incidents and risks. Because incidents are associated with retrospective lagging outcome metrics and risks are associated with prospective leading process metrics, the triangle shown cannot help to interpret safety performance for any category of risk. It is correct to interpret the diagram as indicating that the higher the severity of either a Process Incident or a Process Risk then the lower the Frequency or Likelihood but it is meaningless to have both in the same diagram. Tier 3 consists of near misses (i.e., also incidents) as in Tiers 1 and 2. Tier 4 consists of possible causes of either incidents or risks. The top 3 tiers are Incidents while Tier 4 consists of non-standard behaviours that can be part of the different contributory combinations of causes of ALL incidents of any severity (i.e., they could contribute or relate to all 4 Tiers).

The mixture prevents any meaningful interpretation of causation and triangles and will certainly lead to the perennial problems of *Heinrich 1930* – type triangles as detailed by (Manuele 2009*)*. Even if all 4 tiers are risks, it is an invalid assumption to say that managing the causes of the lower tiered risks will also manage the causes of the upper more severe tiered risks unless we can establish and demonstrate that the causes of incidents in both tiers are not only the same in nature but also the same in sequencing, mixes and combinations with other causes - see Figure 2C.

In this context, an employee who falls from a ladder partly from fatigue could be killed. Fatigue may be one of the direct causal factors. However other underlying root causes would have also contributed, such as not following fatigue risk management policy. This in turn could be due to his manager not supervising use of the policy, which is in turn could be due to management workload pressures, etc.

Similarly, fatigue could be part of a different number of sequences, mixes and combinations of causes leading to an operator not opening a pressurised valve at the appropriate time by the appropriate amount. This could ultimately lead to multiple fatalities due to simultaneous failure of other process risk controls, such as automated ESDs, Interlocks etc. Developing and implementing better risk controls for application of, and adherence to, the fatigue risk management policy does not automatically have the same risk reduction effect for high, as well as low, severity risks. The fatigue risk management control measures may have a greater or lesser effect in both scenarios and therefore there can be no simple assumption that addressing the fatigue risk issue for low severity risks will also be as beneficial for higher severity risks.

It is important to note the following preferences:

1. The authors prefer the descriptor ‘non-standard’ behaviours rather than common undefined terms such as ‘unsafe’ and ‘at-risk’ behaviours.
2. Leading safety performance indicators need to be based on proactive risk-based measures not lagging retrospective outcome measures such as incident statistics

It is recommended that measures of *how well and timely the appropriate risk controls for any specific tiered risk are developed and implemented to target exactly the corresponding sequences, mixes and combinations of causes* can be the only meaningful measure of safety performance – i.e., how well the SMS enables successful identification, analysis, evaluation and implementation of effective controls of any type of safety risk for reducing them to ALARP.

It is interesting to note that one of the tools of engineers, SPC and SPC Charts, are also an effective tool to monitor both personal and process safety. Once the correct balance of lagging and leading indicators has been identified SPC can be used to inform senior management and the workforce of the real trends and changes to the SMS.

6 Addressing the Inadequacies: Engaging Senior Management and the Workforce

All the possible causes of PSM performance deterioration identified in Table 1 in Section 2 are linked to inadequacies in the systems managing risk and the inadequate response of senior management. The need for senior management support for, and engagement with, personal and process safety is also a perpetually covered topic in the literature. There are many contemporary systems, such as Relationship Based Safety and Positive Safety Culture, which assist organisations to avoid the safety culture disconnect identified in the investigation into the *Deepwater Horizon* incident.

Even without the benefit of more effective embedded work cultures there are methods and media which can be used to engage senior managers in process safety. Case studies of real process safety events at regular senior management presentations help them realize that the consequences are probabilistic and could have been reduced through more effective and rigorous process safety management (Kamrath 2014).

Another important communication ‘hook’ is to emphasise the direct links between good process safety management and traditionally perceived ‘business’ imperatives, such as plant reliability, productivity and asset longevity. Senior managers need to be regularly

reminded that the root causes of reliability incidents are usually related to inadequate, ineffective implementation of the same management system elements that are required for process safety and personal safety. The financial benefits of improved reliability through better operational application of the elements of process safety management, which are essentially the same as personal safety, can be readily demonstrated. AIChE/CCPS (2014) recommend that improved productivity and efficiency be a foundation for the development of PSM systems.

7 Addressing the Inadequacies: Reducing Counter-Productive Emphasis on Human Contributions to Safety

A worrying aspect of the argument for more focus on Process Safety is probable perpetuation of the common myth that safety problems are predominantly related to personal behaviours. The descriptions of personal behaviours as part of the way that Personal Safety is being distinguished and even separated from Process Safety, often refers to subjective, ill-defined and misinterpreted terminology such as personal 'unsafe acts' and 'at-risk behaviours' of unsafe workers. 'Unsafe' can only be defined in terms of not being ALARP. Also, all behaviours, including following a procedure, involve risk. So all behaviours are deemed 'at risk'. In their most recent framework for Risk Based Process Management (RBPS) AiChE/CCPS (2014), CCPS use the terms 'safe work', 'safe work procedures' and 'safe work practices'. They also state that "Causes of chemical process incidents can be grouped in one or more of the following categories: Technology failures; Human failures; Management system failures; and External circumstances and natural phenomena".

In 100% of incidents and risks - NOT 80% of causes, as is often claimed - human actions or inactions (often labelled *human errors)* of one or more people are always implicated. Employees and managers will always be involved in terms of actually or potentially doing or not doing things that they were:

- Supposed to do;
- Tried to do;
- Wanted to do;
- Needed to do;
- Told to do; and/or
- Trained to do; etc.

It is a simple fact that even when a pump fails, humans (the process owner, designer, the procurer, the seller, the deliverer, the installer, the quality inspector, the commissioner, the operator, the maintenance system designer, the maintenance person, etc.) would have, or could have, been involved.

Once we recognise that the actions or inactions of a number of people are always involved, the next and most important issue is NOT to label them as 'causes' until we investigate, analyse and probe to establish the following-

- What were, or could be the **underlying root causes** of those actions / inactions?
- Was there any **choice or intent** in those actions / inactions?
- How did or could behaviour-based Causal Factors and Risk factors become **actual Consequences** of deeper underlying non-behavioural Root Causes?

The trend to separate Personal Safety from Process Safety could place further undue emphasis on personal behaviours as the 'causes' without analysing the systemic and physical aspects of underlying causation. This may lead to inaccurate assessment of risks and result in the misapplication of strategies to remedy 'identified' risks

8 Addressing the Inadequacies: Reducing the Chance of Safety Silos

As previously stated, Table 1 in Section 2 indicates that a possible cause of PSM performance deterioration is the lack of integration of safety management systems. The artificial separation at the macro-level of the two personal safety and process safety domains may be related to the traditional views of the practitioners. Engineers, Security Professionals and Safety Professionals have often not experienced and hence do not see the need and value of being involved in each other's processes at the micro-level (i.e., finding and managing the root causes of the safety risk factors).

More importantly, there is a serious lack of recognition that most root causes of the risk factors are the same in both domains, namely, systemic and behavioural. Broader roles and involvement of chemical engineers and security and safety professionals in both Personal Safety and Process Safety can return mutual benefits. Organisations often miss valuable opportunities for security and safety professionals to facilitate risk assessments including those commonly referred to as 'process' related. The facilitation process does not require the same level of in-depth knowledge and skill of the chemical or process engineers in a risk assessment or review team. The facilitator can contribute significantly by asking the traditional *intelligent ignorant* questions which the experts are prone to overlook or wrongly assume are not risk-related.

Security Professionals and Safety Professionals do not always engage in process safety activities, such as initial design reviews. Operatives in an organisation with 'safety' in their position titles and job descriptions often do not offer and also are often not invited to contribute to what is commonly referred to as process safety reviews. Vice-versa, chemical engineers are not always adequately trained in recognition of the breadth of safety risk management activities or the need to consider security issues in the process safety reviews. They correctly, but narrowly, focus on the common considerations of the effects on the process due to abnormal variations of reactivity, pressure, temperature, mass, volume and flow. The narrowness of their scope means that they often cannot see the benefits and value of involvement of security and safety practitioners.

Reasons for this situation are usually due to historically restrictive job descriptions, time poverty due to poorly prioritised work planning, lack of notification or invitation to participate, relative position and status within an organization, and sometimes ignorance of the principles and tools of each other's specialties.

The walls of the silos need to be broken by better communication and cooperation among engineering and non-engineering departments.

9 Summary

All safety risk domains need close analysis and comprehensive risk management within a comprehensive integrated SMS. An integrated SMS may require only minor additions and variations to cater for any unique features of implementation and operation of the same risk management processes, however the financial, risk and safety benefits of such modifications may be sizeable. There is no justifiable need for separating out risk domains into separate stand-alone silos, and indeed there are unwanted threats to sound management by introducing such separations.

10 References

American Institute of Chemical Engineers, Center for Chemical Process Safety (AIChE/CCPS). (2014): *Risk Based Process Safety Overview.*

AIChE/CCPS. (2011): *Process Safety Leading and Lagging Metrics.* http://www.aiche.org/sites/default/files/docs/embedded-pdf/CCPS_ProcessSafety2011_2-24-web.pdf.

AIChE/CCPS. (2007): *Guidelines for Risk Based Process Safety*. New York, Wiley.

ANSI/ASSE Z10. (2012): *Occupational Health and Safety Management Systems Standard (OHSMS).*

API. (2010): American Petroleum Institute, *ANSI/API Recommended Practice 754, Process Safety Performance Indicators for the Refining and Petrochemical Industries, First Edition, Washington D.C.*

API American Petroleum Institute. (1990): API RP750, *Management of Process Hazards*.

API American Petroleum Institute. (1998): API 9100A, *Model Environment, Health and Safety MS.*

API American Petroleum Institute. (1998): API 9100B, *Guidance Document for Model EHS MS.*

Arendt, S. (2008): *Risk-Based Process Safety: The Next-Generation PSM System*, World Energy, **10**(4).

AS/NZS 4801. (2001): *OHSMS – Specifications.*

AS/NZS4804. (2001): *OHSMS- Guidelines for SMSs.*

BS OHSAS 18001. (2006): *OHSMS.*

CSB – Kelly Keim. (2012): Vice-Chair API RP-754 Drafting Committee- *Process Safety Performance Indicators for the Refining & Petrochemical Industries* http://www.csb.gov/UserFiles/file/Keim%20(API)%20-%20PowerPoint%20-%20printed.pdf

Dupont. (2105): *Process Safety Management Systems*. http://www.dupont.com/products-and-services/consulting-services-process-technologies/brands/sustainable-solutions/sub-brands/operational-risk-management/products/process-safety-operational-risk-consulting.html.

Energy Institute. (2015): *Process Safety Framework*. https://www.energyinst.org/technical/PSM/psm_guidelines.

Heinrich, H.W., Petersen, D. & Roos, N. (1980): *Industrial accident prevention*. New York, McGraw-Hill.

Hopkins, A. (2011): *'Management walk-arounds: Lessons from the Gulf of Mexico oil well blowout'*, Safety Science, vol. 49, no. 10, pp. 1421-1425.

IChemE. (2013): Process Safety Versus Personal Safety, on-line webinar http://www.icheme.org/events/events/2013/safety-webinar-pilkington-20-september.aspx#.VSxgCMsfo3E.

ISO/CD 45001. (2014): *Occupational health and safety management systems – Specification.*

JCEC. (2014): *Human & Organisational Factors Process Safety The Top Ten Issues,* Joint Chemical Engineering Ctee Seminar Brisbane 2September 2014,

Kamrath, D.J. (2014): *Engaging Senior Management In Process Safety A Case History, AIChE, 10th Global Conference Process Safety.* http://www.aiche.org/academy/videos/conference-presentations/engaging-senior-management-process-safety-case-history

NSW Department of Infrastructure, Planning and Natural Resources. (2004): (Consultation Draft) Major Industrial Hazards Advisory Paper No. 4 – *Safety Management Systems*.

Manuele, F. A. (2011): *Reviewing Heinrich: Dislodging two myths from the practice of safety.* Professional Safety, **Oct**, 52-61.

NSW Department of Planning. (2011): HIPAP 9: *Safety Management.*

Safe Work Australia. (2012): *Guide for MHF Major Hazard Facilities Safety Management Systems SMS.*

UK HSE. (1998): HSG65, *Successful Health and Safety Management.*

UK HSE. (1999): HSG48, *Reducing Error and Influencing Behaviour.*

US Department of Labour. (2000): OSHA 3132/3133, *Process Safety Management,* https://www.osha.gov/ *Publications/osha3132.pdf.*

US Department of Labour, OSHA CFR Part 1910- *Occupational Safety and Health Standards § 1910.109 Explosives and Blasting Agents.* https://www.osha.gov/pls/oshaweb/owasrch.search_form?p_doc_type=STANDARDS&p_toc_level=1&p_keyvalue=1910.

US Department of Labour, OSHA Standard CFR 29 1910.119, *Process Safety Management* of Highly Hazardous Chemicals. https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9760.

Victorian WorkSafe. (2011): Guidance Note - *Safety Management Systems for MHF Major Hazard Facilities*.

Appendix 1 Glossary

ALARP: As Low As Reasonably Practicable. A risk tolerance criterion defined by many international safety regulators. One example is shown in NOPSEMA (2014).

Cause of an Incident or Risk: Anything that, if better managed, would reduce the likelihood and/or consequences of the incident or risk.

Causal Factors of an Incident: A small number of direct, proximate causes that **did** happen or exist. They are usually macro systemic or behavioural breakdowns due to not being managed effectively due to inadequate or missing risk controls (e.g., an inadequate policy or procedure; a faulty or broken equipment item; a 'nonstandard' human behaviour or action or inaction. 'Nonstandard' behaviour is often called an 'unsafe act' or 'at-risk behaviour', even though those terms are usually meaningless and undefined.

Incident: An unwanted, unplanned occurrence that did have, or could have had, an impact on achievement of a business objective.

Integrated System: A system that is a logical, structured, ordered, combination of apparently dissimilar systems into a whole entity by recognition and exploitation of similarities and commonality of methods and tools for effective management.

Major Hazard Facility (MHF): A facility at which hazardous substances (e.g. chemicals) are present or likely to be present in a quantity that exceeds a threshold quantity that is determined by the Regulator under their Regulations to be a major hazard facility.

Major Incident Hazard: A hazard that could cause, or contribute to causing, a major incident or occurrence.

Major Incident at a Major Hazard Facility: An occurrence that results from an uncontrolled event(s) at the major hazard facility involving, or potentially involving, significant numbers of people being exposed to hazardous substances such as scheduled chemicals and hence exposures to a serious risk to their health and safety in terms of number of people harmed and the severity of the harm resulting from an immediate or imminent exposure to the occurrence. An occurrence at an MHF includes any of the following: an escape, spillage, leakage, release, an implosion, explosion, or fire.

Personal Safety: A label often used to refer to managing safety risks associated with frequent, and usually low severity harm to individuals.

Process: A term used broadly to include the equipment and technology needed for chemical, petrochemical and refining production, including reactors, tanks, piping, boilers, cooling towers, refrigeration systems, etc.

Process Activity: Any activity involving a highly hazardous material or substance (in USA read *chemical*) including using, storing, manufacturing, handling or moving such materials, or any combination of these activities.

Process Safety: A label used to refer to managing safety risks associated with MHF. In addition to Personal Safety risks, these facilities have actual incidents and potential risks including significant fires, explosions, poisoning, releases of toxic materials, etc. usually harming large numbers of exposed people, and broad very serious impacts on the environment, the proximal community and the assets, business continuity, and economic wellbeing of an enterprise. The risks are usually regarded as major because they are often high severity, low likelihood risks associated with processes that could involve loss of control or containment of chemical, and nuclear or biological materials.

Process Safety Management (PSM): A set of management principles and tools focused on preventing loss of control or release from containment of any substance defined as a 'highly hazardous material or 'substance (in USA, EPA and OSHA read *chemical*). PSM refers to a set of inter-related approaches to manage exposure to hazards associated with the process industries and is intended to reduce the frequency and severity of incidents resulting from releases of chemicals and other energy sources.

Risk: A potentially positive opportunity or negative threat – more commonly negative – that could impact on achievement of a business objective often expressed as
R = L * C, where:
* means R has 2 compounded or separate components
R = The Risk of C due to an Exposure Scenario E;
C = a chosen consequence / impact of interest or concern due to exposure E to the opportunity or threat; and
L = the likelihood of an exposure scenario E of all the events and circumstances that could credibly lead to that consequence.

Risk Factors: The same as Causal Factors but COULD happen or exist rather than DID happen or exist.

Root Causes of a Causal Factor or Risk Factor: A larger number of indirect, underlying, more fundamental causes that are usually micro, deeper causes of inadequate or missing risk controls (e.g., inadequate policy/procedure or its enforcement or its implementation process, incomplete maintenance, unskilled/incompetent operators, inconsistent or missing supervision, underlying psychological reasons for behavioural choices).

Appendix 2 API Categorisation of Process Safety Incidents by Severity of Consequences

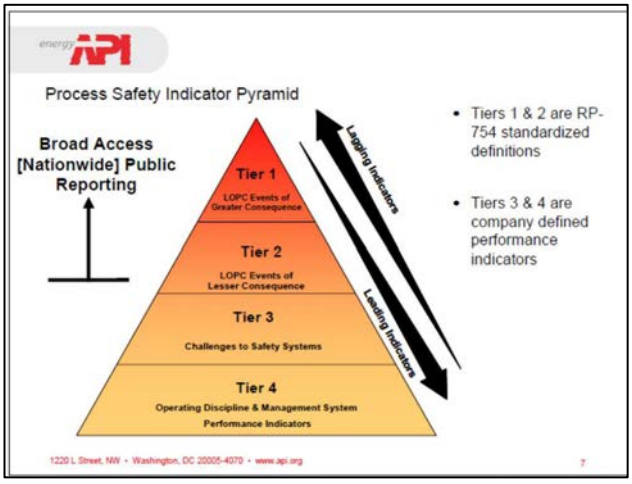
Process Safety Incidents have the:

- Highest potential for multiple injuries/deaths
- Highest potential for significant environmental harm
- Highest potential for significant property damage
- Highest potential for significant business interruption
- Highest potential for damage to reputation

API Process Safety Indicator Pyramid

- Tiers 1 & 2 are RP-754 standardized definitions
- Tiers 3 & 4 are company defined performance indicators

Tier 1 LOPC Events of Greater Consequence
Tier 2 LOPC Events of Lesser Consequence
Tier 3 Challenges to safety System
Tier 4 Operating Discipline & Management System Performance Indicators



The Leading/Lagging labels in the graphic model are misleading because some of the tiers are incidents and some are risks.

Tiers 1 & 2 -- Process Safety Event PSE

- An unplanned or uncontrolled release of any material, including non- toxic and non-flammable materials from a process that results in one or more of the consequences listed below:
  - Harm to people;
  - Impact upon the community;
  - Damage to equipment; or
  - A release of a threshold quantity.
- PSE Rate = (Total PSE Count/Total Work Hours) x 200,000 hours

Tier 3 – Challenge to Safety Systems

- *Purpose:*
  - Typically represent challenges to the barrier system that escalated or progressed along the path to harm, but were stopped short of a Tier 1 or Tier 2 PSE consequence
- *Examples:*
  - Safe Operating Limit Excursions
  - Primary Containment Inspection or Testing Results Outside Acceptable Limits
  - Demands on Safety Systems
  - Other LOPC (Loss of Primary Containment) Events

Tier 4 – Operating Discipline & Management System Performance

- *Purpose*
  - Typically represent the performance of individual components of the barrier system
  - Indicative of process safety system weaknesses that may contribute to future Tier 1, 2 or 3 PSEs
- *Examples*
  - Process Safety Action Item Closure
  - Training Completed on Schedule
  - Safety Critical Equipment Inspection
  - Completion of Emergency Response Drills

Appendix 3 Comparison of the Risk Management elements of common Safety Management Systems (SMS) that cater for ALL categories of risks including Process Risks

ISO CD 45001:2014	AS/NZS 4801:2001	ANSI/ASSE Z10 - 2012
1. Scope 2. **Normative References** 3. **Terms and Definitions** **4. Context of the organization** 4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the OH&S management system 4.4 OH&S management system **5. Leadership** 5.1 Leadership and commitment 5.2 Policy 5.3 Organisational roles, responsibilities, accountabilities and authorities **6. Planning** 6.1 Actions to address risk and opportunities 6.2 OH&S objectives and planning to achieve them **7. Support** 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Information, communication, participation and consultation 7.5 Documented information **8. Operations** 8.1 **Operational planning and control** 8.2 Management of change 8.3 Outsourcing 8.4 Procurement 8.5 Contractors 8.6 Emergency preparedness and response **9. Performance evaluation** 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review **10. Improvement** 10.1 Incident, nonconformity and corrective action 10.2 Continual improvement **Annex A (informative) - Guidance on the use of this Standard**	**4.1 General requirements** **4.2 OHS policy** **4.3 Planning** 4.3.1 Identification of hazards, hazard/risk assessment and control of hazards/risks 4.3.2 Legal and other requirements 4.3.3 Objectives and targets 4.3.4 OHS management plans **4.4.1 Structure and responsibility** **4.4.1.1** Resources **4.4.1.2** Responsibility and accountability **4.4.2** Training and competency **4.4.3** Consultation, communication and reporting **4.4.4** Documentation **4.4.5** Document and data control **4.4.6 Hazard identification, hazard/risk assessment and control of hazards/risks** **4.4.7** Emergency preparedness and response **4.5.1 Monitoring and measurement** **4.5.1.2** Health surveillance **4.5.2** Incident investigation, corrective and preventive action **4.5.3** Records and records management **4.5.4** OHSMS audit **4.6 Management review**	**1. Scope, Purpose and Application** 1.1 Scope 1.2 Purpose 1.3 Application **2. Definitions** **3. Management Leadership and Employee Participation** **3** 3.1 Management Leadership 3.1.1 OHSMS 3.1.2 Policy 3.1.3 Responsibility and Authority 3.2 Employee Participation **4 Planning** 4.1 Initial and Ongoing Reviews 4.2 Assessment and Prioritization 4.3 Objective 4.4 Implementation Plans and Allocation of Resources **5 Implementation and Operation** **5.1 OHSMS Operational Elements** **5.1.1 Risk Assessment** **5.1.2 Hierarchy of Controls** **5.1.3 Design Review and Management of Change** **5.1.4 Procurement** **5.1.5 Contractors** **5.1.6 Emergency Preparedness** 5.2 Education, Training and Awareness 5.3 Communication 5.4 Document and Record Control Process **6 Evaluation and Corrective Action** 6.1 Monitoring and Measurement 6.2 Incident Investigation 6.3 Audits 6.4 Corrective and Preventive Actions 6.5 Feedback to the Planning Process **7 Management Review** 7.1 Management Review Process 7.2 Management Review Outcomes and Follow-Up **+ Guidance Appendices A → O**

Appendix 4 Comparison of the elements of an integrated SMS to illustrate coverage of ALL the Process Safety Management (PSM) components as developed by OSHA and AIChE / CCPS

ISO CD 45001	Current AIChE – CCPS - 4 pillars and 20 elements Developed from the Original OSHA PSM 14 Elements in Column 3	Original OHSA PSM 14 Key Elements
1. Scope **2. Normative References** **3. Terms and Definitions** **4. Context of the organization** 4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the OH&S management system 4.4 OH&S management system **5 Leadership** 5.1 Leadership and commitment 5.2 Policy 5.3 Organizational roles, responsibilities, accountabilities and authorities **6 Planning** 6.1 Actions to address risks and opportunities 6.2 OH&S objectives and planning to achieve them **7 Support** 7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Information, communication, participation and consultation 7.5 Documented information **8 Operations** **8.1 Operational planning & control** 8.2 Management of change 8.3 Outsourcing 8.4 Procurement 8.5 Contractors 8.6 Emergency preparedness and response **9 Performance evaluation** 9.1 Monitoring, measurement, analysis and evaluation 9.2 Internal audit 9.3 Management review **10 Improvement** 10.1 Incident, nonconformity, corrective action 10.2 Continual improvement **Annex A (informative) - Guidance on the use of this Standard**	**I Commit to Process Safety** 1 Process Safety Culture 2 Standards, Codes, Regulations, Laws 3 Process Safety Competency 4 Workforce Involvement 5 Stakeholder Outreach **II Understand Hazards & Evaluate Risks** 6 Process Knowledge Management 7 Hazard Identification and Risk Analysis **III Manage Risk** 8 Operating Procedures 9 Safe Work Practices 10 Asset Integrity and Reliability 11 Contractor Management 12 Training & Performance Assurance 13 Management of Change 14 Operational Readiness 15 Conduct of Operations 16 Emergency Management **IV Learn from Experience** 17 Incident Investigation 18 Measurement and Metrics 19 Auditing 20 Management Review and Continuous Improvement	**Employee Participation Plan** **Process safety Information** (Documentation of the process) **Process Hazard Analysis** **Operating procedures** **Operator Training** **Contractor Evaluation & Selection** **Pre-Start-Up Safety Reviews** **Mechanical Integrity Program** **High Risk Work Permitting Process** **Management of Change** **Incident Investigation** **Emergency Planning and Response** **PSM Compliance Audits** **Control of Trade Secrets**

Open questions and closed minds: mapping the gaps and divisions in the safety body of knowledge

Andrew Rae
Safety Science Innovation Lab
Griffith University
170 Kessels Rd, Nathan 4111, Queensland
d.rae@griffith.edu.au

Abstract

What do we really know about safety? The volume of critique directed at current safety practice, and the academic disagreements about epistemology and research methods suggest a lack of consensus about what safety is, how safety can be investigated, and how safety can be achieved. Further, recruitment advertisements, education programs and accreditation schemes show no clear industry position on the level or type of education a safety practitioner needs. This paper suggests that divisions between safety practice and research communities can be explained by different answers to the primary research question "Why do accidents happen?" The paper explores how these answers manifest as distinct schools of thought which use a common language to conceal fundamental differences in the understanding and practice of safety.

Keywords: Safety education, Epistemology, Safety Terminology

1 Introduction

Central to every academic discipline are one or more big questions. Chemistry asks "What is matter?" Physics asks "Why does the natural world behave as it does?" Safety Science also has such a question: "Why do accidents happen?" Unlike physics and chemistry, however, new answers to the primary question of safety science seldom fully replace older answers. Whilst the solid ball atomic model of Democritus gave way to the "Plum Pudding" model of Thomson, then the nucleus model of Rutherford, the orbital model of Bohr, the shell model of Langmuir and then a sequence of progressively detailed quantum-mechanical models, new ideas in safety do not fully displace existing answers to the central question. Safety Science has experienced neither the slow march of "normal science" nor the "paradigm shifts" described by Kuhn in his "Structure of Scientific Revolutions" (Kuhn, 1996).

Copyright © 2015, Australian Computer Society, Inc. This paper appeared at the Australian System Safety Conference, Australia. (ASSC 2015), Brisbane 27-29 May 2015. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 169. Ed. Tony Cant. Reproduction for academic, not-for-profit purposes permitted provided this text is included

This is not to say that progress in safety has halted. Rather, whilst many subfields of safety have developed through the refinement of models, and replacing discredited ideas with new understanding, progress on the primary question of "Why do accidents happen?" has been in the form of adding new answers without fully discarding the old ones.

My central thesis in this paper is that communities of academic safety thought and industrial safety practice cluster around different answers to the "Why do accidents happen?" question. Since innovators tend to justify their work by critiquing the old-guard, new theories about accident causation reject the relevance of existing theories without fully discrediting them. The new ideas acquire followers at the expense of the old, but even the oldest ideas in safety have modern champions.

The different safety communities use similar language, often adopting and adapting ideas from each other. However, as ideas cross the boundaries of safety paradigms they become transformed, sometimes subtly but occasionally to the point where they are used in direct opposition to their original intentions. Practitioners are usually trained within a single paradigm, and so may be unaware that there are substantial disagreements regarding the theory and practice of safety.

Concepts which are embraced across the safety world, but with marked differences in understanding between safety communities include:

- Safety culture
- Justice and accountability
- Risk assessment
- Systems approach
- Safety management systems; and
- Safety Measurement

In Section 2 of this paper I provide characterisations for eight distinct "schools of thought" in safety. In Section 3 I use three concepts – safety culture, risk assessment, and systems approach – to illustrate how common use of terms can mask significant differences in assumptions and practices. Sections 4 and 5 explore the practical implications of these differences for employment and education of safety practitioners.

2 Disagreement without Contradiction

In this section I describe eight broad answers to the question "Why Do Accidents Happen?" and link them to academic and practice communities. Whilst there may be some overlap between the answers, and occasionally

some academics and practitioners may embrace more than one answer in their work, my contention is that the different answers represent distinct schools of thought. The demarcation between the paradigms can be observed through different constructs for measuring safety, different safety practices, and intellectual communities with strong in-group identity.

None of the answers to the question are definitively wrong. Each correctly identifies a cause of accidents, in the sense that modifying the cause changes the likelihood of the effect. The schools disagree about the appropriateness and effectiveness of focussing on the particular causes.

2.1 Accidents are caused by Poor Work Habits

The "Behaviour Based Safety" approach, as exemplified by Scott Geller (2005) considers that work habits are responsible for accidents. These habits are intrinsic to individuals, and may be modified by changing the activators and consequences of specific behaviours. If individuals are conditioned to expect positive outcomes from safe behaviours, and negative outcomes from unsafe behaviours, they will follow prompts which direct them to the safe behaviours.

Behaviours can be observed (or even counted) before and after interventions, so each behavioural intervention can be tested as a workplace experiment to determine if it successfully improves individual behaviours.

The focus on individual behaviours is a development on the early idea of "accident-prone" individuals, as exemplified by Alexander (1949). This idea takes the observation that a disproportionate number of accidents occur to a sub-group of exposed populations, and concludes that individual personal attributes must be the explanation. Behaviour-based safety adds the contribution of Skinner (1965) that these personal attributes are malleable behaviours, shaped by conditioning forces that can be deliberately controlled.

2.2 Accidents are caused by Poor Collective Attitude to Safety

Another school of thought, sometimes confusingly also labelled as "Behaviour Based Safety", ascribes accidents to organisational culture. This work is exemplified by Zohar (2010), who introduced the practice of safety climate measurement (Zohar, 1980).

This school also considers that work habits are responsible for accidents, but considers these behaviours to arise from shared beliefs and values rather than individual conditioning.

Whilst this school supports some of the behaviour based practices such as workplace observations, the main focus is on shared understanding of safety rather than individual motivation.

2.3 Accidents are caused by System Designs that do not Adequately Control Hazards

"Safety engineering", as described by Möller and Hansson (2008), views accidents as arising from uncontrolled risk. This risk is attached to hazards – particular events, states or entities of concern – which must be managed. The focus on safety engineering is to identify, characterise, and manage the hazards through the design process. Safety engineering is a broad school of thought, since there is little consensus about the correct way to manage hazards (McDermid and Rae, 2012). Approaches include:

- Building "inherent safety" into systems by reducing dangerous forces and materials (Khan and Amyotte, 2002)
- Constructing and testing a "safety case" – a body of argument and evidence for the safety of the system (Kelly, 1998)
- Applying quantitative risk assessment to design systems with acceptable levels of risk (Aven, 2011)

These approaches share the underlying assumption that accidents arise from flawed designs, and that adoption of an appropriate design process will prevent accidents.

2.4 Accidents are caused by Failed Physical Components

The "Layers of Protection" or "Barrier" school of safety describes accidents as occurring due to inadequate protection against known harmful events. An accident begins with an "initiating event" which may be internal to the system (e.g. a process deviation) or external to the system (e.g. a lightning strike). Under normal circumstances, the disturbance will be accommodated and corrected. Failure of these protective mechanisms calls into play further protection, and so on until the disturbance is contained (Baram, 2010). Accidents are explained by inadequate barriers, an insufficient number of barriers, or by common causes that defeat multiple barriers (Hollnagel, 2008).

2.5 Accidents are caused by Inadequate Management Systems

"Safety Management Systems" (SMS) extend safety engineering to consider design and operational systems rather than the technical systems they produce and manage. Accidents are caused by inadequate control and feedback mechanisms within these secondary systems.

Safety Management Systems are an application of "cybernetics" (Clemson, 1991) and Total Quality Management (Feigenbaum, 1956) which recognise organisations as complex systems with interacting feedback loops.

Leveson's Systems Theoretic Accident Model and Process (STAMP) (Leveson, 2004) is an example of this approach. A STAMP model represents accidents as arising from entities failing to meet their safety requirements. Each failure is in turn explained by inadequate control and/or feedback, allowing explanations that "reach upward" through management structures.

2.6 Accidents are caused by Organisational Behaviour

The organisational school of accident causation starts with the observation that accidents are failures of intelligence – viewed with hindsight, there was a period

before the accident in which it could have been recognised and prevented. Major theories in this school include Turner's "Man Made Disasters" (Turner, 1976), Reason's "Vulnerable System Syndrome" (Reason et al., 2001) and "High Reliability Organisations" (La Porte, 1996).

These theories consider that disasters can be understood and prevented by examining how organisations make sense of information (Weick, 1993) and reach decisions (Cohen et al., 1972).

The organisational school of thought has been increasingly drawn to study the gap between work-as-imagined and work-as-conducted, leading to "Safety-II" approaches for safety management (Hollnagel, 2014). Safety-II suggests that accidents should not be seen as exceptional circumstances, but as one possible outcome from normal work. The focus of safety activities should therefore be on understanding and improving normal work rather than on preventing accidents.

2.7 Accidents are caused by Accepting Unacceptable Risk

It was William Lowrance who first suggested that "A thing is safe if its risks are judged to be acceptable" (Lowrance, 1976). Lowrance argued that safety was a value judgement, varying over time and between contexts. Accidents are manifestations of differences between risk judgements. This school of thought embraces the work of Fischhoff (1984) and Slovic (2001), studying socially constructed attitudes to risk rather than means to control risk.

The theory of risk homeostasis (Wilde, 1982), whilst not universally embraced (O'Neill and Williams, 1998) translates this school into action, suggesting the management of risk by manipulation of risk perception and acceptance.

2.8 Accidents are an Inevitable Consequence of Certain Technology

The most pessimistic school of thought suggests that safety is an unattainable social goal. This view was popularised by Charles Perrow in his book "Normal Accidents" (Perrow, 1999). Perrow links accidents to two causes – "tight coupling" and "interactive complexity" – which, according to his use of the terms, are inherent properties of particular technologies. These properties prevent sufficient operational understanding to successfully manage the safety of industries using those technologies.

Amalberti (2001) also suggests that safety is unattainable, but for a different reason. He observes that as industries reduce their accident rate, the acceptability of accidents in those industries also decreases. Further attempts to improve safety may paradoxically increase the chance of an unacceptable event by raising expectations of safety that cannot be met.

3 Separated by a Common Language

In this section I discuss several concept labels in common usage, and show how they refer to different concepts when applied by the different schools of thought.

3.1 Safety Culture

"Safety culture", the shared values and attitudes relevant for safety within an organisation, has an influence on safety. Behind this basic consensus is a wide variety of views on what culture is, and the mechanism by which it affects safety.

For Behavior-Based Safety, there is a direct path from culture to behaviour to outcomes. For the "work habits" school, culture is about the conditions, motivations and rewards that drive individual actions. It is created and adjusted by deliberate acts of management, and exists within the workforce. For the "collective attitude" school, culture is sustained by the workforce through a system of norms and values. It can be transformed over time by sustained championing of new values, but is not readily malleable.

For the "safety engineering and "barrier" schools, culture is a mediating force that drives the effectiveness of safety lifecycle activities. It is the difference between activities performed according to templates, standards and rules, and activities conducted diligently and competently, with due regard for their safety impact. Culture is partly set by the expectations and reward structures of management, partly by education and understanding, and is partly sustained by the values and norms of the workforce.

For the "Safety Management System" school, there is no distinct line between culture and process. A strong safety culture is one with competent people with appropriate authority administering properly functioning safety systems. The existence of these things is, by itself, evidence of the safety culture.

In the organisational school, safety culture is closely linked to organisational learning. Safety culture exists as a sort of collective mind, where a strong safety culture is good at collecting information about itself, and a weak safety culture is not self-aware.

For the "acceptable risk" and "inevitable consequence" schools, culture is simply an average of the individual attitudes to risk. It is subject to group effects, such as risk normalisation and amplification, and may be observed in collective decision making, but it exists within individuals.

Despite these underlying differences, when asked to describe safety culture, all of these groups are likely to give similar summaries. If pressed for a definition, they are most likely to say that culture is "the way things are done around here". These superficial similarities belie fundamental differences. Each school requires different measures of culture. For each school, different strategies for influencing safety culture will be preferred, and will be observed through different effects.

3.2 Risk Assessment

"Risk assessment" is the discipline of estimating the likelihood and consequence of undesirable events. The concept of likelihood in particular suffers from apparent clarity and actual confusion.

For the "work habits" school, likelihood is measured directly by frequency. Practitioners of behaviour-based safety seldom experience uncertainty about their own knowledge of safe and unsafe behaviours. The dependent

variable is simply the rate of these behaviours. A representative example is wearing personal protective equipment (PPE). Risk is expressed as the proportion of observations in which correct PPE is not worn.

For safety engineering, risk is a design-time prediction of future system properties. This prediction is formed by the imaginative anticipation of a set of hazards, and the detailed estimation of the likelihood and consequence of each hazard. Fault Trees are the stereotypical safety engineering risk assessment. The "barrier" school performs risk assessments with similar form, but with a different understanding of the source of risk. Risk is the likelihood and consequence of the failure of protective mechanisms.

In safety management systems, risk assessment is a process to be performed on prescribed occasions. Rather than a means to predict risk, risk assessment is itself a way of controlling risk. SMS risk assessments frequently use forms, templates and checklists.

The organisational school has an evolving attitude towards risk assessment. Turner (1976) viewed risk assessment as an organisational mindfulness exercise – an antidote to cultural blindness. Later authors such as Vaughan (1997) and Rae (2014) recognise risk assessment as a social exercise that can normalise attitudes to specific risks rather than warning of danger.

This position is even more strongly held by the "acceptable risk" school, which views risk assessment entirely as a social construction of meaning, rather than a way of objectively examining reality.

Unlike safety culture, the differences between notions of risk assessment are readily apparent. The various schools are more likely to accuse each other of "not doing risk assessment properly" or "not understanding risk assessment" rather than holding a mistaken belief that there is a shared concept.

3.3 A Systems Approach

"Systems approach", "scientific approach" and "systematic approach" are the badges that almost every new safety method uses to distinguish itself from existing methods. The labels are all supposed to convey some type of merit, but the desirability and nature of a "systems approach" differs from school to school.

Behaviour based safety envisions fixed systems of work, within which humans are unreliable components. A positivist empirical approach is used to trial methods of improving human performance (Geller, 2005).

In safety engineering, the focus is on engineered systems. Hence the alternate label for the school, "system safety". A "systems approach" to safety engineering is sometimes used to refer directly the systems engineering, but also to indicate an expanded view of what comprises "the system", including environmental, social and managerial concerns within the system under consideration.

"System safety engineering" is not to be confused with "safety system engineering", which forms part of the barrier approach to safety. A "systems" approach in the barrier school involves enforcement of constraints through technological rather than procedural barriers.

In the "safety management systems" school, a "systems approach" requires considering control and feedback mechanisms, rather than simply putting in place constraints. A "system" isn't assumed to behave correctly – it has mechanisms for detecting and correcting deviations from optimal behaviour.

A "systems approach" is less unequivocally a good thing in the "organisational" school. Mindfulness and the disciplined examination of assumptions and evidence is encouraged, but a "systems approach" also carries connotations of bureaucracy. The organisational school has also embraced complexity science, suggesting that safety emerges from system interactions which cannot be decomposed or otherwise readily analysed.

The acceptable risk school recognises broader social systems with positive and negative feedback, but places less emphasis on understanding smaller technical systems.

The idea of a systems approach to safety has acquired buzzword status, and lost much of its meaning even within each school. Whilst it is generally recognised as a positive, progressive term, it can refer to contradictory approaches to safety.

4 What is a Safety Practitioner?

The existence of multiple conflicting schools of thought in safety has disconcerting practical implications. The same job title – even the same detailed position description – can refer to vastly different skills and responsibilities.

The following person description is an amalgam of posts on seek.com.au during early 2015 for the position of "Safety Manager".

Responsibilities

- Provide guidance on workplace health and safety legislation
- Design and improve safety systems
- Plan and implement safety initiatives
- Identify and assess risks
- Respond to incidents and accidents
- Promote safety culture
- Build relationships with key stakeholders

Competencies

- Understanding of safety performance measurement
- Understanding of relevant legislation
- Written and spoken communication skills
- Analytical skills

Stripped of industry context, there is little indication whether applicants for this job should be safety engineers, behavioural safety specialists, workplace health and safety advisors, organisational psychologists, or safety systems experts. In fact, the responsibilities and competencies listed here match different posts asking for experience in each of those capacities. Each post additionally asks for experience in a relevant industry, and "suitable" (usually unspecified) tertiary education.

For someone educated or experienced in each of the different schools described in Section 2 and Section 3, the

only unambiguous responsibilities or competencies are those that refer to legislation. All of the other details call for vastly different expertise depending on the approach to safety.

"Design and improve safety systems" could mean:

- Establish a practice of behaviour observation and recording
- Implement a set of rewards and punishments
- Produce a safety case for a product or service
- Engineer electronic monitoring and alarm devices
- Write procedures for hazard identification, risk assessment etc.
- Establish a practice of routine information gathering about what works well and what doesn't work well

"Identify and assess risks" could mean:

- Observe work being conducted, and point out safety problems
- Perform statistical analysis of behavioural observations
- Apply and analyse a safety culture survey
- Lead a hazard identification workshop for a new system design
- Physically inspect plant equipment for safety problems
- Examine company procedures and point out shortfalls
- Study the organisation's approach to understanding risk, and advise senior management on how it could go wrong
- Conduct surveys and interviews to understand how the workforce and customers perceive and relate to risk

5 The Education Solution?

One way to resolve the ambiguity identified in the previous section is via education and experience. It is possible that despite the various academic schools of thought, students are provided with a common training providing consensus and shared understanding.

There is a very limited amount of research on the education of safety professionals, mostly dating from the 1990s when there was a rapid growth in the number of postgraduate safety programs (Arezes and Swuste, 2012). However, as Arezes and Swuste note, there is a large degree of diversity amongst these programs, with little consensus about the topics to be covered.

It is likely that there is even greater diversity than is immediately apparent, since topics are typically described using terms such as "risk assessment", "human factors", and "safety management" which, as described in Section 4, can conceal broad differences in content and approach.

One way to investigate this further may be to consider the publication record of those teaching each program. This would not be reliable, since a researcher could publish within a particular community, but still present a range of ideas and approaches fairly. Another approach would be to compare the program reading lists. These are usually not publicly available, and further investigation was beyond the scope of this paper.

Without this detailed information, there is a high level of ambiguity concealed in program descriptions. Are students attending different universities receiving a common grounding in safety, or being adopted into closed schools of thought? Despite the use of similar terms to describe the curriculum, the output of those who go on to postgraduate study would strongly suggest training in only one school of safety thought.

6 Implications

In 2012, Nancy Leveson published "Engineering a Safer World" (Leveson, 2011), a manifesto for a new approach to safety. In 2014 Eric Hollnagel published "Safety-I and Safety-II" (Hollnagel, 2014), calling for a paradigm shift in safety thinking, and Sidney Dekker published "Safety Differently" (Dekker, 2014) ushering in a "new era" of thinking about safety. The problem with all of these revolutions is that there is no status quo to overturn.

In fact, as shown in Table 1, every school of thought has a paper published since 1990 claiming the school to be a "new approach" to safety. There is no "old view" or "new view", but a multi-way tug of war between paradigms.

Table 1: Every school has a paper claiming it as a "new approach"

School	Reference
Work habits	Geller (2001) Behavior-based safety in industry: Realizing the large-scale potential of psychology to promote human welfare
Collective Attitude	Dejoy (2005) Behavior Change versus Culture Change: Divergent Approaches to Managing Workplace Safety
System Design	Fenelon (1994) Towards Integrated Safety Analysis and Design
Physical Components	Cant (2012) Safety Protocols: A new Safety Engineering Paradigm
Management Systems	Leveson (2004) A New Accident Model for Engineering Safer Systems
Organisational Behavior	Dekker (2014): Safety Differently: Human Factors for a New Era
Unacceptable Risk	Howell (2002) Working Near the Edge: A New Approach to Construction Safety
Inevitable Consequences	Marchi (1999) Risk Management and Governance: A Post-Normal Science Approach

Instead of an established paradigm, ready to be advanced or overthrown, safety science has clustered in entrenched schools of thought. Empirical investigation is slowly advancing understanding within each school, but appears incapable of settling debates between schools.

From a purely academic perspective, there is no problem to be solved. The answer to the question "Why do accidents happen?" does not need to be either simple or definitive, and can embrace all of the proposals. Practitioners, however, are frequently trained within a

single school, but are then exposed, defenceless, to critiques from the other schools. How is a working professional to react when faced with multiple best-selling authors, with decades of experience in both research and polemic? The only options appear to be fight, flight or surrender – adopt an entrenched position despite all arguments to the contrary, refuse to read or listen to new safety research, or switch camps and become an enthusiastic disciple of a different school.

7 References

Alexander, F., 1949. The Accident-Prone Individual. Public Health Rep. 64, 357–362.

Amalberti, R., 2001. The paradoxes of almost totally safe transportation systems. Saf. Sci. 37, 109–126.

Arezes, P.M., Swuste, P., 2012. Occupational Health and Safety post-graduation courses in Europe: A general overview. Saf. Sci. 50, 433–442. doi:10.1016/j.ssci.2011.10.003

Aven, T., 2011. Quantitative Risk Assessment: The Scientific Platform. Cambridge University Press, Cambridge; New York.

Baram, M., 2010. Preventing Accidents in Offshore Oil and Gas Operations: The US Approach and Some Contrasting Features of the Norwegian Approach.

Cant, T., Mahony, B., 2012. Safety Protocols: A New Safety Engineering Paradigm, in: Proceedings of the Australian System Safety Conference - Volume 145, ASSC '12. Australian Computer Society, Inc., Darlinghurst, Australia, Australia, pp. 35–45.

Clemson, B., 1991. Cybernetics: A New Management Tool. CRC Press.

Cohen, M.D., March, J.G., Olsen, J.P., 1972. A Garbage Can Model of Organizational Choice. Adm. Sci. Q. 17, 1–25. doi:10.2307/2392088

DeJoy, D.M., 2005. Behavior change versus culture change: Divergent approaches to managing workplace safety. Saf. Sci. 43, 105–129. doi:10.1016/j.ssci.2005.02.001

Dekker, S., 2014. Safety Differently: Human Factors for a New Era, Second Edition, 2 edition. ed. CRC Press, Boca Raton.

De Marchi, B., Ravetz, J.R., 1999. Risk management and governance:: a post-normal science approach. Futures 31, 743–757. doi:10.1016/S0016-3287(99)00030-0

Feigenbaum, A.V., 1956. Total Quality Control. Harv. Bus. Rev. 34, 93–101.

Fenelon, P., McDermid, J.A., Nicolson, M., Pumfrey, D.J., 1994. Towards Integrated Safety Analysis and Design. SIGAPP Appl Comput Rev 2, 21–32. doi:10.1145/381766.381770

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S.L., Keeney, R., 1984. Acceptable Risk. Cambridge University Press.

Geller, E.S., 2005. Behavior-Based Safety and Occupational Risk Management. Behav. Modif. 29, 539–561. doi:10.1177/0145445504273287

Hollnagel, E., 2014. Safety-I and Safety-II, New edition edition. ed. Ashgate, Farnham, Surrey, UK England ; Burlington, VT, USA.

Hollnagel, E., 2008. Risk + barriers = safety? Saf. Sci., Occupational Accident Scenarios, and Accident Analysis Papers selected from the third international conference Working on Safety (WOS2006), September 12-15th, 2006, Zeewolde, The Netherland 46, 221–229. doi:10.1016/j.ssci.2007.06.028

Howell, G.A., Ballard, G., Abdelhamid, T.S., Mitropoulos, P., 2002. Working near the edge: a new approach to construction safety. Proc. IGLC-10 Garamado Braz.

Kelly, T., 1998. Arguing Safety - A Systematic Approach to Managing Safety Cases. University of York.

Khan, F.I., Amyotte, P.R., 2002. Inherent safety in offshore oil and gas activities: a review of the present status and future directions. J. Loss Prev. Process Ind. 15, 279–289. doi:10.1016/S0950-4230(02)00009-8

Kuhn, T.S., 1996. The Structure of Scientific Revolutions, New ed of 3 Revised ed edition. ed. University of Chicago Press, Chicago, IL.

La Porte, T.R., 1996. High Reliability Organizations: Unlikely, Demanding and At Risk. J. Contingencies Crisis Manag. 4, 60.

Leveson, N., 2011. Engineering a Safer World. MIT Press.

Leveson, N., 2004. A New Accident Model for Engineering Safer Systems. Saf. Sci. 42, 237–270. doi:10.1016/S0925-7535(03)00047-X

Lowrance, W.W., 1976. Of Acceptable Risk: Science and the Determination of Safety. Kaufmann, William, Incorporated, Los Altos, Calif.

McDermid, J.A., Rae, A.J., 2012. Goal Based Safety Standards: Promises and Pitfalls. Presented at the Safety-critical Systems Symposium.

Möller, N., Hansson, S.O., 2008. Principles of engineering safety: Risk and uncertainty reduction. Reliab. Eng. Syst. Saf. 93, 798–805. doi:10.1016/j.ress.2007.03.031

O'Neill, B., Williams, A., 1998. Risk homeostasis hypothesis: a rebuttal. Inj. Prev. 4, 92–93.

Perrow, C., 1999. Normal Accidents: Living with High-Risk Technologies. Princeton University Press.

Rae, A.J., McDermid, J.A., Alexander, R.D., Nicholson, M., 2014. Probative Blindness: How Safety Activity can fail to Update Beliefs about Safety. Presented at the System Safety and Cyber Security, IET, Manchester.

Reason, J.T., Carthey, J., de Leval, M.R., 2001. Diagnosing "vulnerable system syndrome": an essential prerequisite to effective risk management. Qual. Health Care QHC 10 Suppl 2, ii21–25.

Scott Geller, E., 2001. Behavior-based safety in industry: Realizing the large-scale potential of psychology to promote human welfare. Appl. Prev. Psychol. 10, 87–105. doi:10.1017/S0962-1849(02)01002-8

Skinner, B.F., 1965. Science and Human Behaviour, New impression edition. ed. The Free Press, New York, NY.

Slovic, P., 2001. The risk game. J. Hazard. Mater. 86, 17–24. doi:10.1016/S0304-3894(01)00248-5

Turner, B.A., 1976. The Organizational and Interorganizational Development of Disasters. Adm. Sci. Q. 21, 378–397. doi:10.2307/2391850

Vaughan, D., 1997. The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA, 1 edition. ed. University Of Chicago Press, Chicago.

Weick, K.E., 1993. The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. Adm. Sci. Q. 38, 628–652. doi:10.2307/2393339

Wilde, G.J.S., 1982. The Theory of Risk Homeostasis: Implications for Safety and Health. Risk Anal. 2, 209–225. doi:10.1111/j.1539-6924.1982.tb01384.x

Zohar, D., 2010. Thirty years of safety climate research: Reflections and future directions. Accid. Anal. Prev., Safety Climate: New Developments in Conceptualization, Theory, and Research 42, 1517–1522. doi:10.1016/j.aap.2009.12.019

Zohar, D., 1980. Safety climate in industrial organizations: theoretical and applied implications. J. Appl. Psychol. 65, 96.

Unification of Safety Management: The Case to Optimise not Maximise

Peter G W Webb
BAE Systems Australia, Cairns, QLD
peter.webb@baesystems.com

Disclaimer

The views and opinions expressed in this paper are the author's own and do not necessarily reflect those of BAE Systems Australia.

Abstract

There is much interest in the benefits of Integrated Safety Management Systems. However caution is required as a "one system to fit all" approach risks either a compromise that suits no-one or a system so large and cumbersome that it is impractical to use. This paper proposes that the real issue is the level of integration.

Separate disciplines exist for System Safety and Work Health and Safety requiring distinct skills and experience. System Safety is an engineering discipline that addresses the safety of an engineered product. It considers hazards introduced by the system and generally considers impact on equipment, people and environment. Similarly, Work Health and Safety addresses the safety of a workplace. It considers impact of hazards on people but can be extended to cover impact on the environment.

This paper applies Systems Engineering techniques and Enterprise Architecture concepts to characterise these disciplines and then identify possible levels of integration together with their interface characteristics.

The discussed levels of integration range from loose acknowledgement of shared concerns through alignment of ontologies and process interfaces, to use of common business systems.

It is proposed that integration of safety management should be optimised for the enterprise rather than unified to the maximum. This optimisation must consider the nature of the business or undertaking, the products produced and used, and the workplaces managed.

Keywords: Systems Engineering; Enterprise Architecture, Enterprise Integration, Levels of Integration, System Safety, Product Safety, Work Health and Safety (WHS), Safety Health and Environment (SHE).

1 Introduction

Expectations! Everyone expects to return home from work each day, safe and unharmed from the day's activities. Families similarly expect their loved ones to return home safe and unharmed. These daily expectations naturally extend to progressive health effects over a lifetime. Good employers have always embraced these expectations and seek to eliminate health and safety risks to their workers.

Again, everyone expects to be safe and unharmed by the activities of others and also by the goods or services that they use. As with the workplace, this includes short and long term effects.

Over many years, these expectations and consequent responsibilities have become prescribed in legislation across most jurisdictions. Even when less prescribed, these expectations and responsibilities are still implicit, for example, in cultural norms and religious doctrine.

Two inter-related disciplines have developed to address these expectations and responsibilities: Work Health and Safety (WHS) and System Safety.

The WHS discipline focuses on the safety of workers in workplaces. It addresses harm to people but can be extended to cover harm to the environment and therefore to address environmental legislation. Section 2 provides a more detailed description of the WHS discipline.

System Safety is an engineering discipline that addresses the safety of engineered products. Workers can interact with engineered products in their workplaces and in some cases the engineered product actually is the workplace, e.g. processing plants, offshore platforms, ships, trains and aircraft. The system safety discipline addresses hazards and the risk of harm from interacting with these engineered products. The discipline not only considers harm to people but also to the environment and to property. Section 3 provides a more detailed description of the System Safety discipline.

Within Australia, the Commonwealth Work Health and Safety (WHS) Act and Regulations (2011) define and set out the duties of a "Person Conducting a Business or Undertaking" (PCBU). The primary duty of care of a PCBU is to ensure the health and safety of workers and that work carried out does not put the health and safety of other persons at risk. Further duties address: management or control of workplaces; management or control of fixtures, fittings or plant at workplaces; design, manufacture, import and supply of plant, substances or structures; and the installation, construction and commissioning of plant or structures.

The 2011 WHS Act and Regulations build on previous legislation, and by expressing clear duties and penalties, have become a driving focus for enterprises. Recognising that both WHS and System Safety address hazards and risk of harm to people, there has been a drive by many enterprises to bring the two disciplines together and unify Safety Management.

Copyright © 2015, Australian Computer Society, Inc. This paper appeared at the Australian System Safety Conference, Australia. (ASSC 2015), Brisbane 27-29 May 2015. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 169. Ed. Tony Cant. Reproduction for academic, not-for-profit purposes permitted provided this text is included.

While a noble aim, any unification effort must acknowledge the different nature of the two disciplines. The purpose of such unification is to increase the efficiency and effectiveness of the enterprise in managing risks to health and safety. However, if unification compromises either discipline it risks a reduction in the efficiency and effectiveness of the overall enterprise and in the products it provides: Dilution of the WHS discipline risks compromising checks and balances that assure safety of workers; Dilution of the System Safety discipline risks compromising the safe function and performance of products, not only to people but also to the environment and to property. Note that property includes the products themselves, which impacts their fitness for service or purpose.

Clearly, the unification of Safety Management should be optimised and not maximised. This requires maximising their combined performance without compromising safety. It is achieved through optimising the integration of the two disciplines.

It is proposed that integration is best optimised by considering the enterprise in layers of abstraction and by tailoring the level of integration for each layer. Enterprise Architecture provides a framework both to divide the enterprise into layers of abstraction, simplifying analysis, and to organise WHS and System Safety architecture elements ready for the integration effort. A Systems Engineering approach is applied at each layer to progressively analyse and develop the best integrated solution.

This paper first describes the separate disciplines of WHS (section 2) and System Safety (section 3). It then introduces and describes the Enterprise Architecture framework and Systems Engineering approach to be used (section 4).

The application of the Enterprise Architecture framework and Systems Engineering to integrate WHS and System Safety is then described with examples and discussion regarding the optimum level of integration at each layer (section 5).

The paper identifies why unification of safety management must be optimised rather than maximised and shows how systems engineering analysis can be best applied to understand common ground and to achieve optimal integration.

2 Work Health & Safety

In order to integrate WHS and System Safety it is first necessary to characterise them in order to highlight commonalties and differences. This section provides a description of the WHS discipline for use in this paper.

The WHS discipline approaches risks to health and safety from an operational viewpoint by considering work activities or tasks undertaken and potential exposure to hazards. It addresses overall compliance of a business (as a PCBU) with WHS legislation. WHS directly supports the management of workers and workplaces to ensure work is undertaken safely, with adequate consultation and oversight. This requires a proactive approach to worker training, use of safe work practices and hazard risk management. The WHS function also ensures emergency preparedness and response, and that incidents are reported, investigated and notified to authorities when necessary.

The scope of WHS can be easily extended to cover harm to the environment and therefore to address compliance with environmental legislation. This is sometimes known as Safety, Health and Environment (SHE). Although related, WHS and SHE are not directly concerned with harm to property unless this introduces or increases risk of harm to workers (and for SHE, the environment).

Safe work practices are driven through use of: Plans, Procedures and Work Instructions; Safe Work Method Statements (SWMS); Job Safety (and Environment) Assessments (JSAs / JSEAs); and risk management.

Plans, Procedures and Work Instructions are used by an organisation to set out business rules, roles and responsibilities, requirements, and methods for undertaking work. These include safe work aspects.

SWMS are mandated by WHS regulations for all high risk construction work. They state the type of work, identify hazards and consequent risks; and describe control measures, and how they are to be implemented. A SWMS can be generic to a type of work and generally includes names and signatures of workers who are both consulted and engaged in the work.

JSAs / JSEAs are similar to SWMS but are not mandated by legislation. They are used where SWMS are not required, or to provide tailoring where a generic SWMS has been applied to a specific job.

For example, crane operations on a wharf are subject to Procedures and Work Instructions. A generic SWMS identifies relevant hazards, risks and controls. A JSA or JSEA considers the specific job and actual work being undertaken, e.g. who is involved, what is being lifted, where to and where from.

Key to effective WHS is therefore knowledge of hazards, understanding of consequent risk and application of necessary controls. As required by the WHS Act (2011), these controls must “eliminate risks to health and safety, So Far As Is Reasonably Practicable (SFAIRP); and if it is not reasonably practicable to eliminate risks to health and safety, to minimise those risks SFAIRP”. The WHS Act (2011), further defines what is reasonably practicable in ensuring health and safety.

3 System Safety

As stated above, integration of WHS and System Safety first requires the two disciplines to be characterised. Having addressed WHS above, this section provides a definition of the System Safety discipline, again for use in this paper.

As described by Leveson (2003) “System Safety uses systems theory and systems engineering approaches to prevent foreseeable accidents and to minimize the result of unforeseen ones. Losses in general, not just human death or injury, are considered.”

System Safety is an engineering discipline that focuses on the management of hazards associated with an engineered product and the consequent risk of harm, not only to people but also to the environment and to property. Such property includes the product itself and therefore its fitness for service or purpose. System Safety must consider: hazards introduced by the product; the

impact on the product of pre-existing hazards within its deployed environment; and, conversely, the impact of the product itself on pre-existing hazards. Consequent risks include those caused by normal operation as well as the effects of fault conditions or incidents.

For example, a ship is an engineered product that introduces hazards. It is a structure that contains plant and substances: the structure includes high platforms (in tanks, cargo holds, engine rooms and off masts) that result in personnel working at heights; plant includes pressure vessels and sources of heat, cold and kinetic energy. Some equipment radiates harmful energy (radar and radio transmitters); while substances include materials within equipment, fuel, oil, lubricants and coolants. A ship must also interact with external hazards in its environment such as high seas and strong winds or navigational hazards including rocks, reefs, floating objects (such as debris, ice) and other ships. Similarly, a ship can be a hazard to its environment (as a navigation obstruction or through collision, capsize or grounding).

Like WHS, System Safety seeks to eliminate or reduce risk of harm SFAIRP when products are used either for their intended purpose or in any reasonably foreseeable way, including disposal. Residual risks, that have been minimised SFAIRP, become part of an enduring risk baseline that must be monitored appropriately through life. Note however that what is SFAIRP for people is driven by WHS legislation, but for the environment is driven by environmental legislation and for property is driven by business demands.

System Safety is applied throughout the System Life-cycle from the initial concept and requirements phases through design, construction and verification to in service use and eventual disposal. Engineering changes impact throughout the overall life-cycle but are each subject to their own similar life-cycle. This is particularly relevant during in service use where engineering changes are initiated to address a variety of technical issues including emergent defects or deficiencies, sub-system or component obsolescence, and capability changes. Advances in technology and legislative changes can further alter what is deemed reasonably practicable to mitigate risk of harm.

These in service technical issues may introduce or impact existing risks that must be managed until eliminated or reduced SFAIRP, when they again become part of the enduring risk baseline.

System Safety seeks objective quality evidence that risks have been eliminated or reduced SFAIRP.

This evidence can be presented through safety arguments (or justifications) as part of a Safety Case. OQE may take a variety of forms including: audited plans and processes; design acceptance; surveys; quality measurements; test reports and certification. For a ship, high level certification may be provided by a Classification Society that assures compliance with rules for design, construction and ongoing maintenance.

Product Safety is an extension of System Safety to cover developed or traded products that are not only goods but also services, including Intellectual Property. The provision of services can expose an organisation's workers to hazards so there is a degree of overlap with WHS.

System Safety (or Product Safety) provides WHS with knowledge of hazards introduced or impacted by a product, which may be a workplace or in workplace. Both disciplines seek to understand consequent risk and apply necessary controls: WHS from the perspective of the worker; System Safety from the perspective of the product.

4 Enterprise Architecture & Systems Engineering

In section 1 it was proposed that integration of WHS and System Safety is best optimised by considering the enterprise in layers of abstraction and by tailoring the level of integration for each layer. It was stated that Enterprise Architecture provides a framework both to divide the enterprise into layers of abstraction that simplify analysis and to organise architecture elements for the integration effort. A Systems Engineering approach is then applied at each layer to progressively analyse and develop the best integrated solution.

This section describes the Enterprise Architecture framework concepts and Systems Engineering approach to be applied. Their application to the integration of WHS and System safety is described in section 5.

Note also that application to a complete enterprise will result in an Enterprise Architecture model that can facilitate identification of hazards and consequent risks introduced by the enterprise itself.

4.1 Enterprise Architecture

Enterprise Architecture provides an approach to understanding and optimising enterprises. It was shown by Webb (2003) that Enterprise Architecture can provide a generic framework that guides the construction of models using Systems Engineering techniques.

A framework was proposed comprising 6 layers of abstraction mapped against 6 fundamental interrogatives that support analysis of behaviour, structure and constraints (Table 1).

Interrogative	Element	Analysis
What?	Inputs / Outputs	Behaviour (Function)
How?	Functions (tasks / activities)	
When?	Sequence	
Where?	Organisational or "actor" Relationships	Structure (Form)
Who?	Organisational or "actor" Characteristics	
Why?	Requirements & Specification	Constraints (Output)

Table 1: Interrogatives & Elements & Analysis

Table 2 presents the layers of the framework. These are similar to the Zachman Enterprise Architecture Framework (ZEAF), but substitute its perspectives for abstractions that align with enterprise life-cycle phases from ISO15704 (1999) and pre EN ISO 19439 (2002).

While the 6 ZEAF perspectives and 6 layers of abstraction overlap, only 4 are equivalent. Two layers of abstraction are added above the ZEAF perspectives to

align with Needs / Domain Identification and Concept Definition phases. The bottom two ZEAF perspectives are omitted from the abstractions as they address views of the Build layer rather than further systems engineering detail.

Layer of Abstraction	ZEAF Perspective	Life-cycle Phase *(ISO 15704 / EN 19473)*	
Strategic (Capability)	-	Needs *(Domain Identification)*	
Operational (Assets)	-	Concept *Definition*	
Tactical (System Context)	Scope (ZEAF top layer)	Requirements *Definition*	
Operating Intent (System Concept)	Enterprise Model	*Preliminary* Design	Design *Specif-ication*
Design (Logical)	System Model (Logical)	*Detailed* Design	
Build (Physical)	Technology Model (Physical)	Construction & Commissioning *(Implementation Description)*	
-	Detailed Representations (Out of Context)	In Service Use	
-	Functioning Enterprise		

Table 2: Layers of Abstraction

4.2 Systems Engineering

An enterprise is effectively a complex system that can be analysed using Systems Engineering techniques.

As described above, Enterprise Architecture provides a framework for dividing the enterprise into analysable layers and for organising architecture elements ready for the integration effort. Systems Engineering is applied at each layer to progressively analyse and develop the optimum integration solution for WHS and System Safety. In this way, the level of integration can be tailored by layer.

Systems Engineering is described by the International Council on Systems Engineering (INCOSE) (see references) as "an engineering discipline whose responsibility is creating and executing an interdisciplinary process to ensure customer and stakeholders' needs are satisfied in a high quality, trustworthy, cost efficient and schedule compliant manner throughout a system's entire life-cycle."

It is further suggested by INCOSE (see references) that the "Systems Engineering process usually comprises the following seven tasks, summarised by the acronym SIMILAR:

1. State the problem;
2. Investigate alternatives;
3. Model the system;
4. Integrate;
5. Launch the system;
6. Assess performance; and
7. Re-evaluate (following each task)."

In effect, Systems Engineering applies a classic problem solving approach to the creation of systems. A Systems Engineering core process, described by Oliver, Kelliher & Keegan (1997) and adapted by Webb (2003), is shown in Figure 1.

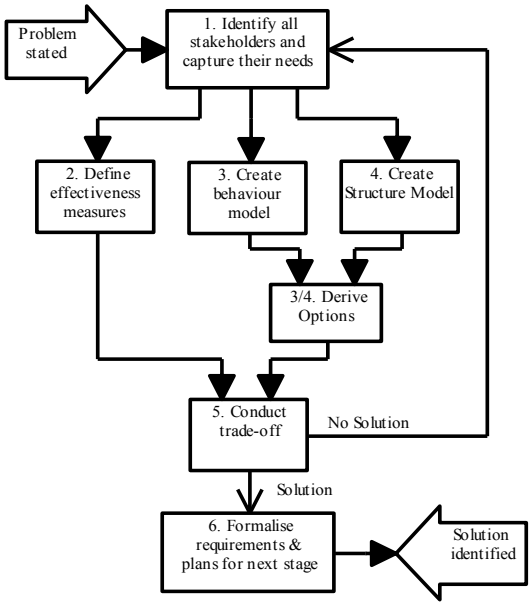


Figure 1: Systems Engineering Core Process

4.3 Applying Systems Engineering to Enterprise Architecture

The Systems Engineering Core Process is applied sequentially to each layer to generate a complete Enterprise Architecture model. As shown in figure 2, this analysis activity ideally works down from the most abstracted layer, each defining context and providing input data for the next. The Systems Engineering activity within each layer defines functions, responsibilities and interfaces. Iteration is undertaken as necessary to correct emergent issues and errors identified by ongoing analysis.

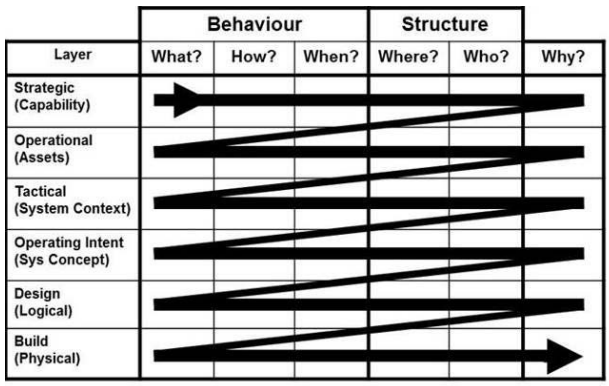


Figure 2: Core Process application to Layers

The top down approach to defining an enterprise, or complex system, matches the left side of the well-known Systems Engineering "V" diagram (shown in figure 3).

As previously stated, analysis of a complete enterprise will result in an Enterprise Architecture model. Such a model can facilitate identification of hazards and consequent risks introduced by the enterprise itself. Furthermore, maintaining this architecture model throughout the life-cycle provides a configuration baseline for analysing and understanding the safety impact of changes (Figure 3).

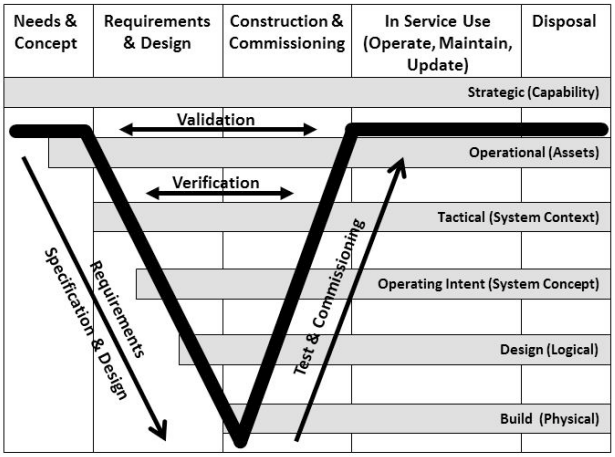


Figure 3: Layers, System Life-cycle & System 'V'

5 Layers and Levels of Integration

As stated in section 1, unification of WHS and System Safety must acknowledge the different nature of these two disciplines. Their difference is highlighted by the characterisation of WHS in section 2 and System Safety in section 3. Within section 4, an Enterprise Architecture framework is described that both divides the enterprise into layers of abstraction and organises architecture elements for the integration effort. Section 4 then outlines a Systems Engineering approach to progressively analyse and develop the optimal integrated solution, layer by layer.

This section outlines how the Enterprise Architecture framework and Systems Engineering approach are applied to integrate WHS and System Safety. It first describes integration and then provides examples and discussion of the optimum level of integration for each layer.

5.1 Integration

Integration means bringing things together so they work as a whole (INCOSE). However, this does not mean to homogenise (make uniform). Rather, integration breaks down barriers, improving communication and efficiency. It can do this in all layers of abstraction, for behaviour and for structure.

Levels of integration range from loose acknowledgement of shared concerns through alignment of ontologies and process interfaces, to use of common business systems: see table 3.

Level	Integration Description
0	Acknowledgement of shared concerns
1	Alignment of ontologies
2	Interfacing processes
3	Common information / data types
4	Shared processes
5	Common business systems / tools

Table 3: Levels of Integration

Information Science uses the term ontology to mean the formal definition of terms, their meanings and their relationships. Domains of expertise and technology, like other communities, tend to develop their own 'language' or use of terms to describe concepts. Differences can also exist between communities, within domains. Barriers to integration are formed by these differences in semantics and in meaning. This includes acronyms!

Interpretation and understanding of language are driven by culture, nurture and education. They are also impacted by management style and work location.

Different terms can be used to express the same concept. For example an event that may result in harm is variously described as:

- an "incident", WHS community;
- a "near miss", also WHS community;
- a "mishap", System Safety communities, US Department of Defence (1993), MIL-STD-882C
- an "accident", also System Safety community but from UK Ministry Of Defence (1996), DEF STAN 00-56 Part 2.

Note that the term "accident" has a different interpretation within the WHS community.

Even where the same terms are used for the same concept, actual definitions can still be confusing, e.g. a Hazard is defined as:

1. "a situation or thing that has the potential to harm a person". Australian WHS Codes of Practice (2011) and Australian Navy (2014), ABR 6303;
2. "a condition that is pre-requisite to a mishap". US Department of Defence (1993), MIL-STD-882C;
3. "a physical situation, often following from some initiating event, that can lead to an accident", UK Ministry Of Defence (1996), DEF STAN 00-56 Part 2;
4. "a source of potential harm or a situation with the potential to cause harm", Australian Navy (2003), ABR 6492.

Note that '1' refers only to a person while '2', '3' and '4' apply to people, the environment and property / equipment.

A further example of confusion in terms is the possible different interpretations of "function", "activity" and "process". For some, functions and activities are synonymous and processes are different. For others it is functions that are different while activities and processes are synonymous.

Differences in ontology lead to misunderstanding including:

- erroneous or mistaken agreement, where the same term is used by different communities for different concepts;

- erroneous or mistaken disagreement, where different terms are used by different communities for the same concept.

A key part of integration is to understand the differences between communities and domains. Differences can then be harmonised (made consistent or compatible), or at least translations agreed.

By analysing behaviour in each domain (functions, their inputs and outputs, and their sequence), Systems Engineering identifies where duplication of functions can be minimised and use of information optimised. Note that consideration of function in this context includes performance, e.g.: capacity, correctness, consistency, timeliness, accuracy, resolution and discrimination.

Similarly, by analysing structure in each domain (organisational or actor relationships and characteristics), Systems Engineering identifies where interfaces can be optimised.

5.2 Strategic (Capability) Layer

The top layer of abstraction to be considered is the "Strategic" layer. It addresses the needed capability that is satisfied by the WHS and System Safety Domains. In effect these are the expectations and responsibilities described within the introduction above.

For Safety, this layer is already well integrated: public expectations, corporate responsibilities and legislation generally align. Both WHS and System Safety reference the same WHS Act and Regulations (2011). Expectations for safety are consistent across Australian society due to a common ethical and moral framework. Corporate responsibility generally follows society's concerns and expectations.

5.3 Operational (Assets)

The "Operational" layer addresses organisational and strategic assets that satisfy needed capability. This encompasses the safety vision, mission and values of organisations forming an enterprise and their related business rules.

Example organisational assets, working together in an enterprise, include the Australian Department of Defence (DoD). Integration at this layer addresses how the DoD is structured. For the industry component it similarly addresses various companies acting as prime contractors, sub-primes and suppliers etc.

Strategic assets could include transport networks (rail, road) and utility infrastructures (power, tele-communications, water).

Single organisations such as DOD can be well integrated at this level with overarching policies and business rules imposed to address safety using a common approach. Commercial components are often less integrated since corporate policies and business rules are seen as proprietary ways of doing business and competition sensitive. Nevertheless, companies are likely to have similar approaches because they address the same requirements from the Strategic Layer above. Alliances can break down these barriers, agreeing common business rules for specific business opportunities.

5.4 Tactical (System Context)

The "Tactical" layer addresses the overall operation of organisations that make up an enterprise. It considers the corporate domains, business units and departments that exist within organisations to deliver against the policy, objectives and business rules. These generally develop around business areas and domains of expertise including WHS and Systems Safety. Other domains include Engineering, Construction, Maintenance and Operations.

It is at this layer that WHS and System Safety domains begin to diverge: WHS focusing on safety of workers in the workplace; and System Safety focusing on safety of products that are "launched" (see section 4) either as workplaces or within workplaces.

Table 3 lists indicative WHS and System Safety functions, their inputs and outputs and an indication of sequence (supporting analysis of behaviour). The life-cycle phase is used to indicate sequence in this case.

Function	Inputs & Outputs	Sequence (Phase)
Identify Hazards and Risks	In: Domain Knowledge, Design & Product Baseline. Materiel (Workplace) State Out: Identification Report & Hazard Log	Needs -> Design Build, Use
Eliminate Hazards & Risks	In: Hazard Log Out: Implemented Design Change, Hazard Log Update	Needs -> Design Build, Use
Mitigate remaining Hazards & Risks	In: Hazard Log Out: Implemented Controls, Hazard Log update, Mitigation Report	Needs -> Design Build, Use
Provide Safety Assurance	In: Certification, OQE, Hazard Log Out: Safety Case arguments	Needs -> Design Build, Use
Develop Safe Work practices	In: Domain Knowledge, Hazard Log Out: Safe Work Plans (Procedures & Instructions; SWMS; JSEAs.)	Build, Use
Inform Workers	In: Hazard Log, Safe Work Plans, Procedures & Instructions; SWMS; JSEAs. Out: Training Records; SWMS & JSEA signatures.	Build, Use
Investigate incidents (mishaps /accidents)	In: Incident details; safety data; terms of reference Out: Incident & Investigation Reports, Recommendations	Build, Use
Report incidents	In: Incident Report Out: Receipt, Investigation Requirements, Report comments	Build, Use
Identify corrective actions and improvements	In: Incident & Investigation Reports Out: Corrective Actions & Improvement Requirements	Build, Use
Implement corrective actions and improvements	In: Corrective Actions & Improvement Requirements; Certification & OQE Out: Changes; Confirmation of implementation.	Build, Use
Report Safety Metrics	In: Hazard Log, Incident Log, Investigations and Corrective Action data etc.	Design Build, Use

	Out: Management Metrics	
Provide Legislative Compliance Assurance	In: Raw metrics, Safety Case Out: Compliance Reports	Build, Use

Table 3: WHS & System Safety Functions

Within the table: "Needs -> Design" includes "Needs / Concept" and "Requirements / Design" phases (figure 3); "Build" refers to "Construction and Commissioning"; and "Use" refers to "In Service Use" (covering Operation, Maintenance and Upgrade together with "Disposal").

Significant overlap of functions can exist between WHS and System Safety. The exact allocation is driven by the nature and complexity of the workplace, by sequence and by availability of hazard log data in later phases. Table 3 presents input data to analysis and, as such, allocation between WHS and System Safety is not shown. Rather, allocation is an output of Systems Engineering analysis at this layer.

Sufficient flexibility at this Tactical layer is required to address a range of situations. Integration ensures compatibility between WHS and System Safety performing similar functions. For example, common risk assessment criteria can be agreed. However, within an enterprise WHS and System Safety may be driven to use different criteria by legitimate but divergent business or customer needs and policies. Within the enterprise, one organisation may undertake design and construction while another undertakes operation. Both organisations may undertake maintenance for the same customer, but both must also satisfy their own common reporting across other projects, using different criteria. In this case integration involves agreement on how to translate criteria and how criteria will be applied.

5.5 Operating Intent (System Concept)

The "Operating Intent" layer addresses the deployment of the Tactical functions, e.g. within Business Units as Projects. Extending the earlier example, this would include DoD System Program Offices, Navy Groups and Industry Projects.

The division of responsibility, and therefore integration, between WHS and System Safety will likely depend on the degree of engineering and complexity involved together with resource availability.

Where the workplace does not include complex engineered products, a hazard log may be generated and maintained through WHS activity. However, where workplaces comprise or include complex engineered systems then System Safety activity is needed to generate and maintain the hazard log. Updates of the Hazard Log will be required during design, build and use to reflect engineering changes and the discovery of previously unidentified hazards or risks. These updates will impact safe work plans and technical documentation (e.g. safety warnings in handbooks).

The Operating Intent defines specific business rules that tailor tactical functions in Table 3 to a particular business or project undertaken by the enterprise. In Systems Engineering terms this is the System Concept.

5.6 Design (Logical)

The "Design" layer addresses the logical implementation of functions within procedures, processes and work instructions, and the allocation of roles and responsibilities within the business unit or project. Integration is highly influenced by the specific approach and nature of work undertaken. Opportunities only exist to integrate safety management functions within higher level constraints. However, commonality can also be sought between similar work areas.

5.7 Build (Physical)

The "Build" layer addresses the physical business systems (e.g. assets and tools) that enable procedures, processes and work instructions to be implemented. Within the Safety Domain this includes the actual Hazard Log as a spreadsheet or database, accessed via a network or over an intranet.

Integration can be achieved by ensuring business systems can support a range of process implementations and users. In this way, common assets/tools can be used in a range of specific applications.

6 Conclusion

This paper demonstrates that unification of Safety Management should be optimised and not maximised. Optimisation means maximising the combined performance of WHS and Systems Safety disciplines without compromising safety. It is achieved by optimising their integration. This unification of WHS and System Safety must also acknowledge the different nature of these two disciplines. Their difference is highlighted by the characterisation of WHS in section 2 and System Safety in section 3.

It is shown in section 4 that Enterprise Architecture provides a framework both to divide the enterprise into layers of abstraction that simplify analysis and to organise architecture elements for the integration effort. Section 4 also outlines how Systems Engineering can be applied at each layer to progressively analyse and develop the optimal integrated solution

Section 5 outlines how the Enterprise Architecture framework and Systems Engineering approach may be applied to integrate WHS and System Safety. It shows that the optimum level of integration varies with the layer of abstraction and with the type of business. Flexibility is needed within higher layers to enable differing application at lower layers but maintaining commonality where ever practical. Key to these efforts is understanding that domain ontologies differ and recognition that these differences may be necessary.

Therefore, integration should to be tailored to the enterprise and restricted to harmonisation (making consistent or compatible) not homogenisation (making uniform). Integration can be optimised by removing duplication between domains but allowing flexibility over which domain undertakes specific functions.

7 References

Commonwealth of Australia: Work Health and Safety Act and Regulations, 2011 (Compilation 1 July 2014).

Leveson, N (2003): White Paper on Approaches to Safety Engineering, http://sunnyday.mit.edu/caib/concepts.pdf

International Council on Systems Engineering (INCOSE): Consensus of the INCOSE fellows, http://www.incose.org/practice/fellowsconsensus.aspx. Accessed 20 March 2015.

Oliver, D.W. Kelliher T.P. Keegan Jr, J.G. (1997): Engineering Complex Systems with Models and Objects.

Webb P.G.W. (2003): Combining Enterprise Architecture and Systems Engineering. CE The Vision for the Future Generation in Research and Applications: 837 – 841. Balkema.

The Open Group Architecture Framework (TOGAF), http://www.opengroup.org/togaf/ . Accessed 20 March 2015

Zachman: Zachman Enterprise Architecture Framework (ZEAF), http://www.zachman.com/ . Accessed 20 March 2015

IS0 14258 (1999). Concepts and rules for enterprise models

ISO 15704 (1999). Industrial automation systems - Requirements for Enterprise Reference Architectures and Methodologies

Commonwealth of Australia (2011): Work Health and Safety Codes of Practice, 2011.

United States Department of Defense (1993): MIL-STD-882C, System Safety Program Requirements.

United Kingdom Ministry Of Defence (1996): DEF STAN 00-56 Part 2, Safety Management Requirements for Defence Systems.

Australian Navy (2003): ABR 6492, Naval Technical Regulations Manual.

Australian Navy (2014): ABR 6303, Navy Safety Systems Manual.

Accentuate the positive…
Can positive performance indicators be used within 'process safety'?

Stephen A. Young
Victorian Institute of Occupational Safety and Health (VIOSH)
School of Health Sciences and Psychology, Faculty of Health,
Federation University Australia
PO Box 663, Ballarat 3353, Victoria, Australia

s.young@federation.edu.au

Abstract

This paper describes the development of predictive indicators for the prevention of occupational injury. It briefly reviews the literature surrounding leading and lagging indicators, before considering the impact of the 'process safety' versus 'personal safety' distinction. Using a series of vectors representing the hazard to injury pathway, hierarchy of controls efficacy, and information flow, it submits that intervention decisions made within 'process' and 'personal' safety distinctions are counterproductive for hazard mitigation. It further submits that a 'balanced scorecard' approach using both lagging and leading indicators may be more appropriate across the entire hazard vector.

Keywords: leading and lagging indicators, process and personal safety, hierarchy of controls, balanced scorecard, and information flow.

1 Introduction

Measuring occupational injury for the purposes of prevention is problematic. Analysis of past events can portend recurrences, but such analysis is often fraught with aetiological bias and attributions of blame (Lundberg, Rollenhagen and Hollnagel, 2009). The recording of historical injury data has been shown to be open to manipulation and discrepancy (Oleinick, 1993; Probst, 2008).

The Australian/New Zealand Standard 1885.1-1990 was published by Worksafe Australia in 1990, providing consistent definitions for injury recording and reporting and has not been altered for almost a quarter of a century[1] (Standards Australia, 1990). This standard prescribes 'lost-time injury' (LTI) as an applicable measurement of safety effectiveness. Accordingly, most Australasian workplaces typically use LTI as an indicator or benchmark of their safety proficiency. The fewer LTIs a company records, the safer it may claim to be. Conversely, a company with a high LTI rate compared to other companies in a similar industry may draw unfavourable attention to itself by regulatory bodies, unions, shareholders and the public.

However, the association of LTIs with remuneration, either in injury compensation levies or in bonus reward systems, has been shown to distort the accuracy of the LTI measurement. Robertson and Keeve (1983) noted, "Lost work time is a misleading indication of severity because it is strongly related to maximum compensation in a given state for certain injuries". Hopkins, (1994) related an anecdote where a container was dropped as it was lifted, without any serious injury, and was therefore ignored; yet a relatively minor injury resulted in the loss of safety awards to staff: "There is no doubt that the lifting incident was much more serious".

Flin, Mearns, O'Connor, and Bryden (2000) called for forward-looking 'leading indicators' for safety rather than the retrospective 'lagging indicators' such as the LTI. At the 1994 Worksafe Australia conference, Hopkins (1994) questioned the often-lauded, presumed link between declining lost-time injury frequency rates (LTIFR) and increasing productivity in Australian mines, demonstrating that there is no causal connection. He stated, "It is well known in the industry that some of the best LTIFR's have been achieved by strenuous efforts to keep the injured at work, on alternative duties if necessary" (Hopkins, 1994). More recently, Hopkins (2012) documented the Deepwater Horizon disaster within the context of its seven years of operation without a lost time injury. Other writers have concurred and called for a better data system to become the major driver of the prevention of death and permanent disabling injury (Hale and Hovden, 1998; Stiller, Depczynski, and Fragar, 2008). Despite these criticisms and calls for more appropriate measures, LTI and LTIFR remain the de facto standard for benchmarking safety performance at large industrial plants in Australasia and beyond.

Nevertheless, there is a need for companies to have a more predictive indicator of their likelihood of experiencing staff injuries in their respective workplaces; and of course, to have the capability to understand this likelihood in time to prevent the injuries. For most of the 20th century, Heinrich, a pioneer of industrial safety writing, was the only writer to offer any intuitive model for predicting accidents. Heinrich's 300:29:1 ratio proposed that attention to small workplace events like near-misses would ultimately prevent a serious injury or a fatality. This perceived relationship is usually represented as Heinrich's triangle. The original representation is reproduced in Figure 1.

Copyright © 2015, Australian Computer Society, Inc. This paper appeared at the Australian System Safety Conference, Australia. (ASSC 2015), Brisbane 27-29 May 2015. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 169. Ed. Tony Cant. Reproduction for academic, not-for-profit purposes permitted provided this text is included.

[1] One minor supplement was issued in 1991.

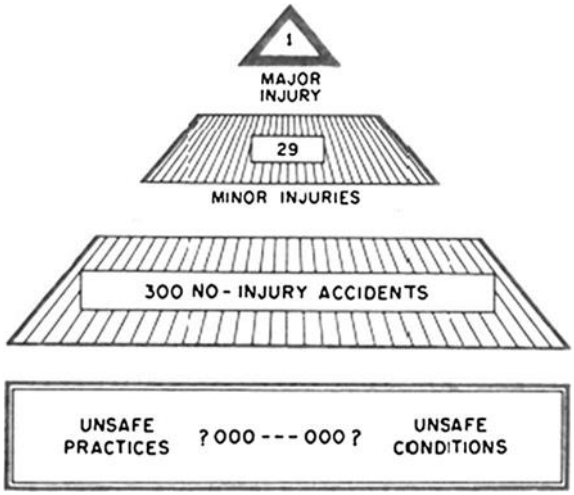


Figure 1: Heinrich's triangle (Heinrich, 1931).

While Heinrich's work is often cited in safety literature and management texts, Heinrich offered no evidence to support his ratios, and his data was never made available for examination (Manuele, 2011). Moreover, his influence grew with each edition as his claim that human error was the cause of most accidents became more assertive: "…it is apparent that man failure is the heart of the problem; equally apparent is the conclusion that methods of control must be directed toward man failure" (Heinrich, cited in Manuele, 2011).

While some of Heinrich's harshest critics have praised him for focusing industry's attention on accident prevention in general, and more specifically, on the importance of near-miss reporting (Manuele, 2011; Ojanen, Seppälä, and Aaltonen, 1988), there has been little confirmation or validation of his work. This is surprising when considering the influence that Heinrich has had on safety practitioners around the world. Many years after Heinrich commented on his methods in the preface to his second edition, "They have been proved to be sound in principle and practicable of application. That which was at one time regarded as theory is now recognized as fact" (Heinrich, 1941), researchers began to test the validity of this widely-held predictive tenet.

Salminen, Saari, Saarela, and Räsänen, (1992) used Heinrich's triangle to analyse a completely new set of accident causation data. They demonstrated differences between fatal and non-fatal accidents, both in the type of accident and the distribution of the accident causation factors examined. Their analysis of their data set therefore contradicted Heinrich's model. The American National Safety Institute's (ANSI) Z10 Safety Management Standard states that the hazards that create the potential for serious injuries and fatalities are inconsistent with those that produce minor injuries; that there is no frequency correlation between minor and serious injury causal factors; and that reducing the total number of hazards or incidents does not guarantee a reduction in serious injury risk (ANSI/AIHA, 2005).

Manuele (2011) carefully compared equivalent, but changing, quotations from Heinrich across the four editions pointing out inconsistencies and vacillation between editions. Ultimately, as well as referring to the United States' National Council on Compensation Insurance data that contradicted the 300:29:1 ratio, Manuele (2011) pointed to the absurdity of Heinrich's observation that 329 lesser events will occur prior to one major event happening. Subsequently, any relationship between the hazards and causal factors that lead to minor injury or near-misses, and those leading to serious injury, has been dismissed (Manuele, 2011; Ojanen, et al., 1988).

The measurement of safety culture has also disappointed in its ability to foreshadow inadequate safety performance. Borys (2014) has examined the diversity of definition of safety culture, and has concluded, "After close to 30 years, the body of safety culture literature is plagued by unresolved debates and definitional and modelling issues. As a result, safety culture is a confusing and ambiguous concept, and there is little evidence of a direct relationship between it and safety performance."

Over recent years however, a significant number of companies have adopted a 'balanced scorecard' approach (Kaplan and Norton, 1996) to build an ongoing composite indicator of their ability to prevent injuries. A 'balanced scorecard' application in safety management combines lagging data such as LTIs and records of near misses, with leading data such as audits, training programs, safety meetings, maintenance inspections, and close-outs of safety recommendations. These leading data are often called Positive Performance Indicators (PPIs). PPIs have been anecdotally linked to their process of continual improvement in safety performance. While requiring further research to verify the effectiveness of this approach, this linking of leading and lagging indicators to predict and thereby prevent injuries through intervention, has shown promise as an effective means for continual safety improvement. Further, an increasing body of work is currently providing encouragement for the use of PPIs as predictors for improved safety performance. Sinelnikov, Inouye, and Kerper, (2015) find that PPIs have "the potential to predict and prevent adverse outcomes by giving organizational leaders an additional set of forward-looking targets for improvement." Safe Work Australia also recommend, "…the identification and validation of effective PPIs to provide valid, reliable and relevant information about work health and safety inputs and processes for driving work health and safety strategy and practices" (Safe Work Australia, 2013). Nevertheless, the argument over whether leading or lagging indicators should be used for selection of interventions, persists across safety management.

2 'Process safety' versus 'personal safety'

The complexity of identifying predictors of occupational injury is exacerbated by a further dichotomy: a popular, and often professional, distinction between 'process safety' and 'personal safety'. Major accidents, a term generally associated with process safety and involving fire, explosion or toxic emissions are rare events and usually result in publically available investigation reports (Bellamy, 2015). The public reports lead to multiple politically-charged interpretations of what happened in the catastrophe. Perhaps as a result of this public interest and subsequent analysis, the distinction between process safety and personal safety has become more pronounced in the academic literature in recent years (Grote, 2012).

Hopkins comments on two pairs of safety indicators: personal safety versus process safety, and lead versus lag

indicators. He states "Personal safety hazards… may have little to do with the processing activity of the plant" (Hopkins, 2009). Hopkins (2002, 2008, 2012) has produced excellent work on the imprudence of assuming that low numbers of LTIs assure a low probability of a catastrophic failure. As well as clearly demonstrating in his books that analysis of relatively minor LTIs is virtually useless in predicting catastrophes, he draws on the apparent misinterpretation of the Heinrich triangle to explain why, through omission, these catastrophes may have occurred (Hopkins, 2009).

Ale (2009) cautions that since we can never be certain of their future effect, so-called leading indicators cannot normally exist. Instead, Ale (2009) explains that indicators are "proxies for the real thing". Because major explosions and other disasters are so rare, what is measured, perceived and often calculated, is process 'unsafety' or risk. Therefore he calls for indicators or signs that signal an increase in the unwanted – but nevertheless accepted – extreme values (Ale, 2009). Kjellen (2009) using the exemplary record of the Norwegian oil industry, explains the use of inspection and maintenance programs to demonstrate that lead indicators in process industries can be effectively used to prevent catastrophes.

3 Discussion

This paper asserts that 'process' and 'personal' safety are integral parts of the continuum of occupational injury analysis – from hazard to the injured (or potentially injured) party. Without a consideration of the full hazard continuum, and reconciliation of the perceived distinction between 'process' and 'personal' safety, an analysis of the optimal point (or points) of intervention is compromised.

The three-stage categorisation of occupational injury resulting from a hazard – i.e. (1) a hazard source, (2) the hazard pathway, and (3) the receiver or injured person – is acknowledged as fundamental to occupational injury intervention (Gordon, 1949; Gibson, 1961; Haddon 1970, 1973, Viner, 1991, Culvenor, 1997.) This is represented in Figure 2.

Grote (2012) argues that breaches of process safety do not necessarily cause harm to the process workers involved whereas personal safety is not necessarily directly linked to the primary work task. While these general observations may be so, this distinction, appears to ignore the universally held concept of the hazard pathway (Figure 2).

Having mapped the hazard vector, if we then relate the ubiquitous hierarchy of control[2] to the conceptual hazard/injury progression, the supposed distinction between 'process safety' and 'personal safety' becomes clear. 'Process safety' inhabits more of the hazard elimination and isolation end of the hierarchy: mitigation focuses on the hazard source and the hazard pathway proximate to the source (isolation); whereas 'personal safety' inhabits the least effective end of the hierarchy: essentially depending upon operator avoidance of the extant hazard.

Behm and Powell's (2014) study of 249 investigation reports from 7 U.S. organisations showed that 87.55% of the reports recommended administrative controls as interventions to prevent recurrence. Without reference to a 'process' versus 'personal' safety distinction, Behm and Powell, (2014) highlight the lower order 'personal safety' distinction whereby "…safety professionals may be stuck in an administrative control rut, fixated on identifying single causes close to the work organization." In apparent confirmation of criticisms of LTI and LTIFR, they comment "it may be that if organizations tend to solve OHS issues with lower-order controls they will impact frequency but not severity" (Behm and Powell, 2014).

Has the discrediting of Heinrich's triangle accentuated the distinction between 'process safety' and 'personal safety'? That is, if we cannot depend on relatively minor (recoverable) 'personal' accidents as a predictor of catastrophic accidents, has that relegated 'personal safety' into its own little discipline, and elevated 'process safety' into a position of primary importance? As identified in Figure 2, 'process safety' deals primarily with the most effective end of the hazard/pathway/receiver categorisation of occupational injury. But, notwithstanding the hierarchy of control efficacy, intervention may be effected anywhere along the hazard pathway – from source to receiver.

McDonald (1995) emphasised that rather than dwelling on personal injury, we should focus on 'damage'– thereby concentrating on the transfer of energy rather than whether or not the energy actually manifests itself in an injury. The energy transfer may damage equipment rather than a person, or there may be no damage at all. But the detection of the energy transfer without injury may well be a predictor of a serious injury (should the same transfer of energy happen again) or even a predictor of a catastrophic event involving multiple fatalities. We may style these predictors as 'near misses'.

How then, does this differ from the much-maligned Heinrich's triangle? Prompted in part by Hale's (2002, cited in Ballamy, 2015) observation that the idea of prevention of minor accidents leads to prevention of major accidents is based on careless and unsupported reasoning, Ballamy (2015) seeks to re-examine the possible relationship between seemingly insignificant 'recoverable' accidents and catastrophic accidents resulting in death. Using a large Dutch database of occupational accidents, Ballamy (2015) presents the hypothesis that a greatly narrowed base of a Heinrich-like accident triangle – so that the diagram compared like accidents with like – regardless of their severity, could be used to predict catastrophic events from seemingly minor ones. When the comparisons are made within particular hazard types, Ballamy (2015) found that there is a significant correlation between the number of non-fatally injured victims and fatally injured victims ($p < 0.0001$).

[2] There are many versions of the hierarchy of control (Barnett and Brickman, 1986; Culvenor 1997). Perhaps the most common is that which specifies 'elimination, substitution, engineering, administration, and personal protective equipment'. This paper applies the simplest, but still procedurally thorough, version of the hierarchy; namely 'eliminate, isolate, minimise'.

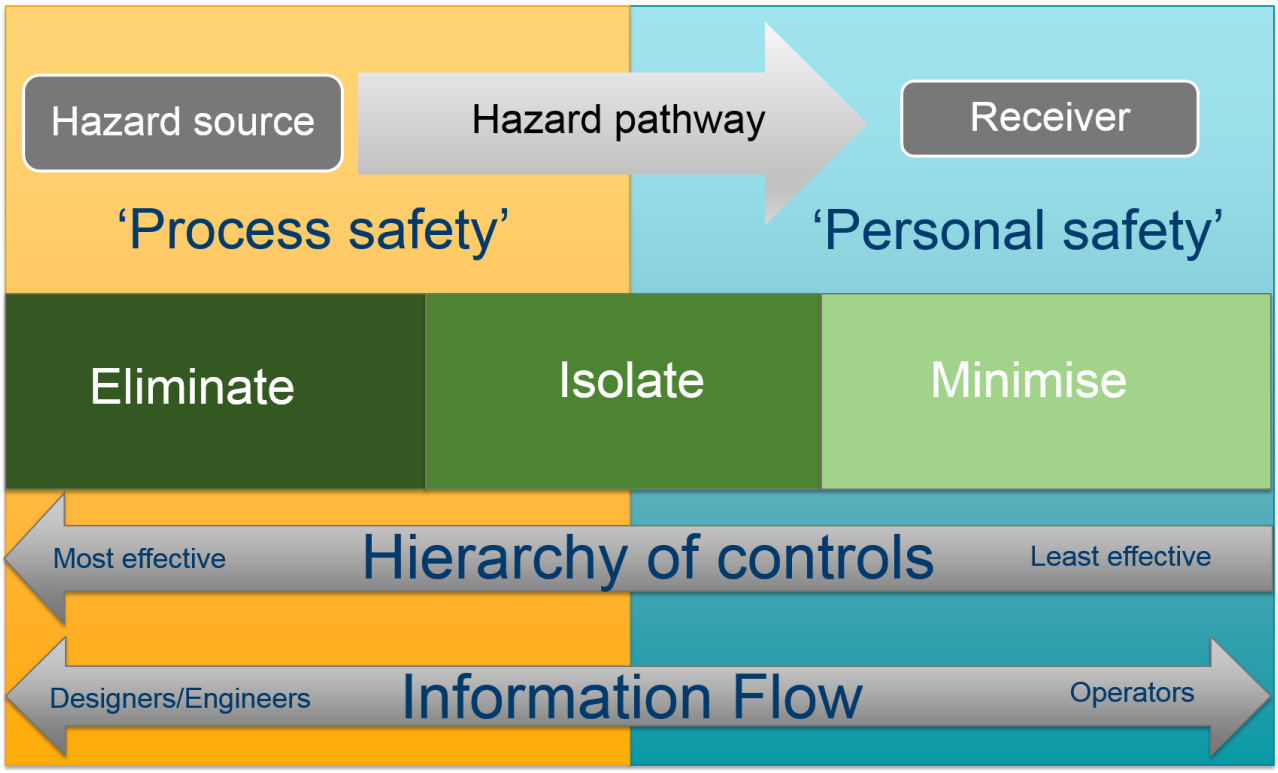


Figure 2. Relationship between hazard progression, the hierarchy of controls, 'process' and 'personal' safety, and information flow.

Hopkins (2009), in distinguishing between personal safety and process safety, stated that the distinction is really between different types of hazards. Bellamy (2015) on the other hand, shows that there is a link between occupational safety and process safety and that the link is the hazard itself. She observes that, within specific hazards, the number of rarer fatal accidents correlates with the number of non-fatal accidents – suggesting common underlying factors. The Buncefield oil storage depot (U.K.) explosion also reveals that 'occupational' accidents may 'portend' process accidents (Bellamy, 2015).

Using IDDR[3] analysis methodology, Ballamy (2015) explains that, in the Buncefield disaster, there were inadequate procedures for handling a repeating failure of the level gauge which had stuck 14 times before the explosion. It is often clear in hindsight, that, but for adequate information flow on what may have appeared as a minor event (like the sticking of a gauge), the catastrophe may not have happened.

Therefore, the third vector in Figure 2 is the flow of information – from designers and engineers to operators, and from operators to designers and engineers. Engineers and designers are often unaware of the issues of the company's operators (Skepper, Straker and Pollock, 2000). It is also reasonable to assume that operators are often unaware of the designers' or engineers' issues, since they (the designers and engineers) are usually absent when the actual work is undertaken by the operators. Organisations are found with blind spots, communication problems and conflicts, incubating accidents and ignoring their warning signs (Turner, 1978).

Behm and Powell (2014) point to the reality of most safety professionals working in the industry: "One must also consider whether safety professionals and the safety function are in a position (organizationally speaking) to realistically and effectively utilize higher order controls. Does the safety function work with the people who can implement higher-order controls (eg. engineers, architects, designers, senior-level executives, operations managers, and planners?"

All three vectors in Figure 2 transcend the 'process' versus 'personal' safety distinction. Moreover, we may deduce that any obstacle that blocks such information flow (such as an arbitrary distinction between process and personal safety) may foil a selected intervention resulting from the hierarchy of controls, and allow the hazard to proceed to an injury.

4 Conclusion

An ability to predict and therefore prevent occupational injury is the 'holy grail' of the safety profession. Debates between leading and lagging indicators, and process and personal safety, continue to fragment and distort our understanding of the energy flow resulting in injury. This paper asserts that the only way to fully understand the progression of energy resulting in injury, is through a consideration of the entire actual or potential timeline. This

[3] **I**ndication (signal) of the deviation, **D**etection of the indication, **D**iagnosis of the indication to determine what should be done about it and the **R**esponse to put it right **(IDDR)**. There are other similar analytical tools such as **F**ailure **R**eporting **A**nalysis and **C**orrective **A**ction taken **(FRACAS)** (US Department of Defence Handbook MIL-HDBK-2155, 1995).

comprehensive understanding can only be achieved by appreciation of the information flow from and towards the timeline extremes or poles. To contrive boundaries by exclusive definition such as 'process safety' and 'personal safety' compromises our ability to understand the hazard pathway, and thereby diminishes the effectiveness of intervention through the hierarchy of control. Comprehensive understanding may only be achieved through an intra-polar flow of information relevant to the existence of a hazard.

The misguided application of Heinrich's triangle may have dissuaded safety professionals from appreciating this need for full understanding of the hazard vector. Even its discrediting may have accentuated this distinction. However, Ballamy (2015) has demonstrated that, if we closely identify, and more precisely define, the appropriate hazard, relatively minor 'personal' injuries can predict similar, but more calamitous catastrophes. Balanced scorecards using leading and lagging indicators relating to both 'process safety' and 'personal safety' may provide more complete information to mitigate hazards. Further research into reporting systems using the full gamut of intra-polar information pertaining to an actual (lagging indicator) or possible (leading indicator) injury may advance our quest for the 'holy grail'.

5 References

Ale, B. (2009): More thinking about process safety indicators. *Safety Science.* 47(4):470-471.

ANSI/AIHA (2005): ANSI/AIHA Z10-2005 Occupational health and safety management systems. Fairfax, VA: American National Standard Institute/American Industrial Hygiene Association.

Ballamy, L. (2015): Exploring the relationship between major hazard, fatal and non-fatal accidents through outcomes and causes. *Safety Science* 71(0):93-103.

Behm, M and Powell, D. (2014). S. H. & E. Problem Solving: Are Higher-Order Controls Ignored? *Professional Safety* 59(2):34-40.

Borys, D. (2014): Organisational Culture. OHS Body of Knowledge.HaSPA. http://www.ohsbok.org.au%2Fwp-content%2Fuploads%2F2013%2F12%2F10.2-OrganisationalCulture.pdf&ei=ZhEBVYOrEdPo8AXz3oDIDw&usg=AFQjCNHRIkssyQsxeaRfMjQENESwtIUDNA&sig2=GqZwYbKxfMLOP_yz1_DzYA&bvm=bv.87920726,d.dGc. Accessed 2 May, 2015.

Culvenor, J. (1997): Breaking the Safety Barrier: Engineering New Paradigms in Safety Design, PhD Thesis. University of Ballarat, Ballarat.

Gibson, J. (1961): Contribution of Experimental Psychology to Formulation of the Problem of Safety. In *Behavioural Approaches to Accident Research.* Association for the Aid of Crippled Children: London.

Flin, R, Mearns, K, O'Connor, P, and Bryden, R. (2000): Measuring safety climate: identifying the common features. *Safety Science, 34*(1-3):177-192.

Gordon, J. (1949): The Epidemiology of Accidents. Proc. Public Health Education and Vital Statistics Sections of the American Public Health Association at the 76th Annual Meeting, Massachusetts, US. November 12, 1948.

Grote, G. (2012): Safety management in different high-risk domains – All the same? *Safety Science,* 50(10):1983-1992.

Haddon, W. (1970): On the escape of tigers: an ecologic note. *American journal of public health and the nation's health, 60*(12):2229-2234.

Haddon, W. (1973): Energy damage and the ten countermeasure strategies. *Journal of trauma: injury, infection, and critical care, 13*(4):321-331.

Hale, A, and Hovden, J. (1998): Management and Culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. In Anne-Marie Feyer and Ann Williamson (Eds.), *Occupational Injury: Risk, Prevention and Intervention*: Taylor and Francis.

Heinrich, H. (1931): *Industrial Accident Prevention*. New York: McGraw Hill.

Heinrich, H. (1941): *Industrial Accident Prevention*. New York: McGraw Hill.

Hopkins, A. (1994): *The Limits of Lost Time Injury Rates*. Proc. Positive Performance Indicators for OHS - beyond lost time injuries, Worksafe Australia, held on 19 May 1994 in Sydney, Australia.

Hopkins, A. (2002): *Lessons from Longford: the trial*. North Ryde, N.S.W.: CCH Australia.

Hopkins, A. (2008): *Failure to Learn: the BP Texas City Refinery Disaster*. North Ryde, N.S.W.: CCH Australia.

Hopkins, A. (2009): Thinking about process safety indicators, *Safety Science.* 47 (4):460-465.

Hopkins, A. (2012): Disastrous decisions: the human and organisational causes of the Gulf of Mexico blowout. North Ryde, N.S.W.: CCH Australia.

Kaplan, R. and Norton, D. (1996): Linking the Balanced Scorecard to Strategy. *California Management Review*, Vol.39(1):53-80.

Kjellen, U. (2009): The safety measurement problem revisited. *Safety Science*, Vol 47(4):486-489.

Lundberg, J.; Rollenhagen, C.; Hollnagel, E. (2009): What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals. *Safety Science*, Vol.47 (10):1297-1311.

McDonald, G. (1995): Focus, don't fiddle: the obscenity of the LTIFR. Geoff McDonald and Associates.

Manuele, F. (2011): Reviewing Heinrich: Dislodging Two Myths from the Practice of Safety. *Professional Safety, 56*(10):52-61.

Ojanen, K, Seppälä, A, and Aaltonen, M. (1988): Measurement methodology for the effects of accident prevention programmes. *Scandinavian journal of work, environment and health, 14.* Proc. Fourth Finnish-US joint symposium on occupational safety and Health: 95-96.

Oleinick, A. (1993): Current methods of estimating severity for occupational injuries and illnesses: Data from the 1986 Michigan comprehensive compensable

injury and illness database. *American Journal of Industrial Medicine, 23*(2):231-252.

Probst, T. (2008): Organizational injury rate underreporting: The moderating effect of organizational safety climate. *Journal of Applied Psychology, 93*(5):1147-1154.

Robertson, L and Keeve. (1983): Worker Injuries: The Effects of Workers' Compensation and OSHA Inspections. *Journal of Health Politics, Policy and Law, 8*(3): 581-597.

Safe Work Australia (2013): Issues in the measurement and reporting of work health and safety performance: a review. http://www.safeworkaustralia.gov.au/sites/SWA/about/Publications/Documents/834/Issues-Measurement-Reporting-WHS-Performance.pdf. Accessed 10 May, 2015.

Salminen, S., Saari, J., Saarela, K., and Räsänen, T. (1992): Fatal and non-fatal occupational accidents: identical versus differential causation. *Safety Science*, Vol 15(2):109-118.

Sinelnikov, S., Inouye, J., and Kerper, S. (2015): Using leading indicators to measure occupational health and safety performance. *Safety Science*, 72(0)240-248.

Skepper, N., Straker, L, and Pollock, C. (2000): A case study of the use of ergonomics information in a heavy engineering design process. *International Journal of Industrial Ergonomics,* Vol 23(3).

Standards Australia, (1990): Workplace injury and disease recording standard. http://www.safeworkaustralia.gov.au/sites/swa/about/publications/pages/ns1990injuryanddiseaserecording, Accessed 15 May, 2015.

Stiller, L., Depczynski, J., Fragar, L, and Franklin, R. (2008): An evidence-consultation base for developing child injury prevention priorities for Australian farms. *Health Promotion Journal of Australia, 19*(2):91-96.

Turner, B. (1978): Man-made Disasters. Wykeham: London.

US Department of Defence, (1995): Handbook MIL-HDBK-2155. http://everyspec.com/MIL-HDBK/MIL-HDBK-2000-2999/MIL-HDBK-2155_21714/-YG4DA&usg=AFQjCNHharE7cGItsxmJ6wEPvPOOs_DnSg&sig2=hevYJgA4COkp109uO8qdfg&bvm=bv.93756505,d.dGY. Accessed 15 May, 2015.

Viner, D. (1991), Accident analysis and risk control, Derek Viner Pty Ltd, Melbourne.