WHITE PAPER 2

Using Operational Readiness to improve the Management of Risk

Volume 1: Concepts

Produced by

The Noordwijk Risk Initiative Foundation

Published and distributed by:

The Noordwijk Risk Initiative Foundation
P.O. Box 286,
2600 AG Delft,
The Netherlands.

Email: Info@nri.eu.com
Website: www.nri.eu.com

ISBN 978-90-77284-12-4

WP2.1

Using Operational Readiness to improve the Management of Risk

Volume 1

1 December 2015

R. Frei, A. Garforth, J. Kingston and J. Pegram

on behalf of the Noordwijk Risk Initiative Foundation,
P.O. Box 286, 2600 AG Delft, The Netherlands.
www.nri.eu.com

[This page is intentionally left blank]

Preface

The NRI Foundation conserves the knowledge created by the MORT (Management Oversight and Risk Tree) programme. The programme, which ran from 1968 to 2002, built-up a wealth of material to support the management of safety, health and environmental protection in the U.S. nuclear industry. The System Safety Development Centre (SSDC) ran the programme under successive contracts for the US Government. As part of their contract, SSDC published a series of monographs; some of these dealt with operational readiness. This white paper aims to complement those monographs, referencing contemporary literature (including ISO standards), and reflecting on recent field use of the core ideas. Furthermore, two of the present authors (Frei and Kingston) have drawn on their experience of working with the staff of SSDC and, in particular, Dr Robert (Bob) Nertney—the leading figure in SSDC's work on operational readiness.

Rationale

Operational readiness and system safety[1] have common roots in the military-industrial complex of cold war America. Operational readiness also shares much of the same philosophy and knowledge base as system safety. However, in contrast to system safety, operational readiness treats safety as one aspect of system readiness to be considered alongside others. The connection between the ideas is described in Appendix 4.

In operational readiness, the staff of the SSDC saw a vehicle for communicating to decision-makers the ideas of system safety. In the late 1960s, the phrase 'operational readiness' had become a well-used term in US military culture. Adopting the phrase for safety work was partly a marketing decision, but mostly a recognition of the usefulness of the concepts. They found in operational readiness a philosophy that could be used to integrate safety into the everyday decision-making of managers.

This document is the first volume in a new series on operational readiness. It aims to fill blanks in the picture of operational readiness given in the documents published by SSDC between 1975-1992. Those documents dealt mostly with tools and techniques. More fundamentally, in the SSDC documents, operational readiness was seen through the lens of safety. In contrast, this white paper sees safety through the lens of operational readiness.

Application

Operational readiness is a philosophy that can be applied to making and keeping ready any purposeful system or activity (operation). Although safety risks are a recurrent theme, operational readiness deals with all aspects of operational performance. This volume, the first in a series, presents the concepts of operational readiness and generic processes for applying them. Later volumes will deal with topics such as operational readiness programmes, readiness review and tools.

Acknowledgements

The authors would like to thank the following people for reviewing earlier versions of this text: Gareth Broughton; Dr Mark J. Cooper, formerly of the Robens Institute, Surrey University, UK; Arthur Dijkstra, ADMC.pro; Jan Jager; Dr Floor Koornneef, Board Member NRI Foundation; Gordon Crick, HM Inspector, and Neil Rothwell, HM Principal Inspector, UK Health and Safety Executive; and, Dr Jaap v.d. Top, Dutch Safety Board.

[1] "System safety. The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system lifecycle." (US Department Of Defense, Standard Practice: System Safety, MIL-STD-882E; page 8).

[This page is intentionally left blank]

Contents

Appendices

[This page is intentionally left blank]

Using Operational Readiness to Improve the Management of Risk

1 Introduction

This volume introduces the philosophy of operational readiness and the principles by which it can be applied in the field. The main intended benefits of the approach are to:

- integrate the consideration of safety into decision-making throughout the life-cycle of an operation;
- identify operational requirements with greater certainty and efficiency;
- avoid the need for rework and retrofit of solutions; and, to
- document the basis for decisions about design and implementation.

Much of the information needed to get a system ready is to be found in the social and technical environment of the operation. The principles are set out here as a guide to acquiring this information and using it effectively. The principles are intrinsically scalable to the context in which they are applied. How critical you will find each one, how you apply them and the effort you need to invest, all depend on the context of the operation.

1.1 Definition of operational readiness

Operational readiness ensures that the right people are in the right places at the right times, working with the right hardware according to the right procedures and management controls, and are functioning in a favourable physical and psychological environment.

> **What determines what is "Right" and "Proper?"**
>
> "Rightness" in achieving operational readiness is based on two kinds of criteria:
>
> 1. Functional Criteria
>   a. The system is accomplishing its functions in an acceptable manner.
>   b. The system is operating at acceptable risk level in terms of environment, safety and health risks as well as business risks.
>
> 2. Applicable codes/standards and regulations established at all control levels inside and outside of the operating organization.
>
> (*from Nertney, 1987; p3*)

When used in a general way, the phrase 'operational readiness' can refer either to *outcomes* (i.e. achieving or maintaining a state of readiness) or to *activities*. Concerning the latter, the authors have encountered several meanings, mainly:

- to prepare and follow an operational readiness plan;
- to document, monitor and review the system and its design;

- to provide evidence of 'readiness to operate' to an operational readiness board (a committee that has the duty to ensure that all decisions have been informed adequately);
- to ensure that the system or activity is operated by competent people;
- to produce a display showing the status of operational readiness by task and task-owner.

1.2 Guiding principles

The twelve principles listed below are general rules to follow when getting a system operationally ready and to maintain readiness. These principles were identified during a project to design a generic procedure for operational readiness. This work is outlined in Appendix 2 on page 41. The authors found all twelve principles to be necessary and widely applicable, but additional principles may be needed in practice.

Dictionary definition

Principle

"A basic generalisation that is accepted as true and that can be used as a basis for reasoning or conduct."

Wordnet, Princeton University (17/5/2014)

1. The **Nertney** principle	*Treat the operational system as a whole made of four parts: people, procedures, equipment and conducive conditions.*
2. The principle of **iteration**	*Re-appraise previous choices in the light of new knowledge.*
3. The principle of **proportionality**	*Invest enough effort, neither too little nor too much.*
4. The **lifecycle** principle	*Know how the system will behave in all modes of operation and throughout the lifecycle.*
5. The **stakeholder** principle	*Engage stakeholders throughout the lifecycle.*
6. The principle of **balance**	*Consider commercial, operational and safety goals jointly, not in isolation.*
7. The principle of **clarity**	*Strive to know what the system is and what stakeholders require of it.*
8. The principle of **impermanence**	*Readiness is time-bound.*
9. The **Kletz** principle	*Conserve knowledge of the system and the logic behind decisions.*
10. The **expert** principle	*Keep subject matter experts close to the decision-making process.*
11. The **analytical** principle	*When analysis ends, all else is hunch.*
12. The **assumed risk** principle	*Accepting a risk in an operation is a deliberate, informed choice made by the right person.*

2 Twelve principles of operational readiness

This paper presents twelve general principles for delivering an operationally ready system or activity. Some, if not all, of the principles may be familiar. However, a special feature of the operational readiness philosophy is that these principles need to be considered together.

The principles were made explicit during the development of a generic procedure for operational readiness. More details are given about that in Appendix 2, on page 41. However, the principles themselves are an amalgam of the implicit knowledge of the authors and the various published sources cited in this volume.

In this paper, the words *system* and *activity* refer to the part of the operation to be made ready or reviewed. A system can be any integrated set of elements which, when operated together, achieve specific results. These elements could be hardware or human. In a similar way, an activity can be any integrated set of tasks which achieve specific results when performed in the right sequence(s). The word *process* could also be used in place of *activity*. There is no hard and fast rule about what constitutes a system, or whether 'system', 'activity' or 'process' is the better term for the part of the operation you are looking at.

The principles are laid out singly, with the emphasis on clarity of exposition. However, although distinct, each principle moderates the meaning of the others to a greater or lesser extent. Some interactions are noted in this text, but mostly you will discover them when you apply the principles in the field. What matters is that you are familiar with all the principles, and that you apply them judiciously.

The principles are presented not as a priority list, but in the best sequence for a first-time reader. This was arrived at by noting cross-references in the draft text of this volume. If the discussion of one principle mentions another, this other principle will have been introduced first.

Be aware, that the relative importance of the principles will depend on the context. A principle that seems critical in one situation may seem unimportant in another. For the same reason, it will be necessary to supplement the vocabulary, too. Each time these ideas are applied in the field, the words must be interpreted and translated to preserve their meaning.

1) The **Nertney** principle	2) The principle of **iteration**
3) The principle of **proportionality**	4) The **lifecycle** principle
5) The **stakeholder** principle	6) The principle of **balance**
7) The principle of **clarity**	8) The principle of **impermanence**
9) The **Kletz** principle	10) The **expert** principle
11) The **analytical** principle	12) The **assumed risk** principle

Table 1. List of the twelve principles (hyperlinked to the relevant sub-sections)

2.1 The Nertney[2] principle

Treat the operational system as a whole made of four parts

Nertney's principle is about building the system and keeping it operationally ready. Just as the two poles of a magnet cohere in a single whole, the principle states that operational systems have four parts that need to be treated as one unit. All four must be ready and congruent before the system can be considered as ready as a whole.

The Nertney principle combines a number of ideas:

- operational systems are built from the elements: *people*, *equipment*[3] and *procedures*;
- that these elements must operate in *conducive conditions,* conditions that allow the elements to perform as expected by the designers of the system;
- that all four parts (*elements and conditions*) must be co-ordinated throughout the lifecycle of the system.

Designers have to make assumptions about how people, equipment and procedures will perform. They also need to specify any critical conditions that need to be maintained. Designers' assumptions will have various degrees of accuracy. During the lifecycle, active monitoring may be needed to verify that the elements and conditions are (still) behaving as the designers expected. This might equate to reliability-centred maintenance for equipment, workplace monitoring of operators/work conditions and periodic review of procedures.

Dictionary definition

Congruent

"Harmoniously joined or related; agreeing; corresponding; appropriate."

The Century Dictionary and Cyclopedia, cited by Wordnik.com

The Nertney principle states the basic constraints of an operationally ready system. The system cannot be ready if any one of the four parts is unready, or if any two of the four parts are misaligned. However, to create and maintain this state of readiness you will have also to apply the other principles.

The connection between the Nertney principle and the 'Nertney Wheel' model of operational readiness is discussed in section 3.2.2, page 21.

[2] The Nertney principle is named after Dr Robert J. Nertney, a leading figure in the MORT Safety Assurance programme.

[3] Note that 'equipment' has a very broad meaning here and includes equipment, premises and any materials. In the original model (see Johnson, 1973, page 254), the terms "Plant, Hardware" was used in place of 'equipment'. This allowed the elements to be referred to as 'PPP'.

2.2 The principle of iteration

Re-appraise previous choices in the light of new knowledge

Iteration can be defined as the "process of repeating a set of instructions until a specific result is achieved." … "In design, iteration allows complex structures to be created by progressively exploring, testing, and tuning the design. The emergence of ordered complexity results from an accumulation of knowledge and experience that is then applied to the design." (Lidwell, et al., 2010, page 142).

> ***Iteration*** "The engineering design process whereby successive calculations yield successively more accurate predictions of an engineering system's behaviour. Iterations often proceed in reaction to the degree to which the latest calculation differs from the previous one, with an increment based on the difference.
>
> *Federal Judicial Center; 2000*

Iteration is normal in an operational readiness process. In the simplest case, everything is clear from the beginning and there are no surprises later. Such cases will involve little or no iteration. In other cases, important information is found as the system is defined and designed. These insights can trigger a cycle of iteration, and may sometimes require previous work to be revised fundamentally. Nonetheless, every iteration yields new insights which avoid stumbling blocks in implementation and difficulties when the system or activity goes live.

Iteration is welcome while everything is still 'on the drawing board'. However, when the system is being built (i.e. equipment bought or fabricated, people hired and trained, procedures written and management systems set-up) iteration can increase costs and create delays.

As well as defining and achieving operational readiness, the principle of iteration also applies to sustaining readiness. Johnson (1973) describes this as investing monitoring with an '*action propensity*'. He lists a number of criteria: the tendency to set up corrective feedback loops; the ability to convert evidence into specific operational responses; general acceptance and ownership by the line organisation, and; visibility.

The principle of iteration also applies to operational readiness in a more abstract way. You may be familiar with Alfred Korzybski's phrase "the map is not the territory" (Kendig, 1990, p.299). Achieving operational readiness can be described as going from the map (e.g. models and blueprints) to the territory (the actual system of people using equipment in the operational environment). Two processes are at work in the progression from map to territory: maps get worked out in increasing detail, and they get translated into different forms. The progression is something like this:

1. high level goals become increasingly detailed requirements;
2. designs and models go from rudimentary to high-fidelity;
3. implementation plans go from block schematics to actions in real time, and;
4. the system goes from partial operation to full operation.

For individuals, iteration is straightforward and commonsense. However, it is much more difficult to embed an iterative approach in the culture and resources of a collective effort.

2.3 The principle of proportionality

Invest enough effort; neither too little nor too much

It is something of a truism to say that the effort one puts into an operational readiness process should be proportionate to the benefits obtained. However, as there are many ways of measuring the benefits, it can be difficult for managers to judge how much effort is truly justified.

Whether the effort is proportionate in a specific case can be assessed in terms of general benefits (such as integrating safety, identifying requirements, avoiding rework and retrofit, and documenting the design of the system). However, how much value stakeholders place on those benefits will vary from case to case.

Effort can also be justified in terms of risk management. This may provide a workable basis for a proportionate approach so long as the preliminary risk assessment is adequate.

However, scaling by risk can be complicated by numerous factors (UKOOA, 1999). For example:

- stakeholders may have different views about what the risks are, and may disagree about the seriousness of particular risks;
- the risk may involve transfers from one party to another, or from one phase of the lifecycle (or operational mode) to another;
- the risk and its control may have large uncertainties.

Independent of risk, scaling the effort to be invested might also take account of the likely complexity of the system or its implementation, and the degree of uncertainty about best practice.

In general, the investment of effort needs to be decided in advance, rather than reactive. Discovering critical criteria late-on creates problems, e.g. unplanned costs of rework, extra trouble-shooting when operational, and restricted design options.

Part of a proactive approach is always to plan reflective STOPs in advance. While working on an operational readiness process, at certain steps or periodically (e.g. every month) you should implement a reflective stop. The purpose is to look at what you have achieved so far and what you still have to do, and to identify critical criteria. Look at the work from the ‘outside’ or from ‘above’ to get an overview picture (one can call this a ‘meta-level’ or a ‘synoptic view’). This keeps you from getting carried away when analysing, planning and designing. It is too easy to dig deeper and deeper and lose context, but it can lead to trouble like running out of time or money. Use this stop to reflect and realign the depth of analysis or work detail.

Reflective stops should include at least one of the following methods:

- SWOT analysis = strengths – weaknesses – opportunities – threats
- Preliminary Risk Analysis / Hazard analysis.

The principle of proportionality is intuitive, but one has to be vigilant to ways that it can be subverted. For example, urgency can be a legitimate reason for taking a "quick and dirty" approach to operational readiness. However, as Lidwell et al. (2010; p. 210) note, one should ensure that time limits are justified, and not determined solely by culture (e.g. hard-driving) or impulse.

The principle of proportionality applies to all other principles and will prevent you from spending too much effort, time and money, going into the wrong subjects.

2.4 The lifecycle principle

Know how the system will behave throughout its life and in all modes of operation

An operational system has a lifecycle. Operational readiness applies not only to normal operations, but to other modes and other phases in the lifecycle of the system. Looking after these 'off-normal' aspects of your system will add to its resilience.

In general, the lifecycle consists of: a conceptual phase; a design phase; a planning phase; an implementation phase; an operational phase, and; a disposal phase. These all need to be considered when defining operational readiness. This is to ensure that choices that are beneficial in one phase do not create unacceptable risks or difficulties in other phases.

The same argument applies to operational modes. An easy-to-operate machine might be very difficult to maintain, or be very unforgiving in an emergency. 'Normal operations' is just one mode of a system that occurs during in one phase of the system lifecycle. Therefore, the definition of the system needs to include all foreseeable modes of operation across the entire lifecycle. Later on, especially when assessing risks, you will also need to consider the transitions between the different modes.

The names that you use to describe modes[4] (and the lifecycle phases) depend on the context of your work. However, an illustrative list of general modes is:

- Normal mode, used for the main operational purpose;
- Maintenance mode, e.g. being cleaned, serviced or repaired;
- Amended mode, e.g. permitted deviation from normal modes;
- Abnormal mode, an unforeseen deviation from normal modes;
- Emergency Mode, e.g. emergency actions to avoid serious incidents.

[4] The Rail Safety and Standards Board, 2004, for example, defines of modes for normal and abnormal railway operations

2.5 The stakeholder principle

Engage stakeholders throughout the lifecycle

Freeman's definition

Stakeholder

"…any group or individual who can affect, or is affected by, the achievement of a corporation's purpose."

Freeman (2010; p.*vi*)

This principle applies to stakeholders as a means to readiness, but also recognises that stakeholders have their own aims. Stakeholders contribute to getting a system ready to operate and to keeping it so. However, stakeholders' purposes and expectations must themselves be respected when defining and achieving readiness.

Diversity is a defining feature of the Stakeholder principle. Stakeholders contribute to every aspect of readiness, and any given stakeholder may be interested in the system in a variety of different ways. Stakeholders include business partners, customers, neighbours, regulators, staff, and many other groups. Each stakeholder contributes a piece of the jigsaw to complete the picture of what is important, what is wanted, what will work, and what has happened before. However, stakeholders can change and so can the nature of their involvement; therefore the picture must be kept updated throughout the lifecycle.

It can be a challenge to engage stakeholders in readiness. Heidrick et al (2009) point out three reasons for this. Firstly, some potential stakeholders will be unaware of issues in which they might have an interest. Secondly, it is difficult to define stakeholders with certainty. This is because the attributes of stakeholders are perceived subjectively and opinions may differ. Thirdly, stakeholder membership can change over the lifecycle as can the interests and attributes of the stakeholders themselves.

In cases where stakeholders are already joined in a network with clear relationships, engagement is likely to be quite straightforward. However, in other cases, engaging stakeholders may be a 'messy problem' in operational readiness, and not a neat and tidy exercise using a set methodology.

2.6 The principle of balance

Consider commercial, operational and safety goals jointly, not in isolation.

An operationally-ready system is one designed and built to meet safety, operational, and commercial goals. However, because of the nature of design processes, especially those for complex systems, these goals must be kept in balance throughout the lifecycle of the system. Hence, the principle of balance applies both to the state and to the process of operational readiness.

Necessarily, the design process starts with function: with what the system or activity is meant to achieve. As soon as function is considered, the designer (see the quotation from Schön, right) also needs to be mindful of the constraints which the design must accommodate. The constraints might be time, physical in nature, or mandatory norms (such as codes, standards and regulations – CS&R) that apply to the system.

> *"Designing in its broader sense constitutes the core of practice in all professions, occupations, and everyday living. As Herbert Simon has taught us, practitioners are of necessity designers; the production of artefacts—a manager's policy, a lawyer's brief, a physician's diagnosis—is essential to their business".*
>
> *Schön (1992; p127)*

Each option for achieving a function of the system, must also be assessed for its potential to fail (Stirling, 2013). In other words, risk assessment needs to be integral to the design process. If risk assessment becomes uncoupled from the process, the design is liable to be unbalanced towards functional criteria, albeit against a back-drop of compliance with norms.

The risks entailed by a particular design option may affect operational, commercial or safety goals. Decoupled assessment can affect any of these aspects of risk. Johnson (1973) makes the point that risk reduction is most efficient when it is integrated into the lifecycle of the system. As illustrated in Figure 1, this is most effective if it enters the "process very early and in fundamental ways (AAAAA) rather than very late and in inferior ways (zz)". Although Johnson had safety in mind, there is no reason to suppose that it does not generalise to the other classes of risk.

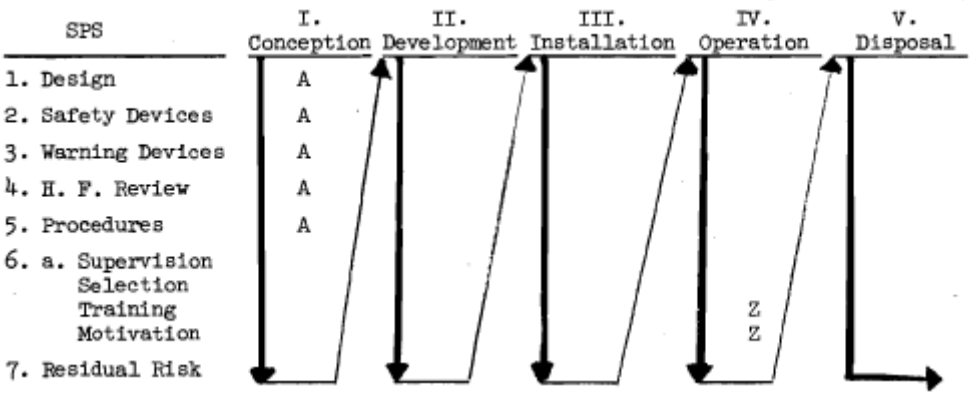


Figure 1. "Sequential Relation of the Safety Precedence Sequence"
(Reproduced from Johnson, 1973)

Finding and treating risks early allows the most effective treatment options to be found at the least cost. Like other design outcomes, safety is affected by the fact that freedom of action decreases and modification costs increase. As Johnson (1973; p.237) says, "*The conceptual phase offers the greatest opportunity for most safety at least cost.*" He continues: "*The amount of time necessary to assemble and apply …*

guidelines is likely to be less than the time spent straightening out problems resulting from unguided or unstructured acceptance efforts." (Ibid., page I-6).

The principle of balance applies not only at the conceptual phase, but throughout the system lifecycle. Although early recognition of risks, goals and constraints is ideal, some criteria will only be discovered as the process unfolds (Alexander and Bues-Dukic, 2009). Each newly discovered criterion will force some degree of rethinking the design of the system. Correspondingly, readying a system that will perform acceptably with respect to safety, operational and commercial performance is a dynamic 'balancing-act'.

In practice, the principle of balance will often have a stakeholder dimension. In the simplest case, the designer of the system is an autonomous individual, but in reality, the 'designer' is likely to be a group. Furthermore, the group will often be an alliance of stakeholders[5], rather than a team under unilateral control. Because of this, the principle of balance has procedural, relational and ethical implications for how the design process is conducted.

The principle of balance is closely connected to the principles of iteration and proportionality. The unfolding, dynamic nature of design processes means that balance is maintained iteratively[6]; that new information forces reconsideration of many of the choices already made. Ensuring that this is well-resourced is crucial; the less 'balanced' a system is, the more likely that operational trouble will follow.

2.7 The principle of clarity

Strive to know what the system is, and what stakeholders require of it.

Operational readiness depends upon accurate definition of the system or activity to be made ready. The definition needs to include interfaces with other systems or activities that might affect, or be affected.

The process of definition has several aspects. Firstly, the system can be defined by its functions—by what it does or should do. This might be a description of a service, or a product. Secondly, the system can also be defined in terms of what it should not do. This includes risks of specific types of accident or other unwanted behaviours. Thirdly, the system needs to be defined by the constraints it must obey. These constraints are the non-negotiable conditions that apply to the operation of the system that is to be made ready. These conditions can be physical, such as dimensions, or norms imposed by laws or technical standards.

[5] Different goals sometimes line-up with membership of different departments or stakeholder groups. Therefore, the principle of balance also highlights communication between stakeholders and the risks to operational readiness of silo-working (silo-working—in which a department operates in isolation from others).

[6] This iterative balance is much the same as Wiener's 'cybernetic cycle' (Wiener, 1948)

The irony of this principle is that clarity is provisional, and not absolute; it is based on the current understanding of the system. Only towards the end of a design process do designers possess the information that they really needed at the start. This is known as the 'design paradox'. As Lindahl and Tingström (2001) point out: *"When the possibility for change is at its greatest, the knowledge of how the product will turn out is at its smallest. As the knowledge of the product grows the possibilities of making changes decrease*" (*Ibid; p.13*). Figure 2 shows the relationship between the manager's/designer's freedom of action, product knowledge and modification cost.

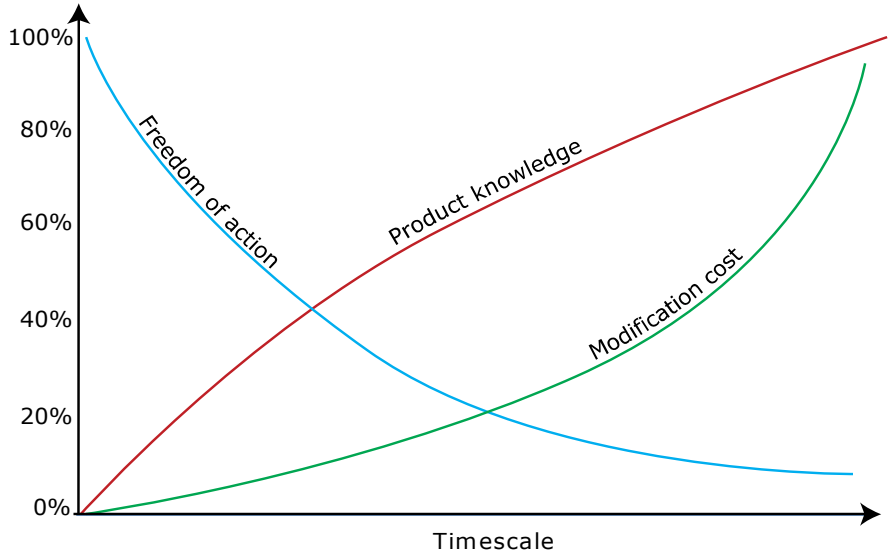


Figure 2. The design paradox (after Lindahl and Tingström, 2001)

Although the 'design paradox' cannot be wholly cheated, it can be managed by applying operational readiness principles. In their book, "Discovering Requirements", Alexander and Bues-Dukic (2009) observe that requirements work is "simple, but not easy": many different approaches need to be combined when discovering, documenting and validating requirements.

The assumption in operational readiness is that, in most, cases, a portion of the knowledge missing from the early stages might actually be available, although hard to access. A research effort to find documented knowledge is indicated here, but so is an approach that seeks to mobilise the tacit knowledge of stakeholders and experts. Although there are limits (Collins, 2001) there is usually some scope for converting tacit knowledge into explicit knowledge.

The principle of clarity is also fundamental to risk management, and can be seen in Briscoe's (1982) classic definition. Paraphrasing, Briscoe defined risk management as delivering a specified product or service:

- *to specification;*
- *on time;*
- *to budget, and;*
- *with only those undesired outputs that management have accepted.*

Applied in its most general form, the principle of clarity applies to all processes of design, management and regulation. As Ashby (1956; p219) states it, "*Before any regulation can be undertaken or even discussed, we must know what is important and what is wanted."* However, this clarity is seldom achieved at the outset, and must be managed through the lifecycle. Like the other principles, clarity is an aspiration to strive towards, rather than a criterion to be fulfilled.

2.8 The principle of impermanence

Readiness is time bound

Change is inevitable. It occurs constantly even when you do not willingly change things. Change can be influenced from the outside of your system or from within. Since there are innumerable changes all the time, a crucial part for you is to detect change and distinguish the important from the unimportant changes.

Change can come into a system as alterations to requirements, or impinge directly on the operation itself. System requirements and the specification of readiness will need to be adapted in the light of new regulations, the evolution of good practice in the industry, and changing customer expectations. Also, the goals of the operation need to be reviewed from time to time to ensure that they are aligned with the current values and policies of the business.

Dictionary definition

Impermanence

"The property of not existing for indefinitely long durations."

Wordnet, Princeton University, 2015.

Similarly, the components of the operation itself (in Nertney terms: people, equipment, procedures and conditions) have their own dynamics. For example, equipment ages and might be replaced with the latest technology, or need new maintenance arrangements to extend its life. People get older, and come and go (in staff and contractor organisations) and their successors bring into the system the norms of their generation and different standards in education and training.

As well as investing in adaptive change, applying the impermanence principle also means embracing continual improvement. According to the Chartered Quality Institute, *"Continual improvement is a type of change that is focused on increasing the effectiveness and/or efficiency of an organisation to fulfil its policy and objectives. It is not limited to quality initiatives. Improvement in business strategy, business results, customer, employee and supplier relationships can be subject to continual improvement. Put simply, it means getting better all the time". (CQI website, accessed 17 May 2014)*

2.9 The Kletz principle

Conserve knowledge of the system and the logic behind decisions

The authors named this principle after the celebrated chemical engineer, *Trevor Kletz*. His 1993 book contained the following advice:

"In every instruction, code and standard make a note of the reason why. Add accounts of accidents which would not have occurred if the instruction, code or standard had been followed."

"Never remove equipment before you know why it was installed. Never abandon a procedure before you know why it was adopted."

Kletz, T.A.
(1993; p21-22)

Trevor Kletz noted that organisations have difficulty managing their knowledge. He recognised that the reasons for decisions, such as to make a rule or a design choice, tend to get lost. Unaware of the reasoning of their predecessors, new staff may unwittingly make damaging changes or sub-optimal decisions. Acting on the Kletz principle means laying down a documentary 'audit trail' from the conceptual phase to the current state of operations.

In general, the operational phase is better documented than the work done in the earlier phases of the lifecycle. Organisations usually put effort into writing procedures that describe how to make the product or provide the service. However, operations manuals and procedures conserve only one part[7] of the knowledge needed in operational readiness work.

The Kletz principle still applies to cases in which change is decided against after due consideration. Work that doesn't progress beyond the planning stage is not wasted if the knowledge behind the decision is conserved. For example, if significant circumstances change in the future, documentation will allow the case to be reviewed quickly. Similarly, if successors spot a similar opportunity in the future, access to the archived documentation will allow them to build on the work done by their predecessors.

The Kletz principle calls attention to how organisations, businesses especially, learn how to transform themselves and to continuously improve their operations. In this respect, the principle is well aligned with Donald Schön's ideas of organisational learning and knowledge. Schön (1971) described two models: the 'classical model' and the 'learning system model'. In the *classical model*, the knowledge to be conserved is about how to make the product or provide the service. In the *learning system* model, the topic is the system as seen across its whole lifecycle. By analogy, the classical model focuses on the fruits, whereas the learning system model includes the tree and its eco-system. The Kletz principle implies that this wider perspective is necessary for achieving, and particularly for sustaining, operational readiness.

[7] As will be explained later, manuals and procures tend to conserve only the knowledge related to the interior segments of the Nertney Wheel (see Figure 6, page 22).

Applying the Kletz principle is also about building your organisation's capacity to learn from operational experiences, such as incidents and accidents. In particular, applying the Kletz principle provides one of the preconditions for what Chris Argyris termed 'double loop learning'. In Argyris' model[8,9], learning in the single loop is about fine-tuning the current operational system. In contrast, learning in the double-loop is about re-appraising the logic of the design in the light of new data, and following that through into changes to the operation. Clearly, if the logic behind design choices has not been conserved, this kind of learning is very difficult. However, applying the Kletz principle is not a complete solution to organisational learning problems; the organisation must also foster cultural conditions that support learning.

The Kletz principle also embraces the fact of change and adaptation. Readiness is a moving target that cannot be met by compliance activity alone. The readiness of the system or activity has to be managed by the organisation, and the Kletz principle is one of the rules governing this transformation.

2.10 The expert principle

Keep Subject Matter Experts close to the decision-making process

Experts bring knowledge to defining and achieving the readiness of an operation. The kind of knowledge will be highly specific to the context, and may come in many different forms. Experts can be considered as a special kind, or aspect, of stakeholders: their engagement is an issue for readiness.

How you lead the process will determine the value you get from experts. Experts "know more than they can tell" (Schön, 1992) and some portion of what they know cannot be made explicit (Polyani, 1967). You cannot simply fire questions at experts and expect their answers to deliver everything that is needed. Operational readiness needs to involve the expert in a way that allows them to apply their *implicit* knowledge, too.

The expert principle emphasises the process of decision-making. Although some decisions are very formal and deliberate, quite often decisions are implicit and embedded in the process of change itself. Even when acting as reviewers, 'little-and-often' consultations with experts can inform readiness work with valuable insights in a timely way.

When applying the expert principle, you should note that experts influence decisions in ways that do not fit perfectly with the hierarchical model represented in an organisational chart. Expert influence is more subtle than that. Rather than a convenient, 'on tap', library of objective knowledge, experts may have an active role and come

[8] For an overview and discussion, see Mark Smith (2013): "Chris Argyris: theories of action, double-loop learning and organizational learning" (accessed, 21 May 2014)

[9] For example, Argyris (1994).

with their own agenda. In some cases, experts may be members of the stakeholder groups involved in defining and achieving readiness.

The view that experts are integral to decision-making is supported by contemporary views of 'highly reliable organisations', or HROs. Weick and Sutcliffe (2007) point out that *"Rigid hierarchies have their own special vulnerability to error*" and that HROs overcome this rigidity by 'deference to expertise'.

The expert principle also applies to the social and psychological conditions of defining and achieving operational readiness. The benefits of expertise can only be fully realised in an environment that supports the open and honest expression of views. To an extent, this can be achieved in specific cases by adept chairing of meetings. It is also visible in such rules as 'deferment of judgement' in brainstorming[10]. However, as the earlier 'rigid hierarchies' remark suggests, the conditions that affect expert functioning are also culturally determined.

2.11 The analytical principle

When analysis ends, all else is hunch

The purpose of analysis is to identify issues that need to be planned for when working towards or maintaining readiness. Furthermore, analysis helps to make the readiness process methodical and rigorous. As well as searching out potential problems, analysis also provides to decision-makers some level of confidence when choosing between alternatives, accepting residual risks and giving permissions.

Dictionary definition

Analysis

"An investigation of the component parts of a whole and their relations in making up the whole."

Wordnet, Princeton University (17 May 2014)

Operational readiness work relies on analysis to a greater or lesser extent depending on the context. Activities that are very well understood, and that have known acceptable risks, may need little if any analysis. In contrast, novel operations, or even novel applications of well-established technology, may rely on analysis to discover requirements, foresee problems and identify the detailed steps needed to get the system ready to operate.

Analysts need to retain a good share of humility about their analyses. Although an analytical approach is generally helpful, and contributes to a 'duly diligent' approach, real-life will always be more complex than the models we can make of it. Furthermore, the principles of iteration and impermanence apply: analyses are approximate and provisional; they are useful, but they are not 'the truth'.

[10] For example, those stated by Stein, M (1975, p28)

Analysis happens throughout the system lifecycle. For example, not exhaustive, but in order of occurrence:

- Requirements analysis;
- Change analysis;
- Risk Analysis;
- Task analysis;
- Training needs analysis;
- Analysis of monitoring data.

Although the analytical principle is a good guide, it is possible to go too far. As discussed above (the principle of proportionality) one should avoid going into too much depth.

2.12 The assumed risk principle

Accepting a risk is a deliberate, informed choice made by the right person

Risks that have been identified and accepted correctly are called *assumed risks (*Kingston et al., 2009). These might be risks to safety, to profitability, and to the goals of the operation itself. In contrast, risks that have not been accepted correctly are called *oversights*[11] *and omissions*.[12]

In defining what this means, Johnson (1985) says: “proper evaluation of accepted or assumed risk” … “is specific, identified, analysed, quantified to the maximum practicable degree and accepted by the right level of management.”

The decision, as well as being properly informed and taken at the right level, must be taken within an appropriate system of accountability. This view of risk acceptance connects well with the idea in business ethics that accountability must be accompanied by two other attributes: duty and rationality. Taken together, accountability, duty and responsibility are sometimes called ‘the three senses of responsibility”.

To be accountable for one's actions is to behave within given constraints or beyond some minimum standard as given by law, the organisation, or society. The “right person” to make a decision about a risk is, therefore, someone accountable within the organisation and, ultimately, accountable under the law.

Duty is the reciprocal of accountability. To have a duty is to look after somebody or something; a role derived from the specific requirements placed upon the actor by higher authority. The “right person” must be able, and enabled, to recognise that the decision about the risk is one that they should take.

[11] The word ‘oversight‘ is used here in the sense of "error", "mistake", "slip", "failing to perceive".

[12] Kingston et al., 2009; *pg. xv and 56.*

However, accountability and duty both depend on the responsible party being rational, in the sense of being able to make informed decisions. A "*deliberate, informed choice*" requires the decision-maker to have competent knowledge of the relevant facts, the cognitive ability to consider all the repercussions, and the ability to act on what they know.

You might have noticed that although the foregoing talks about the "right person" and "the decision-maker": assuming risks involves others in support, supervisory or consultative roles. Hence, applying the assumed risk principle means relying upon, or creating, an organisation that can enable valid decisions.

A particular issue in operational readiness work is *risk transfer*. As the authors of UKOOA (1999; p.9) explain:

> *"Often the options open to us may reduce risk in one area of our work at the expense of some increase elsewhere in the business or lifecycle. There is a need to consider the overall risk impacts of an option on different populations and at different lifecycle phases. Care must be taken not to transfer risks to some population or organisation that does not have the freedom, skills and experience to manage these risks successfully. Decisions, significantly influenced by the risk increase to a population remote from the normally perceived boundaries of the offshore industry, may not be well received by all stakeholders."*

In reality, just as risk itself is complicated by uncertainty and subjective values, assuming risk is often complex. As Paté-Cornell (1996) observed in her classic paper on risk analysis, sound decisions about risks are a scientific and social challenge. Like the eleven others, the assumed risk principle represents an ideal to strive towards. However, just as risk analysis is not an end in itself, the assumed risk principle is a practical proposition only when your approach is informed by the other principles.

3 Application of the Principles

Operational readiness principles can be applied to a very wide range of activities and systems. However, the desire for consistent application, usual in corporate settings, may require the principles to be expressed in the form of procedures. For that reason, and also because of the advantages mentioned in Table 2, this section describes two generic processes for operational readiness. These processes can be used as the basis for writing your own operational readiness procedures.

Table 2 also lists some *disadvantages* that procedures may bring to operational readiness work. To avoid these drawbacks, any operational readiness procedure needs to be supported in the field by an operational readiness programme. An *operational readiness programme* is the name given to the whole set of activities that enable an organisation to apply operational readiness principles. The requirements for operational readiness programmes will be the subject of a separate volume of this white paper.

Advantages	Drawbacks
An operational readiness procedure may:	
• **help to bring the principles into use;** • **provide users with a structured approach;** • **provide criteria to assess use of the principles;** • **communicate criteria for assessing risks;** • **help the user better estimate the (project) management task at an early stage.**	• encourage a linear view, leading users to underestimate the role of feedback and iteration; • overemphasise what the user must do, but underemphasise the contribution of the organisation in making it work; • put the user in the role of servant to the tool (the procedure); • disconnect the user from the principles and their assumptions; • highlight only those aspects of operational readiness philosophy that are relevant to the scope of the procedure; • be simplistic or overly complex, if inflexible.

Table 2. Pros and Cons of Operational Readiness Procedures

3.1 The operational readiness cycle

In the sub-sections that follow, we will introduce two generic operational readiness processes: the 'get ready' process and the readiness review process. These processes are best imagined in the light of the *operational readiness cycle*.

A state of operational readiness requires continuous effort rather than establishment by a one-off exercise. However, this ongoing effort has a structure that is repeated from time to time: a cycle.

An operational readiness cycle begins by defining readiness and ends in a steady state operation. A cycle can be triggered by the need to ready new systems or activities, to review those that already exist, or to guide the management of change. Figure 3 represents the idea that readiness is an open-ended commitment that ends only when a system has been decommissioned. The cycle has two distinct modes: *achieving readiness* (shown as the upper arc of Figure 3) and *maintaining readiness* (the lower arc of Figure 3).

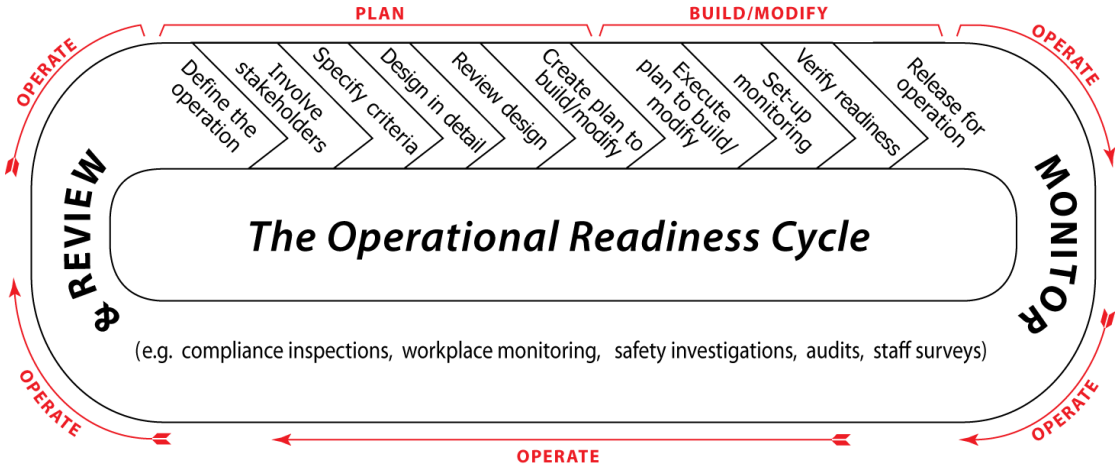


Figure 3. The Operational Readiness Cycle

Superimposed on the cycle, is *readiness review*. Readiness reviews are opportunities to improve system readiness and to find any critical requirements missing from specifications. Furthermore, readiness review is the means by which legacy systems are included in organisations that are adopting the operational readiness philosophy.

3.2 A generic process for getting a system operationally ready

The aim of an operational readiness process is to establish an operationally ready system. In an operationally ready system, the right people are in the right places at the right times, working with the right hardware according to the right procedures and management controls, and are functioning in a favourable physical and psychological environment.

The ‘get ready’ process is a sequence of broadly defined actions through which to apply the twelve principles described in the previous chapter. You should keep in mind that this sequence describes a logical progression that, in reality, will be characterised by many feedback loops. The extent to which the process is dominated by feedback depends on context. Factors such as complexity, uncertainty, alignment among stakeholders, or rather the lack of it, will all have an effect.

The ‘get ready’ process is shown in two different ways in the two subsections that follow. In the first, the process is shown as a flowchart and, in the second, it is shown as concentric circles closing in on the target of an operationally ready system.

3.2.1 The 'get ready' process represented as flowchart

Figure 4 depicts the process as flow chart in 10 steps and is laid out as a sequence of tasks to be performed. However, Figure 4 lacks all of the necessary feedback loops. (Appendix 1 contains a more detailed flowchart and shows the main feedback loops.)

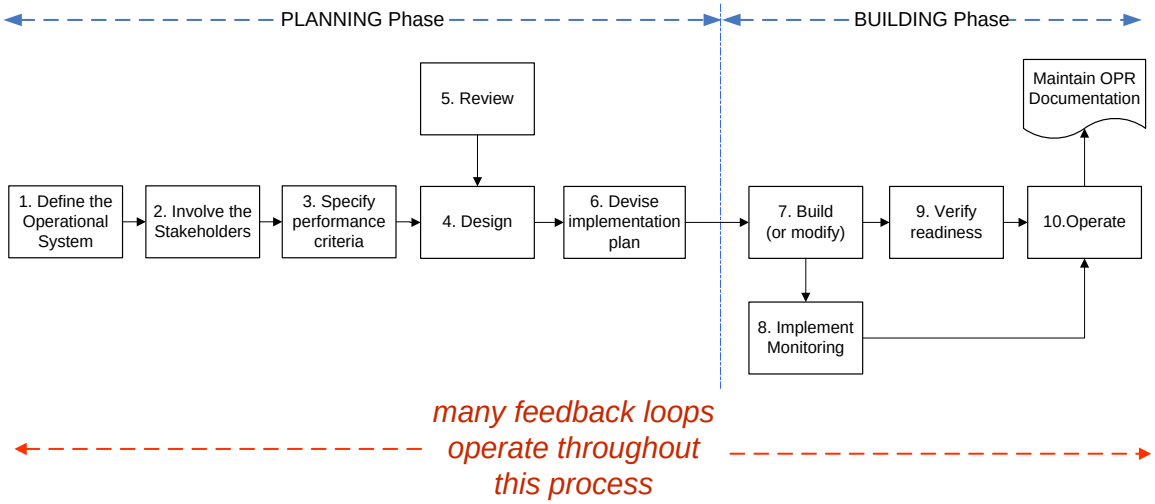


Figure 4. Generic process for operational readiness

The process is split into two distinct phases: a *planning* phase and a *building* phase.

The **planning phase** exists primarily in a virtual world since nothing is yet in the 'real' world. Everything is still on paper, in one's mind, or in a computer environment as bits and bytes. One has here the chance to be creative: all possibilities are open to be considered for a likely design or redesign.

The planning phase has three tasks:

a) Analysis, which includes,
   i. breaking down the system by functional analysis[13] into subsystems[14];
   ii. defining the criteria that the system and sub-systems must satisfy;
   iii. identifying the resources needed to fulfil these criteria.
b) Synthesis—designing a configuration of resources that will satisfy the criteria;
c) Scheduling—the realisation of the design in the next phase (the building phase).

The **building phase**, in contrast, is the realisation or execution phase where everything is turned into reality, when one builds or modifies a system. There are very few design choices left. Now, the manager's freedom of decision is almost nil, because the design and plan are finished and given. There is usually just ONE solution, one way for the plan to be converted into reality. At the end of the building phase, the resources needed to fulfil the given criteria or functions should now be readily available.

[13] see more about functional analysis and Readiness Trees in Appendix 3

[14] in order to define the system in enough detail

The main advantage of this two-phase process is its efficiency. The more effort is put into the first phase, the better the results in the second phase will be. This is because getting the design right early avoids unnecessary design trade-offs, rework and cost overruns. Furthermore, by reducing uncertainties about how to implement the design, time spent in the planning phase will reduce the time needed in the building phase.

In an ideal case, there will be no design changes on the way to the final build. The effort one spends in the planning phase will be more then compensated for in the building phase, and in most cases one will reach the final operational stage earlier, usually much earlier and with lower costs then when one spends too little effort during the first phase.

We assume in this paper that it is reasonable to discuss the operational readiness process in general terms. However, the process must reflect the context of your organisation and the specifics of the system to be made ready. Ultimately, the information needed for readiness comes mostly from the context.

As operational readiness crosses many departmental lines, the process needs to be integrated into the host organisation. Achieving this will entail an organisation-wide effort. As mentioned earlier, a subsequent volume of this white paper will deal with how to implement a programme of operational readiness.

An operational readiness process has a number of generic aims and activities. If any of these are missing in a given context, then the process is likely to be inadequate. Either the system or activity will not be fully ready, or its readiness cannot be assured without further work. However, the principle of iteration applies: earlier steps are revisited in the light of new information. You should keep the operation of feedback in mind when looking at graphical models of operational readiness.

3.2.2 The 'get ready' process represented by the Nertney Wheel

The Nertney Wheel is the most widely known graphical model in operational readi-readiness. It is an attempt to convey the need for system designers and managers to treat the operation as an integrated whole consisting of people, procedures, equipment and conducive conditions.

The Nertney principle says that operational systems have four parts that need to be treated as one. These parts are people, hardware, procedures and conducive (supportive) operating conditions. The first three of these are depicted in Figure 5, which illustrates the point that equipment, procedural and people subsystems must be integrated in an operational system. Procedures must correspond to the equipment as it actually is, and must match the literacy and needs of the people who use them.

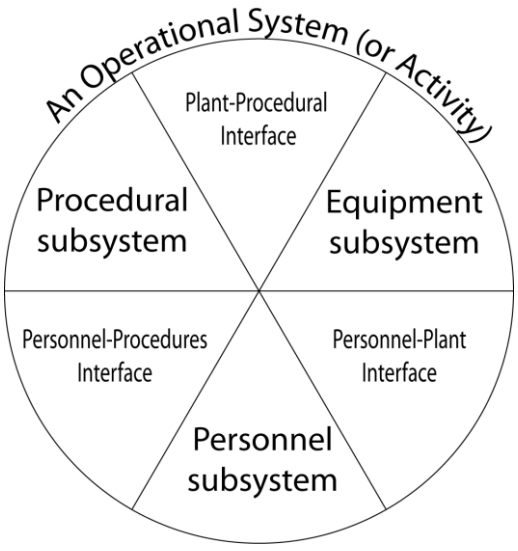


Figure 5. Three elements and their interfaces

The Nertney wheel develops this idea by adding a developmental dimension. As shown in Figure 6, a system is moved from an unready state to an operational ready state through a sequence of developmental stages shown as concentric circles.

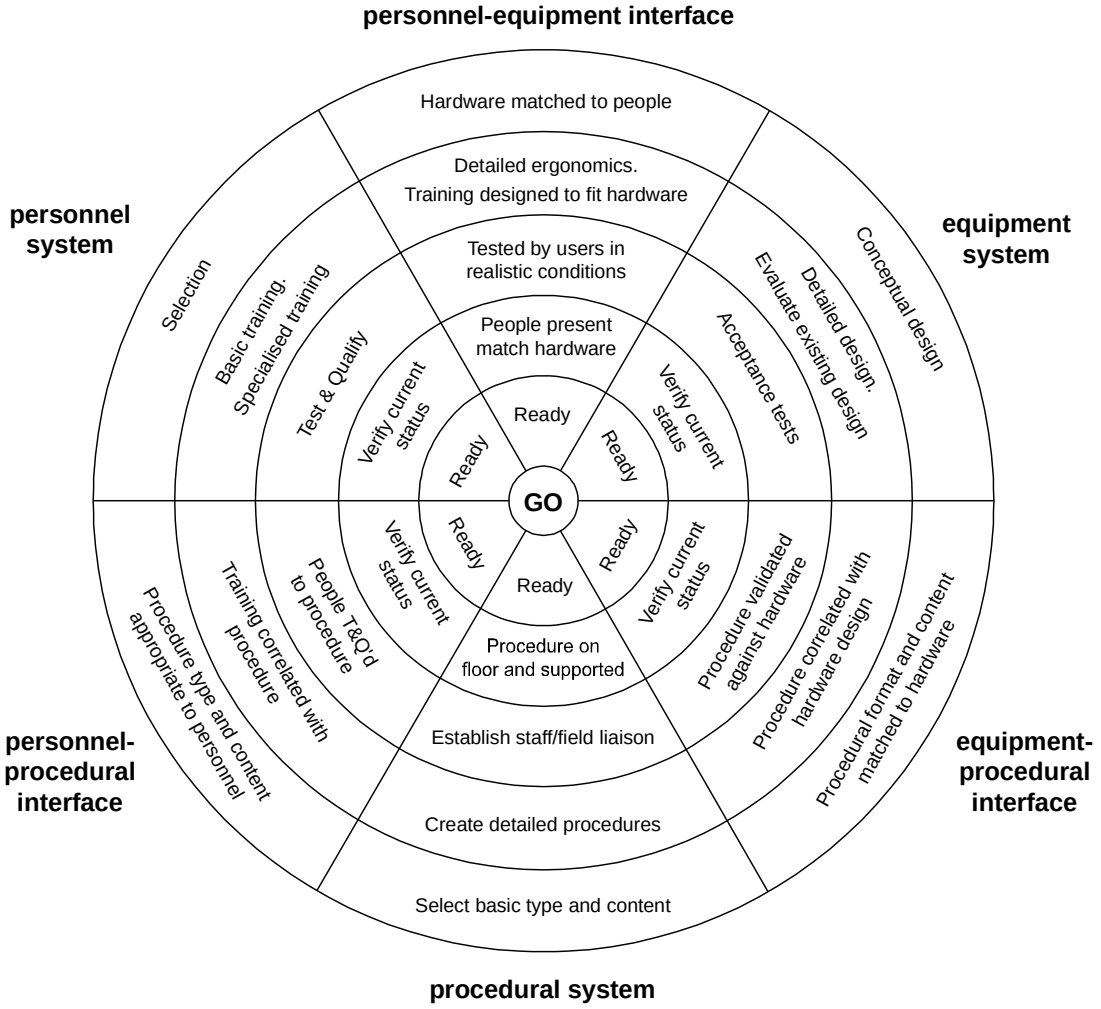


Figure 6. The Nertney Wheel (adapted from Nertney, 1987)

Nertney describes it as follows:

> *"Operational readiness is accomplished by proceeding along selection/development lines as indicated in [Figure 6]. The status of operational readiness is indicated by the bull's-eye at the centre of the diagram. As may be seen, each of the major elements achieves its state of readiness by progressing from an establishment of conceptual specifications and selection criteria to a final state of 'here-and-now' readiness labelled "GO" on the diagram.*
>
> *It should be noted that the interface development cycles must evolve through the same sort of progression if we are to arrive at a final state of system readiness. For example, (equipment-personnel interface) if we have valves in the system which require 'two strong men and a boy' to manipulate, we do not select 90-pound weaklings to operate the system. If components and displays are colour-coded, we must establish and maintain proper colour discrimination criteria in personal selection. Similarly, (personnel-procedural interface) if we select com-*

plex written technical procedures as a control medium, we must maintain functional literacy requirements in our personnel selection criteria.

Finally, (equipment-procedural interface) we must select procedural types which are appropriate to the hardware systems which our operators are controlling. The procedures should be sufficient to establish proper control but should be no more than are necessary in terms of the hardware design and the characteristics of the personnel themselves.

In short, the personnel, procedures and equipment cannot be taken to a state of readiness individually. They must be in a collective state of readiness in accordance with system operational requirements." (Nertney, 1987; p6)

The Nertney Wheel, like any model, depicts some aspects, but excludes others. The Wheel shows the activities needed to get a system ready and to keep its elements congruent. However, the Wheel neither shows feedback loops, nor the conditions needed to support development of the system or sustain its readiness (although they can be imagined as thickness, as illustrated in Figure 7). Also excluded is the use of principles described in this white paper, which facilitate the developmental activities shown in the Wheel.

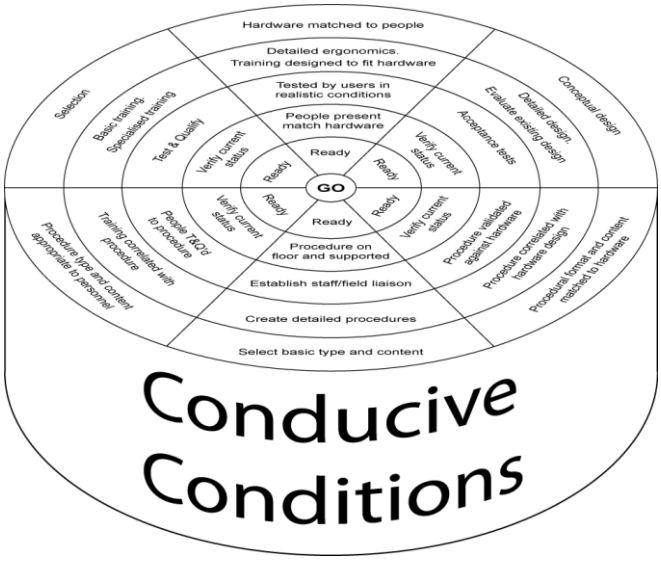


Figure 7. The 'Nertney Drum'.

The first implication of the Nertney principle is that an operation can only be ready *as a whole* if all its four parts (people, procedures, equipment and conducive conditions) are ready. Unreadiness may present itself as poor performance of normal operations, or during other operational modes such as maintenance and handling of emergencies.

The second implication of the principle is that the system is ready only if these four components are kept *congruent*. The parts must match each other in all operational circumstances (i.e. all modes of operation throughout the entire system lifecycle).

Keeping the four parts congruent means ensuring that they all match each other in the field. Once operational, the components will require continuous adjustment to stay congruent with each other and aligned to system requirements.

3.3 Readiness review

Readiness reviews are done to find significant opportunities to improve readiness and to detect any critical requirements missing from the specification of a system or activity. Readiness reviews are additional to routine monitoring and compliance checking, not an alternative to them. Unlike readiness review, routine monitoring and compliance checking are part of the day-to-day control arrangements built into the operation. Indeed, systems of monitoring and compliance checking might themselves be the subjects of a readiness review.

Readiness reviews can be triggered by:

- radical changes to an operation;
- operational trouble not adequately diagnosed by routine investigations;
- exceptional performance that surpassed the limits of what was thought to be technically possible in a given operation;
- the end of a temporary or experimental method of performing an operation;
- reaching pre-set dates that were defined by operational readiness projects;
- the desire to document a legacy system and discover ways in which its performance can be improved significantly.

The process for readiness review will be described in a separate volume, but is shown in outline in Figure 8. Depending upon the context, the scale and difficulty of the review can vary greatly.

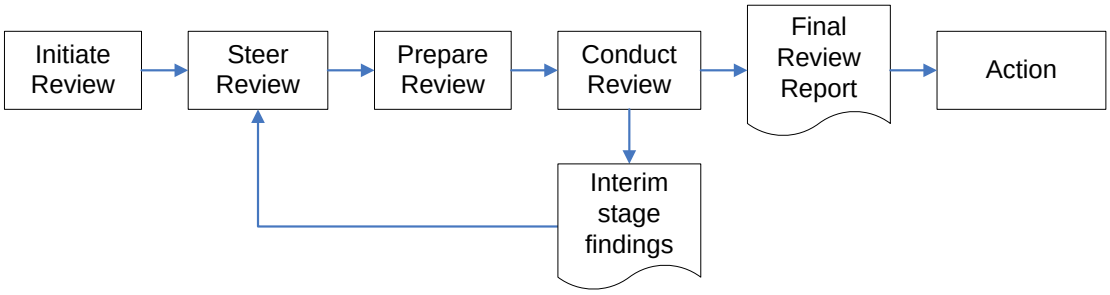


Figure 8. Generic Readiness Review Process Flowchart

3.4 Summary

This section has described generic operational readiness processes. The aim has been to illustrate how the twelve principles apply to getting a system operationally ready. What are laid out are at best sketches, and certainly not recipes. When you get a system ready, or review it, the process may have a different structure and terminology.

We have argued that benefits can result from applying operational readiness principles. These benefits stem from reducing uncertainty in the design and implementation of a new or modified system. For the most part, this is achieved by timely mobilisation of the knowledge possessed by stakeholders and experts. In this way, an operational readiness process can lessen the effects of the design paradox. Similarly, readiness review—with its accent on finding significant improvements and missing critical criteria—derives many of its benefits from mobilising knowledge.

Although an operational readiness process can deliver benefits, readiness is time-bound. Keeping the system operationally ready is as important as getting the system ready. However, some organisations attach more value to getting ready than to staying ready[15]. If these cultural norms exist in your organisation, challenging them will be as important to its operational readiness as implementing an operational readiness process.

4 Conclusions

Operational readiness is a philosophy for making a product, or providing a service, to specification, on time, on budget and with only those unwanted events that have been foreseen and accepted in advance. The principles of operational readiness are very general and will apply in most situations. However, the processes in this volume assume that the operations to be made ready, or reviewed, are front line systems and activities. The operational readiness philosophy is, to a large extent, a design philosophy. However, design is seen here as an open-ended process that extends through the lifecycle of the production system or service activity. Furthermore, design is seen in its broader sense, as "the core of practice in all professions, occupations, and everyday living". As such, design is not a one-off activity done by specialists, but a continuous effort in which everyone has a role.

The advice contained in the twelve operational readiness principles can be summarised in two paragraphs.

> *Treat the operational system as a whole made of four parts: people, equipment, processes and operating conditions. Strive to be clear about what the system actually is, what it should do and how it will behave in all modes of its operation throughout the lifecycle. Invest enough resources in the design process to make sure that you re-appraise old choices in the light of new knowledge. Remember that everything about the system is provisional, and that the only thing that doesn't change is change itself.*
>
> *Most, if not all, man-made systems are joint ventures. Engage stakeholders throughout the lifecycle, keep subject matter experts close, and make sure your organisation helps people to make sound, balanced decisions. Although many decisions need to be deliberate and visible, many more will be implicit. Whenever possible, take an analytical approach and write things down for those that follow.*

The authors have found all twelve principles necessary and widely applicable. How to apply them needs to reflect the situation to hand. Similarly, be ready to add to the principles if you need to. If you find a recipe that works, remember that the principles will also apply to your recipe; particularly the principle of impermanence. 'Falling in

[15] By way of illustration, in 2014, the UK House of Commons' Committee of Public Accounts noted that "…the Civil Service has prioritised the work involved in letting contracts and deemed the monitoring of contracts as mechanical and unimportant".

love' with a particular way of applying the principles, is probably as unwise as applying any one of them unthinkingly.

For the operational readiness philosophy to be truly effective, it needs to be embedded in the culture and processes of your organisation. A subsequent volume of this white paper will deal with how to set up an operational readiness programme.

5 Definitions[16]

Term	Meaning	Origin, Reference
Activity	An event or phase where one or many environmental effects occur. Any integrated set of tasks which achieve specific results when performed in the right sequence.	P13 (Lindahl), Environment
Communication and consultation	Continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (3.2.1.1) regarding the management of risk (1.1) NOTE 1 The information can relate to the existence, nature, form, likelihood (3.6.1.1), significance, evaluation, acceptability and treatment of the management of risk. NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: - a process which impacts on a decision through influence rather than power; and - an input to decision making, not joint decision making.	ISO GUIDE 73:2009 (E/F)
Control	A measure that is modifying risk. *NOTE 1 Controls include any process, policy, device, practice, or other actions designed to modify risk.* *NOTE 2 Controls may not always exert the intended or assumed modifying effect.*	Section 3.8.1.1, ISO GUIDE 73:2009(E/F)
Consequence	An outcome of an event affecting objectives. *NOTE 1 An event can lead to a range of consequences.* *NOTE 2 A consequence can be certain or uncertain and can have positive or negative effects on objectives.* *NOTE 3 Consequences can be expressed qualitatively or quantitatively.* *NOTE 4 Initial consequences can escalate through knock-on effects.*	ISO GUIDE 73:2009(E/F)
Criterion	A standard, rule, or test on which a judgment or decision can be based	From the American Heritage® Dictionary of the English Language, Fourth Edition; cited by http://www.wordnik.com/words/criterion, *accessed 02 April 2013.*

[16] see mainly:
- Wikipedia (English, German)
- EN ISO 9001:2000, Quality management systems – Requirements
- BS EN ISO 14001:2004 – Environmental management systems - Requirements with guidance for use, pp. 1-4
- BS ISO 31000 - 2009 – Risk Management - Principles and Guidelines, pp. 1-7
- BS EN 31100-2011 – RM Code of Practice, pp. 4-10

Term	Meaning	Origin, Reference
Cybernetics	A transdisciplinary approach for exploring regulatory systems, their structures, constraints, and possibilities. The science of communication and control in the animal and the machine.	Wikipedia: http://en.wikipedia.org/wiki/Cybernetics Norbert Wiener (1948)
Environment	(a) The sum of things, circumstances, and conditions that surround one and may have an effect on one; surroundings. Synonyms: milieu, setting, surroundings (b) The sum of everything that surrounds animals and humans in the natural world, including the air, the water, and the soil. (c) The circumstances or conditions that surround one. (d) The circumstances, objects, or conditions by which one is surrounded. (e) The aggregate of social and cultural conditions that influence the life of an individual or community.	(a) www.Wordsmyth.net (c) www.thefreedictionary.com (d),(e) www.merriam-webster.com
Evaluation	1) Assessment used as the basis for finding out if something is adequate or not. Determination of the value. 2) Process of comparing the results of an analysis with criteria to determine whether the result of an analysis is in accordance with given criteria. *NOTE: Risk evaluation assists in the decision about risk treatment.*	1) Adapted from Wiktionary http://en.wiktionary.org/wiki/evaluation. 2) Adapted from ISO Guide 73
Event	An occurrence or change of a particular set of circumstances. *NOTE 1 An event can be one or more occurrences, and can have several causes.* *NOTE 2 An event can consist of something not happening.* *NOTE 3 An event can sometimes be referred to as an "incident" or "accident".* *NOTE 4 An event without consequences can also be referred to as a "near miss", "incident", "near hit" or "close call".*	ISO GUIDE 73:2009(E/F)
Framework	see '*management framework*'	
Function	What something does or is used for.	Wiktionary http://en.wiktionary.org/wiki/function
Function (systems engineering)	A structured representation of the functions (activities, actions, processes, operations) within the modelled system or subject area. Describes the requested behaviour of an engineering system.	Wikipedia http://en.wikipedia.org/wiki/Function_model http://en.wikipedia.org/wiki/Functional_specification
Function (mathematics)	A relation between a set of inputs and a set of permissible outputs with the property that each input is related to exactly one output.	Wikipedia http://en.wikipedia.org/wiki/Function_(mathematics)

Term	Meaning	Origin, Reference
Hazard	A source of potential harm NOTE Hazard can be a risk source (3.5.1.2).	Section 3.5.1.4, ISO GUIDE 73:2009(E/F)
Instance (of a (OPR) process, cycle)	A specific application of the (operational readiness) process described in the operational readiness framework, to a specific, logical set of circumstances related to a particular area or activity of the organization.	Adapted from ISO Guide 73
Lifecycle	The series of developmental stages through which a system passes. According to Johnson (1973): The lifecycle phases of concern in any system are: • Conception • Definition, Requirement • Design, Development (including procedures and training plans) • Construction, or manufacture and Installation • Operation • Maintenance • Disposal	MORT SAN 821-1, page 99.
Management framework	The set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving (operational readiness) management throughout the organization. *NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage operational readiness.* *NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.* *NOTE 3 The operational readiness framework is embedded within the organization's overall strategic and operational policies and practices.*	adapted from ISO Guide 73:2009

Term	Meaning	Origin, Reference
Method	Scientific: a series of steps, or collection of methods, taken to acquire knowledge In the context of problem solving: Step-by-step approach consisting of (1) identifying and defining a problem, (2) accumulating relevant data, (3) formulating a tentative hypothesis, (4) conducting experiments to test the hypothesis, (5) interpreting the results objectively, and (6) repeating the steps until an acceptable solution is found. 1. A procedure, technique, or way of doing something, especially in accordance with a definite plan: There are three possible methods of repairing this motor. 2. A manner or mode of procedure, especially an orderly, logical, or systematic way of instruction, inquiry, investigation, experiment, presentation, etc.: the empirical method of inquiry. 3. Order or system in doing anything: to work with method.	Wikipedia http://en.wikipedia.org/wiki/Method www.BusinessDictionary.com http://dictionary.reference.com
Methodology	Comparison or study and critique of individual methods that are used in a given discipline or field of inquiry	Wikipedia: http://en.wikipedia.org/wiki/Method
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. NOTE Monitoring can be applied to a risk management framework (2.1.1), risk management process (3.1), risk (1.1) or control (3.8.1.1).	Section 3.8.2.1, ISO GUIDE 73:2009(E/F) and clause 2.28, BS ISO 31000:2009(E)
Operability	The ability to keep equipment, a system or a whole industrial installation in a safe and reliable functioning condition, according to pre-defined operational requirements.	Wikipedia: http://en.wikipedia.org/wiki/Operability
Operational readiness	Operational readiness means that there are the right people in the right places at the right times working with the right hardware according to the right procedures and management controls, and functioning in a proper or given physical and psychological environment.	Nertney, 1987.
Principle	A basic generalization that is accepted as true and that can be used as a basis for reasoning or conduct.	Definition from Wordnet 3.0 (*accessed 17 May 2014*). About WordNet; WordNet. Princeton University, 2010.
Procedure	A set of commands that show how to prepare or make something; describing the Who, What, Where, When, and Why.	Wikipedia: http://en.wikipedia.org/wiki/Procedure
Process (philosophy)	Unifying principles which operate in many different systemic contexts.	Wikipedia: http://en.wikipedia.org/wiki/Process

Term	Meaning	Origin, Reference
Process	A series of events to produce a result; a set of procedures used to produce a product.	Wiktionary: http://en.wiktionary.org/wiki/process
Policy	A statement of the overall intentions and direction of an organization (related to e.g. operational readiness management).	adapted from ISO Guide 73
Review	An activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. NOTE 1 Review can be applied to a risk management framework (2.1.1), risk management process (3.1), risk (1.1) or control (3.8.1.1). Note 2: Looks only at one specific place, not an overall view.	Section 3.8.2.2, ISO GUIDE 73:2009(E/F), adapted and note added
Risk acceptance	An informed decision to take a particular risk. NOTE 1 Risk acceptance can occur without risk treatment (3.8.1) or during the process of risk treatment. NOTE 2 Accepted risks are subject to monitoring (3.8.2.1) and review (3.8.2.2).	Section 3.8.1.6, ISO GUIDE 73:2009(E/F)
Risk analysis	A process to comprehend the nature of risk (1.1) and to determine the level of risk (3.6.1.8) NOTE 1 Risk analysis provides the basis for risk evaluation (3.7.1) and decisions about risk treatment (3.8.1). NOTE 2 Risk analysis includes **risk estimation**. **(this term is no longer defined)**	ISO GUIDE 73:2009(E/F)
Risk assessment	The overall process of risk identification (3.5.1), risk analysis (3.6.1) and risk evaluation (3.7.1).	ISO GUIDE 73:2009(E/F)
Risk avoidance	An informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk (1.1). NOTE Risk avoidance can be based on the result of risk evaluation (3.7.1) and/or legal and regulatory obligations.	Section 3.8.1.2, ISO GUIDE 73:2009(E/F)
Risk evaluation	The process of comparing the results of risk analysis (3.6.1) with risk criteria (3.3.1.3) to determine whether the risk (1.1) and/or its magnitude is acceptable or tolerable. NOTE: Risk evaluation assists in the decision about risk treatment (3.8.1).	Section 3.7.1, ISO GUIDE 73:2009(E/F)
Risk financing	A form of risk treatment (3.8.1) involving contingent arrangements for the provision of funds to meet or modify the financial consequences (3.6.1.3) should they occur	Section 3.8.1.4, ISO GUIDE 73:2009(E/F)

Term	Meaning	Origin, Reference
Risk identification	The process of finding, recognizing and describing risks (1.1) NOTE 1 Risk identification involves the identification of risk sources (3.5.1.2), events (3.5.1.3), their causes and their potential consequences (3.6.1.3). NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's (3.2.1.1) needs.	ISO GUIDE 73:2009(E/F)
Risk management	Coordinated activities to direct and control an organisation with regard to risk.	ISO GUIDE 73:2009(E/F)
Risk management framework	The set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring (3.8.2.1), reviewing and continually improving risk management (2.1) throughout the organization. NOTE 1 The foundations include the policy, objectives, mandate and commitment to manage risk (1.1). NOTE 2 The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. NOTE 3 The risk management framework is embedded within the organization's overall strategic and operational policies and practices.	ISO GUIDE 73:2009(E/F)
Risk owner	A person or entity with the accountability and authority to manage a risk (1.1)	Section 3.5.1.5, ISO GUIDE 73:2009(E/F)
Risk retention	Acceptance of the potential benefit of gain, or burden of loss, from a particular risk (1.1) NOTE 1 Risk retention includes the acceptance of residual risks (3.8.1.6). NOTE 2 The level of risk (3.6.1.8) retained can depend on risk criteria (3.3.1.3).	Section 3.8.1.5, ISO GUIDE 73:2009(E/F)
Risk sharing	A form of risk treatment (3.8.1) involving the agreed distribution of risk (1.1) with other parties. NOTE 1 Legal or regulatory requirements can limit, prohibit or mandate risk sharing. NOTE 2 Risk sharing can be carried out through insurance or other forms of contract. NOTE 3 The extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements. NOTE 4 Risk transfer is a form of risk sharing.	Section 3.8.1.3, ISO GUIDE 73:2009(E/F)

Term	Meaning	Origin, Reference
Risk source	An element which alone or in combination has the intrinsic potential to give rise to risk (1.1) NOTE A risk source can be tangible or intangible.	Section 3.5.1.2, ISO GUIDE 73:2009(E/F)
Risk treatment	A process to modify risk (1.1) NOTE 1 Risk treatment can involve: - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; - taking or increasing risk in order to pursue an opportunity; - removing the risk source (3.5.1.2); - changing the likelihood (3.6.1.1); - changing the consequences (3.6.1.3); - sharing the risk with another party or parties [including contracts and risk financing (3.8.1.4)]; and - retaining the risk by informed decision. NOTE 2 Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”. NOTE 3 Risk treatment can create new risks or modify existing risks.	Section 3.8.1, ISO GUIDE 73:2009(E/F)
Should	*Should* is used to express recommendations.	BS 31100:2011
Stakeholder	A person or organization that can affect, be affected by, or perceive themselves to be affected by decision or activity. *NOTE A decision maker can be a stakeholder.*	Section 3.2.1.1, ISO GUIDE 73:2009(E/F)
Surrounding(s)	a. all the things around you; b. the environment of anything, including all that affects it	www.Wordsmyth.net
System	A system can be a new one or an alteration or modification or amendment of an existing one. A system can be anything from as small as a knob on a door of an airplane up to huge and extremely complex systems like a big airport.	Current authors
System	A set of interacting or interdependent components forming an integrated whole.	Wikipedia http://en.wikipedia.org/wiki/System
System	People, procedures, and plant/hardware performing specific tasks in a given environment. Any integrated set of elements which, when operated together, achieve specific results.	

Term	Meaning	Origin, Reference
System	(1) A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific production, support, or mission requirement. (2) An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.	(1) MIL-STD-882b 1977: 3.1.15 (2) MIL-STD-882D, 2010: 3.2.12
System of interest	The system under consideration; the system being analysed, or; the system being made operationally ready. By 'system' we mean the object, project, undertaking or activity that will be dealt with in the following operational readiness process.	Current authors
Tool	Anything used for accomplishing a task or purpose.	Random House Webster's Dictionary, 3rd edition, 1998
TOR = Terms of Reference	(1) The instructions that someone must follow when they study or examine something. (2) The specific limits of responsibility that determine the activities of an investigating body, etc. In operational readiness, a TOR might include: - the objectives of the operational readiness cycle; - any limitations; - the methodology.	(1) Macmillan Dictionary (accessed 17 May 2014) (2) Collins English Dictionary (accessed 17 May 2014)
Upstream processes	The engineering and scientific development of elements of a work situation, e.g. design, construction, training.	Johnson 1973: MORT SAN 821-1, Appendix I, page 5.

[This page is intentionally left blank]

6 References

Alexander, I., and Bues-Dukic, L. (2009). Discovering Requirements. Wiley.

Argyris, C. (1994). Good communication that blocks learning. Harvard Business Review, July-August 1994, pp. 77-85.

Ashby, W.R. (1956). Introduction to Cybernetics. London, Chapman and Hall.

Blanchard, B.S. and Fabrycky, W.J. (2014) Systems Engineering and Analysis (fifth edition) Prentice Hall, NJ.

Briscoe, G. (1982). Risk management guide. DOE-76-45/11, SSDC 11, EG&G Idaho, Idaho Falls, USA.

British Standards Institution (2009). BS *ISO 31000:2009, Risk management — Principles and guidelines*. *Milton Keynes: BSI.*

British Standards Institution (2011). *BS 31100:2011 Risk management — Code of practice and guidance for the implementation of BS ISO 31000.* Milton Keynes: BSI.

Collins, H.M. (2001). Tacit Knowledge, Trust and the Q of Sapphire. Social Studies of Science, Vol. 31, No. 1 (Feb., 2001), pp. 71-85.

Federal Judicial Centre (2000). Reference Manual on Scientific Evidence; Second Edition. (Note: The FJC published a third edition in 2011)

Freeman, R.E. (2010). Strategic Management: A Stakeholder Approach. Cambridge University Press.

Heidrich, O., Harvey, J. and Tollin, N. (2009). Stakeholder analysis for industrial waste management systems. Waste Management, 29 (2009), pp. 965–973.

House of Commons Committee of Public Accounts (2014). "Transforming contract management". Twenty-third Report of Session 2014–15. HC 585, HMSO.

International Organization For Standardization (2009). *Guide 73, Risk management — Vocabulary.* Genève, Switzerland: ISO.

Johnson, W.G. (1973). MORT - The Management Oversight and Risk Tree. SAN 821-2. US Atomic Energy Commission.

Johnson, W.G. (1985). Accident/Incident Investigation Manual; Second Edition. DOE/SSDC 76-45/27.

Kepner, B.B. and Tregoe, C.H. (1981). "*The New Rational Manager*". Pub. Princeton Press, New Jersey.

Kingston, J., Koornneef, F., van den Ruit, J., Frei, R., and Schallier, P. (2009). NRI MORT User's Manual; 2nd Edition. NRI-1 (EN). Noordwijk Risk Initiative Foundation. The Netherlands.

Kletz, T.A. (1993) "Lessons from Disaster: How Organizations Have No Memory and Accidents Recur" Pub. IChemE. Pages 21-23

Korzybski, A (1948) "General Semantics, Psychiatry, Psychotherapy and Prevention." In Kendig, M. (1990). Alfred Korzybski: Collected Writings, 1920-1950. Institute of General Semantics.

Lidwell, W., Holden, K., and Butler, J. (2010). Universal Principles of Design. Rockport Publishers; Second Edition.

Lindahl, M., and Tingström, J. (2001). A small textbook on Environmental Effect Analysis. Department of Technology, University of Kalmar, Sweden.

Nertney, R.J. (1987). Process Operational Readiness and Operational Readiness Follow-On. DOE-76-45/39, SSDC-39, EG&G Idaho, Idaho Falls, USA.

Paté-Cornell, M.E. (1996). Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering & System Safety. Vol. 54, Issue 2-3, Pages: 95-111.

Polanyi, M. (1967). The Tacit Dimension, New York: Anchor Books.

Rail Safety and Standards Board (2004). Definition of abnormal and degraded working.

Schön, D. A. (1971). Beyond the Stable State. Public and private learning in a changing society. Temple Smith, London. [Note that this book develops ideas that Schön presented in his series of six Reith Lectures in 1970. These are still available via the BBC website].

Schön, D. A. (1992). The Theory of Inquiry: Dewey's Legacy to Education. Curriculum Inquiry 22 (2): 119-139.

Smith, M. (2013). Chris Argyris: theories of action, double-loop learning and organizational learning. www.Infed.org. (*Accessed, 21 May 2014.)*

Stein, M.I. (1975). Stimulating Creativity. Volume 2, Group Procedures. Academic Press.

Stirling, W.C. (2013). Neo-Satisficing Control for Cooperative Systems. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics. Manchester, UK. 13-16 Oct. 2013. Pages 559-564.

UK Offshore Oil Operators Association (UKOOA), 1999. Industry Guidelines on a Framework for Risk Related Decision Support. UKOOA, London.

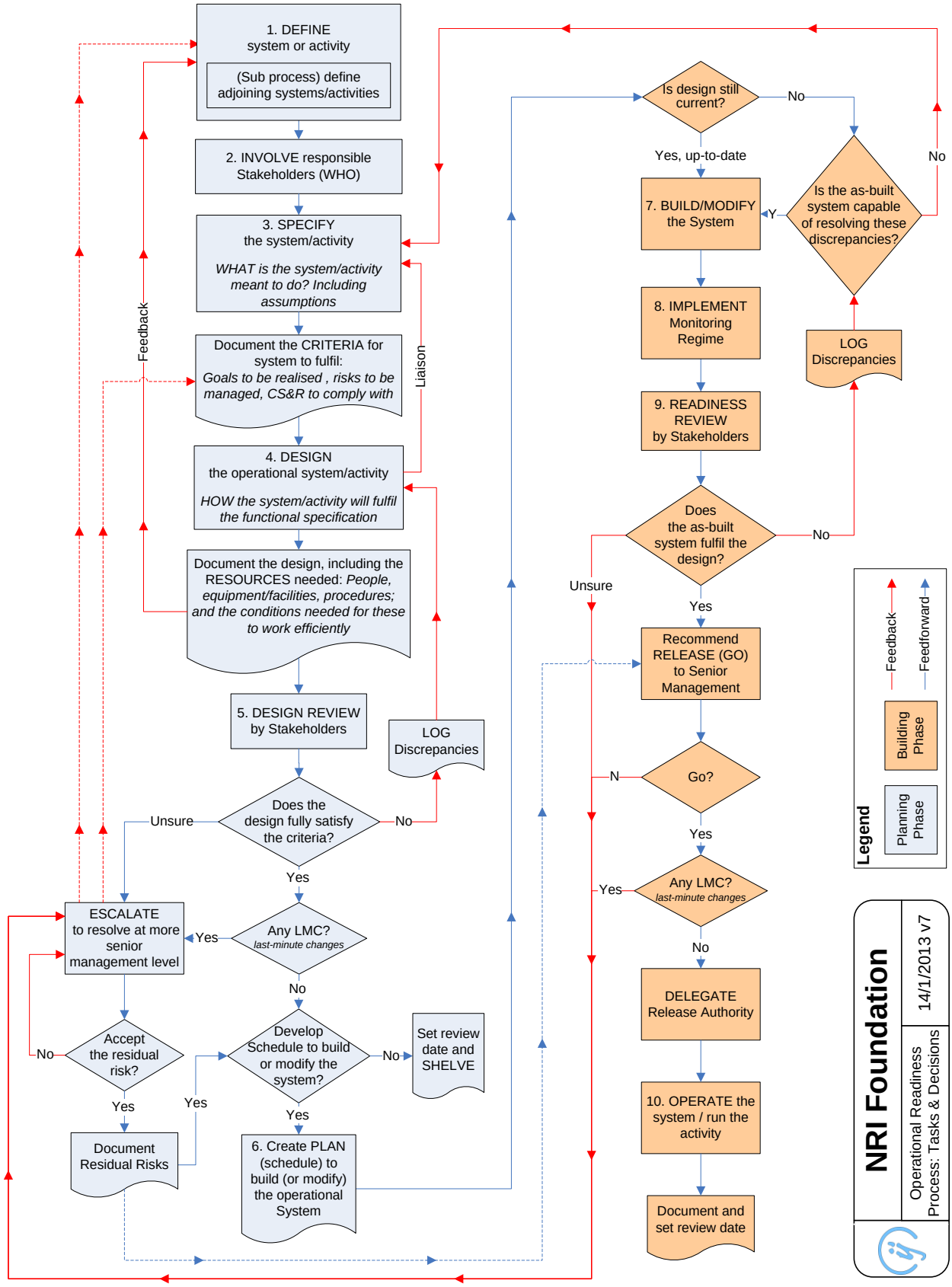
United States Department of Defense (2012). Standard Practice: System Safety. MIL-STD-882E

Weick, K.E., and Sutcliffe , K.M. (2007). Managing the Unexpected (2nd edition). Wiley and Sons, NY.

Wiener, N. (1948). Cybernetics. John Wiley & Sons, Inc.

[This page is intentionally left blank]

Appendix 1: Operational Readiness Process: Tasks & Decisions



[This page is intentionally left blank]

Appendix 2: Identifying the twelve principles of operational readiness

The principles in this white paper are generally well known. However, in respect to operational readiness, the relevance of the principles had to be 'flushed-out'. In this case, they were brought to the surface when we, the present authors, wrote a generic operational readiness procedure for a large business. This is an example of Donald Schön's point that "experts know more than they can tell" (*see page 14*).

The generic operational readiness procedure was written in two stages. The first stage was to create an outline process from the sketchy information found in published sources. The authors provided the missing information from their understanding of operational readiness processes. This quickly brought some principles to the surface (the *Nertney, Iteration, Balance, Stakeholder, Kletz,* and *Assumed risk* principles). The outcome of the first stage was an outline operational readiness process. A version of this outline is shown as Figure 4, on page 20.

The next stage was to identify the tasks subsumed in the outline process. In effect this involved expanding a 10-step outline to reveal the criteria that a generic readiness procedure would need to satisfy.

To ensure that the procedure contained only what was needed; the authors imagined what the criterion would contribute in practical settings and what effect its absence would have. If a criterion survived these tests, we tried to justify it in principle. In some cases this forced us to recognise principles that had been implicit up to that point. However, each new criterion would bring a new insight that shaped our understanding of the principles.

During the design of the generic procedure, the principles were written down to explain the intent of procedural steps. That guidance material had only the detail needed to help implement the procedure. Our aim in writing this white paper has been to more fully explain the principles to the reader. We have used the writing process to refine the principles as far as we can, and ground them in published work.

[This page is intentionally left blank]

Appendix 3: Operational readiness and positive trees

A later volume of this white paper is planned which will be dedicated to tools for operational readiness. However, as positive trees figured so prominently in the original SSDC (System Safety Development Center) work, the authors judged that it would be useful to mention them here.

Positive trees referred to a class of analysis performed to reveal the required functions of a system. Positive trees are related to functional analysis methods (as described in Blanchard and Fabrycky, p773-782; 2014) and the FAST[17] method used in Value Analysis.

The following rules are based on the graphic sequences shown below in Figure 9:

- The basic goal is to have any operation in a state of readiness.
- Developing an analytical tree which gets progressively deeper in detail showing the things needed to be ready to do a job.
- The tree is used to define a complete set of tasks or functions to attain operational readiness. The amount of detail needed can be varied through the various tiers or levels of the tree.

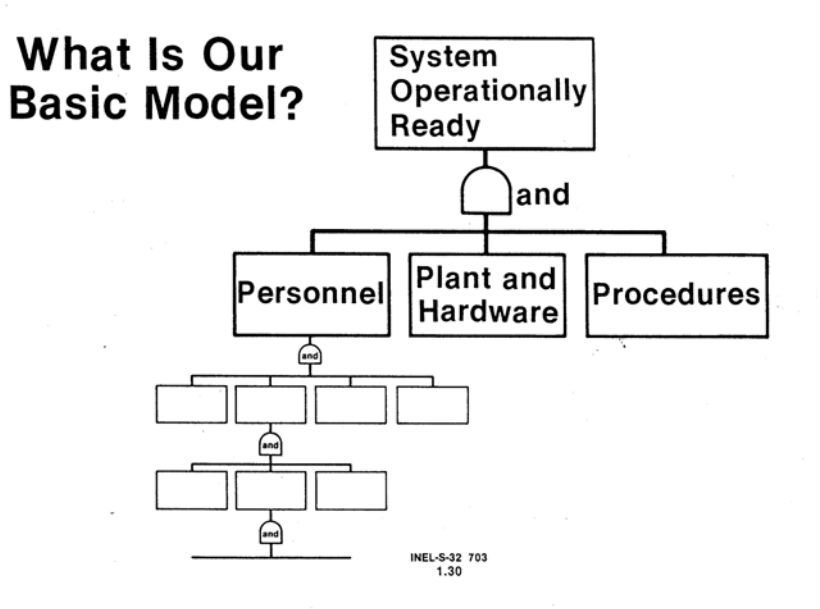


Figure 9. A generic example of a positive (readiness) tree

Trees and project planning

It is usual to start Readiness Trees in the conceptual phase of system development, but to refine it iteratively in the light of new information. “As design and development continues, the functional analysis is accomplished to greater depth, to the sub-

[17] A description of FAST, the Function Analysis System Technique, is published by The Canadian Society of Value Analysis.

system level and below, during the preliminary system design phase" (Blanchard and Fabrycky, p773; 2014).

When the functional analysis is accomplished in sufficient detail, it can be used to methodically plan the tasks needed to build, or implement, the system. Figure 10 shows the interdependencies of different representations and tools for accomplishing operational readiness. On top is the positive tree that shows all the necessary functions required in the operational system. These functions need to be realised in the real-world, and the tasks needed to achieve this can be represented as 'work sequence charts'. In the sequence chart (flow chart) the sequence of the work to be done is shown with its interdependencies and time frame. Many project management software tools exist that can fulfil the role of sequence chart. Less often encountered is the 'Operational Readiness Matrix' which provides an overview of what is to be done by whom and the state of readiness at any time.

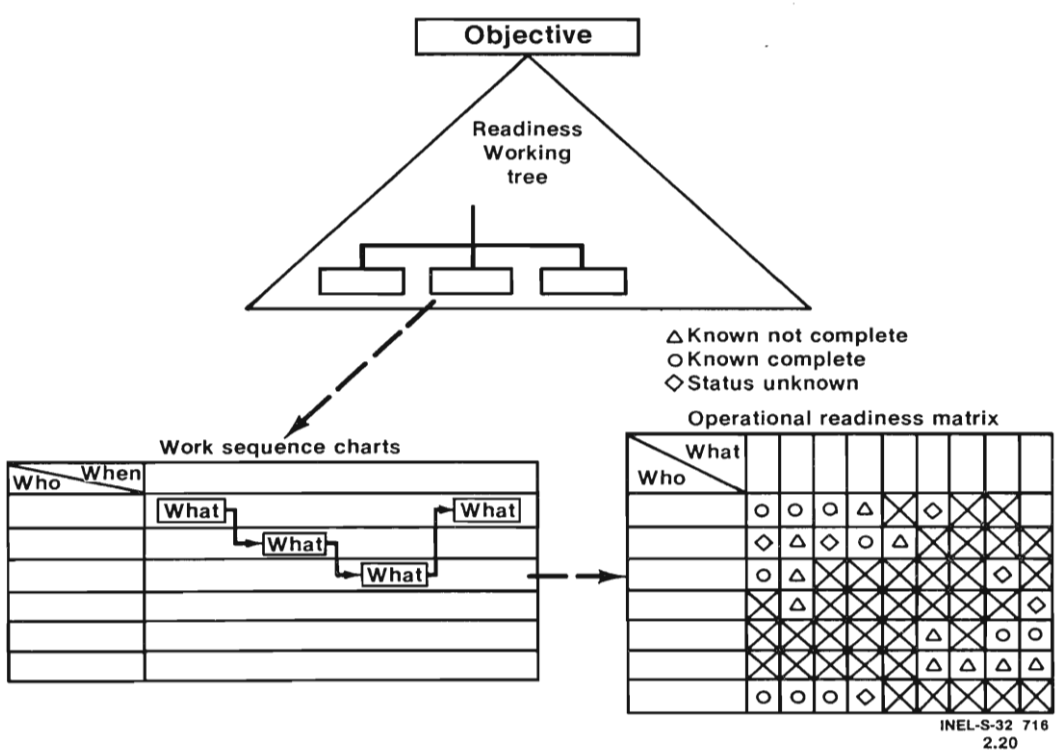


Figure 10. Interrelation of positive (Readiness) trees and project planning graphics

Appendix 4: The origins of operational readiness in the US Military-industrial complex

The term 'operational readiness' began to be used by the United States Air Force (USAF) in the 1950s. The earliest use occurs in the 'USAF Statistical Digest' published in 1953; earlier editions of the Digest refer to 'combat readiness', or just 'readiness'. The USAF Statistical Digest, 1956, defined operational readiness as a "measurement of relative capability"… "It is the degree to which a unit is manned, equipped and trained for the satisfactory performance of its, primary mission."

Over the next twenty years, 'operational readiness' became more widely used. Originally it was applied only to weapons systems, but this broadened to include other aspects of the military-industrial complex. By the 1960's, the phrase 'operational readiness' was used in discussions of civil defence (e.g. US Department of Defense, 1964) and, by the 1970's, of the nuclear programme.

Over time, users of the term 'operational readiness' began to invest it with deeper meanings. This was perhaps driven by the need to make more accurate measurements of operational readiness than merely ready or unready. Something of this kind of thinking is at work in the following report of the status of the NIKE missile system:

> *"As a test of how to present the status of typical Army programs most effectively to top management, ORO has analysed the NIKE 1 programme as of 30 September 1954"… "On the basis of the data and information on policy available at the Pentagon" … "it is not possible to quantify either goals or relative progress of these groups."… "Furthermore, it indicates that standards for judging the operational readiness of the NIKE battalion are inadequate"… "In carrying out a programme, the Army now relies on informal staff coordination. Balanced progress would be more likely if all important elements were formally brought into control groups, and if status reports considered all these groups."*
>
> Operations Research Office (1954; p12-13)

By the 1960's, operational readiness is being discussed in ways that recognise it as a property of socio-technical systems. Discussing the provision of civil defence shelters, Siroky and Eninger (1963) state:

> *"a civil defense shelter is operationally ready when it has been (1) stocked with the equipment and materials essential for its operation, (2) staffed with a trained shelter management cadre, and (3) equipped with the plans and procedures which will characterize its operation in the event of a nuclear attack. The definition is admittedly arbitrary. Nevertheless, it is the opinion of this report that this concept of operational readiness is essential to the achievement of the shelter goals defined in chapter I. In this respect, a civil defense shelter is analogous to a complex weapon system. It is not the hardware per se that makes a weapon system operational. It is the integration of equipment, personnel, and procedures into a ready capability."*
>
> *Siroky and Eninger (1963; p.42).*

In the late 1960s, as Stephans (2004) recalls, "the Atomic Energy Commission (AEC) aware of system safety efforts in the DOD and NASA communities, made the decision to hire William G. Johnson, retired manager of the Na-

tional Safety Council, to develop a system safety program for the AEC" (Stephans, 2004; p5). Johnson's idea was "to formulate an ideal, comprehensive systems concept of accidents and their control, and to test the usefulness of the concept" ... "The formulation of an ideal system appears to be a valuable precondition for knowing what information to seek after an accident and what aspects of performance to seek to measure" (Johnson, 1973). This work developed through successive stages into what became known as the Management Oversight and Risk Tree (MORT) programme.

From 1973 to 1990, the MORT programme was run by the System Safety Development Centre (SSDC), which was set up specifically for the work. During the period, they took the early MORT work (described in Johnson, 1973) and sought to implement the emerging 'ideal system' for control of accidents as widely as possible in the US Nuclear Industry. Much of the 'ideal system' is these days identified with System Safety, which the US Department of Defense defines as:

> *"The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system lifecycle"*
>
> *US Department of Defense, 2012*

Although the ideas of system safety are well-documented, the means that SSDC used to implement those ideas is not. The SSDC, and notably W.G. Johnson and R.J. Nertney, recognised that system safety concepts held little appeal for the senior managers of operations. However, they also recognised that these same managers were very interested in operational readiness. The breakthrough in the thinking was to integrate the ideas of system safety into operational readiness, and to promulgate those ideas through a long-running (1975-1989) series of 'MORT' seminars and operational readiness workshops. As Nertney (2003) describes it:

> *"You can see this in how we set our priorities in the workshops: we consciously left some students behind – we wouldn't certify them if they were incompetent, but their education was our second priority. Our first priority was to create disciples (using the same logic as the innovation diffusion[18] effort in agriculture) and if a workshop yielded just one, then it was a success. In the agricultural innovation diffusion setting, they would try to identify young farmers with a University degree. We weren't bothered about that sort of thing; we had four criteria (1) that they were interested, (2) that they seemed to understand (3) that they had passion, and (4) that they had influence in their organisation."*

The didactic orientation of the SSDC meant that many decision-makers started to integrate system safety into their areas of responsibility. However, although operational readiness was the philosophy taught, the SSDC published relatively few papers explaining it. The end of the cold war allowed the US Department of Energy to change its focus from maintaining nuclear sites to decommissioning them; the funding for the SSDC work soon ceased.

[18] 'Innovation diffusion' was the name given to a means of promoting new technology and practices amongst conservative farming communities in the USA.

References (Appendix 4)

Johnson, W.G. (1973). MORT - The Management Oversight and Risk Tree. SAN 821-2. US Atomic Energy Commission.

Nertney, R.J. (2003). Personal correspondence with the author (Kingston).

Operations Research Office (1954). Semiannual Report, VOLUME VII, NUMBER II. 1 July—31 December 1954, John Hopkins University.

Siroky, F.R., and Eninger, M.U. (1963). Planning and Organizing Shelter Non-Operational Activity Programs. American Institutes for Research Pittsburgh, PA. AD0410891

Stephans, R.A. (2004) System Safety for the 21st Century. John Wiley & Sons, NJ.

USAF (1953) United States Air Force Statistical Digest, Fiscal Year 1953. Operations Statistics Division, D Statistical Services, DCS Comptroller, USAF, Washington, DC

US Department Of Defense (1964). Annual Report of the Office of Civil Defense For Fiscal Year 1964.

US Department Of Defense (2012). Standard Practice: System Safety, MIL-STD-882E