More than process restart/pre-start: Operational readiness – alive and kicking.

John Kingston-Howlett[1], Rudolf Frei[2], Anthony Garforth[3], and Paul Lindhout[4]

'Operational Readiness' is a term coined in the 1950s to describe the developmental state of weapons systems. However, by 1980, the phrase had taken on a wider meaning, close to 'system safety'. Operational readiness was a means to encapsulate the practices of safe design and to integrate them into corporate decision-making.

Documentation of the work done on operational readiness between 1970 and 1990 is not plentiful or widely published. The theoretical foundation of operational readiness was only partly described. Now, in the process safety field, operational readiness exists only in a limited way; chiefly as a protocol for restarting processes after shutdowns.

A large European airline has adopted the operational readiness concept as a means to manage change in their systems and processes. Aviation is a highly competitive market. Increasingly, commercial viability depends on operational innovation. It is equally critical to sustain high levels of safety. These are assumed by passengers and demanded by regulators. In 2012, the European Aviation Safety Agency (EASA) introduced new regulations. These have spurred aviation companies to find new ways to manage safety. The airline is using operational readiness to:

- integrate the consideration of safety into decision-making throughout the life-cycle of operations;
- 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.

The airline is using the operational readiness concept as a basis for its management of change procedures. In parallel to developing the procedures, the authors took the opportunity to locate the concept of operational readiness in published literature. This was done in three steps. First, based on the original published (and unpublished) work, a generic management of change process was flow-charted. Next, the generic process was analysed to make explicit the two hundred or so criteria that the process should satisfy. Lastly, the list of criteria was examined to identify underlying principles, which were subject to further refinement and literature research. This produced twelve general principles.

Engineers will recognise several of the operational readiness principles as those of design. However, many of the stakeholders involved in creating and modifying operational systems are not engineers. The airline project aimed to create a management of change process in which the stakeholders co-operate and share knowledge efficiently. This reduces uncertainty in the design process and allows risks to be recognised early with the greatest opportunity for the most safety at least cost.

The time may be ripe for the process industries to rediscover the operational readiness concept. At one end of the lifecycle, businesses are keen to embrace key enabling/emerging technologies (KETs). Towards the other end of the lifecycle, businesses are often looking for ways to safely extend plant life. This paper will argue that the operational readiness philosophy may be a source of strategies for both.

Operational readiness: origins and development

In this paper, the authors present the main ideas of a design and management philosophy called operational readiness. This philosophy originated in the US nuclear industry as a means to integrate safety into operational and commercial decision-making. At a general level, operational readiness provided a vehicle for inculcating system safety ideas into managerial practice.

The present paper uses the definition stated in Frei (2015). An operationally ready system is one in which the right people are in the right places at the right times, working with the right hardware/software according to the right procedures and management controls, and are functioning in a favourable physical and psychological environment.

Concerning the evaluative term 'right', Nertney (1987; p3) states: "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.

[1] Corresponding author. Tel +44 (0)121 288 3206; J.kingston@nri.eu.com
[2] Noordwijk Risk Initiative Foundation
[3] School of Air Transport, Cranfield University
[4] Ministry of Social Affairs (SZW), The Netherlands

2. Applicable codes/standards and regulations established at all control levels inside and outside of the operating organization."

The underlying similarity between process plant and other types of socio-technical system was understood by the originators of the operational readiness philosophy. The military industrial complex referred to earlier, was highly diverse. It included process plants, laboratories, manufacturing facilities, and all the services one might associate with them, including air and ground transportation. In most, if not all, of these settings were found hardware design, operation and maintenance, and activities to ensure that competent people work with the equipment according to adequate procedures.

Frei et al (2015; p25) summarise the operational readiness philosophy 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 original work was done between 1975 and 1987 as an offshoot of the so-called MORT project (Johnson, 1973). In those twelve years the main focus was to encourage field application by providing methods and training. The cessation of the cold war marked the end of funding for that project and many others. With its theoretical basis only partially documented, operational readiness in the broader sense has largely been forgotten. What remains are marginal, specialised activities aimed at verifying readiness before process start-ups/re-starts.

This paper will concentrate on the relevance of operational readiness to two topics in the process industries: plant ageing; and, KETs—key enabling/emerging technologies. The philosophy of operational readiness will be described only in outline, as it is explained in detail elsewhere (Frei et al, 2015).

Operational readiness as a design philosophy

Frei et al (2015) identified twelve principles for operational readiness; readers with an engineering background will recognise many of the principles as those of design. However, three points distinguish operational readiness:

- the first is that the principles must be applied together, not in isolation;
- the second point is that design is done not just by engineers, but by many of the stakeholders involved in creating and modifying operational systems. However, all these stakeholders can be considered as designers. As Schön noted, "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" (1992; p127);
- the third is that design is an open-ended task, not a finite phase that finishes when implementation is complete and operations begin.

The following subsections show how certain operational readiness principles apply to plant ageing and KETs. However, the reader is encouraged to consult Frei et al. (2015) for a full account of the principles.

People, Plant, Procedures and Conducive conditions

Operational readiness treats systems,[5] as composed of four parts that need to be coordinated as one unit throughout the lifecycle. These four parts are people, plant, procedures and the conducive conditions needed for them to perform as expected by the system designers. The first three of those– people, plant, procedures—must be kept congruent and matching. The fourth part, the conducive conditions, is needed to allow people, plant, and procedures to perform as expected by the system designers.

Seen in this light, the challenges of plant ageing are clear. Each of the parts described are mentioned by the Horrocks study for HSE and the Hokstad SINTEF study as the subjects of unwanted change. In the aviation project, the operational readiness procedure emphasised the importance of defining the performance of these elements of the system.

Conducive conditions—the properties of the operating environment that are critical for the performance of the people, plant and procedures—seem to be particularly vulnerable to ageing. This appears to be because these conditions are simply assumed and not made explicit. Staff turnover will tend to whittle away implicit knowledge. One strategy here is to make conducive conditions subject to KPIs, we have argued the case for this elsewhere in respect of readability (Lindhout et al.

[5] 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.

2009). As discussed in Lindhout and Kingston-Howlett (2011), the demands of text (such as procedures) must be matched to the reading ability of the people who use them. In that study, the authors found Safety documents in high risk chemical companies to be insufficiently readable by half of their users.

Another feature of plant ageing is what might be called patching: adding piecemeal to plant or procedures, or even to the workforce. Unlike well-managed modifications, patching does not take into account all the interfaces with other parts of the system, may miss requirements, and may unknowingly violate design assumptions. All of these will tend to produce sub-optimal results. Furthermore, and this is something seen in many sectors, patching has the tendency to implement safety measures at the lower levels of the safety precedence sequence (i.e. adding new rules to procedures, placing more reliance on supervision and training). The safety precedence sequence is explained in more detail on page 8.

The airline work shows that it is possible to devise a management of change procedure that is usable for small modifications as well as for large scale changes. However, the process-driven culture of aviation is seen as part of the discipline that gets the procedure followed.

In respect of KETs, one of the issues when adopting a new technology is its immaturity. This places an extra burden on monitoring to identify problems at an early stage, which given the uncertainties, may be difficult to predict. In terms of the people component, systems exploiting KETS may need over-competent operators—staff with sufficient depth of knowledge to recognise problems and look into them. Furthermore, the extra vigilance needed may require special efforts of organisation and leadership.

Feedback, iteration and monitoring

Iteration is normal in operational readiness work. In the simplest case when modifying a system, 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.

As well as defining and achieving 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.

With respect to plant ageing, iteration can be planned in the form of periodic readiness reviews. 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 development and adoption of KETs, appears to be highly reliant on feedback within and between basic scientific research, technical standards, production/process, the supply chain, regulators, and customers. However, iteration depends on the free flow of new knowledge. IP rights, commercial secrecy and the ordinary inefficiency of institutional communication may all present obstacles to this flow. In this respect, even the three pillars envisaged by the EC High level group of experts on KETs (EC, 2011) have the potential to become three silos.

Investing enough effort in operational readiness

It is easy to say that the effort one puts into an operational readiness process (like modifying a system) 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.

Scaling by risk is one approach, but this can be complicated by numerous factors. For example, as noted in UKOOA, 1999:

- 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.

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

In the case of ageing plants, it may be hard to make the case for investing lots of effort in legacy plant unless the business case is particularly compelling. In the case of the Airbus A320, the business case was very compelling and a 25-year design service life has been extended by 10-20 years (Flight Global, 2008).

Here, the UKOOA argument about uncertainty may offer a more viable way of scaling. Wintles et al (2006; vii) makes the point that "…ageing is not about how old the equipment is, but is about what is known about its condition". In the airbus case, the company developed new fatigue tests and applied them on sections of real aircraft built for the purpose. Perhaps the uncertainty about plant condition could be developed as a metric for scaling operational readiness work?

In the case of KETs, the risks and their controls may have large uncertainties, strong stakeholder views, novel design etc. All of these justify a large expenditure of effort.

Application of operational readiness in Aviation and in the process industries

This section gives an account of the context surrounding the recent application of operational readiness, and introduces the arguments for its relevance to plant ageing and KETs.

Operational readiness applied in aviation

Aviation has an enviable reputation for 'ultra-safety'. To some extent this reflects the quality of the engineered parts of the system, the obedience to rules of operational staff, and the nature of aviation regulation and standards. However these still leave an envelope of operational freedom in which airlines innovate new ways to use their assets and provide their services. As noted by Franke (2007) and illustrated by Nicolau and Santa-María (2012), innovation is linked to the commercial success of airlines[6]. By its nature, innovation will find new configurations of equipment, tasks and operating conditions, some of which have not been foreseen by the makers of aircraft or givers of aviation rules. Therefore, the safety of aviation operations cannot be wholly delivered by prescriptive rules and conformity, but also by the management of change.

In 2014, new regulations[7] came into force in Europe. These regulations required airlines, and other parties in the industry, to formalise their arrangements for managing safety. This included arrangements to ensure compliance with regulations, conformity to technical standards and also for managing change.

As part of their preparation to comply with these regulations, a large European airline has looked into how to integrate the safety management arrangements specified by the regulations into its general management structures and processes. One aspect of this is the management of change, for which the airline was keen to devise a process that achieved the highest level of safety, operational excellence and commercial performance.

There is nothing new about integrating safety, operational goals and commercial performance. However, well-established theoretical treatments such as ALARP are more often applied in retrospect than as a means to guide the management of change. The question was how to achieve the balancing implied in ALARP in a practical way that could be made to work in the diverse settings of an airline. For example, among the cases to which the airline applied operational readiness are: engine testing, aircraft taxiing, passenger electronic devices, use of defibrillators, setting-up a new base of operation, changing how baggage is loaded into aircraft holds, and new methods for de-icing aircraft.

The EASA regulations gave important impetus to the work described here, but the airline's concern with managing safety risks preceded it. The work began with methodological questions about assessment of safety risks: how should it be done, when and by whom? Three points became clear quite quickly:

1. There is more to informing decisions about risks than risk analysis;
2. Decisions must be reconsidered in the light of monitoring data, throughout the life of the operation;
3. As well as triggers from monitoring systems, proactive decisions about risks were in general prompted by two types of situation: when planning changes to operations, and when undertaking planned reviews of operations.

Taking the first of those, the UKOOA risk decision making model (UKOOA, 1999; Aven et al, 2007) shows how the context of the decision greatly influences the importance of risk analysis in informing the decision. Furthermore, the UKOOA model underlines the involvement of various stakeholders, and the need for decisions about risks to be integrated with decision-making in general. It is worth noting that figure 8 of UKOOA (1999; p.20), was found to be very helpful in swiftly communicating quite complex ideas to a very diverse group of stakeholders—including, amongst others, engineers, pilots, ground staff, and members of cabin crew.

[6] In a recent interview (11 February 2016) with the Swiss newspaper Tages-Anzeiger, Carolyn McCall, the CEO of easyJet, mentioned the importance of innovations (including technological innovations such as fast baggage changes, and use of mobile technology) to the airline's commercial performance.

[7] There a number of regulatory documents, but of particular relevance is the 'Acceptable Means of Compliance' published by the European Aviation Safety Agency.

The second point—that risk decision-making should be responsive to monitoring data—made it clear that risk decision-making is cyclic and not a one-off activity.

As the airline had already identified change management as a priority, this became the focus for developing an operational readiness procedure. An airline is a diverse business, and one of the issues about change management was that it was called many different things depending on its scale and which department was leading it. If the change entailed relatively large resources, it was typically subject to the company's project management processes. However, most changes were not subject to this. One of the advantages of developing an operational readiness procedure has been to bring consistency to the myriad ways in which changes are made to operations.

The operational readiness procedure was based on the model of change management shown below in Figure 1. The work progressed along two lines: one was development of a computer supported workflow and the other was development of the detailed change management process.

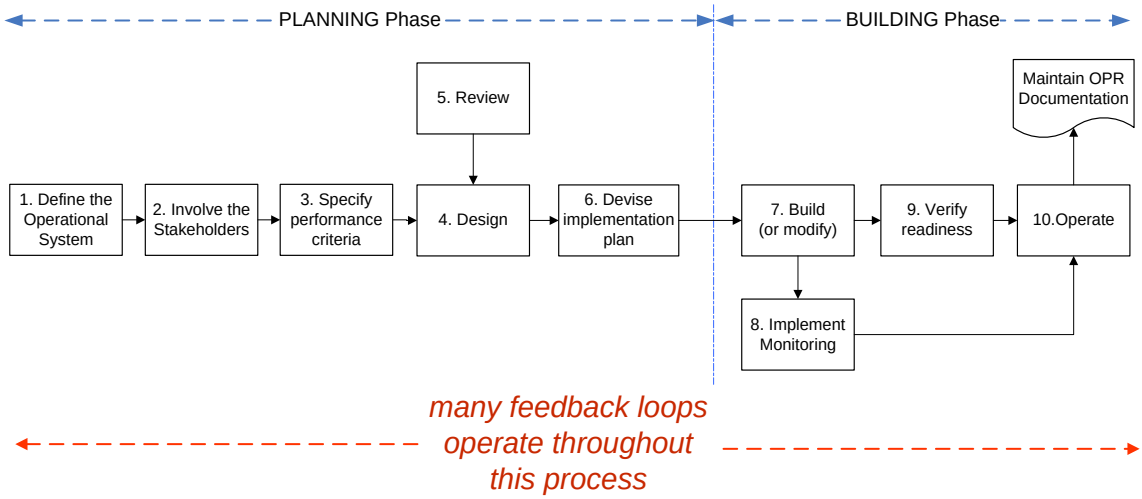

Figure 1. Generic process for operational readiness (reproduced from Frei et al. 2015)

The operational readiness procedure was written in two stages. First, an outline process was created from the sketchy information found in published sources (chiefly Nertney et al., 1975; Bullock, 1976; and, Nertney, 1987). The authors (Frei and Kingston) were able to supplement these by drawing on experience gained as PhD researchers working with Nertney and his co-workers.

The second stage was to identify the tasks subsumed in the outline process. In effect this involved expanding the 10-steps of Figure 1 to reveal the criteria that a generic operational readiness procedure would need to satisfy. This step produced about 200 criteria.

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, further effort was invested to identify the principles on which the criterion relied. In this way, a set of general twelve principles for operational readiness were identified. These are discussed further in Section 3.

Operational readiness applied to plant ageing in the process industry

Horrocks et al (2009) and Hokstad et al (2010) identify loss of knowledge as an issue. Reducing uncertainty by mobilising knowledge is a dominant theme in Operational readiness.

Ageing plants are associated with degradation mechanisms such as wear, fatigue, corrosion and erosion. Horrocks et al. (2010) noted that these mechanisms resulted in half of the 96 European major hazard 'loss of containment' events reported (in the MARS database) between 1980 and 2006. The life-span of a plant ends in a predominantly economic trade off: whether to continue or to invest in a new plant. Increased maintenance cost might well be acceptable from a business point of view. The question is how to maintain acceptable safety performance throughout the lifecycle of a plant, whether extended or not.

The business case, and constituent safety case, for extended life is based on the known and monitored degradation mechanisms of the plant. However, plant ageing may be accompanied by other, latent safety risks. Latent risks are manifested through poorly understood or unknown degradation mechanisms. Furthermore, these latent risks may be compounded by other non-technical changes that further obscure them from detection and treatment. In this paper, we focus on the non-technical factors noted by Horrocks (2010; page 98):

- procedures—both operational process procedures and management of change procedures;
- operational knowledge of plant and equipment;
- risk review throughout the lifecycle of the plant.

An increased incident rate in such an installation may indicate that maintenance according to the prevailing model of the plant, is no longer viable as the means to ensure safe operations. We argue that maintenance can offer a greater level of risk management and business performance, but only if it is embedded in an operational readiness philosophy.

Operational readiness and Key Enabling/Emerging Technologies

Plant Ageing and KETs may seem at first sight to be rather mismatched concepts. However, underlying both is the issue of reducing uncertainty by mobilising knowledge. In respect of KETs, according to EC (2009 and 2011) mobilising knowledge is the critical factor in safely exploiting these new technologies. In the final analysis, operational readiness is about mobilising knowledge efficiently. This reduces uncertainty in the design process and allows risks to be recognised early with the greatest opportunity for the most safety at least cost.

In contrast to plant ageing, the challenges of KETs are focussed, at first sight at least, at the beginning of the plant lifecycle. According to the European Commission (2009), KETs include[8]:

- Nanotechnology;
- Micro- and nanoelectronics, including semiconductors;
- Photonics;
- Advanced materials; and,
- Biotechnology.

The European Commission has identified these as priority areas for improving European industrial competitiveness. However, embracing these new technologies will require management of their commercial, safety, and environmental risks. Furthermore, in respect of safety and environment, public acceptance of these technologies is likely to hinge on the perceived effectiveness of risk management (PEROSH, 2015).

The novel context of KETs clearly presents a challenge to design and management. The Commission paper cited earlier recognises knowledge and knowledge transfer as a crucial element in this. In this paper we consider how these challenges might be approached using operational readiness concepts.

Cross-sectoral lessons from applying operational readiness to manage change in an airline

The subsections that follow describe the main principles of operational readiness and the lessons they contain for managing plant ageing and embracing KETs.

The lessons presented below have two themes: change and decision-making. Within the operational readiness philosophy, operational systems—such as air transport or process plants—are treated as dynamic and constantly in flux throughout their lifecycle. Readiness is time-bound with respect to both the definition of readiness for a given system, and the actual state of readiness of the system. The definition of requirements, and how they are fulfilled by a design, is treated as provisional.

Whereas project management stops on implementation, readiness entails active open-ended vigilance to changes in requirements, good practices and technology. This is not to say that all opportunities to upgrade ageing plant must be taken, but it is to say that they should be decided upon and kept subject to future review.

In the case of KETs, at a recent conference (Planned Adaptive Regulation, UCL, January 2016; *conference proceedings are in preparation*) it was clear that this principle is of particular relevance. Given the uncertainty that is definitive to KETs, monitoring must be as good as possible. And, for the same reason, the definition of readiness is subject to rapid evolution: forcing consideration of how to make current methods of defining laws and technical standards more responsive.

Whether in the rapid evolution of KETs, or in the more gradual incremental ‘career’ of a process plant, the only thing that doesn’t change is change itself.

Stakeholders’ awareness of operational modes and a lifecycle perspective

In operational readiness, the lifecycle concept is used in two ways. The first is that that design requirements are specified for the whole lifecycle from development through to disposal. The second is that at any time, the lifecycle can revert to an earlier phase for a part or the whole system. To put it another way, modifications should be made within the discipline of a design context, and not outside of it.

The other aspect here is the deliberate identification of off-normal modes that the system may occupy in its lifecycle. Accommodating these modes will add to the resilience of the system. What these modes actually equate to depends on the

[8] There is no consensus as to what constitutes a KET. The European Commission (2009) uses the phrase ‘Key Enabling Technologies’, Whereas the OECD talks about ‘Key Emerging Technologies’. The OECD appears to place KETs in a context that overlaps with that discussed by the Commission but is wider. For example, the OECD (2012) includes food, drinking water, housing and forest resources in list of emerging fields of research in science, technology and innovation (STI). Porcari and Mantovani (2015) use the term enabling/emerging, which we have adopted for this paper.

specifics of the system, but will include modes such as maintenance, extended life, and permitted deviation from normal operations[9]. An example can be found in the Rail Safety and Standards Board, 2004.

The widespread extension of plant life, and of service life of aircraft such as the A320, suggest that extended life should be a routine consideration in design. In the case of KETs, uncertainty at the design stage means that regular reviews will be needed to update the lifecycle assumptions.

A dynamic view of stakeholders and relationships

Freeman (2010) defines a stakeholder as "…any group or individual who can affect, or is affected by, the achievement of a corporation's purpose." 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. However, 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.

In respect to ageing, some of the stakeholders will change or simply disappear. For example a component manufacturer or a works union. Even if the stakeholder still exists after 20 years, the relationship to the plant may have changed, they may have more or less effect on the plant or the plant may have more or less effect on them. The upshot of this is that maintaining stakeholder relationships is a dynamic and open-ended task.

Concerning KETs, Porcari and Mantovani (2015) note that the well-established stakeholder dialogue on nanotechnology represents an exemplary instance of responsible and ethical development. They point out that this "helped to smooth out controversial positions".

The 'sweet spot' between safety performance, operational performance and commercial goals is a moving target

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, this principle of balance applies both to the state and to the process of operational readiness.

The risks entailed by a particular design option may affect operational, commercial or safety goals. 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 2, 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)".

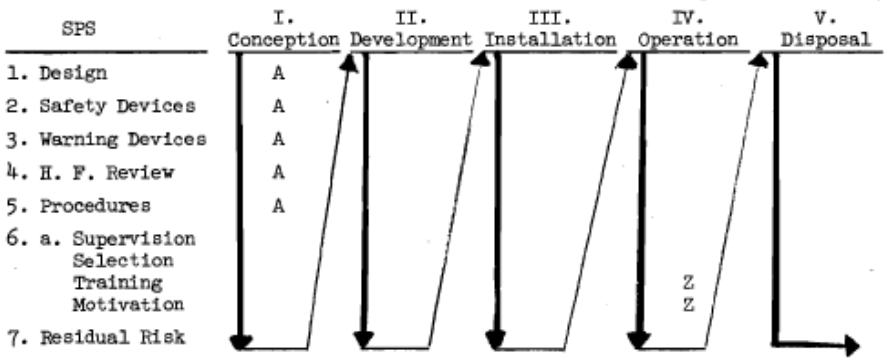

Figure2. "Sequential Relation of the Safety Precedence Sequence" (Reproduced from Johnson, 1973)

In the case of ageing plant the balance of safety, operational performance and commercial goals must still be maintained. However, market volatility (the oil price is a salutary example) may make it very difficult to stay balanced. Another challenge is the availability of the goals as stated at the time of initial design: businesses may find themselves making poor or risky choices simply through ignorance of the original design intent and assumptions.

[9] In the UK railways, a permitted deviation is generally referred to as an *amended mode*.

Knowledge about the system operational system has its own dynamics

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 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; p.13) 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".

Although the 'design paradox' cannot be wholly cheated, it can be managed. The assumption in operational readiness is that, in most cases, some portion of the knowledge missing from the early stages might actually be available, although hard to access. The operational readiness philosophy is in large part about mobilising knowledge.

A serious issue in plant ageing is the diminution of the available fund of knowledge about the plant. If coupled with poor quality or inaccessible documentation; design work, monitoring and maintenance are very likely to become inefficient and prone to knowledge based errors.

For KETs, the argument was made earlier about staffing with 'over-competent' operators. In well-understood, mature technologies, technical standards and education provide an agreed system for knowledge sharing. However, emerging technologies often evolve too fast for such systems to keep pace. Therefore, knowledge sharing between production systems, scientists and regulators requires extra resources and special attention.

Corporate memory: conserve knowledge of the system and the logic behind decisions

Frei et al (2015) call this the Kletz principle, in testimony to Trevor Kletz's life-long exhortations to excellent documentation. For example, Kletz (1993) gives the 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." He also looked at this from the other end of the communication: "Never remove equipment before you know why it was installed. Never abandon a procedure before you know why it was adopted." (Ibid, p21-22)

In the airline project, the importance of documentation was well appreciated, and the majority of the project budget was invested in creating a system that supported the creation and retrieval of documents. Partly this was to avoid corporate amnesia, but mostly it was to make it easy for people to document design choices well. It was also noted that contemporaneous accounts of risk decisions are more convincing to regulators, and also in courts should the risks manifest as an accident.

Schön (1971) recognised that organisations succeed better at documenting their operating processes, than they are at documenting how they transform their systems. He noted that if the logic 'behind these transformations' is only partly known, it is difficult to learn from operational experiences. 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.

In terms of plant ageing, the older the plant, the less implicit knowledge is left by staff turnover. By making as much knowledge explicit, readable and completely shareable, the logic behind the design assumptions can be preserved.

Contract boundaries imposed on a technical system tend to inhibit the flow of knowledge in an operation. This could be argued of the railways after privatisation. This is true of all phases, but in KETs, it is especially pertinent in the design and development phases. This may be a limiting factor in the rapid learning needed by organisations exploiting KETs.

Mobilising knowledge: experts know more than they can tell

Operational readiness needs to involve experts in a way that allows them to apply their tacit knowledge as well as their explicit knowledge. Tacit knowledge is the portion of knowledge that we don't know that we have until engaging with a problem or making a decision. Given what has already been said about the centrality of mobilising knowledge, the mode and extent of expert involvement is a critical issue. It is noted that the benefits of expertise can only be fully realised in an environment that supports the open and honest expression of views.

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 (arguably, should have) an active role and come 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'.

One of the issues for plant ageing is the thinning out of expertise, especially when one recognises continuity and experience as sources of expertise. KETs will entail a similar problem, but from the other direction.

When analysis stops, all else is hunch

The subsections above underline the topics of retaining and communicating knowledge, but operational readiness also considers how knowledge is applied.

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 earlier points about iteration and change apply here; analyses are approximate and provisional—they are useful, but they are not 'the truth'.

A recent salutary example in aviation was the group of lithium battery fires onboard a number of Boeing 787 aircraft. The NTSB report into one of these concluded that neither Boeing or the FAA went far enough in their analysis of the new battery. "Boeing's electrical power system safety assessment did not consider the most severe effects of a cell internal short circuit and include requirements to mitigate related risks, and the review of the assessment by Boeing authorized representatives and Federal Aviation Administration certification engineers did not reveal this deficiency." (NTSB, 2014).

The various parties involved in developing KETs, need analyses to demonstrate due diligence to stakeholders, and to get the technology as close to right first time as possible. However, the bind for regulators is that few if any analyses can provide certainty.

Risks to be decided on by the right people in the right way

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. The decision to assume a risk, 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".

However, accountability and duty both depend on the decision maker 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.

Given the diminution of knowledge in an ageing plant, responsible risk decision-making has clear implications for knowledge and for competence. Horrocks' recommendation for risk review throughout the lifecycle of the plant depend on this principle and the others set out earlier.

Concerning KETs, it is noted that the intrinsic uncertainty of the technology makes sound decisions about risks a particular social and scientific challenge. There is also the possibility that a jurisdiction that hasn't the appetite for this challenge may in effect transfer the risk to a jurisdiction that has, irrespective of its competence.

Future application of operational readiness to managing plant ageing and embracing KETs

Newer plants can adopt the operational readiness philosophy into their management of change, but there is also scope for older plants to apply the principles by conducting readiness reviews. In the airline project, operational readiness reviews were seen as a way to assess legacy systems in terms of current standards. The purpose is to allow comparison between the performance characteristics of an existing system and the current state of the art. If a business case supports it, the review might result in modifications to upgrade one or more aspects of the operation into line with current standards. Alternatively, management might opt just to monitor the gap between the unmodified elements of the current system and the performance that would be expected if the improvements were made.

Readiness reviews might prove valuable for ageing process plants for another reason. The practicalities of review require that documentation of the system be gathered together and put into good order (e.g. paper documents digitised, scattered documents brought into one archive and indexed). However, in some cases, documentation will be incomplete, and some aspects of the system design and development history missing. A readiness review is an opportunity for the current cohort of staff to learn about the operational system, to discover the rationale behind its design, and to challenge it where needed. This may be a means of restoring the missing knowledge noted by the Horrocks et al, and Hokstad et al, studies.

The periods between readiness reviews of a given system are determined by a range of factors. However, the usual expectation will be for periods greater than one year. Current monitoring of installations with annual targets covers only a short time span. Assessing ageing problems requires information to be gathered by installation rather than by type of data. It is noted that one year will generally be too short a time period to reveal the dynamics of the system.

For KETs, the 'knowledge mobilising' philosophy of operational readiness is the chief attraction. It may provide ways to manage the design paradox, speeding development. As noted by PEROSH (2015) Prevention through design (PtD) can avoid safety hazards by design. Operational readiness provides a set of principles on which to base PtD. It also allows a wide gamut of risks to be considered, not only those to safety.

For KETs, for ageing plants and for operations that are neither of these, operational readiness represents a scalable approach to integrating safety with operational and commercial decision making. What are needed now are case study demonstrations of how it works in variety of settings, and under what conditions it delivers benefits.

References

Aven, T., Vinnem, J.E., and Wiencke, H.S. (2007) A decision framework for risk management, with application to the offshore oil and gas industry. Reliability Engineering and System Safety, 92 (2007); 433–448.

Bullock, M.G. (1979) Work Process Control Guide. DOE 76-45/15, SSDC-15

CCPS. Guidelines for Risk Based Process Safety. John Wiley & Sons and Center for Chemical Process Safety, Hoboken, New Jersey, 1st edition, 2007.

European Aviation Safety Agency (2014) "Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Part-ORO (Consolidated version)". Issue 2, 24 April 2014.

European Commission (2009) Preparing for our future: Developing a common strategy for key enabling technologies in the EU. COM(2009) 512 final.

Frei, R., Garforth, A., Kingston, J., and Pegram, J. (2015) Using Operational Readiness to improve the Management of Risk. Noordwijk Risk Initiative Foundation, The Netherlands.

European Commission (2011) High Level Expert Group on Key Enabling Technologies: Final report. June, 2011.

Flight Global (2008) Airbus begins tests to extend service life of A320 family. January, 2008.

Franke, M. (2007). Innovation: The winning formula to regain profitability in aviation? Journal of Air Transport Management 13 (2007) 23–30.

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

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

Hokstad, P., Håbrekke, S., Johnsen, R.., and Sangesland, S. (2010) Ageing and life extension for offshore facilities in general and specific systems. SINTEF, A15322, 19 March 2010.

Horrocks, P., Mansfield, D., Thomson, J., Parker, K., and Winter, P. (2010) Plant Ageing Study – Phase 1 Report, ESR/D0010909/003/Issue2. A report prepared for the Health and Safety Executive, 27th February 2009.

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.

Lindhout, P., Kingston-Howlett, J. and Ale, B.J.M. (2009) Controlled readability of Seveso II company safety documents, introduction of a new KPI, Safety Science 48(2010) 734-746.

Lindhout, P., Kingston-Howlett, J. (2011) Language issues, an underestimated safety risk. Loss Prevention Bulletin, 218, 26-30, April 2011.

National Transportation Safety Board (2014) Aircraft Incident Report: Auxiliary Power Unit Battery Fire Japan Airlines Boeing 787-8, JA829J, Boston, Massachusetts, January 7, 2013. NTSB/AIR-14/01, PB2014-108867, Notation 8604, Adopted November 21, 2014.

Nertney, R.J., Clark, J.L., and Eicher, R.W. (1975) Occupancy-Use Readiness Manual –Safety Considerations. ERDA-76-45-1, SSDC-1, UC-41.

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

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

Nicolau, J.L., and Santa-María, M.J. (2012) Gauging innovation worth for airlines. Journal of Air Transport Management 20 (2012) 9-11.

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

PEROSH (2015) Position Paper 2, Leadership in enabling and industrial technologies: Prevention through Design. Partnership for European Research in Occupational Safety and Health.

Porcari, A., Mantovani E., (2015) Ethics assessment in emerging technologies: the case of nanotechnologies, a report of the Satori Project, June 2015. Italian Association for Industrial Research (AIRI)

OECD (2012) Policies for Emerging Technologies. [extract available] In OECD (2012), OECD Science, Technology and Industry Outlook 2012, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/sti_outlook-2012-en

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

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

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

UKOOA (1999) ‘‘A framework for risk related decision support: industry guidelines.’’ United Kingdom Offshore Operators Association.

US Department of Defense (1964). Annual Report of the Office of Civil Defense. Office of the Secretary of the Army.

US 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.

Wintle, J., Moore, P., Henry, N., Smalley, S., and Amphlett, G. (2006). Plant ageing, Management of equipment containing hazardous fluids or pressure. HSE Research Report RR509, HSE Books, 2006