Process Contracting Limited

Human Factors Consultancy

The process-based approach to assurance of operability and safety

The use of the HS model in safety assurance

PCL/WP2

Sept 2001

Brian Sherwood Jones & Jonathan Earthy (Lloyd's Register of Shipping)

Process Contracting Limited
www.processforusability.co.uk
☎01292 678598 mobile 07932 750487
brian@sherwood-jones.sol.co.uk
Registered Office: 6 Burgh Rd., Prestwick, Ayrshire, KA9 1QU
Registered in Scotland No SC 191175 VAT Registration No. 724 2067 58

Summary

This paper explores the use of the Human-System process (HS) model in managing the human-related risk in complex systems. The HS model is a proposed ISO Publicly Available Specification (PAS) [ISO PAS tba:2002] A specification for the process assessment of human-system issues. It presents a view of the system life cycle with an emphasis on the identification and handling of issues related to people (users and other stakeholders). The model is focused on system acquisition and operation but includes processes related to Human Resources (e.g. selection and training). It is intended for use in process assessment and improvement, but could also support planning and the assessment of competence. A process assessment approach to IEC 61508 [IEC 61508:1998] has been proposed for software-related processes [Benediktsson *et al* 2001], and is recommended here as a validated means of assessing organisational capability to deliver systems in a user-centred manner. The relationship between the processes in the HS model and those required by Health and Safety is discussed. The HS model is also proposed as a means of addressing compliance with Regulations across sectors in a consistent way.

The paper is one of a series of white papers; the aim is to set out topics that have received considerable discussion within a small group where it is considered that a wider distribution would be useful. As such, the material is not speculative, but it is recognised that it sets out to be controversial. In the case of this paper, it is considered that the process-based approach offers a significant opportunity to safety assurance; advocacy of this approach is not intended to imply that the other approaches contrasted are inadequate.

Part of the authors' work was carried out under projects for the European Commission and the UK Ministry of Defence. The support of these bodies is gratefully acknowledged. The opinions expressed in this paper are the authors' own and not those of Lloyd's Register.

Authors Brian Sherwood Jones (Process) Jonathan Earthy (Lloyd's Register of Shipping)
Date: Sept 01
Version Number.v1

Version history

Sept 01 - New Document issued

1. Introduction

This paper describes recent work on process-based approaches to assurance of system properties (including but not exclusively, safety) and situates these approaches in the context of safety assurance. The thesis is that process-based approaches have a key role (but not an exclusive one) in providing assurance of safety-related or safety-critical systems.

The focus is on the human-related risk in complex systems. A system is considered as a work system, rather than a piece of equipment. ISO 6385 [ISO 6385:1981] defines a work system as *"a combination of people and working equipment, acting together in the work process, to perform the work task, at the work space, in the work environment, under the conditions imposed by the work task"*. From this point of view the authors contend that human-related risks are the major system risks. The paper has a strong emphasis on the need to integrate assurance of human-system (HS) issues with other engineering activities.

The aim of the work discussed is to achieve 'quality in use', colloquially referred to in this paper as operability. Quality in use is defined [ISO 9126:2000] as *"the capability of a system to enable specified users to achieve specified goals with effectiveness, productivity, safety and satisfaction in specified contexts of use."*

The paper discusses the nature of safety assurance, the types of indicator that might be used, and their strengths and weaknesses. In particular, indicators are examined with respect to the extent to which they are lead indicators, i.e. they predict problems, as opposed to a lagged indicator, where we are wise after the event.

The basics of the process-based approach are then described, with an outline of its potential role in safety assurance. The scope and nature of a process model to encompass human-system (HS) issues is presented, together with the background in process-based developments in system and software engineering and their application to safety-critical systems.

Process-based approaches are then discussed in relation to other types of indicator that are used in safety assurance.

The paper draws conclusions concerning the use of a process-based approach. In particular, it concludes that a process-base approach has the potential to become the mainstream approach to safety assurance as regards human aspects of systems (and possibly for all aspects, though this goes beyond the scope of the paper).

2. Safety assurance as prediction

Turner [Turner 1978] was one of the first to try and identify indicators that might predict man-made disasters. He proposed the idea of an 'incubation period' prior to a disaster, and that the characteristics of an incubation period could be identified. The identification of the characteristics of potential disaster, or likely success, has occupied many minds since.

Lead (rather than lagged) indicators are vital to safety assurance. A range of diverse indicators will probably always be required. Some candidate indicators are:

- The 'three P's' of Product, Performance and Process characteristics,
- Compliance with Regulations,
- The extent to which best practice methods are being followed,
- Organisational characteristics such as safety culture,
- The vigour (and rigour) of risk management,
- The quality of design decision making.

The merits of process over the other P's of product and performance are clear. Specification and assurance of product characteristics will always lag behind new technology, cannot consider system-level effects beyond the item of equipment, and are sensitive to the context of use. Performance is inevitably a lagged indicator. Compliance with Regulations is clearly necessary, but offers no assurance of being sufficient. Furthermore, the move to open-textured Regulation makes assurance more judgmental. The other indicators listed above are widely used in day to day project working, but present difficulties in providing assurance.

3. The process-based approach and its potential

The attraction of a process-based approach to safety assurance lies in the potential for lead indicators. The work (led by the software community) on defining process in a way that can be measured can enable this potential to be realised. This section describes the process-base approach and summarises the Human-System (HS) model (being developed as ISO PAS tba *A specification for the process assessment of human-system issues* (ISO PAS 'HS')). It then discusses the scope of the HS model in relation to the demands of safety assurance for human-related risks.

3.1 The process-based approach

Processes are defined at the level of what is done to develop and operate a system. They are specified through methods, techniques, work instructions, etc. A process has a purpose and fulfils a business requirement. A technical or management task that contributes to the creation of the output (work products) of a process or enhances the capability of a process is called an activity or a practice. The elements of the format used to describe processes in ISO 15504 [ISO TR 15504:1998-2] are listed in Table 1. These have been followed in ISO TR 18529 *Human-centred lifecycle process descriptions* [ISO TR 18529:2000] and in ISO PAS 'HS' [ISO PAS tba:2002].

Name	Description of component
Process number	For precise reference
Process name	Summary of the process
Purpose of process	What is done by the process
Outcome	Why it is done, the result of successful application of a process
Practices	What is done to fulfil the purpose
Practice number	For precise reference
Practice name	Summary of the practice
Description of practice	What task is performed
Work products	The items used and produced by the process including the following: pieces of information, documents, hardware, software, training courses, awareness in individuals.

Table 1: the components of a process have precise definitions in ISO 15504 to enable rigorous assessment

A disciplined evaluation of an organisation's processes against a model is called process assessment. Process assessments generally focus on identifying improvement priorities (i.e. a formative evaluation). Action taken to change an organisation's processes so that they meet the organisation's business needs and achieve its business goals more effectively is called process improvement.

Process assessment seeks firstly to establish whether processes are performed successfully and secondly the degree to which processes are under control. A process assessment examines the evidence for the performance of practices and the existence and quality of work products. Process attributes are features of a process that can be evaluated, providing a measure of capability in doing the process. However, the final decision as to the degree of performance of a project is based on the degree to which the outcomes are achieved.

A capability scale (an ordinal scale of types of control) is used in this assessment. Table 2 describes the six-level ISO 15504 capability scale.

Level	Description
0	No achievement of results from a processes or processes
1	Performance in an *ad hoc* manner
2	Monitoring of time and product quality
3	Use of defined corporate procedures and infrastructure
4	Use of statistical control
5	Optimisation of each process to meet current and future business needs

Table 2: Capability levels in ISO TR 15504 *Software Process Assessment* are used to describe how well processes are performed

3.2 The HS Model

The HS model [ISO PAS tba:2002] comprises 3+1 processes that address issues associated with people through the system lifecycle. The expectation in the (very wide) community that developed the standard is that assessments are likely to focus on the level 0-1 capability distinction. The processes are described in Table 3. The relationship between the processes and their sub-processes is outlined in Figure 1.

HS.1 Life cycle involvement.
This process anticipates the particular HS issues at specific stages of the life cycle. It makes the system life cycle efficient by addressing people in the stage enabling systems for the system. Its is to consider the interests and needs of the individuals and/or groups that will work with the system. It is achieved through performance of five sub-processes which are in general grouped according to the example stages provided in Annex B of ISO CD 15288 [ISO CD 15288]. However, in order to create meaningful groups of HS activities the utilisation stage is split between the early stages (installation and transition to use) and the mainstream use of the system (operation and support of the system).
HS.2 Integrate human factors.
This process ensures that HS issues are addressed by the appropriate stakeholders. It reduces life cycle costs by ensuring that design for people is used within the organisation. The purpose of the Integrate human factors process is the satisfactory deployment of human-system processes for a system. It is achieved through performance of eight sub-processes.
HS.3 Human-centred design.
This process enables user centred technical activity to be focused appropriately. It contributes to a better system by designing for people who use the system of interest in its context of use. The purpose of the Human-centred design process is to apply HS processes and HF data as appropriate in order to ensure the usability of the system throughout its life cycle. It is achieved through performance of four sub-processes.
HS.4 Human resources.
This process provides the means to resolve issues by means of the human part of the system, rather than the equipment-centred part. It ensures the continued delivery of the correct number of competent people required to use the most suitable equipment. The purpose of the Human resources process is for usability to be achieved in the most timely and cost-effective manner by provision of the correct number of competent users. It is achieved through performance of four sub-processes.

Table 3: The HS model has four processes. The first addresses the needs of the lifecycle. The second addresses the various interfaces to the organisation. The third comprises the iterative technical cycle, and the fourth addresses the timely delivery of trained operators.

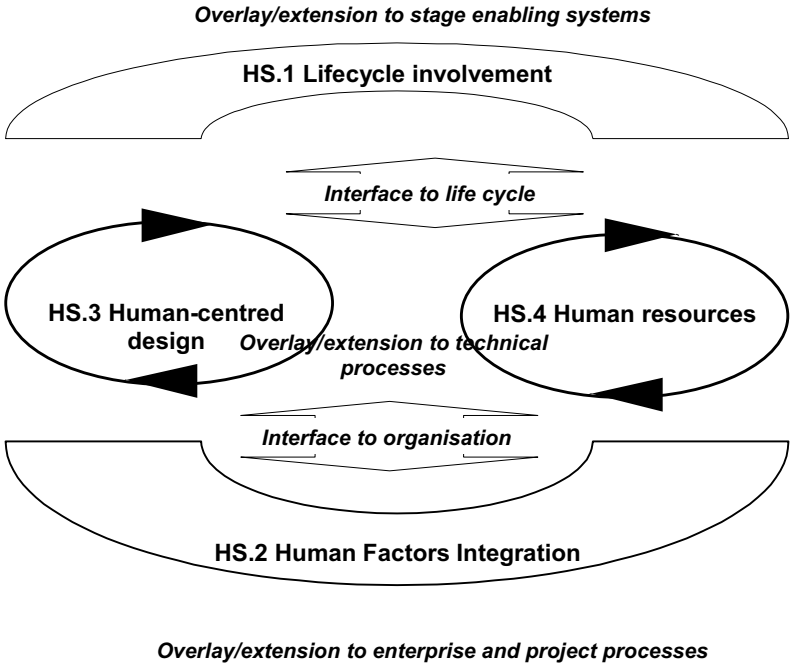

Figure 1 Process HS.1 manages the interface between the technical processes and the lifecycle, while HS.2 manages the interface to stakeholders.

3.3 The scope of assurance required for HS issues

The scope of work necessary to prevent human error is characterised by its breadth, embracing the safety management systems of both supply and operation organisations, and coverage of the whole work system. For example, the HSE framework [HS(G) 65: 1991], [HSG48: 1999] for setting (and presumably assessing) performance standards covers organisational factors, job factors and personal factors (where job factors include plant and substances, procedures and the premises). This breadth of coverage, where (for example) the whole process of equipment design is a sub-sub-set, brings problems of complexity and scale to any attempt to describe the processes involved. Indeed, minimising complexity and scale was perhaps the major issue confronting the development of the HS model. In that work, the area that was found to be the least well-developed was the human resources area; there was considerable background work relating to "putting the machine in front of the user" but much less of relevance to describe "putting the user in front of the machine".

The nature of activity to prevent human error is frequently seen as the province of ergonomics specialists. It is currently the case that the enumeration of human error potential requires deep skills possessed by a small group of specialists. However, the scope of human error mitigation activity demands that it cannot be a specialist activity. One of the characteristics of recent process-based work such as ISO PAS 'HS' is that it has removed specialist "push" from the description of the scene, and has concentrated on the outcomes to be achieved. The development of a process model that can be used for rigorous assessment has also demonstrated that the "soft, fuzzy" attribution given to user-centred design is no longer valid (or rather is no more valid than for any other branch of engineering).

4. Process in the context of safety assurance

The sections below situate process indicators in the context of other (possibly more established) indicators used for safety assurance. The intention is to identify the role that could be played by each.

4.1 Process and methodology

The 1980's saw the development of many heavyweight methodologies for software development, human factors, and for system engineering. These have since been found to pose difficulties in practical implementation. They require tailoring, but provide no guidance as to what constitutes satisfactory tailoring as opposed to non-compliance, and still posed significant cost penalties.

Since then there have been two developments. The first, the development of lightweight methodologies, such as eXtreme Programming, poses the risk of "hack and hope", and is not appropriate to safety-critical systems. The other development has been the rise of 'process' rather than method. The aspiration of the process-based approach has been to offer flexibility in application and brevity in description whilst still providing rigour in the assessment of outcome or activity.

The arrival (or imminent arrival) of process-based standards offering rigorous assessment for system engineering, software engineering and operability offers the safety community the potential for a more integrated approach. Some promising investigations in this area have already been undertaken. [Benediktsson *et al* 2001] have proposed a correspondence between the safety integrity levels (SILs) of IEC 61508 and the capability levels (CLs) of ISO 15504, (both built on ISO/IEC 12207 *Software lifecycle processes*). They considered the ISO 15504 reference model to be an appropriate framework for assessing safety critical software processes, and provided empirical support for this based on the SPICE trials. The reference model of ISO 15504 provides a way to define and assess *what* is to be achieved. IEC 61508 describes the what but also the *how*. Benediktsson *et al* showed that the greater demands of higher SIL levels can be expressed as higher levels of process capability. An assessment model at the 'how' level of safety aspects of systems would be both possible and necessary and would enable safety to be considered in line with other aspects of systems and software. The benefits to be obtained are considerable and are mostly concerned with reducing cost. The use of a process-based approach would:

- Allow safety to take advantage of Off The Shelf (OTS) assessment methods, tools etc.
- Permit integration with other assessments, including assessment of human-system issues, system engineering processes and software engineering processes.
- Provide an OTS framework for Process Improvement.
- (Arguably) provide a more systematic and rigorous approach to assessment.

From an operability point of view, the ability to draw on ISO 15288 for system engineering aspects and ISO PAS 'HS' would solve the ongoing discussions about whether people are part of the system, and would enable coverage of the full work system - particularly where software cost avoidance has moved safety criticality from equipment to people.

In brief, the potential for the process-based approach to underpin both project execution and safety assurance (of both technical and human-system issues) offers the benefits of simplicity and lower cost.

4.2 Process and lifecycle

Processes should not be confused with the stages of a lifecycle. Processes are enacted at more than one stage in the lifecycle, and it may be useful to think of them as essentially continuous through the lifecycle. In particular, the life cycle processes in ISO PAS 'HS' have a role throughout the system life cycle. At each life cycle stage, it is necessary to look ahead to future stages ("how will we deal with disposal?"), and to check that the requirements and constraints generated by previous stages have been met ("is the original concept still valid?"). This is shown in Figure 2 below.

Stakeholder	**HS1 Lifecycle involvement process; Human-System Issues in ..**				
	HS1.1 Concept	HS1.2 Development	HS1.3 Production and Utilization	HS1.4 Utilization and Support	HS1.5 Retirement
Conceiver	Needs, Concepts, Feasibility	Consistency, Viability	Consistency, Viability	Consistency, Viability	Consistency, Viability
Developer	Compatibility Feasibility	Engineering, Solutions, Practicability	Consistency, Viability	Consistency, Viability	Consistency, Viability
Deliverer (HR, trainer)	Compatibility Feasibility	Compatibility Feasibility	Manufacture, Roll-out, Installation	Consistency, Viability	Consistency, Viability
User	Compatibility Feasibility	Compatibility Feasibility	Compatibility Feasibility	Operation, Support, Validation	Consistency, Viability
Disposer	Compatibility Feasibility	Compatibility Feasibility	Compatibility Feasibility	Compatibility Feasibility	Reuse Archiving Destruction

Figure 2 The continuing nature of processes and stakeholder involvement

Perhaps the stakeholder that needs explanation in Figure 2 is the Human Resources (HR) personnel provider and trainer. Most of the other stakeholders are likely to be most concerned with getting equipment off the drawing board and into operation. However, the Human Resources process (HS.4) to deliver Suitably Qualified and Experienced Personnel (SQEP) operators and maintainers in a timely manner must fully engage with the equipment processes.

The emphasis between the outcomes of a process will vary depending on the stage at which it is performed. This variation in emphasis will in turn affect the conduct of the practices that comprise the process. The effect of stage and project context on the performance of processes and practices is one of the main differences between process models and methods/methodologies for system development.

The process models developed have the ability to provide assurance of lifecycle issues - a potential defence against latent errors [Reason 1990].

4.3 Process, culture and maturity

This section examines the relationship between organisational culture and maturity, and discusses the role of process in relation to them. It then goes on to discuss the possible role of user-centred design as a healthy culture.

To the person starting to work in an organisation, it is clear whether or not the organisation has "got its act together", or whether there is fragmentation, poor information flow, politics and re-work. Experience - within or across organisations - can frequently lead to adaptation to the second situation. There have been a number of attempts to formalise intuitions about culture, particularly because of its safety connotations. Turner [Turner 1978] proposed that a cultural disruption occurs during the incubation period whereby groups and individuals gradually come to develop and rely on a mistaken view of the world. He associated this with the development and maintenance of 'bounded decision zones' which lead to the risk that contingencies are missed, ignored or under-estimated. Vaughan [Vaughan 1996] conveys the ease of being ensnared by the production of culture, and gives a compelling account of the subtlety of its interaction with the culture of production and structural secrecy.

Westrum [Westrum 1997] proposed types of organisational climate, ranging from the pathological, through the bureaucratic to the generative. The distinguishing features are the quality of information flow and the vigour of questioning and enquiry. Perhaps the key indicator is the treatment of bad news, which ranges from 'messengers are shot' through 'messengers are listened to if they arrive' to 'messengers are trained'. The first author's personal experience is that it is easy for people in an organisation to identify where they are on the scale with some consistency. However, it would be a difficult judgement call to try to correlate SIL with a required point on the pathological/generative scale.

Figure 3 offers a caricature of a questionnaire to investigate safety culture in a formal context. The difficulty of obtaining realistic attitudinal information in a context with serious consequences should be apparent. There are a number of excellent schemes to encourage safety culture in a formal manner. These are used by organisations that are already safe to improve matters further, but the target organisations may altenatively be able to buy OTS paper trail generators that meet the letter without the spirit.

Attitudinal indicator	Tick if you agree	Consequences
Safety is my highest concern	☐	Win contract, keep working
Safety is for wimps	☐	Dismissal, Stop Work Order, lost contract

Figure 3 - Attitudinal indicators in formal safety assurance. The official form may not have the consequences itemised, but word gets around.....

The process-based approach started with the concept of organisational plateau of performance [Paulk *et al* 1993], termed maturity levels. These represent similar behavioural syndromes to Westrum's climates. In essence, a *gradus ad Parnassum* was proposed. This starts with *ad hoc* activity where results are achieved by individuals, and moves up through levels of greater process definition, control, management and optimisation. There is an assumption that formalisation is 'a good thing'. In terms of

starting software process improvement, the idea that "we need to get to the next level" has a compelling simplicity. There are many implicit assumptions about organisational characteristics and evolution, with something of a "one size fits all" set of Key Process Areas to move from one level to the next.

The Human-centredness scale - a supplement to the process definitions in the Usability Maturity Model precursor to ISO TR 18529 [Earthy 1998] presented a similar set of steps, but with greater account of cultural issues. A key step of relevance to the safety community is from Level C (Implemented) where human-centred processes are carried out and produce good results but where "too late to change that" is a frequent problem, to Level D (Integrated) where the lifecycles are managed to ensure that the results of human-centred processes are visible in all relevant work products.

The practical disadvantages of organisational maturity (as opposed to process capability) relate to the "one size fits all" character and the assumptions about evolution. Knowing that your organisation is at a specific level does not help to diagnose any root causes, or to identify priorities in terms of process improvement for your specific business at that time. It is probably better - though perhaps less attractive than taking an organisational maturity level as a target - to bite the bullet and identify the processes that are vital to the business, set target capability levels and base process improvement on the gaps found.

Although there is a clear organisational element in the achievement of safety culture, we would argue that an appropriate 'wiring diagram', though necessary, is not sufficient, and that process measures are more powerful than structural measures in finding out whether or not management processes 'work'.

The thesis offered is that indicators of safety culture are vital to safety assurance but have to be used informally for the purposes of self-assessment and improvement rather than vendor assessment, regulation, or formal management. Further, they face the inevitable difficulty of the self-deception they are there to resolve. Maturity models developed for software development or for human-centredness have similarities to cultural models, but no particular attraction to safety assurance. Capability evaluation has a role to play that complements safety culture, being suitable for formal purposes and offering a role in self-assessment and process improvement that would support cultural improvement or maintenance.

Simply put, safety culture metrics are best used informally for improvement programmes, while capability evaluation is appropriate for formal assessments.

An entirely separate point about the relation between user-centred design and culture can be made - that user-centred design (which can be measured for formal purposes) promotes a safe culture (which can't). The user community is the place to spot - and stop - resident pathogens [Reason 1990]. Westrum's words (*op. cit.*) make the point eloquently:

"...Similarly, the safe system is one whose design is carefully thought through and tested, typically in conjunction with users. Its design takes into account the activities and habits of social groups that are going to use the system. It brings these groups into the design process, either through field studies or by placing them on design committees. Even the best design requires thorough training for the users and an open line of communication between the users and the designers.

Once the system is operational in the field, it needs to be monitored by the design group. Some kinds of hardware and software problems will become apparent only through use in the field. The problems that arise need to be carefully studied and rapidly corrected. But above all, somebody needs to be paying attention."

4.4 Process and safety principles

To some extent, this section is a generic version of the usual project discussion on the mapping between Product Breakdown Structure and Work Breakdown Structure - the relationship between "doing the right things" and "achieving the correct design intent". This is a particular concern to operability and safety, where it can be the case that the right things are being done by specialists, but mainstream design engineers are ignoring them. Operability (or safety) cannot be achieved in a context-free fashion; the specific targets and meanings for generic statements of design intent must be determined (as well as met) by the work programme.

Safety principles, design principles, safety criteria are phrases that are widely used in standards and guidance. The attraction of principles is their brevity. This is also their weakness - their abstraction and loss of context makes interpretation difficult and trade-offs between conflicting principles impossible. Design principles such as conservative design, segregation, diversity, redundancy inform the designer, but the assessment of achievement is highly context-specific. Functional safety goals (such as appear at the top of fault trees) inform the design, but provide very limited guidance. Principles can often end up including both work programme requirements e.g. "a task analysis should be carried out, procedures should be produced and validated" and design intent e.g. "user interface design should follow good ergonomics practice". Three examples of principles related to operability are given in Table 4.

Safety of machinery - Ergonomic design principles. Part 1. Terminology and general principles [BS EN 614-1:1995]
This standard called up by the Safety of Machinery Regulations sets out a high level goal of achieving an efficient, healthy and safe interaction of operators with work equipment. It observes that a task analysis is required to meet the goal of designing the work system to be consistent with human capabilities, limitations and needs - otherwise there is no explicit linkage between the design principles given and the specification of ergonomics tasks to be performed. The design principles specify human-machine matches to be achieved taking task characteristics into account and are at two levels of abstraction e.g. "Work equipment shall be designed with proper regard to the body dimensions of the expected population of operators..." and "the type, location and adjustability of any seating provided shall be appropriate to the dimensions of the operator, and to the tasks the operator performs".
A Crew-Centered Flight Deck Design Philosophy for High-Speed Civil Transport (HSCT) Aircraft [Palmer *et al* 1995]
Perhaps the most structured set of design principles relating to operability, these were developed by NASA for future cockpits. They start with three high level philosophy statements, and state a set of principles to support four specified roles the crew play e.g. acting as team members, or being individual operators, which then underpin guidelines on four specific flight deck features e.g. displays, automation. Guidance on conflicts between principles is given. (Material on work activities was being developed separately). The (fairly detailed) principles given for specific features will still need specialist knowledge to generate project-specific design standards.
General principles for the development and use of programmable electronic systems in marine applications [ISO/CD 17894:2001]
Developed by the EC ATOMOS II on Marine Programmable Electronic Systems (PES) [Earthy 1999], ISO 17894 distinguishes between high level product principles (e.g. the PES shall be tolerant of faults and input errors) and lifecycle principles (e.g. user centred activities shall be employed throughout the lifecycle). In addition, the high level principles are supported by more detailed criteria (e.g. The PES interface should assist the user in avoiding input errors and in detecting input errors where they are made and alert the user when they occur.) and specific guidance for project stakeholders. The traditional difficulties of using high level principles are balanced by specifying a scheme for assessing conformance [Messer 2000] that aims give freedom to the design team without loss of rigour.

Table 4, Examples of principles related to operability

The specification of processes given in ISO PAS 'HS' concentrates on the work activities - even the statements of benefits are related to activity rather than design intent. The decision as to timing and scope of the work programme required to achieve operability as an outcome remains a matter for expertise within the project team. Underpinning ISO PAS 'HS', ISO TR 18529 and ISO 13407 [ISO 13407:1999] is a set of principles that defines human-centred design:

- The active involvement of users and a clear understanding of user and task requirements
- An appropriate allocation of function between users and technology
- The iteration of design solutions
- Multi-disciplinary design.

These principles can be seen as management principles that generate work activities and culture.

The conclusion is that both design principles and work activities need to be specified and their achievement assessed. Palmer *et al* (*op.cit.*) conclude as follows: *"Many engineers and designers would claim that they already perform human-centred design. It is important to note, however, that we do not define human-centred design as simply applying "human factors" to the design process. Rather, we believe that an explicit design philosophy must be clearly described and applied systematically within the framework of a well-defined design process."* As regards the design process, we would claim that ISO PAS 'HS' meets the criterion of being well-defined, and can be used as the basis for formal assessment. A work programme based on ISO PAS 'HS' would provide the material to enable the achievement of design principles to be assessed.

In summary, we need both design principles and process specifications, but indicators from design principles are lagged, dependent indicators, placing greater weight on the role of process indicators for safety assurance.

4.5 Process and risk management

The effective management of safety risk (= hazard) and project risk (= cost, time) is essential to safety assurance. There are three points to be made about the relationship with process models.

Firstly, project (or safety) risk assessment can be used as the driver for capability evaluation and subsequent process improvement, i.e. once the risks have been assessed the processes that mitigate the risks can be determined and then used to tailor the assessment and improvement programmes. The MOD uses project risk in this manner for pre-contract award capability evaluations of candidate suppliers [Jones *et al* 1997]. Mandated process improvement is used as a form of risk mitigation.

The second point is that a capability evaluation (possibly relatively quick and informal) is a powerful way of identifying risks (of both varieties) - particularly in relation to management processes.

Finally, the use of standard process models allows organisations such as large customers or regulators to build up cumulative data on generic risks.

4.6 Process and Regulation

To the desk engineer, the regulator appears to have unlimited powers, resources and small print. The reality is somewhat different. There are political limits to regulation and its enforcement, and a real desire to work by encouragement as much as sanction. ISO 17894

is an example of this [Earthy, 1999]. The move to open-textured regulation and broad goal-setting objectives places greater onus on the supply or operating organisation to demonstrate compliance. It is proposed that the process-based approach has much to offer. For example, process improvement can be used as a form of encouragement, but with the potential for formal lawyer-proof evaluations. An informal analysis by one of the authors of (stated or implied) operability process requirements in a range of regulatory settings indicated a high degree of commonality. The prospect of achieving cross-sector commonality by using a process-based approach has considerable attractions.

Some work on process-based approaches to regulation has started. ISO 17894 for the marine sector has a sizeable process element that includes operability. The iCMM developed by the FAA [FAA 1997] has modules that address operability. The HSE [Blackmore 1996] found that senior line managers had few means to measure health and safety in design, and sought to find indicators of the effectiveness of the design process. It has since has sponsored research into the development of Design Process Indicators [Busby *et al* 2000].

In brief, there is work in a number of sectors to exploit the potential of the process-base approach for regulatory purposes. The generic nature of the process models offers the potential for cross-sector commonality.

5. Conclusions and recommendations

The authors conclude that, given suitable support by industry and regulators, a process-based approach has the potential to become the mainstream approach to safety assurance as regards human aspects of systems (and possibly for all aspects, though that goes beyond the scope of the paper). Design principles have been found to complement process measures, but achievement of design principles is dependent upon process capability. In order to adopt a process-centred approach project teams will require detailed method statements for guidance, audit trail and quality purposes, and a 'body of knowledge' to supplement design principles. For practical project purposes, safety culture can be considered separately from a process-based approach, but the use of process metrics can (rightly) relieve safety culture of a role in safety assurance. The possibility of using process metrics in the context of Regulation is intriguing and appears to be under consideration in a number of places.

The principal recommendation is that ISO PAS 'HS', in conjunction with ISO CD 15288, is given further piloting on real projects with an explicit role in safety assurance. There are existing trials analysis resources that could be used to support this. A related recommendation is to progress the work started by [Benediktsson *et al* 2001] on the mapping of process models and IEC 61508:1998.

6. References

[BS EN 614-1:1995] BS EN 614-1: Safety of machinery - Ergonomic design principles. Part 1. Terminology and general principles 1995

[IEC 61508:1998] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, 1998

[ISO/CD 17894:2001] ISO/CD 17894: Ships and marine technology - Computer applications - General principles for the development and use of programmable electronic systems in marine applications, 2001

[ISO 6385:1981] ISO 6385: Ergonomic principles of the design of work systems, 1981

[ISO 9126:2000] ISO 9126: Software product quality - quality model, 2000

[ISO 12207:1995] ISO 12207: Software process - Software lifecycle processes, 1995

[ISO 13407:1999] ISO 13407: Human-centred design processes for interactive systems, 1999

[ISO CD 15288] ISO CD 15288: System engineering - System lifecycle processes.

[ISO TR 15504:1998-2] ISO TR 15504: Software process assessment - A reference model for processes and process capability, 1998

[ISO TR 18529:2000] Ergonomics of human system interaction - Human-centred lifecycle process descriptions, 2000

[ISO PAS tba-:2002] ISO PAS tba:2002 A specification for the process assessment of human-system issues, 2002 in press

[Benediktsson *et al* 2001] Benediktsson O, Hunter R B, McGettrick A D: Processes for Software in Safety Critical Systems in Software Process: Improvement and Practice, 6 (1): 47-62, John Wiley and Sons Ltd., 2001

[Blackmore 1996] Blackmore G A: Safety Management Systems in Offshore Oil and Gas Companies - Experience from Asessment and Audit of UK North Sea Operations, New Orleans, December 1996

[Busby *et al* 2000] Busby J, Strutt JE, Sharp JV: "Lessons learnt from Offshore & Marine Incidents & accidents - input to the Design Process", ERA Conference on Major Hazards Offshore, London, November 2000

[Earthy 1998] Earthy J V: Usability Maturity Model: Human-Centredness Scale. IE2016 INUSE Deliverable D5.1.4s, 1998. http://www.lboro.ac.uk/eusc

[Earthy, 1999] Earthy J V: A new approach to marine programmable systems assessment, 9th Intnl. Symp. of the Intnl. Council On Systems Engineering (INCOSE), Brighton, UK, 1999

[Messer, 2000] Messer A.C: Draft Survey Procedures, Assessment scheme realisation, ATOMOS IV ref A408.02.08.055.001, 2000 www.atomos.org/atomos2/

[FAA 1997] Ibrahim L, Deloney R, Gantzer D, LaBruyere L, Laws B, Malpass P, Marciniak J, Reed N, Ridgway R, Scott A, Sheard S: The Federal Aviation Administration Integrated Capability Maturity Model, (FAAiCMM), Version 1.0, 1997 http://www.faa.gov/aio/ProcessEngr/iCMM/

[FAA, 1999] FAA Human Factors Job Aid, Federal Aviation Administration Office of the Chief Scientific and Technical Advisor for Human Factors, AAR-100, (202)267-7125, 1999 www.hf.faa.gov

[HS(G)65: 1991] Successful Health and Safety Management. HSE Books, 1991

[HSG48: 1999] Reducing error and influencing behaviour. HSE Books, 1999

[Jones *et al* 1997] Jones R L, Hamilton J M: A co-ordinated approach to identifying software development risks in MOD projects, Proc. European SEPG conference, 1997

[Palmer *et al* 1995] Palmer MT, Rogers W H, Press H N, Latorella K A, Abbott T S: A Crew-Centered Flight Deck Design Philosophy for High-Speed Civil Transport (HSCT) Aircraft, NASA Langley Research Center, NASA Technical Memorandum 109171, 1995

[Paulk *et al* 1993] Capability Maturity Model for Software, Version 1.1 CMU/SEI-93-TR-24 Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 1993

[Reason 1990] Reason J T: Human Error, Cambridge University Press, 1990

[Turner 1978] Turner B A: Man-Made Disasters. Second edition: Turner B A, Pidgeon N K: Butterworth-Heinemann, 1997

[Vaughan 1996] Vaughan D: The Challenger Launch Decision. Risky Technology, Culture and Deviance at NASA. The University of Chicago Press, 1996

[Westrum 1997] Westrum R: Social Factors in Safety-critical Systems. in Redmill F, Rajan J: Human Factors in Safety-critical Systems, Butterworth-Heinemann, 1997