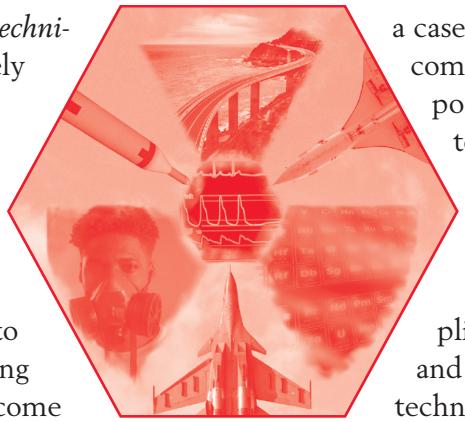
Implications of STAMP for Warhead Safety at AWE

by Malcolm Jones
Reading, U.K.

STAMP (System-Theoretic Accident Model and Processes)[1] is a relatively new approach to safety assessment methodology and post-accident cause analysis; its prime developer is Nancy Leveson of MIT [Ref. 1]. STAMP is a holistic system-level approach to overall organizational structure and to technical operations and design. It takes a comprehensive look at all possible *organizational* and *technical* system influences that can ultimately affect the safety of technical processes and product designs in whatever *scenarios or environments* in which they operate or to which they are subjected. Of course, the process can be applied equally to both reliability of performance and security, in addition to safety. Its essence is based on identifying all the reasons for a detriment (an outcome penalty or mishap) and not just those from failures in physical items. This is largely based on control theory. Perhaps the STAMP scene is set by the following system description:



Johansson describes a production system in terms of four subsystems: physical, human, information and management [Ref. 2]. The physical subsystem includes the inanimate objects — equipment, facilities and materials. The human subsystem controls the physical subsystem. The information subsystem provides flow and exchange of information that authorizes activity, guides effort, evaluates performance and provides overall direction. The organizational and management subsystem establishes goals and objectives for the organization and its functional components, allocates authority and responsibility, and generally guides activities for operations.

STAMP operates in this general context. It identifies the characteristics of any contributing element to safety, but in the full context of the system, rather than treating each element separately and aggregating the individual characteristics. This aims to prevent missing system interaction contributions that would lead to inadequate safety assessment. It has long been known that safety is not equivalent to reliability, even though reliability is a substantial contributor to safety. STAMP recognizes the fact that safety detriments can occur even when all elements of a system operate perfectly according to their design specification. This is a case of the design specification being incomplete in the context of covering all the possible system scenarios that could lead to detriments.

Because of its holistic system approach, STAMP can be applied in many ways:

Top Level — STAMP can be applied to the whole company organization and governance structure within which a technical operation occurs, or to a technical design or process that is performed within that organization. It recognizes that organizational safety culture and structure will have an impact on the safety of any technical process or product for which it is responsible. STAMP sees the governance process as a tightly controlled top-down hierarchical control approach where each organizational level sets the policy, culture, standards, training, procedures, behaviors, etc. that enable the next level to perform and operate at its appropriate level of detail, responsibility and accountability. This process transcends down to the detailed level of technical operations and product design. Failure at any level can ripple down and ultimately lead to failures in the technical processes and designs.

Of course, we are talking about a company's safety culture and its enactment with the associated identification of the potential hazards and detriments that might occur and the controls that must be put in place to prevent these detriments from manifesting themselves. In "STAMP speak," these controls are called *Constraints*. These Constraints are intended to perme-

[1] The contents of this document represent the views of the author and not necessarily those of AWE (Atomic Weapons Establishment) plc.

ate throughout the organizational structure and to take the appropriate form at each level. Each layer in the organization's structure needs to identify the potential routes to detriments that might occur, and inform and control the next layer accordingly.

Lower Levels — STAMP can also be applied directly to the technical operations and product designs given the Constraints passed down through organizational and governance levels. Again, the process concerns itself with the identification of the potential hazards that can arise — and which can lead to detriments — and, in turn, applies controls (Constraints) to prevent detriment occurrence. Failures at these lower levels are often identified as "root causes" but do not necessarily point to the origin of earlier failures in the organizational governance process. For example, a weakness in the organization's safety culture, lack of approved processes, lack of suitable personnel training and supervision, allowing poor/slippage of standards, etc. can eventually give rise to unsafe technical processes and products.

Because of its holistic system-level approach, STAMP claims to be more successful in ensuring safety than more traditional causation approaches such as FMECA and FTA because:

- It identifies potential hazards leading to failures that are missed by more traditional approaches.
- It allows the creation of more powerful tools, such as STPA (hazard analysis) safety-guided design, CAST (analyzing previous accidents), identification and management of leading indicators of increasing risk, organizational analysis, etc. These tools have been developed to support the application of STAMP.
- It clearly acknowledges that reliability does not guarantee safety. An operating system (OS) can operate reliably as per design, but can still have the potential to lead to hazardous conditions and safety detriments.
- STAMP claims to be more resource and cost effective than other approaches.
- As noted previously, STAMP includes the whole organization governance element as part of a wider integrated system-level approach to avoid missing issues that would arise in a more piecemeal approach.

In summary the overall approach operates in the following form:

STAMP: Accidents (detriments) are caused by inadequate controls. The STAMP approach notes that failures are not restricted simply to component unreliability. The need is to ensure that appropriate controls are in place to prevent the detriments from occurring for the full set of scenarios/environments that are possible for the operation of an organization, design or process.

CAST (Casual Analysis based on STAMP): Inadequate controls that led to past safety failures (detriments) are identified — lessons to be learned after the event — RLI? Potential application to new cases and STPA.

STPA (Systems-Theoretic Process Analysis)*:* The process for identifying inadequate control in a proposed process or design. This process searches for inadequate control possibilities and ensures that the necessary improvements are in place to satisfy STAMP. STPA steps are:

1. Identify potential loss (detriment).
2. Produce functional control structure for both organizational and technical considerations.
3. Identify potential unsafe or missing control actions
4. Apply to target loss or detriment scenarios and ensure appropriate controls are in place.

STAMP is seen as providing a better approach to ensuring safety in a world that is becoming more and more complex both in organization/governance structures and technical applications.

STAMP in the Context of Today's Complexity

Today, many organizational structures, technical processes and designs have become so complex that full understanding of this complexity becomes increasingly more difficult. One clear example lies with the proliferation of micro-electronic technologies and associated software (IT), and their impact on advisory and control functions. Another example is associated with the increasing complexity of human machine interactions and the contextual conditions and environments under which activities occur. If not fully understood and accounted for, all can lead to detrimental events. At the company level, organizational structures are also becoming more complex, potentially leading to less transparency in terms of "how it all cohesively fits together." This raises the question of how effective the communication and control processes are from both the top down (controls) and the bottom up (situation awareness), and whether the governance process is correct and complete.

Organizational Aspects: Any technical process or design will sit under the responsibility and account-

ability of a company organization/governance structure and, as such, this structure needs to look down to ensure that everything is put in place so that the processes and products undertaken by the company are suitably safe. Therefore, a complex socio-technical approach describes the overall system and the level of understanding, guidance and control that is key to the success of the technical processes and products for which it is responsible. The top-down process passes through several layers in the organization, with each layer responsible for identifying the appropriate safety requirements (what should happen and what should not happen) that are to be passed down to the layer below — and to monitor that such requirements are understood and met.

In STAMP speak, the prime requirement is that each layer passes down the so-called safety *Constraints* in the form of making clear what should happen and what should not happen (identifying the requirements and controls that should be put in place to prevent the unsafe state/detriment occurring) and tasking the next layer with executing these requirements with clear explanation and with the resources required at this next layer. In addition, each layer will require a monitoring, auditing feedback structure to ensure that the Constraints are fully understood and are being actioned effectively. The dynamic nature of the overall structure depends on an "open" feedback, bottom-up, complementary approach to ensure that each layer is encouraged to "report up" on difficulties in applying the Constraints or on aspects that may have been overlooked at an upper level. These will need corrective action by those upper layers, which have the appropriate authority and resource control to enable any remedial action deemed necessary. This stepped, two-way safety process reaches right down to the basic technical process and product levels of the organization.

The key is that each layer has a complete understanding of the responsibilities and accountabilities passed down to it, together with an understanding of how these should be interpreted and passed on in the correct form to the next layer, given an understanding of the needs of that layer. This will be coupled with an audit/assurance/improvement process to confirm/maintain successful implementation.

In the wider sense, this structure extends above the manufacturing organization itself, as operations and products may have to comply with national and international safety standards and associated external regulation. These, in turn, can place their own Constraints and auditing structures on the manufacturing organization.

Technical Aspects: With the increasing proliferation of IT in today's technical processes and product design, the level of transparency and understanding becomes more difficult to achieve. It becomes increasingly more difficult to envisage all the IT data state configuration possibilities and interactions that might take place between entities in the overall technical and physical systems. The STAMP process for dealing with this complexity is based on limiting the need to identify only the potential physical system detriments and to ensure the hazardous IT configurations that can lead to these are recognized by a control system (CS), so that the appropriate controls (Constraints) are applied by the CS to the operating system (OS) to prevent the physical detriment occurrence. Of course, the secret here lies in how well (and how complete) such hazardous conditions leading to potential physical detriments are understood and identified and how effective the applied Constraints are. Problems can still arise if the CS is not aware of all the potentially physically harmful OS encounters that can occur, and its IT control aspect has not been configured to deal adequately with such conditions. Hence, limitations in the overall understanding of the OS model by the CS, which includes the physical system, can result in a "properly operating" CS still giving rise to inadequate control of the OS. Typical examples of lack of a full system understanding of the OS can arise through dysfunctional interactions between different part of that system — for example, the occurrence of unexpected "wrong order" of IT information transmission or unexpected "incorrect" relative timings of such transmissions. The secret lies in a full CS understanding of all the characteristics of the OS.

Of course, errors in IT scripting themselves can lead to hazardous situations just as failures in technical hardware can.

The Operational System (OS) and Control System (CS) Concept

STAMP effectively breaks down the total technical system into two basic parts — the control system (CS) and the operating system (OS). Both may have human elements and the latter has both IT and physical components. The strategy broadly follows the basic tenets of Communication Control Theory, with its associated feedback loops and controls.

The CS interact with the OS in two ways. It receives continuous IT status reports on OS configura-

tions, makes decisions based on what it receives and issues a Constraint if it detects a present (or impending) hazardous condition for the physical system (or any other form of detriment). The purpose of the Constraint is to prevent the OS from turning the hazardous configuration into a physical (or any other form of) detriment. These Constraints can be logged and the reasons for the hazardous conditions arising can lead to an improved understanding of the OS system model and/ or can form the basis for OS technical re-design. To operate correctly, the CS will require as complete as possible model of the OS to fully comprehend the significance and context of any OS data information it receives in order to respond appropriately. Such a system model must also incorporate the context and environment within which the OS (and CS) is operating at that time. This understanding of the OS model by the CS is a key requirement of the STAMP strategy. In turn the CS will need to ensure that the Constraints have been successfully received and successfully acted upon by the OS via feedback loops.

What is the basis for STAMP's claim that it is a more successful approach for complex IT-based processes and products? STAMP safety is based upon the CS not needing to know all of the possible data configuration it might receive from the OS, but to recognize only those that are hazardous in the context of the current state of the physical system. Any particular OS action at this stage can be either harmless, necessary to ensure safety or can lead to unsafe conditions, all dependent on the exact configuration of the physical system (including the environmental and scenario aspects) at that moment in time. It is the responsibility of the CS to enforce the correct response. The key to success lies in the level of completeness of the CS's model of the OS system (including the environment and scenario) and its ability to identify and respond correctly to OS safety critical IT messages. The process begins with compiling possible OS detrimental (unsafe) physical actions; then, the CS identifies the associated OS data transfers that warn of the hazardous conditions. The CS, in turn, applies the necessary Constraint actions to prevent a detriment occurrence. The STAMP contention is that this process coupled with its feedback control approach to confirm constraint application (and a supporting evidence-based track record of its application in many areas) is better configured to eliminate detriments than the more familiar causation approaches when applied to systems with a high degree of complexity. STAMP claims it can cite many

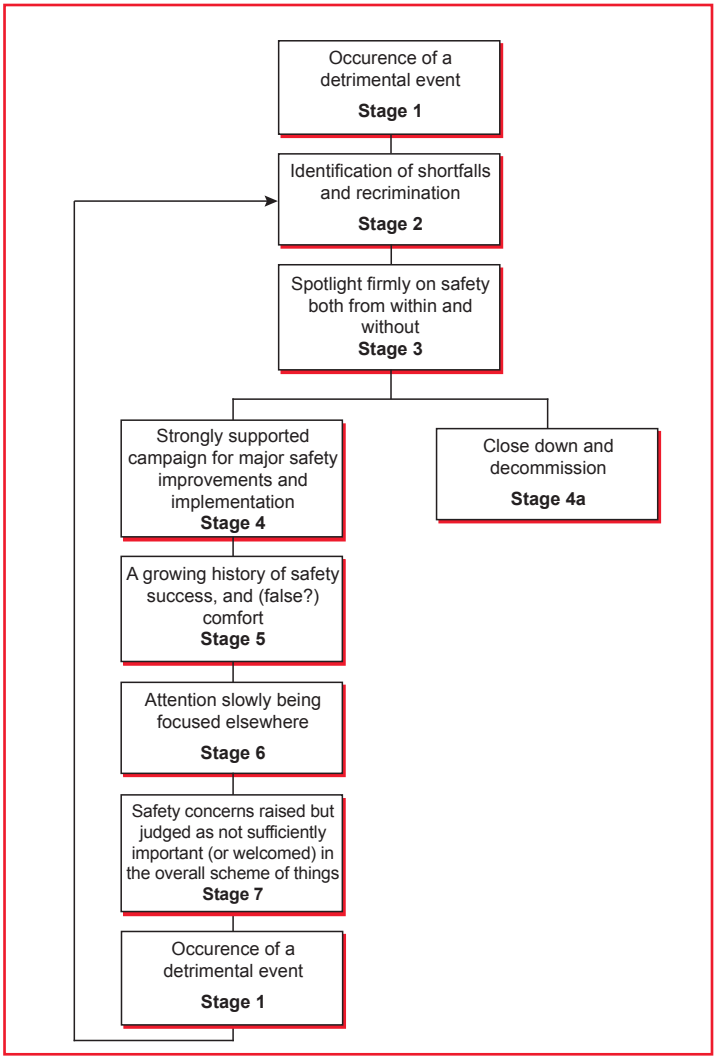


Figure 1 — The Normal Accident Cycle.

examples where it has identified extra hazardous conditions not recognized by other more established safety methodologies.

Some Historical Examples of Failures in the STAMP Context

Two examples are given — one from each end of the socio-technical spectrum — to illustrate organizational and technical failures that might have been detected by the STAMP approach.

Example 1 — Figure 1 illustrates how an organization may drift in its safety culture (with the associated slippage in its Constraints discipline), leading to a safety problem by way of a step-by-step progression in the so-called Normal Accident Cycle [Ref. 3]. This is an example where both top-down implementation and maintenance of Constraints and the openness and responsiveness to the bottom up-process both fail in terms of their original intent due to dysfunctional interactions (as far as safety is concerned). Each step in the

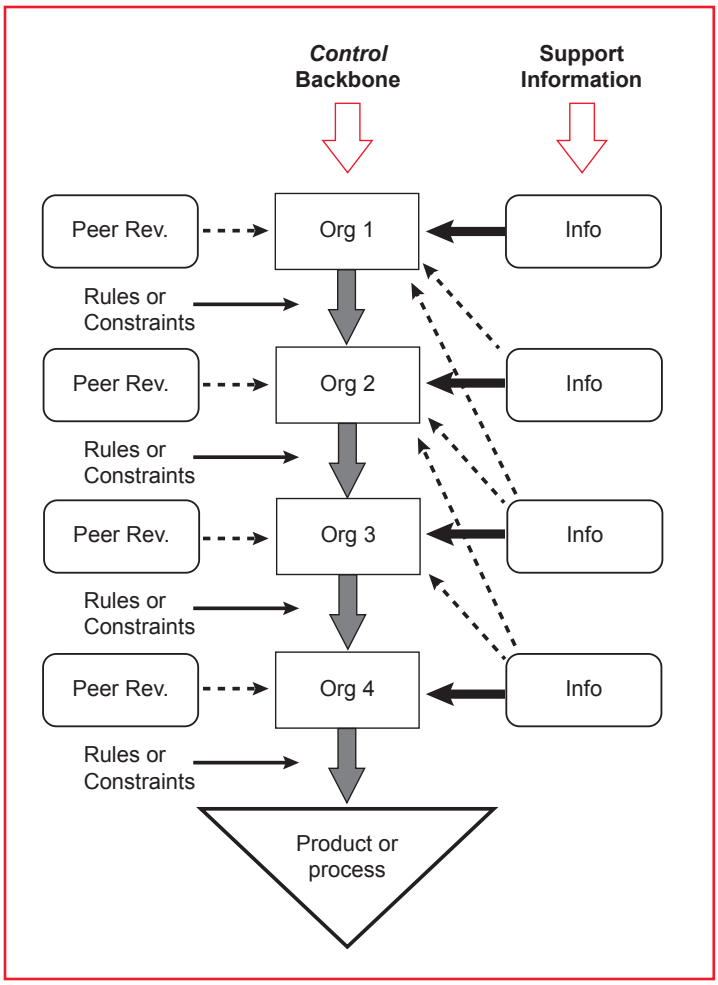


Figure 2 — The Control and Information System.

failure process is driven by an organization's tendency to raise the importance of other aspects in conflict with safety. Each step, taken individually, would appear to have a limited and acceptable impact on safety, but it is the accumulated effect of a series of such steps (each with apparent limited safety consequence and supported by past absence of failure) that is important. This results in the dilution of the effectiveness of the organization's backbone CS safety structure. STAMP would claim to recognize the onset of dysfunctional failure of this type and warn about the growing weakness of the safety Constraint process. This slippage can change the governance strategy from *"prove it's safe"* to *"prove it's unsafe."*

In fact, both the *Columbia* and *Challenger* space shuttle catastrophes had examples of this drift to failure.

Example 2 — This is a technical failure example and illustrates the danger of an incomplete CS model of the OS in which all items operated as per the specification with no element of "technical failure," but still resulted in an overall major detriment. It is a real example, often used by Nancy Levenson in her teaching classes, and STAMP apparently played a part in determining the reason for failure. It concerns a Mars Polar Landing loss. To land safely the lander used parachute retardation and descent engines to slow down the descent. The intention was that sensors in the lander's legs would detect the mechanical environment of landing and the CS software would instruct the turn-off of the descent engine. However, the deployment of the parachute also produced a mechanical environment detected by the leg sensors, which was interpreted by the CS as a constraint requirement to turn off the descent engines, resulting in lander loss. The CS system control software was, in fact, made active at an earlier stage than was necessary in order to better manage the processor load and as such was active during — and was unaware of — the parachute deployment phase. This condition/scenario had not been envisaged in the CS model of the OS in the overall scenario context and, as such, the CS model of the OS was incomplete. A dysfunctional relationship between the CS and OS resulted. However, both the CS and OS systems operated as specified, but under the wrong conditions.

The dysfunctional interaction in this case occurred through a lack of cohesion (or disconnection) between those dealing with the safety logic (CS) and those dealing with the processor loading requirements (OS). This was a system, rather than a component, technical failure.

Application of the STAMP Approach in the AWE Context

Organizational Structures: The "central backbone" (Figure 2) is that part of an organization's control/governance structure that is responsible for safety and which ensures that the appropriate constraints/safety requirements are passed down through the organization's safety levels, terminating at the technical processes or product designs levels. At AWE, this flows down through the chief executive officer, relevant directors, design, production and facility authorities for the warhead.

This central backbone requires that appropriate supporting information be given to the appropriate structure level(s), in order to generate the requirements and constraints that must to be put in place — and that is gained from the reservoir of core knowledge and capabilities resident at AWE and external sources. The backbone is further supported by an independent peer review assurance organization, which is tasked with reviewing and challenging the probity of the backbone's management and technical decision-making process and auditing the success (or lack thereof) of its imple-

mentation at the various levels of operations. Both the information and peer review structures act as feedback loops to give the organizational structure confidence that it is itself working correctly.

It is the backbone's responsibility and accountability alone to properly assess the information it receives and to act accordingly. Both the information and peer review structures are important elements in supporting the organization's safety backbone, but they do not directly set constraints or requirements or provide final ensurance that they are correctly implemented — that is the responsibility and accountability of the backbone (CS).

This structure meets one of the STAMP concerns in that there should be no dysfunctional interactions between entities involved in the overall safety operations process. The responsibilities and accountabilities are clearly defined. No information is acted upon for implementation unless authorized by the backbone. As such, the backbone, acting as the CS in this process, issues the Constraints and must maintain maximum visibility and understanding of the equivalent OS. The description shown in Figure 2 broadly maps out the AWE organization's governance safety structure and is seen to comply with the STAMP methodology

In the special case of nuclear warhead design, AWE makes use of another key element in the overall structure, which continues to ensure that, in a complex technical product, there are as yet no undiscovered weaknesses in the depth of understanding of the technologies involved that can give rise to a significant safety threat. This is illustrated in Figure 3 [Ref. 4], which shows this overarching continuous scrutiny process (enacted by encouraging the best brains in the organization to continue to probe into the relevant technologies in a "what if" manner). This continues to interact with the traditional ensurance, assurance and executive processes even after "safe processes" and "safe designs" have been accepted. This process acts as an enhanced "what if" safeguard against the possibility of a "Black Swan." In doing so, it provides continuing advice but has no direct role in setting constraints.

STAMP In the Context of NW Technical Design

It is instructive to follow the STAMP process in its approach to meeting safety in the context of a complete nuclear warhead in isolation of the overall weapon system. Perhaps the most important aspect in relation to STAMP is that the NW design, as a separate entity, normally lives in a passive state. There are no active processes present and no need to monitor for the pres-

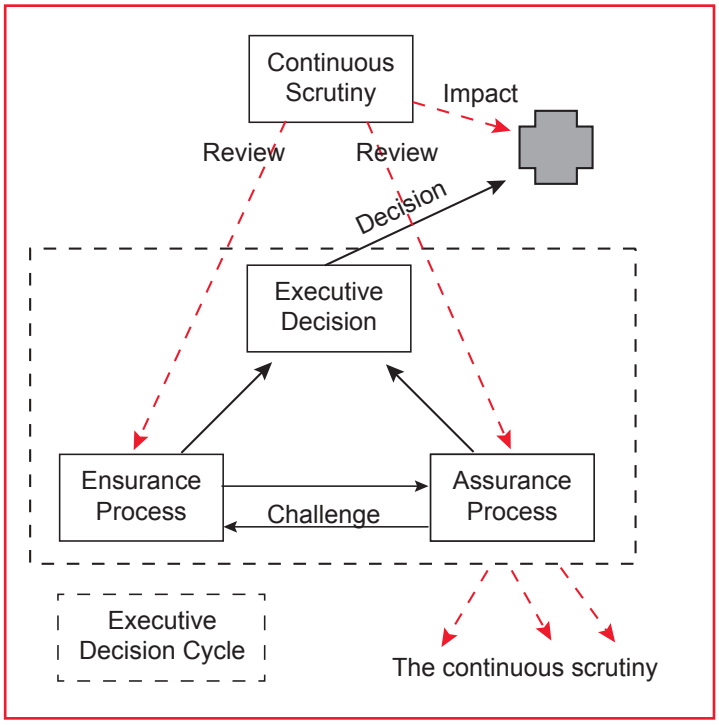


Figure 3 — The Continuous Assessment Process.

ence of so-called IT hazardous configurations and dysfunctional interactions. As such, there is no parallel to the idea of IT actively recognizing hazardous conditions and providing Constraint instructions or the concept of OS and CS. However, Constraints are built into the design in passive form. In fact, one of the guiding principles of safe warhead design is to avoid complexity and lack of transparency to aid confidence in carrying out safety assessments. It is possible to monitor the general "health" of the NW with safety being one area of interest, but this is done with approaches that are explicitly independent of Inadvertent Nuclear Yield (INY) safety, which will be used as the detriment example for illustration in this paper.

Fundamental STAMP requirements — These are identified as:

1. Identification of detriments
2. Identification of all the possible hazardous paths to detriments
3. Identification of all the necessary Constraints that need be put in place to prevent such hazards leading to detriments

Detriment — To make this review manageable, we will use the example of the most serious detriment of Inadvertent Nuclear Yield (INY) and apply this to the warhead as an isolated item (as opposed to a whole weapon system). In principle, the approach can be applied to all the other detriments that can arise for the

warhead, such as radioactive (RA) material release, etc. Of course, the analysis is somewhat complicated by the fact that the warhead is designed to produce nuclear yield, but only after due authorization. So what are the potential paths to INY?

Paths to the INY detriment are:

1. Insufficient protection in the authorization mechanism to prevent inadvertent INY
2. Insufficient protection in the inherent design of the technical system
3. Insufficiently robust design that does not cater for all the envisaged abnormal safety challenges (scenarios and environments in the STAMP context) that can occur. As such, there is a need to identify the full spectrum of safety challenges.

Authorization —

- If the authorizing information has been supplied to the warhead, it must be positively removed prior to the stage when the warhead configuration first becomes nuclear capable.
- That the warhead, independently, cannot generate such authorization through fault processes.

The authorization-enabling information should either never be resident in the warhead during its manufacturing process, or should be positively removed before there is any possible linkage to INY. Although there are reasons why such information may be resident in the warhead — such as for reliability testing reasons at earlier stages — this should only occur for a period prior to the warhead forming a nuclear-capable configuration. Such authorizing "information" must be positively overwritten to safe mode before the warhead reaches the nuclear-capable configuration. Removal of access to power at this stage also leads to the inability to store information in the active memories. This represents the *first Constraint*.

In addition, the form of the authorization information must be of a form such that its inadvertent generation by the warhead should be shown to be extremely unlikely. This is accomplished by the so-called construction rules for *Unique Signals,* together with the associated evidential analysis demonstrating that the faults needed to generate such an authorizing signal are themselves extremely unlikely. This represents the *second Constraints* in the STAMP context.

Technical Design in Normal Environments — Normal environments are those which the warhead will typically experience during its lifetime, as opposed to abnormal environments that might arise from unintended conditions (see later). These are identified in detail in the Normal Environment portion of the *Environmental Definition Document* (EDD) for the warhead.

There are two potential paths to INY in relation to the inherent technical design of the warhead, when it is in its nuclear capable configuration:

- Inherent safety failure of the technical system designed to enable nuclear yield, in the absence of its authorization — designated a *Route 1* safety failure.
- Inadvertent operation of the physics package itself to produce INY independent of a Route 1 failure — designated a *Route 2* safety failure.

Route 1 — Prevention of INY is based on the absence of active internal power sources, the inability to generate safety-critical power formats and the isolation of such formats from nuclear-critical functions. The latter take the form of a comprehensive set of barriers to prevent energy transfer by way of passive structures (exclusion walls), or movable barriers which only "close" when authorized to do so for warhead operation *(Isolation Constraint)*. Any "unlocking" information supplied to these removable barriers that does not comply with the unique nature of the authorizing signal will cause them to irreversibly lock in the safe position *(the Incompatibility Constraint)*. In addition, these removable barriers will also need to "register" the correct release and trajectory environments associated with intended authorized weapon use, as part of the authorization process.

The *Route 1* safety system is designed to ensure that internal passive power sources are not inadvertently activated and that such sources are isolated from critical regions. The isolation strength in-depth strategy is also based on an *Independence Constraint* so that barriers are not prone to common mode or domino failure modes. Independence of barrier design is based on application of different concepts, different engineering implementation, different material source, etc. In addition, the "removable" barriers are designed to be single-point failure safe and their predominant mode of failure typically gives rise to energy isolation or diversion away from nuclear-critical regions. The ideal number of such barriers is dictated by the somewhat competing requirements of design resilience, maintenance of true independence, need to produce yield reliably when authorized to do so, need for transparency (avoidance of complexity) and confidence in safety assessment

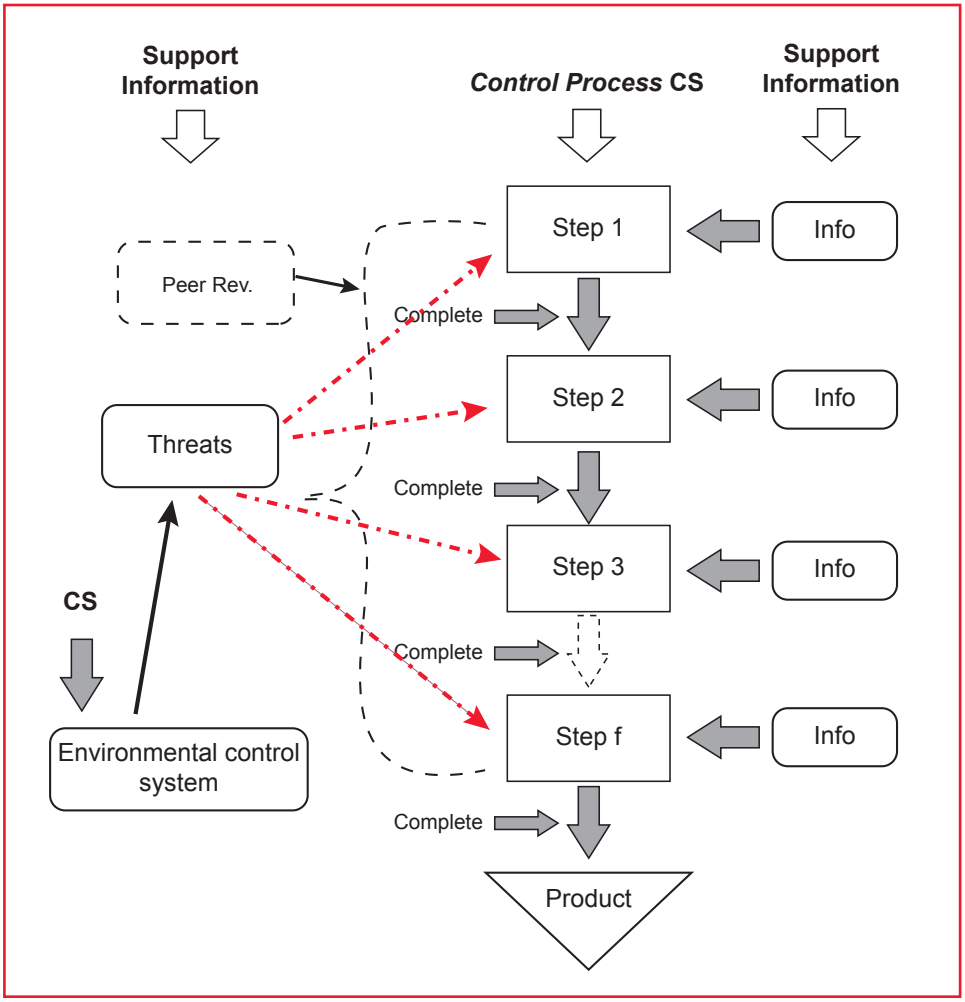


Figure 4 — The Control and Information System.

analysis, particularly in the context of abnormal environments (later). The system is also designed to have irreversible fail-safe elements to cater for abnormal environment levels above which the barrier isolation strategy might not be *fully assured* — the *Inoperability Constraint*.

It is also a principle that, apart from the unique authorization aspect, any other IT that might be associated with the warhead should be explicitly demonstrated to be independent of INY safety.

Route 2 — INY safety is based on the physical protection of critical items, the low detonation sensitivity of high explosives (HE) trains *(Inoperability Constraint)*, and the inherent uniqueness of the physics package design which can only lead to INY for unique detonation geometries of the HE *(the Incompatibility Constraint)*. In principle, the physics package can also be set in a non-nuclear configuration *(Inoperability Constraint)* until enabled by unique *Route 1* authorized control. The *Route 2* elements themselves play no part in controlling warhead operations and are essentially passive in nature. As such, *Route 2* safety is based on demonstrating that the characteristics identified here meet acceptable standards even in the presence of abnormal environments. These characteristics represent the fundamental *Constraints* for this Route and are certified through an exhaustive program of testing and scientific analysis, which involves state-of-the-art scientific experimental and computational tools.

The technical design meets the intent of STAMP through the constraints of *Isolation*, *Incompatibility*, *Inoperability*, *Independence* and *Protection*.

Technical Design in Abnormal Environments — The greatest challenge to the safety of the warhead comes in relation to its potential response to abnormal (inadvertent/accident) environments. These take the form of a range of credible inadvertent energy sources that can act upon the warhead and create environments that fall outside those complying with normal environment definitions. These can be broadly described as uncontrolled external or internal electrical energy sources (inadvertent electrical supply sources, lightning attachment, EMR exposure, ESD generation, etc.), uncontrolled disruptive internal energy sources of a different nature (pressure vessel failure, inadvertent sub-ordnance initiation, etc.), uncontrolled atmospheric conditions (excessive humidity, chemical contamination, etc.) and the range of potential stressing environments following accidents (shock, accelerations, pressure, crush, penetration, vibration, fire, etc).

There are obviously human factors elements related to the prevention of the occurrence of many of these environments. In STAMP speak, these represent the credible range of environments and scenarios within which technical systems will need to demonstrate appropriate safety. These credible environments together with their detailed characteristics, are listed in comprehensive form in the Abnormal Environmental portion of the warhead's EDD, and, as such, this sets the template for the safety assessment of all envisaged scenarios (a STAMP requirement). It should be noted here that, because of the unique approach

to authorization, abnormal environments have little direct impact on the authorization level of protection. Of course, great care is exercised during the lifecycle of the warhead to avoid such abnormal environments and provide extra external protection as appropriate, which adds to the inherent robustness of the warhead's own safety systems. The robustness of the *Route 1* and *Route 2* safety systems (and their assurance safety arguments) is then examined through a comprehensive program of testing and analysis against each of the credible abnormal environments identified in the EDD (a STAMP requirement) and to identify any severity levels that might limit the assurance arguments for each route. For these latter conditions, an assessment will be based on any remaining assurance arguments still in place, the probability of such an abnormal environment occurrence and the assessed level of potential assurance loss, together with the assessed response of the fail-safe aspects of the warhead. This finally takes the form of an annual probabilistic risk assessment which is set against the national annual risk standards for the nuclear warhead stockpile. These take the form of a Basic Safety Limit (BSL) above which the risk is not tolerable, a Basic Safety Objective (BSO) below which the risk takes one broadly out of the so-called As Low As Reasonably Practicable (ALARP) region, and the need for a supporting ALARP argument to demonstrate why it is impracticable to reduce risk further.

> "(STAMP) is claimed to be a more effective and efficient resource in today's complex and less transparent world in which the application of IT technologies proliferates. STAMP also makes clear that technical reliability does not guarantee safety, in that detriments can occur even when technical elements work as specified. Failure can still occur due to a lack of full understanding of all the possible paths to failure."

For the abnormal environment case, the warhead safety approach meets the STAMP requirement not only through the constraints of *Isolation*, *Incompatibility, Inoperability, Independence* and *Protection* but also through a comprehensive process of identification of all credible abnormal environments/scenarios, coupled with a detailed examination of the of the robustness of the Constraint arguments for each case — and, of course, coupled with *Constraints* to prevent such abnormal occurrences.

STAMP in Assembly Safety

Not only is INY safety a requirement for the full design of a warhead and its subsequent ownership, but it is also a requirement for the processes associated with its manufacture (assembly and disassembly). The stages of the build of the warhead are still characterized by passive states. There are no direct IT (or automation) interactions with the warhead during these assembly or disassembly processes apart from the application of test equipment where the *Constraint* is that such equipment shall have no implications for INY. The human factor element takes on a greater importance during this phase because in the earlier stages of the warhead build, there will be less intrinsic warhead safety in place and more direct human activity impact on the warhead. This takes us back to the organization/governance structure of Figure 1 where one of the outputs is a comprehensive set of operating procedures which are designed to ensure full compliance *(Constraints)* with safe manufacturing procedures. The technical process follows a backbone structure, but in the form of a process specification that sets down the safety requirements at each step in the activity, as shown in Figure 4, which have been agreed upon and formalized by the company safety governance organization. This, in fact, represents the CS for the manufacturing process. As such, there should be no deviation from this procedure unless formally authorized by the appropriate element in the organization backbone structure shown in Figure 2. Correct implementation of procedures in the OS is ensured by the supervision, which forms a part of the CS and is supported where appropriate by independent peer review.

The operators (OS) themselves are fully trained and assessed to be suitable for the tasks involved. Modification to the process resulting from operating experience may arise, but changes can be authorized only by the backbone structure. This arrangement minimizes the chance of dysfunctional interactions by ensuring that no other entity — other than the safety organization's backbone — can directly make changes to the specification. Safety in the manufacturing phase will rely on the safe design and application of tooling equipment and the protective characteristics of the facility within which manufacture takes place. Such tooling will be designed to remove/minimize the

chance of safety failure resulting in insult to the warhead. Credible failures of this kind will again be listed in the abnormal environments section of the EDD and each will be assessed for warhead safety implications. The facility within which manufacture takes place is responsible to protect against external threats and to prevent threats from arising though failures of the facility. Failures of this kind also forms part of the "credible abnormal scenario" and are themselves subject to safety impact assessment.

Conclusions

This paper reviews the STAMP approach to safety assessment methodology and how it covers organizational, scenario and technical aspects — all elements that can ultimately lead to technical system safety failures. It is claimed to be a more effective and efficient resource in today's complex and less transparent world in which the application of IT technologies proliferates. STAMP also makes clear that technical reliability does not guarantee safety, in that detriments can occur even when technical elements work as specified. Failure can still occur due to a lack of full understanding of all the possible paths to failure.

The nuclear warhead world has generated its own comprehensive approaches to safety design and compliance assessment over many decades, learning from concerns that have arisen and even through failures, but fortunately not of the worst kind. The approach has also been strengthened by the lessons learned from tragedies suffered by other high-consequence industries. The comprehensive safety design and assessment methodologies that have been developed are meant to show compliance with the demanding national safety standards and align to the level of consequences given the failure. As an example, this paper has reviewed these current safety approaches to the prevention of Inadvertent Nuclear Yield (INY) as a vehicle for comparison against the STAMP methodology, both from organizational governance and technical points of view.

Apart from the specific application of the tools advocated by STAMP, the current approaches to INY prevention broadly envelops the core of the STAMP approach. These approaches do this through the principles (or *Constraints* in STAMP methodology language) of *Isolation*, *Incompatibility*, *Inoperability*, *Independence* and *Protection*. Both the design of and processes by which nuclear warheads are manufactured broadly excludes the application of IT technologies, where many of the dysfunctional problems reside in other technical products and processes, and where lack of transparency becomes a major emerging safety issue. The nuclear warhead in isolation is a passive device and as such, it avoids the potential dysfunctional related concerns that plague interactive IT-based designs and processes. For the limiting cases where IT has an application, it is a cardinal requirement to show that its presence does not provide a path to INY. When integrated into a complete weapon system the warhead characteristic is still passive, but there may be additional paths to INY due to overall weapon system interactions, which would have to be considered separately. This aspect has been excluded from this assessment.

About the Author

Malcolm Jones has previously led the Distinguished Scientists group at AWE and currently holds the position of Scientific Adviser to AWE's Chief Scientist, directly supporting AWE's Chief of Product Assurance. His career at AWE has taken him through a wide range of scientific and engineering topics, but he has maintained a continuous association with nuclear weapon design and process safety and top-level nuclear safety standards. His interests extend to corporate safety cultures and the root cause reasons for failures. He is a Fellow of the International System Safety Society and is an adviser to a number of senior U.K. Ministry of Defence and AWE safety bodies. He has been awarded an MBE in the Queen's Birthday Honours List for contributions to the UK defence industry and is a recipient of the John Challens' Medal, which is AWE's highest award for lifetime contributions to science, engineering and technology. He has also been honoured by VNIIA in the Russian Federation for his work in fostering nuclear weapon safety collaboration between the U.K and the RF.

References

1. Leveson, N. "A New Accident Model for Engineering Safer Systems," *Safety Science*, 2004, pp 237-270.
2. Suokas, J. "On the reliability and validity of safety analysis," Technical Report Publications 25, Technical Research Centre of Finland, Espoo, Finland, September, 1985.
3. Jones, M. "Safety Culture and High Consequence Accident/Failure Theories," International System Safety Conference (ISSC 22), 2004.
4. Jones, M. "Chasing the Black Swan," International System Safety Conference (ISSC36), 2018.