ASSURING SUBMARINE SAFETY FOR THE FUTURE SSBN

A Coverdale TC Safety Ltd, UK
T Roberts BAE Systems, UK
Y Stone MoD, UK
J Williams, FNC, UK

SUMMARY

The 2006 White Paper on the Future of the UK's Nuclear Deterrent stated: "We have therefore decided to maintain our nuclear deterrent by building a new class of submarines". The assurance of safety of such a vessel must start during the concept phase of development and this paper describes the strategy for designing safety into the future submarine. A principal design aim is to reduce physical risk, protect people and protect the environment. To achieve this, the submarine design must: enable control the major accident hazards inherent with delivery of the user requirement; provide a safe working environment for individuals onboard the submarine; and be protective of the environment. This paper describes the development of the SSBN(F) safety strategy and the reports on the experience of implementing that strategy during the concept phase of development.

1 INTRODUCTION

In December 2006, HM Government published a White Paper on the Future of the United Kingdom's Nuclear Deterrent (Reference 1), which stated:

"We have therefore decided to maintain our nuclear deterrent by building a new class of submarines".

The White Paper continues:

"Much has changed since 1980. Safety and regulatory standards have been raised over the last 25 years."

"Safety will be a key element of the design and operation of the replacement SSBNs. The operation of our nuclear-powered submarines is regulated by independent safety authorities within the MOD, whilst the Nuclear Installations Inspectorate license facilities for reactor construction and deep maintenance. A fundamental principle applied by those authorities is that successful safety risk management is founded in a proper understanding of nuclear technologies."

This RINA paper outlines the strategy that is being applied to ensure that the new class of submarine, the SSBN(F), will be safe throughout their life. A key aim of that strategy is to design safety into the future submarine; hence the process must start during the concept phase of development.

A nuclear submarine is one of the most complex machines in the world. To be successful, it must not only be able to counter the range of external hazards it may face in the environment in which it operates, e.g. collision, flood or pressure hull collapse, but must also be able to control the range of internal hazards that will exist, not least the munitions it must carry and the nuclear power plant that will provide its principal energy source.

A range of rigorous safety regulations exist against which the submarine design must be compliant, but those regulations are hazard specific, e.g. ship safety, nuclear safety or munitions safety. Compliance is essential, but as any operator in a hazardous industry realises, compliance on its own is insufficient.

It is very difficult to produce holistic regulations that recognise the demands of all other regulations; hence simple compliance with regulations is not necessarily sufficient to assure the safety of the vessel. The skill of the designer, and the skill of the operator, is equally as important as the skill of the regulator in delivering a safe solution.

2 GOAL BASED SAFETY STRATEGY

The safety strategy adopted for the control of major accident hazards is goal based, as opposed to prescription based, differentiated by the following simplistic examples:

- Goal Based: "People shall be prevented from falling over the edge of a cliff"
- Prescriptive: "You shall install a 1 metre high rail at the edge of the cliff"

2.1 INTERNATIONAL MARITIME ORGANISATION

Such a goal based strategy has been proposed by the International Maritime Organisation (IMO), the Maritime Safety Committee (Reference 4) agreeing a five-tier system comprising:

- Tier 1 - Goals.

- Tier 2 - Functional Requirements.
- Tier 3 - Verification of Compliance Criteria.
- Tier 4 - Technical Procedures & Guidelines; Classification Rules; and Industry Standards.
- Tier 5 - Codes of Practice; Safety & Quality Systems; Operation; Maintenance; Training; Manning.

The future submarine safety strategy is consistent with the IMO approach and the case it is intended to produce will draw upon the concepts of Goal Structuring Notation outlined by Kelly (Reference 1).The case will comprise:

- Goals: articulating the claims that must be achieved to ensure safety.
- Strategies: presenting the argument how the goals are to be achieved.
- Justification: to provide the evidence to substantiate that the goals can be achieved.

Bench-marking the two methodologies:

- Tier 1 Goals; correspond to the goals that the safety case must substantiate.
- Tier 2 Functional Requirements; correspond to the strategy how the safety case will be made.
- Tier 3, 4 & 5 Criteria, Rules and Standards; correspond to the justification to substantiate the safety case.

This paper is focused on the derivation of the Functional Requirements.

2.2 FUTURE SUBMARINE SAFETY GOAL

The top tier safety goal for the future submarine is to:

To develop a cost-effective submarine for which all risks to the workforces, the public and the environment have been reduced so far as is reasonably practicable , when it is operated independently or in conjunction with a shore support facility throughout the life of the submarine.

To achieve this, the submarine must incorporate measures to:

- Reduce the probability of major accidents to a level that is as low as reasonably practicable (ALARP) and tolerable.
- Limit the consequence to people and the environment of any major accidents which do occur.
- Provide a safe working environment for individuals onboard the submarine.
- Impose acceptable environmental impact.

To reduce project risk, the management safety must also:

- Reduce the financial risk of safety driven cost escalation.
- Reduce the risk of programme delays caused by back-fitting safety analysis and back-fitting safety driven changes to the design.

3 SAFETY STRATEGY

A strategy is essential for producing a coherent case that seeks to achieve the top tier safety goal, which must addresses:

- Control of Major Accident Hazards.
- Provision of a Safe Working Environment.
- Protection of the Environment.

The requirement to differentiate between the Control of Major Accident Hazards and the Control of Local Hazards to Individuals to provide a Safe Working Environment is emphasised by Baker (Reference 3) in his assessment of the BP Texas City refinery accident in March 2005, which states:

"BP appears to have established a relatively effective personal safety management system by embedding personal safety aspirations and expectations within the U.S. refining workforce. However, BP has not effectively implemented its corporate-level aspirational guidelines and expectations relating to process risk. Therefore, the Panel found that BP has not implemented an integrated, comprehensive, and effective process safety management system for its five U.S. refineries."

The Baker report presented the findings of an independent investigation into a catastrophic process accident at the BP Texas City refinery on March 23, 2005. It was described as one of the most serious U.S. workplace disasters of the past two decades, resulting in 15 deaths and more than 170 injuries.

In the Baker Report, Process Risk refers to the Control of Major Accident Hazards and Personal Safety refers to the control of local hazards to individuals to achieve occupational health and safety in order to provide a Safe Working Environment. The significance of the report is that while BP believed they had an effective safety management system, it was focused on one aspect of safety only - personal risk. It did not address process risk or the control of major accident hazards.

Implementation of a strategy requires a number of supporting tactics, including:

- Plan, for the Control of Major Accident Hazards.
- Plan, to provide a Safe Working Environment.
- Plan, to enable Environmental Protection.

- Management System, to define Roles and Responsibilities.

The safety and environmental strategy for the future submarine is summarised at Figure 1.

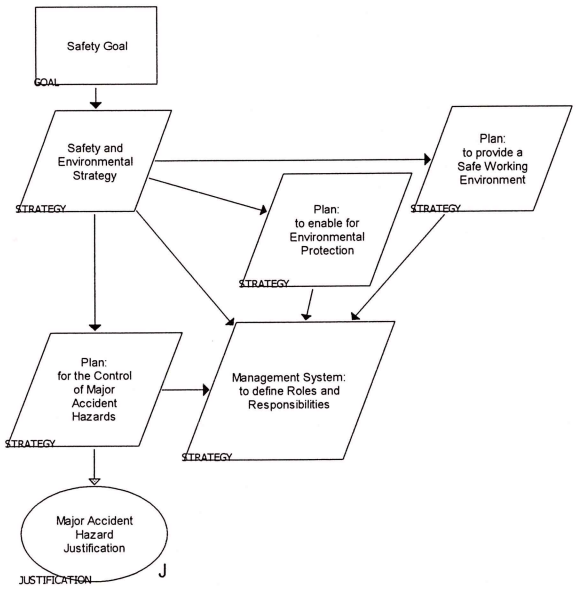

Figure 1. Safety Strategy and Plans

3.1 HAZARDS AND THE CONTROL OF HAZARDS

Hazard, Risk and Safety have the following meanings:

- A Hazard is the intrinsic property of an entity that has the potential to cause harm.
- Risk is the chance that someone will be adversely affected by a Hazard.
- Safety is the state achieved when the Risk arising from a Hazard has been reduced to an acceptably low level.

Hazards are addressed in two categories:

- Major Accident Hazards: hazards that could
  - cause loss of the submarine;
  - cause serious injury or death of multiple persons onboard the submarine; or
  - present a serious threat to life, property or the environment external to the submarine.
- Local Hazards to Individuals: hazards that could
  - cause the death, serious injury or minor injury of an individual person onboard the submarine.

The safety strategy requires the application of different approaches to mitigation of the two categories of hazard, defined as:

- 'Top Down' Control of Major Accident Hazards.
- 'Bottom Up' provision of Occupational Health and Safety.

The strategy for protection of the environment will follow a similar method. A major accident is equally likely to cause environmental damage as loss of life. The Control of Major Accident Hazards is therefore equally applicable to environmental protection as safety. The environmental equivalent of Occupational Health and Safety is:

- 'Bottom Up' Pollution Prevention and Control.

This paper focuses on the Control of Major Accident Hazards.

3.2 'TOP DOWN' CONTROL OF MAJOR ACCIDENT HAZARDS

The strategy for the 'Top Down' Control of Major Accident Hazards is based upon three tenets, shown diagrammatically at Figure 2:

Tenet 0.1 Function: the functions necessary to control the major accident hazards inherent with delivery of the user requirement will be derived.
Tenet 0.2 Management: management arrangements will be put in place to enable the design and construction of structures, systems and components to enable the performance of those functions.
Tenet 0.3 Substantiation: evidence will be presented as justification that the structures, systems and components are able to perform the necessary functions in order to substantiate the case.

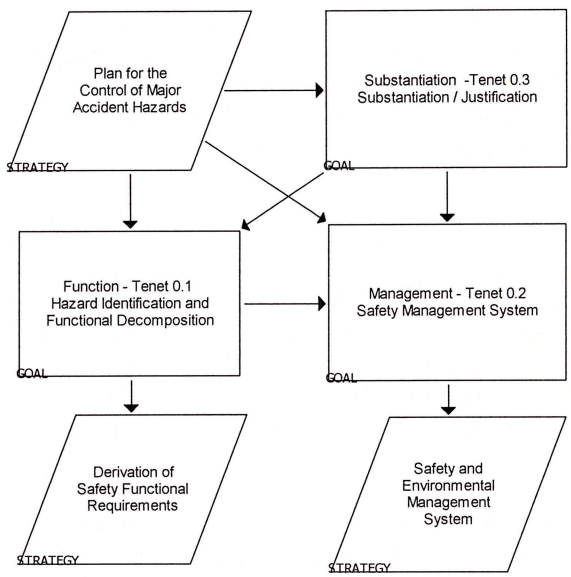

Figure 2. Control of Major Accident Hazard Tenets

The significant points to note are:

- The strategy is safety lead, not compliance lead; i.e the aim of the strategy is to develop a logical argument, supported with appropriate evidence, to demonstrate that the submarine is safe, and thereby satisfy appropriate legislation. The aim is not to simply demonstrate compliance with standards and regulations.
- The strategy aims to inform the design process; i.e the aim is not to retrospectively assess a pre-existing design.
- The strategy is function lead, not system lead; i.e. the aim is demonstrate that those functions necessary to control major accident hazards can be performed, not to simply assess the performance of bounded sub-systems.

The achievement of Tenet 0.1, Function, requires derivation of the Functional Requirements, which involves:

- Identification of those hazards having the potential to cause a major accident that the submarine is required to face in order to deliver the user requirement.
- Challenge of the user requirement to reduce or eliminate the hazards to which the submarine must be exposed.
- Identification of the safety functions that must be performed to control the residual major accident hazards.
- Option generation to propose the combination of submarine systems and sub-systems that could perform the identified safety functions.
- Application of the defence in depth methodology to achieve the safety function integrity commensurate with the unmitigated consequences of each hazard.
- Reduction of the sub-system options to the preferred, chosen, submarine system configuration.

This process requires Functional Decomposition of the User Requirement, and the Safety Functional Requirements necessary to mitigate the major accident hazards inherent with delivery of the User Requirement, to establish the proposed submarine system architecture. Early performance of this exercise will be key to successful implementation of the safety strategy.
The major accident hazards considered include, but are not limited to:

- External Hazards: arising from the environment within which the submarine is required to operate:
  - Sea: pressure creating the potential for hull collapse.
  - Sea: creating the potential for flooding leading to excess submarine weight.
  - Weather: causing extreme motion, acceleration and displacement.
  - Navigation hazards: creating the potential for collision or grounding.
- External Hazards: Impact:
  - Dropped Loads.
- Internal Hazards:
  - Nuclear Materials.
  - Radioactive Materials.
  - Breathable Atmosphere:
    - Temperature and Humidity.
    - Chemical Composition.
  - Flammable Materials.
  - Explosive Materials.
  - Oxidants.
  - Propellants.

4 FUNCTIONAL REQUIREMENTS

An SSBN must perform numerous safety functions in order to control the range of major accident hazards that it will face in service. In order to develop a coherent safety case, it is necessary to derive a logical decomposition of the Safety Functional Requirements (SFR) that are necessary to control the identified major accident hazards. Derivation of that logical derivation is the first challenge facing the SSBN(F) design team.

4.1 FUNDAMENTAL SAFETY FUNCTIONS

Such an approach has been applied by the nuclear industry for a number of years, articulated in the concept of Fundamental Safety Functions. The International Atomic Energy Agency (IAEA) identify three fundamental safety functions that must be performed in order to control the major accident hazards inherent with the delivery of nuclear power (Reference 5):

- Control of Reactivity.
- Removal of Heat from the Core.
- Confinement of Radioactive Materials.

These Fundamental Safety Functions are applicable to the SSBN(F), but address the hazard associated with nuclear materials used for power generation only. There are clearly more fundamental functions required to address the full range of hazards. The question is therefore asked:

- Can a family of Fundamental Safety Functions be defined that describe all of the safety functional requirements for the submarine?
- Can those functions be expressed as a single logical decomposition?
- Can the interaction between those functions be identified and managed?

The first step is to define what constitutes a Fundamental Safety Function, the resultant definition being:

A high level operation that the submarine must perform to control a major accident hazard, and which, if lost, will result in an initiating event that could cause a major accident.

4.2 KEY SAFETY FUNCTIONS

The IAEA Fundamental Safety Functions are applicable to nuclear power. To achieve the aspiration of a whole boat safety functional decomposition it is necessary to start at a tier above the fundamental safety functions. The expression chosen to define such top level functions is 'Key Safety Functions', around which the Fundamental Safety Functions are brigaded. Six Key Safety Functions are identified:

- Vehicle Control:
  Control the submarine vehicle in six degrees of freedom.
- Power and Propel:
  Provide the propulsive power, non propulsive power and waste heat removal required to control the submarine vehicle.
- Generate Nuclear Power:
  Generate the power necessary to control the submarine vehicle from nuclear heat.
- Sustain Life:
  Sustain life onboard the submarine vehicle.
- Handle Ordnance, Munitions and Explosives:
  Control the major accident hazards associated with embarking, handling, storing, discharging and disembarking munitions.
- Control Fire Hazards:
  Fire threatens each of the Key Safety Functions, hence the control of fire hazards is managed as a Key Safety Function in its own right.

The nature of a nuclear submarine is such that a significant major accident hazard remains even when along side, by nature of its propulsion plant and onboard munitions. The safety case must therefore be considered in context of its operating regimes, giving rise to the operating regimes:

- **Sea**:
  Operations under self control in open water.
- **Shore**:
  Operations under external controls when alongside, docked or being manoeuvred by tugs. The Shore case also considered the through life case of maintenance, long overhaul and disposal.

The Key Safety Functions, the major accident hazards they control, and the regimes in which the submarine will be operated are shown diagrammatically at Figure 4.

4.3 VEHICLE CONTROL

The fundamental safety functions to enable vehicle control are shown at Figure 5.
The accidents that the vehicle control function seeks to prevent are:

- Collisions;
- Grounding, either surfaced or dived; and
- Exceeding the submarine's crush depth, caused either by flooding or by uncontrolled manoeuvring.

The function also includes the means to enable external control of the submarine, either by towing or salvage, to regain control the submarine and its installed systems and equipment, should the submarine's ability for self control be lost.

The fundamental safety functions that enable vehicle control are:

- Provide structural integrity;
- Control buoyancy and weight;
- Maintain stability;
- Navigate the submarine, including communication with third parties;
- Self control of submarine manoeuvring, surfaced and dived; and
- External control of the submarine by mooring, berthing, anchoring, towing and salvage.

The key points to note are:

- Vehicle control involves the application of naval architecture disciplines to enable the control of an underwater vehicle, navigation disciplines and communication disciplines.
- Vehicle control makes demands on marine engineering for propulsion, recognising that without forward motion hydrodynamic control surfaces are ineffective.
- Vehicle control makes demands on marine engineering for non-propulsive power, to actuate control surfaces.

The division of analysis by physical system or technical discipline tends to encourage 'stove-piping' of the design, which hinders the construction of a logical case that the submarine is safe.

The benefit of functional analysis is that a logical case can be made to articulate those functions must be performed in order to control the major accident hazards faced by the submarine. The design of systems to enable the performance of those functions can be informed by that analysis and evidence can be collated to provide a justification that those functions can be performed with

the correct integrity; hence a substantiated safety case can be made.

4.4 POWER AND PROPEL

The fundamental safety functions brigaded under power & propel are at Figure 6.

The power & propel function differs from the other key safety functions in that its does not directly control any major accident hazards; it is however essential to enabling performance of the other key safety functions.

The three fundamental safety functions brigaded under power & propel are:

- Deliver Propulsive Power: deliver own ship thrust, as demanded by vehicle control.
- Deliver Non-Propulsive Power: generate, transmit, store, distribute, convert and deliver non-propulsive power to perform the key safety functions.
- Remove Waste Heat: remove waste heat and transfer that heat to an ultimate heat sink.

The key points to note are:

- The delivery of propulsive power is in direct support of vehicle control. The integrity of propulsive power is key to safe vehicle control, in particular, in extremis, the ability to provide emergency propulsive power to restore vehicle control in response to a manoeuvring incident or major flood.
- The delivery of non-propulsive power is in direct support of each of the key safety functions:
  - Vehicle control: to actuate control services.
  - Generate nuclear power: to drive rotating machinery necessary to remove heat from the core.
  - Sustain life: to control the internal environment of the submarine.
  - Handle munitions: to control the induced climatic environment in munitions storage compartments.
- The removal of waste heat is in direct support of each of the key safety functions:
  - To transfer nuclear decay heat to an ultimate heat sink.
  - To transfer waste heat from the habitable areas of the submarine to an ultimate heat sink.
  - To transfer waste heat from munitions storage compartments to an ultimate heat sink.
- In order to deliver the power & propel function a number of additional hazards may be introduced into the submarine, including high energy electrical power, lubricating oil, high pressure hydraulic fluid and high pressure air.
- Such secondary hazards may contribute to the onboard fire hazard; hence the control of fire hazards is a supporting function to the delivery of power and propulsion.

4.5 GENERATE NUCLEAR POWER

The fundamental safety functions supporting the generation of nuclear power are shown at Figure 7. The accidents that the nuclear power function seeks to prevent are:

- The uncontrolled exposure of people to radiation.
- The uncontrolled release of energy from nuclear material.
- The uncontrolled release of radioactive material to the environment.

Nuclear power must also be generated with adequate integrity to support the power & propel function, which in turn supports the other key safety functions, most notably vehicle control.

The three fundamental safety functions identified by the IAEA that enable the safe generation of nuclear power are:

- Control of reactivity.
- Removal of heat from the core.
- Confinement of radioactive materials.

In addition, the IAEA identify four radiological protection requirements:

- Shield radioactive materials.
- Minimise human activity in radiation fields.
- Minimise the quantity of radioactive materials produced.
- Treat radioactive materials to reduce the dispersal of radioactive materials within the plant.

The key points to note are:

- The control of reactivity to prevent the uncontrolled release of nuclear energy is synonymous with the control of power generation to support the power & propel function.
- The removal of heat from the core is dependent on the provision of non-propulsive power to drive the rotating equipment employed in the transfer of that heat.
- The removal of heat from the core is also dependent on the provision of heat sink to which nuclear heat can be transferred.
- Claims are made on the structural integrity of the submarine hull for the containment of radioactive materials.
- Claims are made on the confinement, shielding, treatment and minimisation of radioactive materials in order to sustain life onboard the submarine.

- Claims are made on the control of human activity in radiation fields to sustain life onboard the submarine.
- Claims are made on the control of fire hazards to protect nuclear safety critical systems.

4.6 SUSTAIN LIFE

The fundamental safety functions required to sustain life are shown at Figure 8.

The accidents that the sustain life function seeks to prevent are the loss of multiple lives as a result of a gross excursion of the environment onboard the submarine, including:

- Asphyxiation due to loss of atmospheric control.
- Heat exhaustion and heat stoke due to loss of control of the onboard thermal environment.
- Uncontrolled exposure to radiation.

The sustain life function also seeks to:

- Prevent crew fatigue, which would be a contributory factor to the failure to perform other safety functions.
- Enable escape, rescue and abandonment, which may be necessary should it prove impossible to sustain life onboard.

The sustain life function does not encompass occupational health and safety, which is addressed in a separate strategy focused on the control of local hazards to individuals.

The safety functional requirements to sustain life are:

- Control the internal environment of the submarine.
- Provide hotel services to prevent fatigue and illness.
- Protect people from radiation.
- Enable escape, rescue and abandonment.

The key points to note are:

- The sustain life function is dependent upon the power & propel function to drive the equipment required to control the internal environment of the submarine.
- The sustain life function is dependent upon confinement, shielding, treatment and minimisation of radioactive materials.
- The sustain life function is dependent upon the control of human activity in radiation fields.
- The grace time between the failure of certain sustain life functions and catastrophic consequences can be large, but if such failures are not corrected the consequences will be realised. The hazards to sustaining life onboard a submarine must not therefore be underestimated.

4.7 HANDLE MUNITIONS

The fundamental safety functions required to handle munitions safely are shown at Figure 9.

The accidents that the handle munitions function seek to prevent are:

- The uncontrolled discharge of weapons.
- The uncontrolled ignition of fuel and propellants.
- The uncontrolled detonation of explosives.
- The uncontrolled exposure of people to radiation.
- Yield.

The context within which the handling of munitions is addressed is the:

- Embarkation of munitions.
- Storage of munitions.
- Onboard handling of munitions.
- Discharge of munitions.
- Disembarkation of munitions.

The key points to note are:

- The principle strategy for the safe handling of munitions revolves around the provision of a general naval environment within which munitions are demonstrable stable. The general naval environment is defined by the:
  - Natural and induced climatic environment.
  - Chemical and biological environment.
  - Mechanical environment.
  - Threat and accident environment.
  - Electromagnetic environment.
- The provision of a general naval environment is dependent upon other key safety functions, principally the power & propel function for the delivery of non-propulsive power and the removal of waste heat.
- The handling of munitions is also closely linked to the control of fire hazards. A further fundamental safety function is therefore to contain fuels, propellants and explosives in properly constituted storage systems in support of fire prevention.

4.8 NAVAL SHIP CODES

The SSBN(F) strategy is consistent with the concept of 'Naval Ship Codes' (Reference 6), which considers:

- General Provisions.
- Structure.
- Buoyancy and Stability.
- Machinery installations.
- Electrical installations.
- Fire Safety.

- Escape, Evacuation and Rescue.
- Radio communications.
- Safety of Navigation.
- Carriage of Dangerous Cargoes.

Bench-marking the two concepts:

SSBN(F) Strategy	Naval Ship Code
Vehicle Control	Structure
	Buoyancy and Stability
	Radiocommunications
	Safety of Navigation
Power & Propel	Machinery Installations
	Electrical Installations
Generate Nuclear Power	
Sustain Life	Escape, Evacuation and Rescue
Handle Munitions	Carriage of Dangerous Cargoes
Control Fire Hazards	Fire Safety

5 SYSTEM FUNCTIONAL REQUIREMENTS

It has thus been demonstrated necessary to perform thirty two fundamental safety functions in order to achieve the six key safety functions. To relate the fundamental safety functions to the submarine design it is next necessary to further decompose the fundamental safety functions into the functional requirements for physical systems.

Two examples of such decompositions are considered in this paper:

- Control of Buoyancy and Weight.
- Provision of propulsion and non-propulsive power.

CONTROL OF BUOYANCY AND WEIGHT
An obvious submarine function is the control of buoyancy and weight, the functional model for which is at Figure 11.

It is necessary to adjust submarine weight in order to achieve neutral buoyancy when dived in response to:

- Changes in internal weight, including weapons discharge; and
- Changes in buoyancy arising from changes in sea water density and submarine compressibility.

Control of weight is achieved by:

- Coarse control of fixed bodily weight; and
- Fine control, or trim, of variable bodily weight.

In order to control variable bodily weight it is necessary to control the:

- Ingress of water;
- Egress of water; and
- Distribution of weight in order to control pitch and heel.

The control of watertight integrity also supports the control of the ingress of water, the loss of watertight integrity being an uncontrolled ingress of water.

The control of buoyancy and weight also supports the control of depth, the control of depth being dependent upon two functions:

- The control of variable weight; and
- The dynamic control of lift from the hydroplanes.

Dynamic lift is further dependent upon the two functions:

- Control of submarine hydroplanes.
- Control of speed.

5.1.1 Power and Propulsion

The control of submarine speed makes claims on the provision of propulsive power to provide submarine thrust and the control of hydroplanes makes claims on the provision of non-propulsive power for actuation. The control of variable weight is also dependent upon the provision of non-propulsive power, either to pump water out of the submarine, or to blow main ballast.

5.2 PROPULSIVE AND NON-PROPULSIVE POWER

The functional diagram for the provision of non-propulsive power is shown at Figure 12.

5.2.1 Non-Propulsive Power

The option exists to provide non-propulsive power in a number of forms, including:

- Electrical power;
- Hydraulic power; and
- HP air.

With each power source are embodied the supporting functions:

- Generate power;
- Distribute power; and
- Store energy.

Each power source however draws from a common energy source of distributed electrical power, which in turn draws upon the electrical power transmission. Differentiation is made between transmission and distribution:

- Power Transmission: is the process of bulk transfer of electrical power between generators, main switchboards, switchboard inter-connectors and main propulsion motors;
- Electricity Distribution: is the delivery of electrical power to discrete equipments.

The electrical transmission system draws it power from one of a number of sources:

- Onboard generated electrical power.
- Onboard stored electrical power (main battery).
- Over side supplied electrical power (harbour supplies).

Options also exist for onboard generation:

- Turbo-generators; or
- Diesel-generators.

The generation of electrical power by turbo generator is dependent upon nuclear power.

5.2.2 Propulsion

Propulsive power and non-propulsive power are closely linked:

- Main turbines draw upon the same steam source as the turbo-generators;
- Propulsion motors draw upon electrical transmission; and the option exists to use
- Hydraulic motors which draw upon the hydraulic system.

Having established the system functional requirements, it is necessary to establish the means by which the required integrity of function can be achieved, which requires the application of defence in depth.

6 DEFENCE IN DEPTH

Defence in depth is a methodology that has been in use in the nuclear industry for a number of years, the methodology being described in the guidance at Reference 7. The guidance states:

"All safety activities, whether organisational, behavioural or equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large. This idea of multiple levels of protection is the central feature of defence in depth."

The objectives of Defence in Depth are:

- To compensate for potential human and component failures.
- To maintain the effectiveness of barriers by averting damage to the plant and to the barriers themselves.
- To protect the public and the environment from harm in the event that these barriers are not fully effective.

The IAEA identify five Levels of Defence, summarised in Figure 3.

Defence in Depth		
	Objective	Essential Means
1	Prevention of Abnormal Operation and Failures	Conservative Design and High Quality in Construction and Operation
2	Detection of Failures and Control of Abnormal Operation	Control, limiting and protection systems and other protection features.
3	Control of accidents within the design basis	Engineered safety features and accident procedures.
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
5	Mitigation of the Radiological Consequences of significant releases of radioactive materials	Off site emergency response

Figure 3. Defence in Depth

The methodology was developed for civil nuclear power plant, but is equally applicable to other hazardous industries. Levels 1 to 4 are generic to all major accident hazards, whereas level 5 is specific to radiological release. Level 5 can be considered more generic if the means of achievement are considered to include any form of external support in response to a major accident, levels 1 to 4 being achieved by means that are indigenous to the plant.

The concept can also be expressed as a 'bow-tie', as shown in Figure 13.

An accident sequence can be envisaged:

- Normal operation; the failure of which results in
- Abnormal operation; the failure of which is a
- Postulated initiating event; the consequences of which are considered an
- Incident; which if unchecked will result in an
- Accident.

Defence in depth is provided to present barriers to the progression of such an accident sequence. Arrangements must be provided to:

- Prevent deviations from normal operation; which must include the means of
- Detecting a deviation from normal operation; in response to which the means must be provided to
- Prevent deviations from normal operation becoming accidents; which must be reinforced with
- Engineered safeguards; themselves reinforced with onboard
- Severe accident management arrangements; supported by
- External accident management arrangements.

6.1 CONTROL FIRE HAZARDS

The control of fire hazards underpins each of the key safety functions, and hence whole ship safety; fire having the potential to inhibit any or all of the fundamental safety functions. Rather than have multiple strategies for the control of fire hazards, it is proposed to apply one whole boat strategy which will:

- Address the control of fire hazards as a coherent whole ship strategy; but apply
- Targeted strategies in circumstances where specific hazards demand it.

The control of fire hazards is an example of the application of defence in depth, but in recognition of its whole boat significance it is treated as a key safety function.

The fundamental safety functions to enable the control of fire hazards are shown at Figure 10. Those functions are:

- Prevent fire;
- Detect fire;
- Control fire; including the suppression and extinguishing of fire
- Protect safety critical systems; and
- Recover from fire.

7 SUBMARINE SAFETY CASE

The submarine safety case will be made when:

- The key safety functions are defined; the achievement of which requires derivation of
- The fundamental safety functions; the achievement of which requires derivation of
- The system functional requirements; the achievement of the required integrity requires
- Defence in depth.

The amount of defence in depth requires consideration of:

- The consequences of loss of a fundamental safety function; and
- The inherent integrity of systems.

7.1 TOOLS

The management of the SSBN(F) safety strategy is heavily dependent upon information management and information management tools. Reliable relational databases are essential for efficient management, two tools in particular being applied, the:

- Adelard Safety Case Editor; and
- Telelogic System Architect.

The tools are being used in a complementary fashion: the Adelard tool being used for model building in conjunction with facilitated workshops, and for post workshop optioneering and refinement; and the Telelogic tool being used as the archive for agreed solutions to which many users will have access. Both tools enable the presentation of data using graphical techniques, which is essential for functional modelling. Experience shows that complex interactions quickly become difficult to follow when using non graphical databases and spreadsheets.

8 CONCLUSIONS

The strategy for production of a federated whole boat safety case for the SSBN(F) seeks to produce a logical decomposition of the functions that the submarine must be able to perform in order to control the major hazards that are inherent with delivery of the users requirement.

The division of analysis by physical system or technical discipline tends to encourage 'stove-piping' of the design, which hinders the construction of a logical case that the submarine is safe.

The benefit of functional analysis is that a logical case can be made to articulate those functions must be

performed in order to control the major accident hazards faced by the submarine. The design of systems to enable the performance of those functions can be informed by that analysis and evidence can be collated to provide a justification that those functions can be performed with the correct integrity; hence a substantiated safety case can be made.

The strategy is consistent with a number of safety methodologies for the control of major accident hazards in a number of hazardous industries, including:

- IMO goal based safety strategy.
- IAEA fundamental safety functions.
- NATO naval ship codes.
- IAEA defence in depth.

The strategy also incorporates the lessons learnt from major accidents, such as the BP Texas accident in March 2004, by differentiating between the control of major accident hazards and the achievement of occupational health and safety.

The strategy is being applied at the earliest point in the design cycle to:

- Inform the design.
- Enable the establishment of the level of defence in depth by the end of the concept phase.

9 REFERENCES

1. *HM GOVERNMENT, 'The Future of the United Kingdom's Deterrent',* Secretary of State for Defence, *2006*

2. *KELLY, T., 'A systematic approach to safety case management',* University of York, *2003.*

3. *BAKER, J. A., 'The Report of the BP US Refineries Independent Safety Review Panel',* BP US Refineries Independent Safety Review Panel, *2007*

4. *INTERNATIONAL MARITIME ORGANISATION, 'Goal-Based Construction Standards for New Ships'* , Maritime Safety Committee, *79th Session, 2004.*

5. *INTERNATIONAL ATOMIC ENERGY AGENCY, 'Safety of Nuclear Power Plants: Design',* IAEA Nuclear Safety Requirements, *2000*

6. *RUDGLEY, G., BOXALL, P., ter BEKKE, E., and HUMPHREY, R., 'Development of a NATO 'Naval Ship Code',* Transactions of RINA, *2005*

7. *INTERNATIONAL ATOMIC ENERGY AGENCY, 'Defence in Depth in Nuclear Safety,* International Nuclear Safety Advisory Group, *1996*

10 AUTHORS

The authors comprise the safety management team for the successor SSBN.

Tony Coverdale (TC Safety Ltd, contracted to the Ministry of Defence) is the Platform Safety Manager for the SSBN(F) and part of the Client Team for development of the submarine.

Tim Roberts (BAE Systems) is the Safety Manager within the Provider organisation, working opposite the Platform Safety Manager to provide Client / Provider collaboration.

Yvonne Stone (Ministry of Defence) is the Assurance Manager within the Client Team, co-ordinating assurance of the work performed by the safety managers on behalf of the Integrated Project Team Leader.

John Williams (FNC) is currently the Independent Safety Advisor supporting the Assurance Manager.

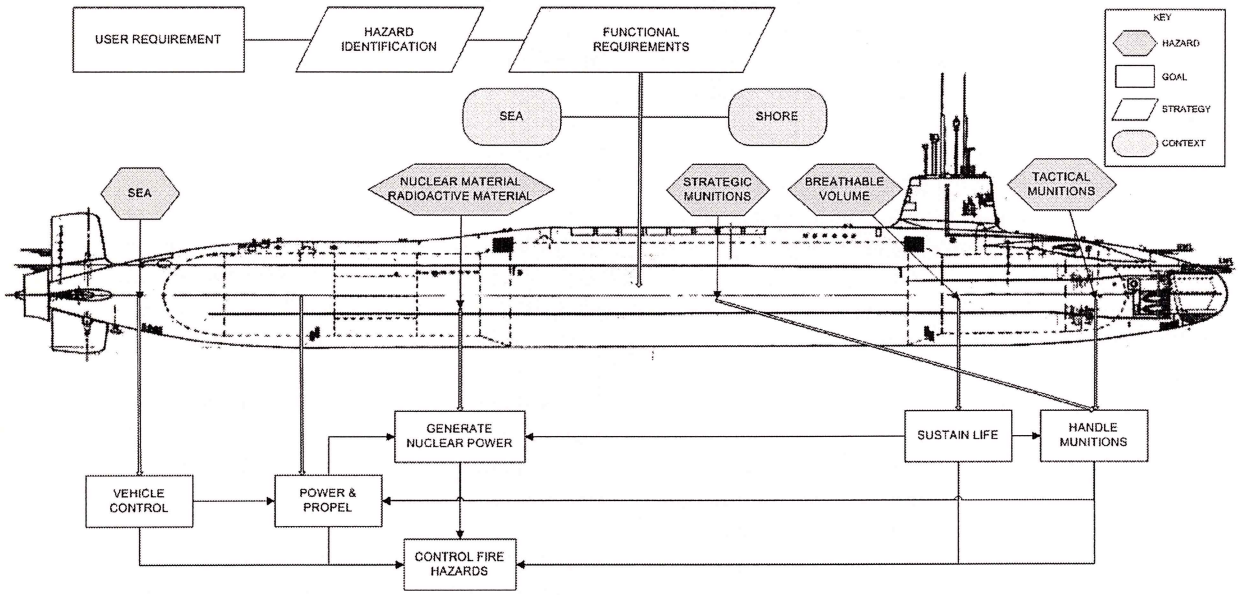

Figure 4. Key Safety Functions

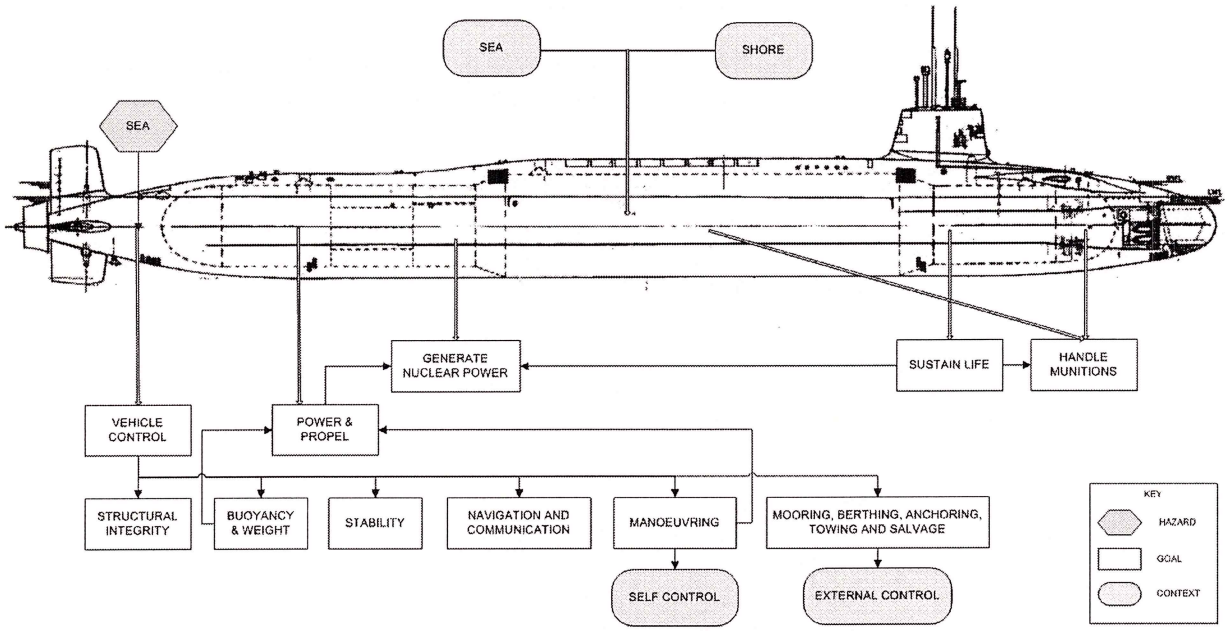

Figure 5. Vehicle Control

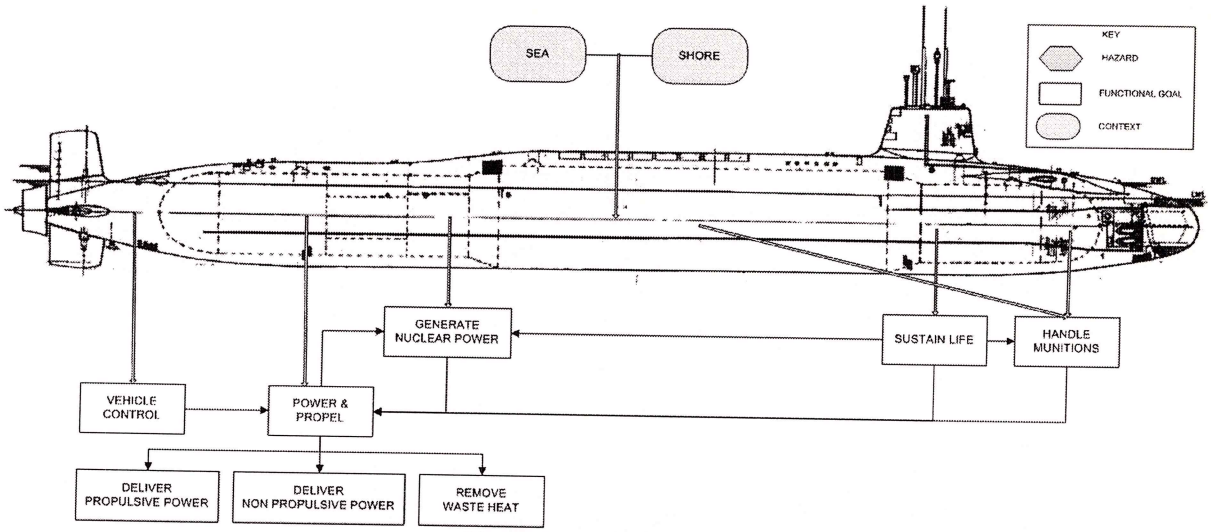

Figure 6. Power and Propel

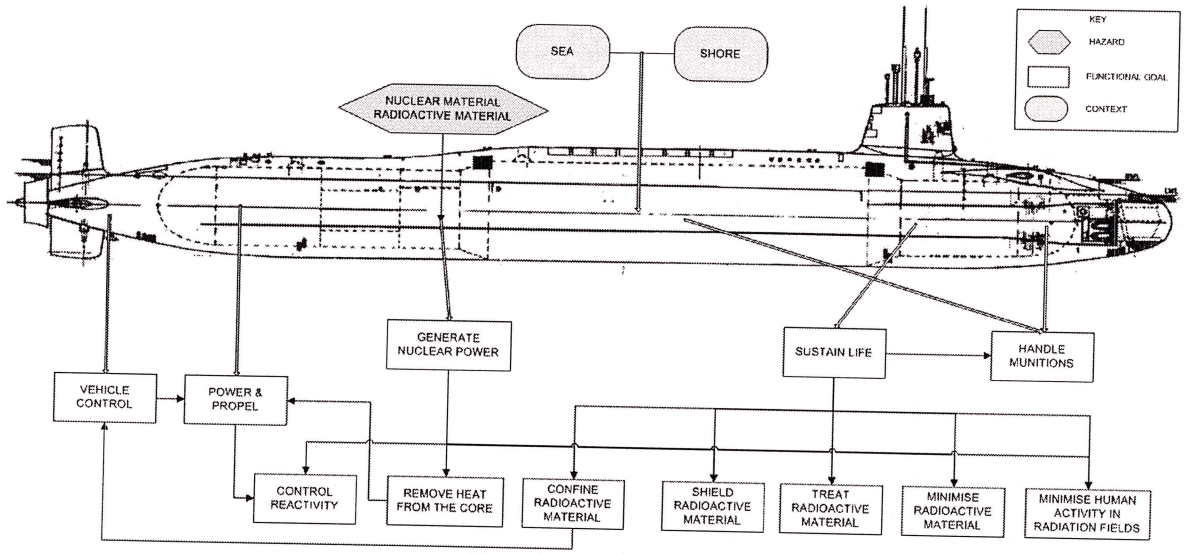

Figure 7. Nuclear Power

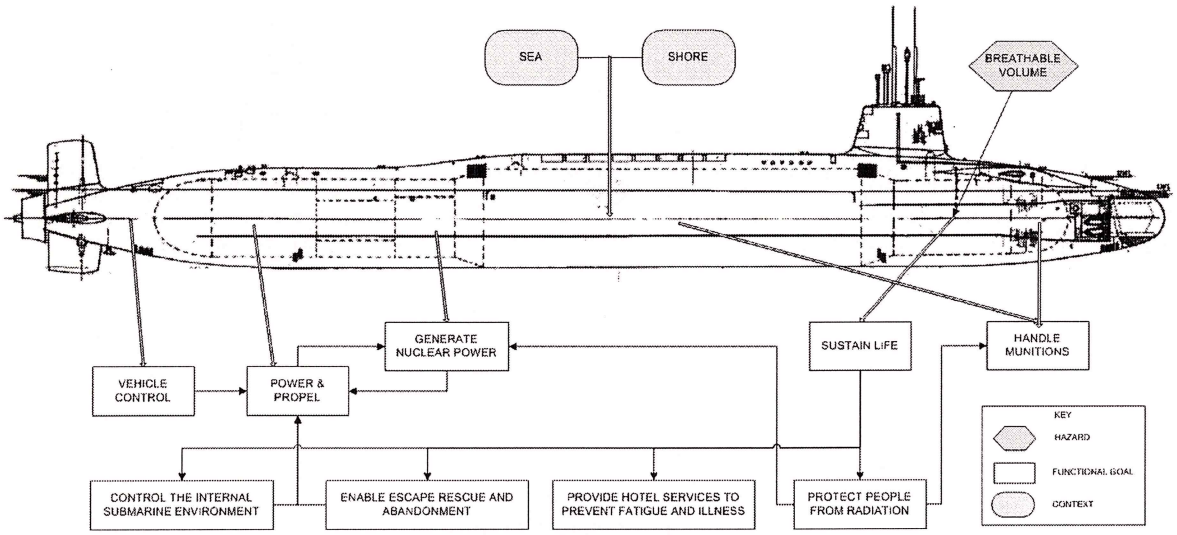

Figure 8. Sustain Life

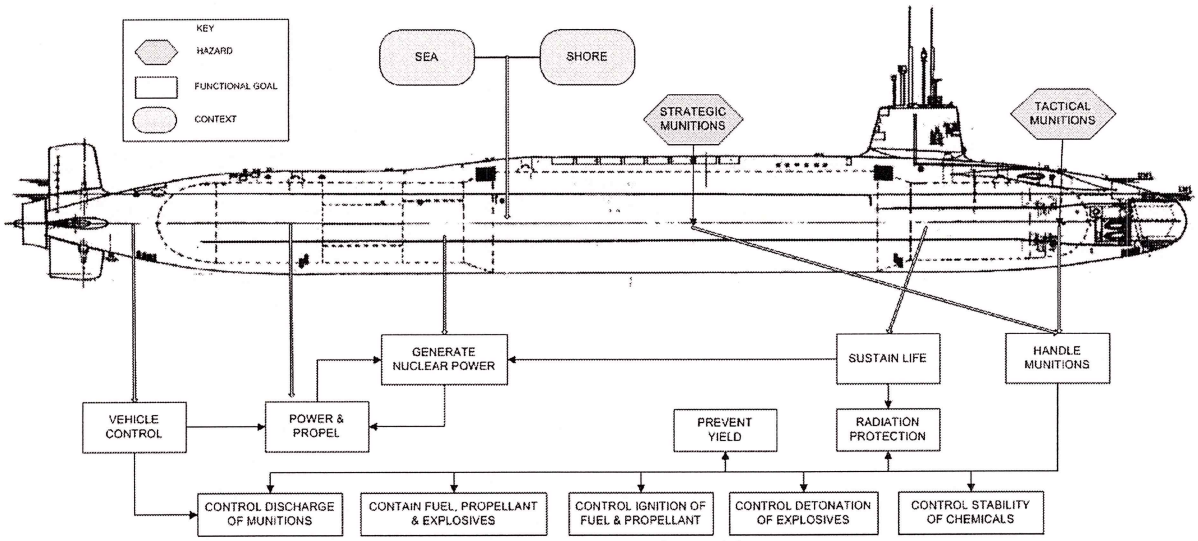

Figure 9. Handling of Munitions

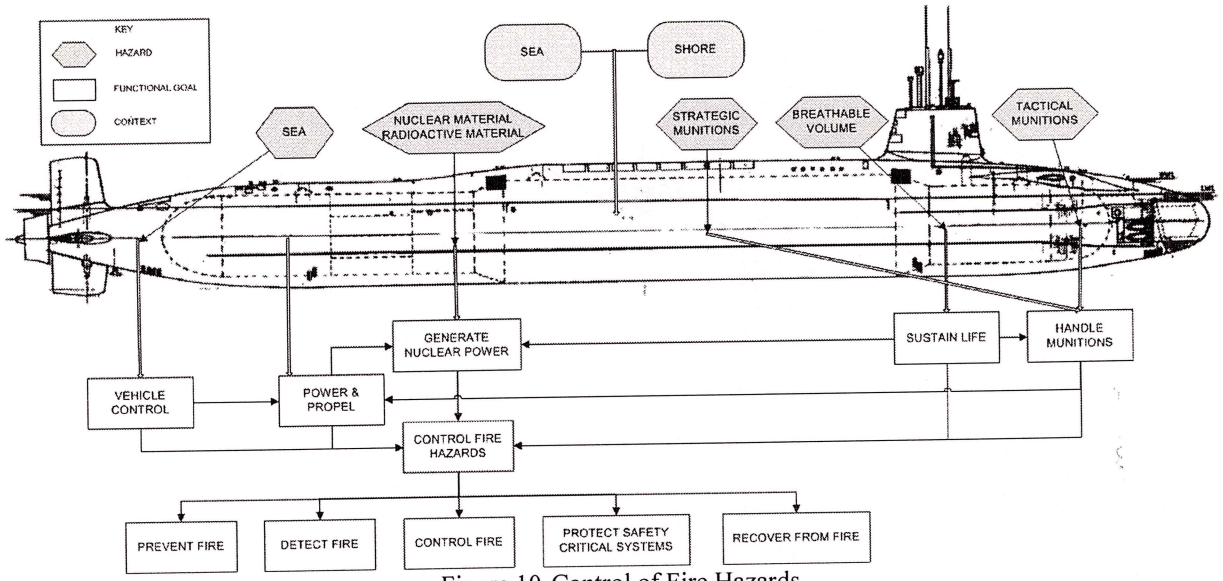

Figure 10. Control of Fire Hazards

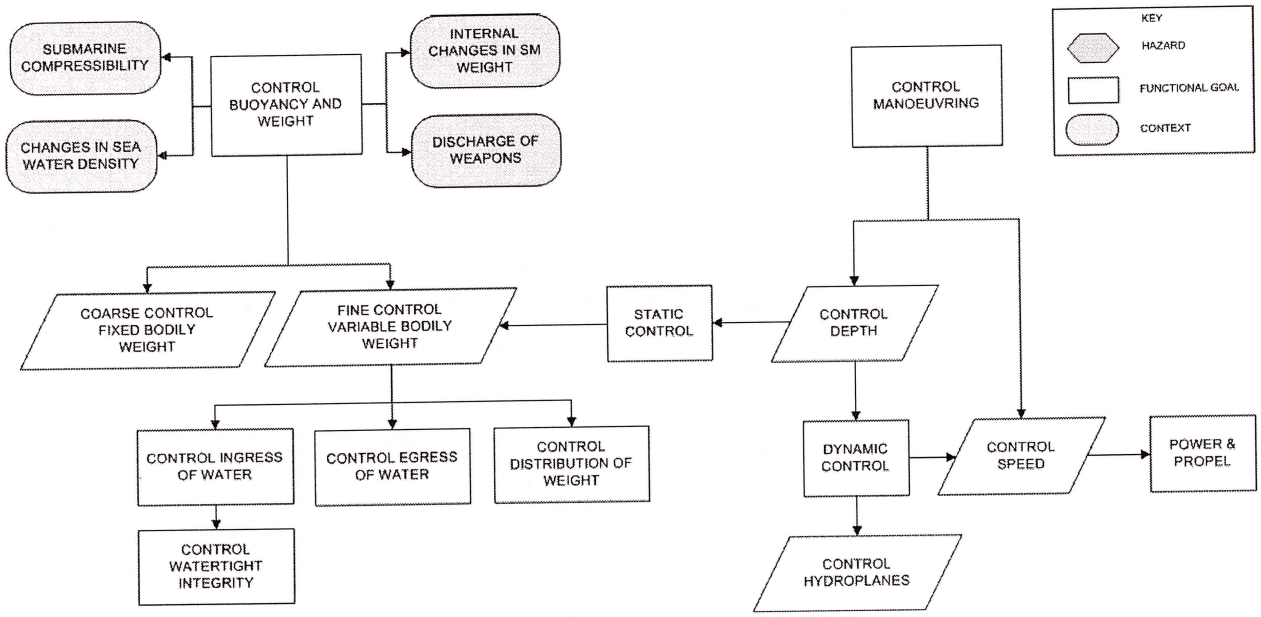

Figure 11. Control of Buoyancy and Weight

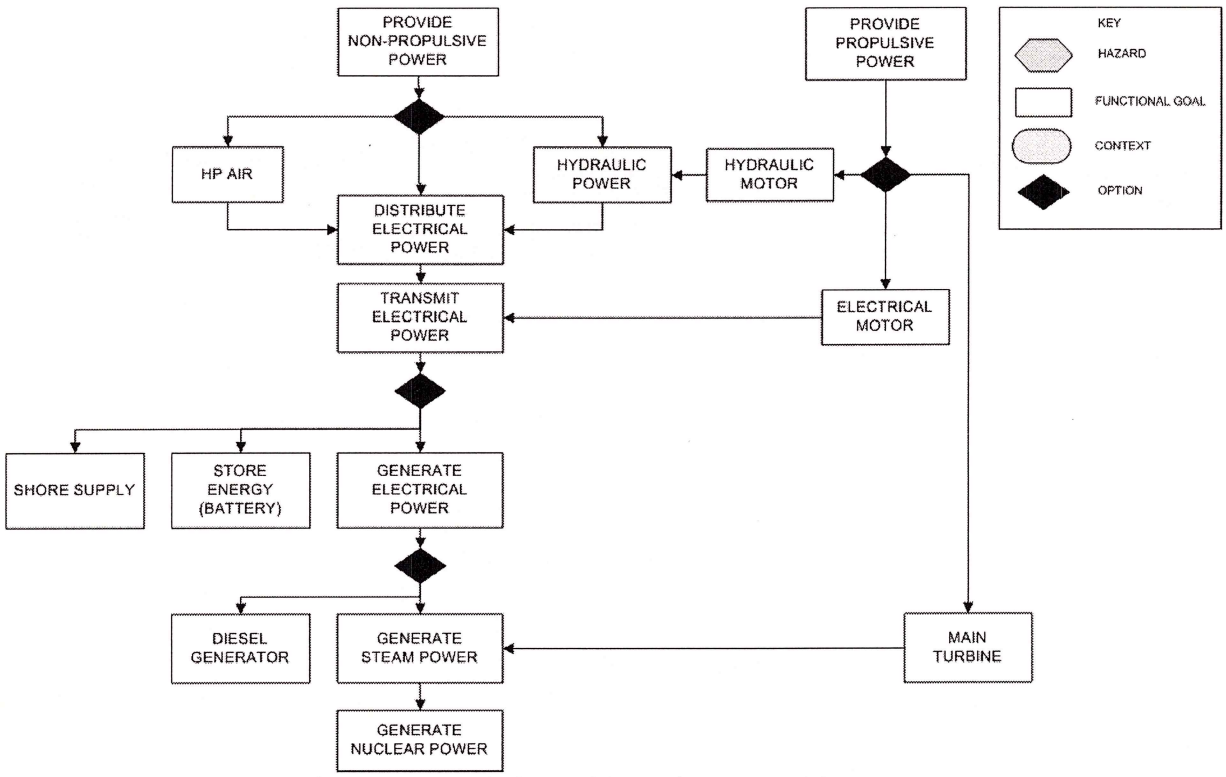

Figure 12. Control of Propulsion and Non Propulsive Power

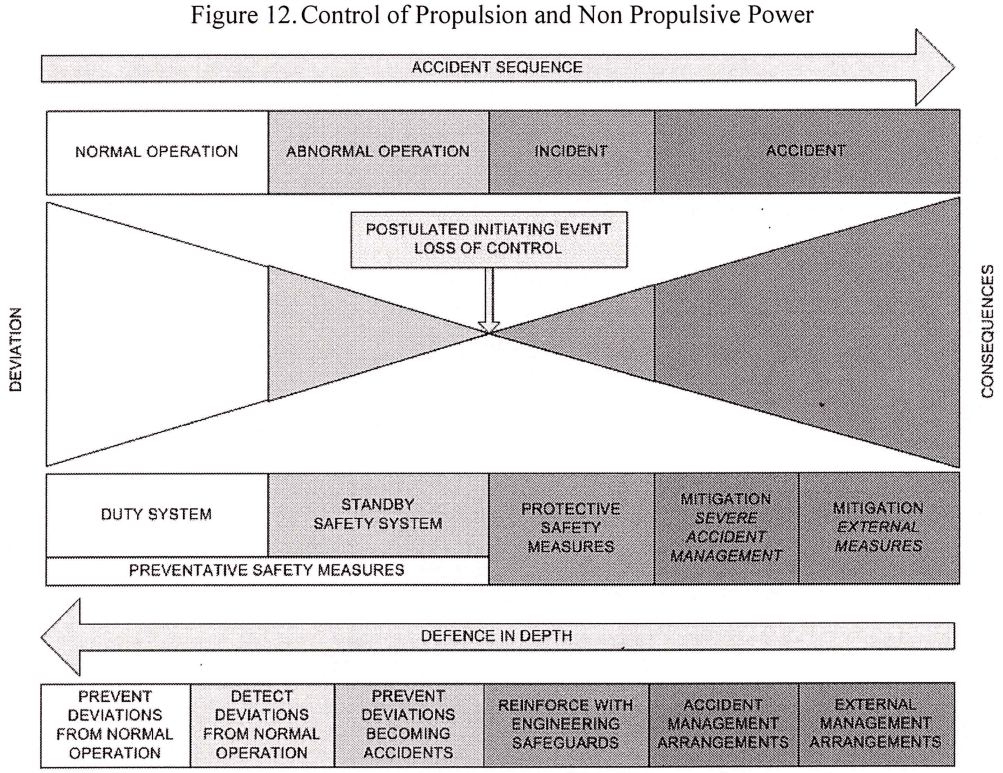

Figure 13. Bow-Tie Diagram