STPA Based Approach for a Resilience Assessment at an Early Design Stage of a Cruise Ship

C. Bongermino[1] , P. Gualeni[1]
[1] University of Genoa (Italy)

corresponding author: Paola Gualeni – paola.gualeni@unige.it

ABSTRACT

Several definitions and approaches have been proposed to study resilience in different fields like materials, ecology, psychology and infrastructures. A general definition, applicable also to human-made or engineered systems, describes resilience as the ability to maintain capability in case of disruption.

Thanks to its systemic, top-down approach, STAMP (System-Theoretic Accident Model and Processes) has been already identified in literature as a very effective and "conductive" reference when reasoning about the possible need of resilience of a complex system. The STAMP-based tool named STPA (System Theoretic Process Analysis) establishes the following steps: identify system accidents, hazards; draw functional control structure; identify unsafe control actions (UCAs); identify accident scenarios; formulate decisions and recommendations. It focuses on what actually is in the hands of the system designer and operator i.e. the possibility to take action on hazards that can be eliminated or controlled.

In this paper an approach to design resilience into a cruise vessel will be proposed. An application case will be developed considering the specific hazard of dead ship condition i.e. of energy black-out on board. In case of navigation close to the shore and in heavy weather condition, this situation can rapidly evolve into a loss. The ship energy production and delivery system, both for the propulsion and for the hotel services, will be considered. Running the procedure up to the level of UCAs enables the identification of the possible disruptive events capable to degrade the operational performance of the system. Starting from this point, suggestions will be discussed for a selected UCA, able to prevent or mitigate it. A metric for ship resilience will be proposed as well with the aim to allow comparisons among different design solutions.

Keywords: STPA, Resilience; Dead-ship condition.

1. INTRODUCTION

The issue of power generation and delivery on board is very relevant for any kind of ship. It is well known for example that for both passenger and cargo vessels an emergency sources of electrical power shall be provided, for essential services under emergency conditions (IMO, 2014). Emergency generator and emergency switchboard of the ship should be located above the uppermost continuous deck, should have independent fuel supply and be capable of giving power for the period of 18 hours for the cargo ship and 36 hours for the passenger ship.

It should be capable of supplying simultaneously at least the following services, very basic:

- Emergency lightening (at the alleyway, stairways, and exits, muster and embarkation stations, machinery space, control room, main and emergency switchboard, firemen's outfits storage positions, steering gear room)
- Fire detecting and alarming system
- Internal communication equipment
- Daylight signalling lamp and ship's whistle
- Navigation equipment
- Radio installations, (VHF, MF, MF/HF)

- Watertight doors
- Fire pumps, emergency bilge pump

The dead-ship condition however is when the ship has just the emergency generator/s working in compliance with what above, but there is no power for ship propulsion and manoeuvring, neither for the hotel services. It is a very critical situation especially for cruise ships due to the significant number of human lives on board. In recent years characterized by the increment of cruise vessels size, the concept that the ship herself represents the best possible lifeboat has earned credit in the safety rules framework. Therefore, the need to guarantee a proper amount of energy, in addition to the traditional emergency generator support, has become evident. For passenger ships, the safety implications of power availability on board are so relevant that from June 2010 the Safe Return to Port standard (IMO, 2006) has been introduced. The regulation requires that passenger vessels with a length of 120 metres or more or with three or more main vertical zones is to be designed in such a way that in the event of a flood or fire emergency, passengers and crew can stay safely on board as the ship proceeds to port under her own power. Safe Rerturn to Port criteria defines a threshold where the ship's crew should be able to return to port without requiring passengers to evacuate. The power generation that is to be guaranteed onboard is meant not only for propulsion but also for the hotel services that can provide a sufficient level of vital comfort to passengers while the ship is on the way back to the safe port.

The overall functional requirements are intended to provide the following capabilities after an incident of fire or flooding:

— Ensure propulsion, steering, manoeuvring and navigational capabilities

— Ensure necessary service of the safety systems (fire safety and watertight integrity) in the remaining part of the ship that is not directly affected by the casualty

— Support safe areas for passenger and crew for the duration of the return to port voyage (e.g. water, sanitation, food, ventilation and light).

If the casualty extends beyond the defined threshold and the ship must be abandoned, the regulations require a limited number of systems to be remain available for 3 hours to facilitate an orderly abandonment.

The outcomes of Safe Return to Port in terms of design features of modern large passenger ships is an increased redundancy on board for propulsion, steering systems and electrical power delivery as well as new adapted architecture of safety or any other relevant systems.

Nevertheless it is well known that safety is not only a matter of redundancy and systems availability. In fact also for ships complying with the Safe Return to Port standards and the relevant implied redundancy, black-out is still an issue therefore worth to be investigated with a different perspective.

The dead-ship situation (i.e. the ship in black-out, the loss of energy for propulsion and minimum services vital for human beings) in fact is an emergency situation that can occur unexpectedly and in case of adverse weather condition and proximity to the shore it can rapidly evolve in ship loss.

In this paper an approach enabling the integration by design of resilience capability against black-out on board a cruise vessel will be proposed and discussed. The importance of a proper framework to model and discuss at an early design level interactions and integration among the energy system, the automation system and the human operators become evident during the application, evidencing also the importance of designing for operations.

The current evolution of safety paradigm (from safety-I to safety-II) defines safety as the ability to succeed under varying conditions. The understanding of everyday functioning is therefore a necessary prerequisite for the understanding of safety performance (Hollnagel et al. 2006; Hollnagel, 2016). In 'Safety II', humans are seen as a resource necessary for flexibility and resilience. But in an era where human error is considered the cause of the majority of maritime casualties, the view of humans as a safeguard and not a problem is one of the biggest challenge.

In this respect, a starting point for organizations interested in Safety II is to enhance their employees' resilience, as the ability to monitor things and handle situations (Hollnagel et al. 2015). At present and for the specific case of ships, these abilities have to be considered as the result of a virtuous integration with IT on board and in particular with the automation system (Rahimia & Madni, 2014).

Focusing on what goes right, rather than on what goes wrong, changes the definition of safety from ’avoiding that something goes wrong’ to ’ensuring that everything goes right’ (Hollnagel., 2014). The attitude implied in Safety-II is ensuring that things go right but the first step is to acknowledge the inevitability and necessity of performance variability, second to find ways to monitor it, and third to find ways to control it (Hollnagel, 2016).

To this aim it seems very helpful the use of STAMP technique and in particular of STPA and the Safety Control Structure appears to be effective to model and reason about the best ways to enforce and implement safety from the top to the bottom of the structure, by monitor and control.

2. STPA APPROACH FOR RESILIENCE ASSESSMENT

Systems-Theoretic Accident Model and Process (STAMP) is a top-down system-based accident model that focuses on enforcing constraints rather than preventing failures (Leveson, 2011). In this approach, safety is a dynamic control problem rather than a reliability problem. The system is described by a hierarchical Safety Control Structure in which each part of the system is identified and analysed with its relationship with the other parts of the system, underlining what they communicate and do. The main focus of this approach is to identify the safety constraints that are exerted from the Safety Control Structure, because events leading to a loss can occur only when safety constraints from a higher level in the Safety Control Structure are not enforced.

STAMP is used to come up with high-level list of hazards in which disruptive events could arise, considering each part of the system as a contributor to the ongoing development of the emergent behaviours properties.

System-Theoretic Process Analysis (STPA) is the hazard technique (Leveson, 2011) built upon the foundation provided by STAMP, that mainly consists of creating basic system engineering information, identifying unsafe control actions and identifying causal factors of unsafe actions.

The roadmap of STPA consists of: define the purpose of the analysis (identify losses and hazards, define system boundaries), model the control structure, identify the unsafe control actions, identify loss scenarios.

In this perspective STPA is applied as a very effective way to understand where and how performance variability might happen (Leveson at al. 2006). Therefore it can also suggest how to better handle situations. An interesting application of STPA to favour resilience integration is formulated in Beach et al. (2018) where a particular attention to the development of metrics is given in order to compare different resilience solutions.

The STPA approach can be assumed as a possible technique to spot the need of resilience when pursuing an emergent property like safety and to subsequently guide its implementation during the design process with a link to the operational life of a complex system and the involved human operators. The perspective is that safety represents the overall target and resilience is just an enabling mean or better “the ability of the system to monitor the changing risk profile and take timely action to prevent the likelihood of damage” (Madni & Jackson, 2008). As already mentioned, STPA focuses on behavioural safety constraints and it enables the analysis at the socio-organizational level. Therefore it can suggest the most appropriate level and “typology” of resilience that should be enforced to manage such aspects.

STPA outputs can be used in many different ways, among which:

- Drive the system architecture
- Create executable requirements
- Identify design recommendations
- Identify mitigations and safeguards needed
- Drive new design decisions (if STPA is used during development)

Therefore the four possible resilience modes i.e. avoiding, absorbing, adapting and recovering (Madni & Jackson, 2009) can be formulated and implemented in a logic of interactions and interfaces to manage (monitor and take timely actions) an hazard.

The integration of resilience can be performed by design methods grounded in experience. One of the most popular is the so called physical redundancy but since we are interested to overcome the traditional reliability, the functional redundancy should be considered at least as more promising for the purpose of this paper. Many other design methods can be mentioned and a comprehensive list is reported in Madni & Jackson (2009), useful for the last part of the application and significant because able to involve also crew members in the process of design for operations.

3. APPLICATION TO A LARGE CRUISE SHIP

A typical solution for cruise ships is the propulsion performed by electric engines, that are the main load for what concerns the electric power generation and delivery system on board. Nevertheless for large passenger ships, the sum of all the electric loads necessary for the ship operational profile (generally indicated as the “hotel loads”) is comparable to the electric load for propulsion. The shipboard power plant consists of electric generator units, for instance synchronous generators, that are usually coupled with turbines or diesel engines.

The power generated by the whole power plant is provided by different units and delivered to the main electrical panel (main switchboard) in medium voltage. For the ships with more than 3 MW installed on board, the Safety of Life at Sea Convention – SOLAS (IMO, 2014) requires that the main panel has to be splitted in at least two sections. The rated voltage usually used for the main panel are 3,3kV, 6,6 kV and 11kV. On board cruisers the rated voltage is usually 6,6 kV or 11 kV.

The power supply of the electrical users is ensured by the distribution grid, that is usually subdivided in primary and secondary grid. The first one is in medium voltage, the second one in low voltage. Low voltage is usually 690, 440, 230 and 120V. The primary grid supplies the loads that need high power, such as the propulsion engines, the thrusters and the air conditioning compressors. The low voltage switchboards power the loads that require limited voltage (i.e. 230 V, 120 V). Moreover, in order to supply high power required by some specific user groups, there are some substations to ensure a specific service, for instance the galley (440 V) or the engine room (690 V). The shipboard distribution grids can be structured in different ways, depending on the type of ship and the power installed on board, such as radial or ring grid.

An example of a typical power generation and distribution system of a large cruise ship is shown in figure 1 (Vie, 2014).

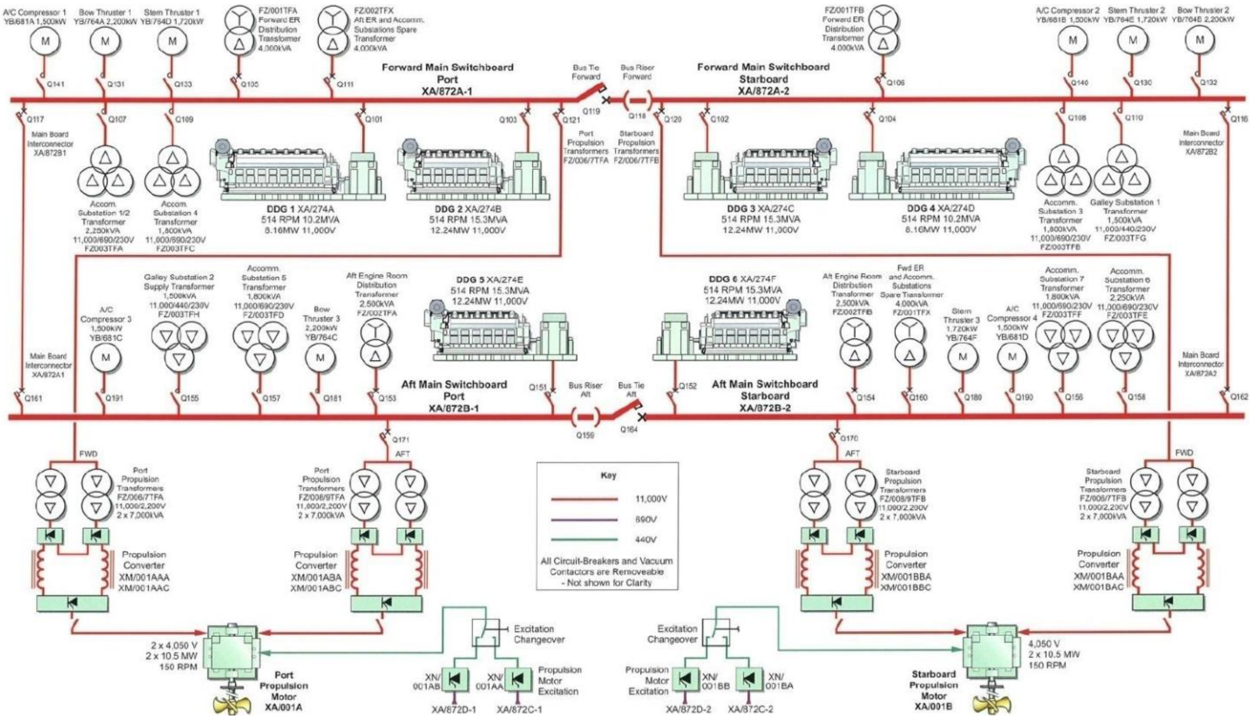
A/C Compressor 1 YB/681A 1,500kW
Bow Thruster 1 YB/764A 2,200kW
Stern Thruster 1 YB/764D 1,720kW
M
FZ/001TFA Forward ER Distribution Transformer 4,000kVA
FZ/002TFX Aft ER and Accomm. Substations Spare Transformer 4,000kVA
Forward Main Switchboard Port XA/872A-1
Bus Tie Forward
Bus Riser Forward
Forward Main Switchboard Starboard XA/872A-2
FZ/001TFB Forward ER Distribution Transformer 4,000kVA
A/C Compressor 2 YB/681B 1,500kW
Stern Thruster 2 YB/764E 1,720kW
Bow Thruster 2 YB/764B 2,200kW
Q141
Q131
Q133
Q105
Q111
Q106
Q140
Q130
Q132
Q117
Q107
Q109
Q101
Q103
Q121
Q119
Q118
Q120
Q102
Q104
Q108
Q110
Q116
Main Board Interconnector XA/872B1
Port Propulsion Transformers FZ/006/7TFA
Starboard Propulsion Transformers FZ/006/7TFB
Main Board Interconnector XA/872B2
Accom. Substation 1/2 Transformer 2,250kVA 11,000/690/230V FZ003TFA
Accom. Substation 4 Transformer 1,800kVA 11,000/690/230V FZ003TFC
DDG 1 XA/274A 514 RPM 10.2MVA 8.16MW 11,000V
DDG 2 XA/274B 514 RPM 15.3MVA 12.24MW 11,000V
DDG 3 XA/274C 514 RPM 15.3MVA 12.24MW 11,000V
DDG 4 XA/274D 514 RPM 10.2MVA 8.16MW 11,000V
Accomm. Substation 3 Transformer 1,800kVA 11,000/690/230V FZ/003TFB
Galley Substation 1 Transformer 1,500kVA 11,000/440/230V FZ/003TFG
A/C Compressor 3 1,500kW YB/681C
Galley Substation 2 Supply Transformer 1,500kVA 11,000/440/230V FZ/003TFH
Accomm. Substation 5 Transformer 1,800kVA 11,000/690/230V FZ/003TFD
Bow Thruster 3 2,200kW YB/764C
Aft Engine Room Distribution Transformer 2,500kVA FZ/002TFA
DDG 5 XA/274E 514 RPM 15.3MVA 12.24MW 11,000V
DDG 6 XA/274F 514 RPM 15.3MVA 12.24MW 11,000V
Aft Engine Room Distribution Transformer 2,500kVA FZ/002TFB
Fwd ER and Accomm. Substations Spare Transformer 4,000kVA FZ/001TFX
Stern Thruster 3 1,720kW YB/764F
A/C Compressor 4 1,500kW YB/681D
Accomm. Substation 7 Transformer 1,800kVA 11,000/690/230V FZ/003TFF
Accomm. Substation 6 Transformer 2,250kVA 11,000/690/230V FZ/003TFE
Main Board Interconnector XA/872A1
Main Board Interconnector XA/872A2
Aft Main Switchboard Port XA/872B-1
Bus Riser Aft
Bus Tie Aft
Aft Main Switchboard Starboard XA/872B-2
Q161
Q191
Q155
Q157
Q181
Q153
Q151
Q159
Q164
Q152
Q154
Q160
Q180
Q190
Q156
Q158
Q162
Q171
Q170
FWD
AFT
AFT
FWD
Port Propulsion Transformers FZ/006/7TFA 11,000/2,200V 2 x 7,000kVA
Port Propulsion Transformers FZ/008/9TFA 11,000/2,200V 2 x 7,000kVA
Key
11,000V
690V
440V
All Circuit-Breakers and Vacuum Contactors are Removeable - Not shown for Clarity
Starboard Propulsion Transformers FZ/008/9TFB 11,000/2,200V 2 x 7,000kVA
Starboard Propulsion Transformers FZ/006/7TFB 11,000/2,200V 2 x 7,000kVA
Propulsion Converter XM/001AAA XM/001AAC
Propulsion Converter XM/001ABA XM/001ABC
Propulsion Converter XM/001BBA XM/001BBC
Propulsion Converter XM/001BAA XM/001BAC
2 x 4,050 V 2 x 10.5 MW 150 RPM
Port Propulsion Motor XA/001A
Excitation Changeover
XN/ 001AB
XN/ 001AA
Propulsion Motor Excitation
XA/872D-1
XA/872C-1
Excitation Changeover
Propulsion Motor Excitation
XN/ 001BB
XN/ 001BA
XA/872D-2
XA/872C-2
Starboard Propulsion Motor XA/001B
4,050 V 2 x 10.5 MW 150 RPM

Figure 1: a typical layout of the power generation and distribution system for a cruise ship (Vie, 2014)

In this paper the attention will be focussed on a large cruise ship, during a very preliminary design phase when some reasoning about the black-out issue is very appropriate: it is both a safety issue (in case the ship propulsion is lost, especially in stormy weather close to the shore) and a commercial issue (in case the hotel service is lost with strong disappointment and discomfort for passengers). Usually, the starting point is a scheme like the one shown in figure 1. In an innovative perspective, the human factor, its integration with the automation system and the socio-organizational aspects as well, should be added into the discussion.

Following the STPA steps as mentioned in the previous paragraph, the hazards, the Safety Control Structure and the UCAs have been identified. Since the focus is on the black-out issue onboard, the identified hazards are the ones reported in table 1:

Table 1 the identified hazards for a focus on black-out on board

H 1	the ship propulsion is lost
H 2	the ship hotel services are lost

In figure 2 the Safety Control Structure sketched for the application is presented.

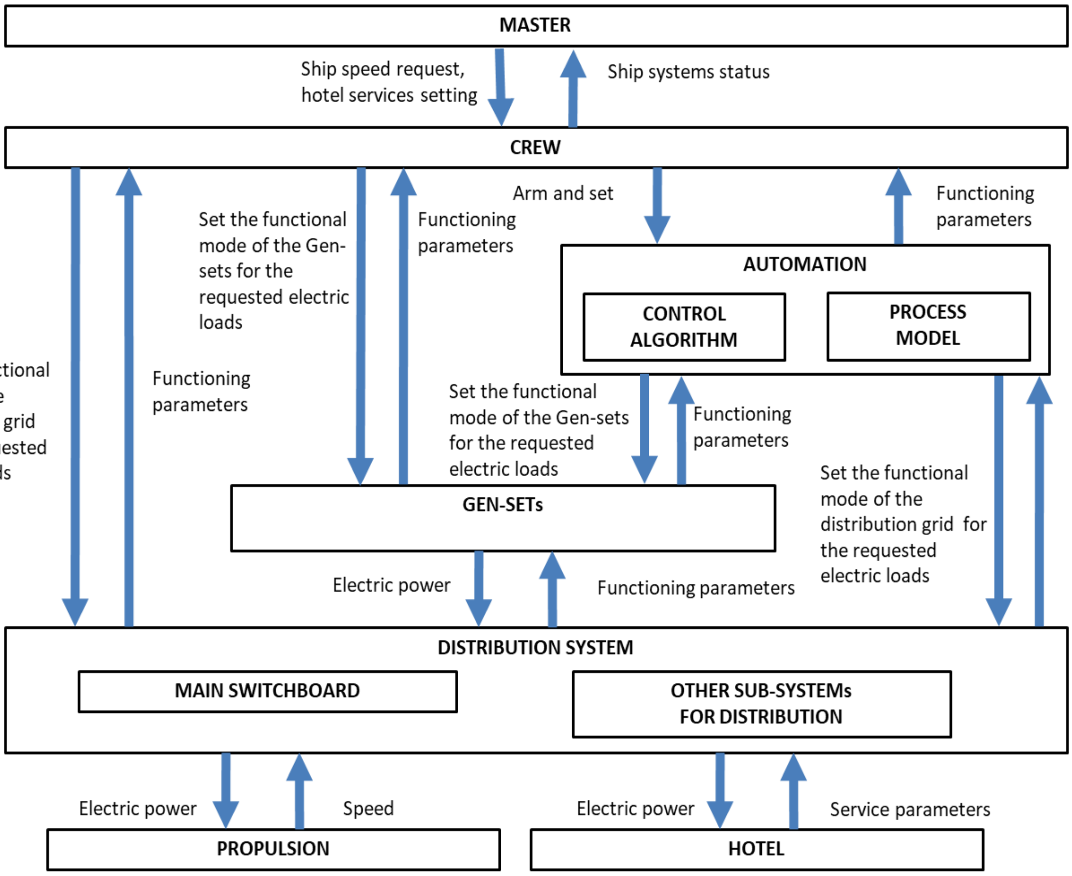
MASTER
Ship speed request, hotel services setting
Ship systems status
CREW
Set the functional mode of the Gen-sets for the requested electric loads
Functioning parameters
Arm and set
Functioning parameters
AUTOMATION
CONTROL ALGORITHM
PROCESS MODEL
Set the functional mode of the distribution grid for the requested electric loads
Functioning parameters
Set the functional mode of the Gen-sets for the requested electric loads
Functioning parameters
Set the functional mode of the distribution grid for the requested electric loads
GEN-SETs
Electric power
Functioning parameters
DISTRIBUTION SYSTEM
MAIN SWITCHBOARD
OTHER SUB-SYSTEMs FOR DISTRIBUTION
Electric power
Speed
Electric power
Service parameters
PROPULSION
HOTEL

Figure 2: the Safety Control Structure (GEN-SETs indicate the diesel generators, MSWB is the main switchboard and GRID is the general indication for distribution grid)

The diagram has been used then to derive the Unsafe Control Actions (UCAs). Such phase is very long and resource consuming, therefore for the purpose of this paper, only a sub domain of UCAs has been reported in table 2 (where GEN-SETs indicate the diesel generators, MSWB is the main switchboard and GRID is the general indication for distribution grid).

The considered UCAs are relevant only to the control and feed-back actions between the Automation System and the GEN-SETs. Power generators, in fact, they are assumed as one of the most important elements when analysing the black-out condition and their functioning is strongly dependent on the Automation System. This in turn means that the safety of the ship deriving from power delivery is strongly dependent on the proper Automation Systems actions.

A further selection will be made among the considered UCAs in order to create some examples to be finalized with proposal of resilience implementation. To this aim the attention has been focused only on one control action i.e. “set the functional mode of the Gen-sets for the requested electric loads" and UCAs have been formulated only for the class "not providing causes hazard" (UCAs from 1 to 9 in Table 2).

The further step, i.e. the definition of scenarios, means that two question are arising:

a) Why would Unsafe Control Actions occur?
b) Why would control actions be improperly executed or not executed, leading to hazards?

The definition of scenarios for all the UCAs mentioned in Table 2 would be too long and challenging for the purpose of this paper. Therefore only selected scenarios for UCA – 1 are formulated and reported, limiting the analysis to the area of the Safety Control Structure as evidenced in figure 3.

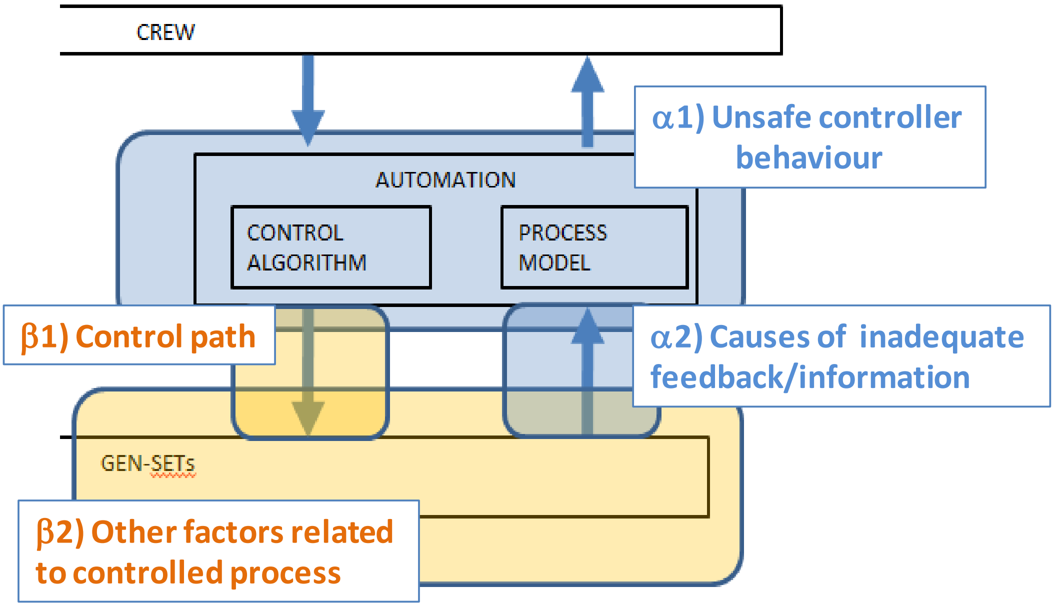
CREW
AUTOMATION
CONTROL ALGORITHM
PROCESS MODEL
GEN-SETs
α1) Unsafe controller behaviour
α2) Causes of inadequate feedback/information
β1) Control path
β2) Other factors related to controlled process

Figure 3: A specific focus on the Safety Control Structure in the perspective of scenarios definition

In the same figure 3 it is clarified that, thinking about the specific UCA, the two above mentioned questions a) and b) in turn requires to meditate on:

α1) Unsafe controller behavior
α2) Causes of inadequate feedback /information
β1) Control path
β2) Other factors related to controlled process

As described in Table 2, UCA-1 is: "AUTOMATION does not provide the functional mode of the Gen-sets for the requested electric loads during navigation [H 1, H 2]".

The identified scenarios are summarized in table 3.

For the purpose of this paper scenarios 2 and 3 are considered. It is worth mentioning that in some cases the sensors and the algorithm of the automation system can be challenged by the ship large motions when operating in extreme weather conditions.

With reference to them, a selection of design heuristics i.e. qualitative design methods grounded in experience are identified as a practical basis to provide resilience to the ship in operations for example in heavy seas.

Table 2 The list of Unsafe Control Actions (UCAs): a subset

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
Set the functional mode of the Gen-sets for the requested electric loads	UCA-1 AUTOMATION does not provide the functional mode of the Gen-sets for the requested electric loads during navigation [H 1, H 2] UCA -2 AUTOMATION does not provide the functional mode of the Gen-sets for the requested electric loads during manoeuvring [H 1, H 2] UCA -3 AUTOMATION does not provide the functional mode of the Gen-sets for the requested electric loads in harbor [H 1, H 2]	NOT CONSIDERED FOR THE PURPOSE OF THIS PAPER	NOT CONSIDERED FOR THE PURPOSE OF THIS PAPER	NOT CONSIDERED FOR THE PURPOSE OF THIS PAPER

Table 3 The definition of scenarios for UCA -1

Scenario 1 for UCA – 1: the Gen-Sets controller (automation system) fails during navigation, causing an interruption of power delivery.
Scenario 2 for UCA – 1: the sensors report inadequately to the automation system that parameters are out of the safety range.
The Gen-Sets do not provide power to the ship in navigation because the automation system has ordered the shutdown: it detects that the engines are going to suffer a significant damage due to some functioning parameters out of safety range, due to inadequate sensor feedback.
Scenario 3 for UCA – 1: the specified control algorithm is flawed, so the automation system detects that the Gen-Sets parameters are out of the safety range.
The Gen-Sets do not provide power to the ship in navigation because the automation system has ordered the shutdown: it detects that the engines are going to suffer a significant damage due to some functioning parameters out of safety range, decided by a flawed control algorithm.
Scenario 4 for UCA – 1: the automation system sets the Gen-Sets parameters but this is not received by the system.
Scenario 5 for UCA – 1: the Gen-Sets suffers of a technical breakdown or malfunction.

From Madni & Jacknson (2009), among the fourteen design heuristics proposed by the authors, six could be defined as appropriate for the application:

- Functional redundancy: there should be alternative ways to perform a particular function that does not rely on the same physical systems.
- Human backup: humans should be able to back up automation when there is a context change that automation is not sensitive to and when there is sufficient time for human intervention.

- “Human in the loop”: humans should be in the loop when there is a need for “rapid cognition” and creative option generation
- Intent awareness: system and humans should maintain a shared intent model to back up each other when called upon
- Learning/Adaptation: continually acquiring new knowledge from the environment to reconfigure, re-optimize, and grow
- Context spanning: system should be able to survive most likely and worst case scenarios, either natural or man-made.

Starting from these selection, In table 4 and 5 some proposals are made in order to implement resilience in relation with selected scenarios 2 and 3. The reason why such scenarios are selected is because they seem more appropriate to formulate resilience as the integration of operators, automation and design.

For scenario 2, functional redundancy, human backup and context spanning are selected as suitable design heuristic. For scenario 3 the learning/adaptation option has been preferred to the functional redundancy.

Table 4 Proposal for discussion of resilience implementation – UCA - 1 Scenario 2

	Functional redundancy	Human backup	Context spanning
Scenario 2	Subsidiary devices should provide information about parameters working point to assess whether they actually are outside the safety range	The operators should be able to make decisions independently from automation system and act accordingly. Possibly supported by subsidiary devices (see column on the left).	In the preliminary design all the possible operational scenarios have to be identified in order to define the operational domain of on board systems (to be assumed in the technical specifications, for example with reference to roll angle and/or list angle in heavy seas).

Table 5 Proposal for discussion of resilience implementation – UCA - 1 Scenario 3

	Learning/Adaptation	Human backup	Context spanning
Scenario 3	The control algorithm should be able to introduce in the logic of the procedure the awareness for example of stormy weather condition and in such case submit to human beings the decision about engine shutdown.	In specific cases like engine shut down the operators should be “consulted” by the automation system. Operators should receive the proper training for this.	In the preliminary design all the possible operational scenarios has to be identified in order to define the operational domain of on board systems (to be assumed in the technical specifications, for example with reference to roll angle and/or list angle in heavy seas).

From what above it appears how ship resilience is the result of an effective integration between operators and automation systems. This is a very important issue at present since automation is more and more exploited on board ships. The issue is even more important when automation has the total control on systems like GEN-SETs having a strong relation with safety: a stronger integration between human operators and the automation should be developed to drive a successful decision making for safety. The Safety Control Structure (the relevant part is reported in Figure 4) is very effective to put in evidence the hierarchy among them and the necessary control and feedback.

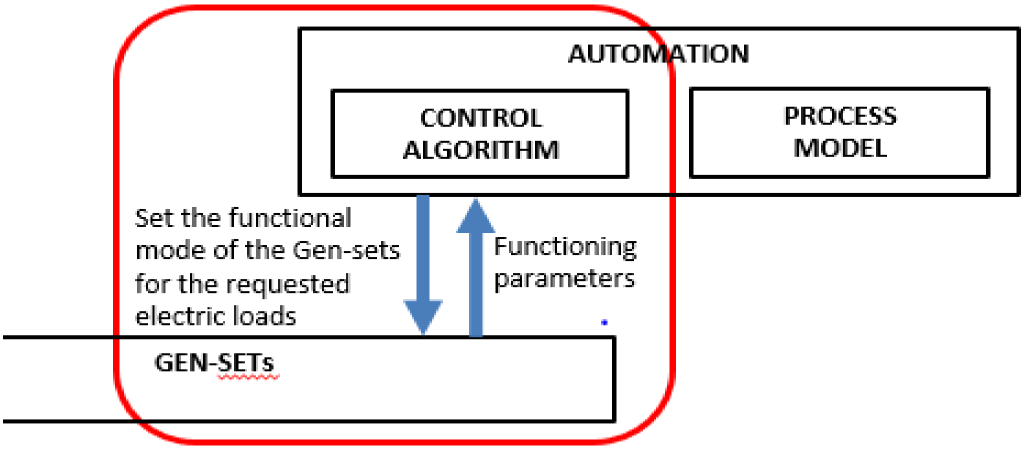
AUTOMATION
CONTROL ALGORITHM
PROCESS MODEL
Set the functional mode of the Gen-sets for the requested electric loads
Functioning parameters
GEN-SETs

Figure 4: A specific focus on the Safety Control Structure with GEN-Sets, Automation and Crew members connections

When mitigations and safeguards are identified it might be useful to investigate and compare different alternative solutions. In this perspective quantifiable metrics for resilience are in principle necessary.

Of course more than one indicator can be used and moreover a proper characterization also in terms of costs could help to better appreciate the cost/benefit ratio of the alternatives under investigation (Yodo & Wang, 2016).

With an approach based on STPA, which focuses on the possibility to take action on hazards that can be eliminated or controlled, it seems natural to define the metric hinged on the identified hazard.

For the proposed application, the identified hazard is the missing or insufficient power delivery. A possible indication for the purpose of this paper is to define as a quantitative indicator the percentage of available power with respect to the total power needed, as described below.

$$\varepsilon\ (t) = \frac{P\ (t)_{delivered}}{P\ (t)_{needed}}$$

It ranges from 0 to 1. When $\varepsilon = 1$ it means that the implemented resilience makes possible the complete delivery of the necessary power. The possibility to monitor with subsidiary devices the GEN-SETs could be implemented for all the units or just the number considered sufficient for avoiding the situation of total black-out. When $\varepsilon = 0.5$ it means that only one half of the needed power is available. Whether it is sufficiently safe or not is to be decided assuming criteria that set the minimum power necessary for propulsion (the weather condition should be considered in this case) and for hotel services.

The resilience by human backup is strongly linked with the provision of subsidiary information and training since the decision to interfere with the automation system should be based on the possibility to increase the situational awareness in terms of safety.

Finally it is worthwhile mentioning that this kind of metric is able to quantify the effect of resilience over a specific issue like electric power production and delivery. The assessment of an overall and more comprehensive ship resilience is, in principle, possible but very complex.

5. CONCLUSIONS

In the paper the possibility to apply STPA technique has been investigated in order to find out where and how resilience should be implemented on board relying on appropriate design heuristics.

An application case has been carried out with reference to a large cruise vessels. The specific issue of black-out on board has been selected and the hazards of propulsion and/or hotel services loss have been identified. Relying on the Safety Control Structure, a selection of Unsafe Control

Actions has been reported. One UCA has then been selected for the development of scenarios and the relevant need for resilience is spotted out.

STPA has enabled the visualization of the hierarchy among the ship energy system, the automation system and the crew members useful to discuss in a design stage the characteristics and the logic of the automation system (integration with crew members in decision making included), especially when some disruptive conditions like extreme ship motions can characterize the scenario and make things difficult for the automation system reliability.

The implementation of resilience has been proposed in terms of functional redundancy, learning/adaptation, human back up and context spanning. It has been put in evidence, in a design for operations perspectives, how the capability of a better integration between humans and the automation systems is envisaged in such a way that system should allow for human intervention needed without requiring humans to make unsubstantiated assumptions.

REFERENCES

Beach, P.M., Mills, R.F., Burfeind, B.C., Langhals, B.T., Mailloux, L.O., (2018) A STAMP-Based Approach to Developing Quantifiable Measures of Resilience, 16th Int'l Conf on Embedded Systems, Cyber-physical Systems, and Applications, Las Vegas

Hollnagel, E., Woods, D.P., Leveson, N. (2006) Resilience Engineering: Concepts and Precepts, Aldershot, pp 397.ISBN 0754646416

Hollnagel, E. (2014) Safety-I and Safety-II: The Past and Future of Safety Management CRC PressISBN 9781472423085

Hollnagel, E., Braithwaite, J., Wears, R. (2015) From Safety-I to Safety-II: A White Paper Technical Report · DOI: 10.13140/RG.2.1.4051.5282

Hollnagel, E. (2016) Resilience Engineering: A New Understanding of Safety, J Ergon Soc Korea 2016; 35(3): 185-191

IMO 2014 SOLAS consolidated edition

IMO 2006 Resolution MSC.216(82) Amendments to the International Convention for the Safety of Life at Sea, 1974, as amended

Leveson, N.G., Thomas, J.P. (2018) STPA Handbook

Leveson N.G. (2011) Engineering a safer world: Systems thinking applied to safety, MIT Press

Leveson, N., Dulac, N., Zipkin, D., Cutcher-Gershenfed, J. Carroll, J. Barrett, B. (2006) - Engineering Resilience into Safety-critical Systems - MIT – Boston - USA

Rahimia, M., Madni, A.M., (2014) Toward A Resilience Framework for Sustainable Engineered Systems, Procedia Computer Science 28, pp. 809 – 817

Madni, A.M., Jackson, S. (2009) Towards a Conceptual Framework for Resilience Engineering, IEEE Systems Journal, Special Issue in Resilience Engineering.

Vie, R. (2014) President’s Day Lecture - The Design and Construction of a Modern Cruise Vessel, Institute of Marine Engineering, Science and Technology, IMarEST London.

Yodo, N., Wang, P., (2016) Engineering Resilience Quantification and System Design Implications: a Literature Survey Journal of Mechanical Design Vol. 138