Broad approach ensures safety and availability

ALF KÅRE ÅDNANES – Ever since shipping began, seafarers have depended on the safety of their vessels and skills of their crews. International regulations, classification rules and national legislation have been developed through the years to set standards for shipping. Taking a broad approach from the design stage onwards is also necessary to ensure safety and availability.

Today's vessels are advanced constructions that perform complicated tasks or can be part of a complex set of logistics. Safe and effective operation demands higher and new competence from the crew, as well as from designers, builders and suppliers and also regulatory and advisory bodies.

There is no single simple way to achieve safety and high availability of a ship's systems, but it is a fact that the optimal and best solution will be more challenging to add on as a modification to a system, than when a broad approach is taken from the design phase, building and verification, and through to operation. This is illustrated in Figure 1.

In this issue of *Generations* we present articles that cover a variety of concerns and solutions to enhance availability of the installations, in different phases of the life-cycles of vessels.

Safety and availability are related, though not completely overlapping, terms. While safety is mainly about the risk to crew, passengers and others who may be affected; eg, through environmental spill and pollution, availability is more about using the vessel for its intended purpose and keeping up a steady flow of income.

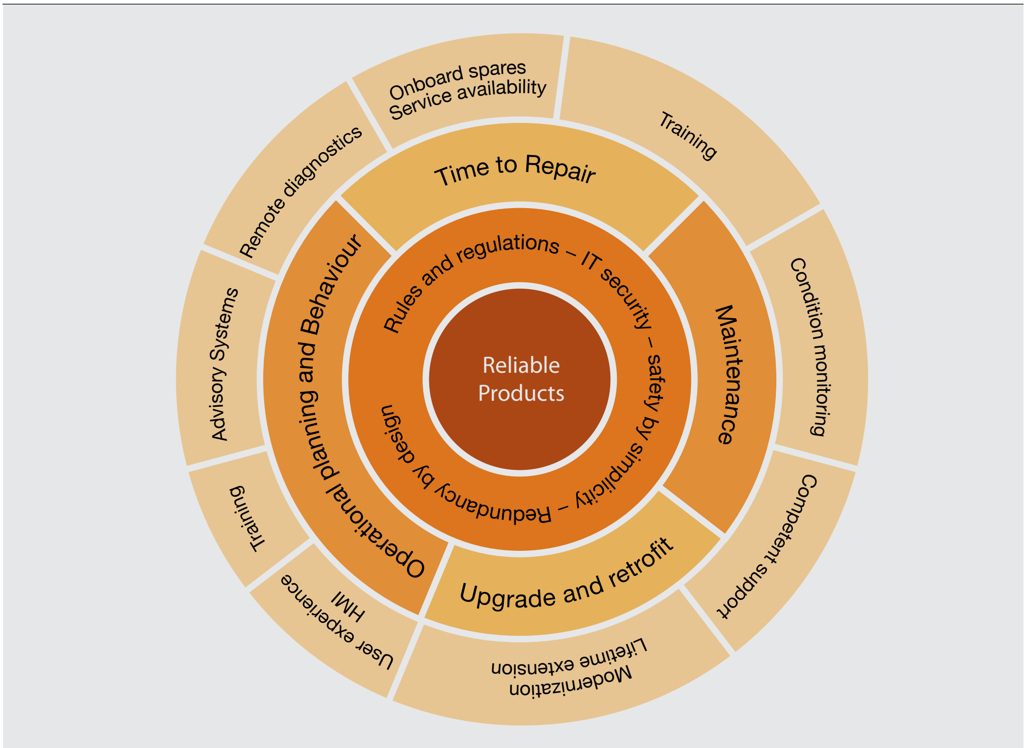
However, it is fully possible to build up the availability of the vessel's installations and at the same time improve the level of safety. This requires a broad approach to design and risk analysis, as well as proper risk mitigation. And firstly, it requires the ability to understand the risks inherent in today's solutions and to take note of the lessons learned from operations, as well as the ability to solve reliability issues without creating new ones.

Reliability versus availability

In order to better understand the terms used a few definitions are needed:

Reliability (λ): The probability that a component or system (set of components) will maintain their intended functions; often represented by a statistic number such as MTTF (Mean Time to Failure). $\lambda = MTTR^{-1}$

1 A broad approach is needed to achieve a high level of availability and safety.

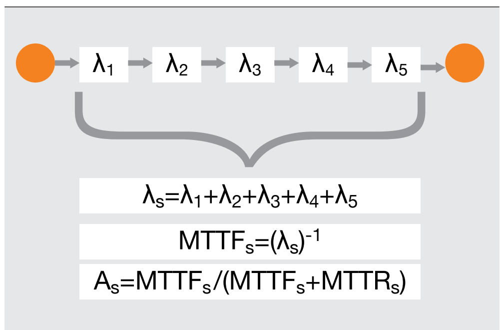


Availability (A): The degree to which a component or system (set of components) is in its functional condition; the term functional condition being understood as capable of carrying out its intended operation within defined constraints. For one system or component with failure rate MTTF, the availability is calculated as a percentage number: A=MTTF/(MTTF+MTTR); where MTTR is Mean Time To Repair.

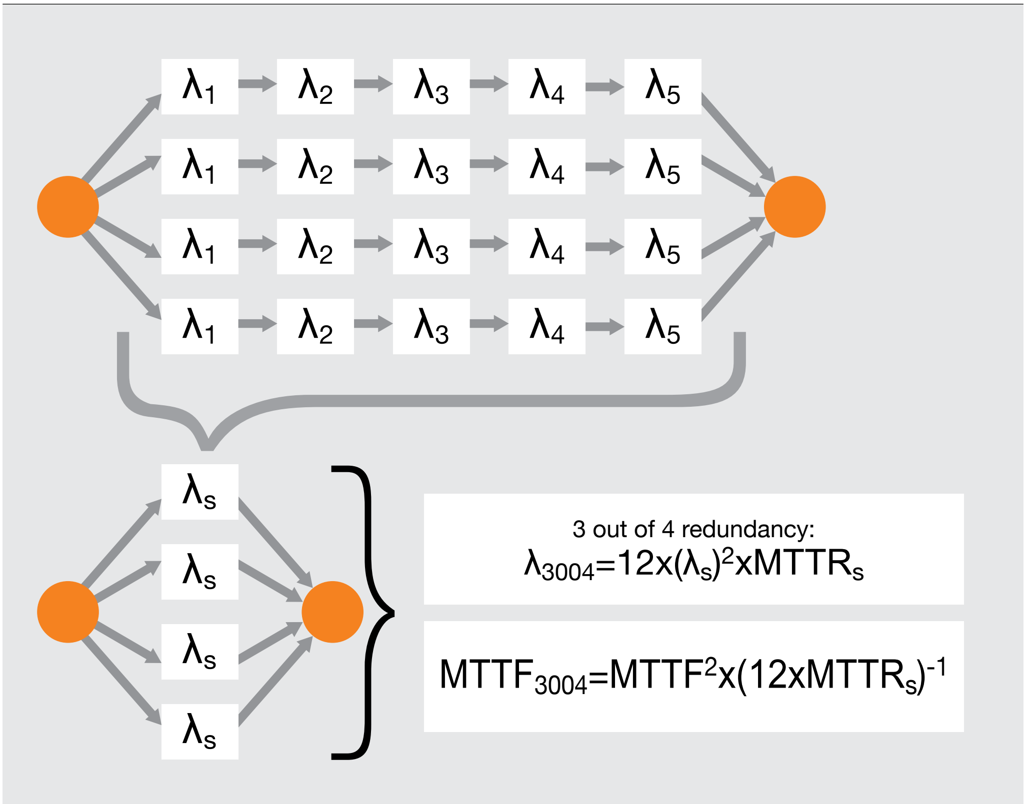
Safety: How well something or somebody is protected against damage, accident, or other undesirable events. Safety cannot be quantified in absolute measures and must be considered relative to the consequences of being in an unsafe condition. Safety assessment is typically approached by a risk analysis, where the risk for entering an unsafe condition is assessed against the consequences of not being safe; and a definition of what is a safe situation. For example, in running an oil well, a safe condition can be to shut down all process, while for an aircraft that would obviously not be the case.

A simple system with one chain of events that can lead to loss of the intended function is shown in the single-path reliability diagram of Figure 2.

2 Redundancy diagram for a simple installation without redundancy



3 Availability by system redundancy



There are several ways to approach high availability, Figures 3 and 4a show two different philosophies, presented in a reliability diagram.

For propulsion systems, availability and safety targets largely coincide as the ability to maneuver and control a vessel require both; not unlike the case with aircraft. While the approaches in Figures 3 and 4a may give an apparent increase of availability, the concept in Figure 4a includes additional components that, by pure parts count, increase the overall failure rates and may also contain common hidden or undetected failure modes. These additional components may also make it difficult to identify the risks and to quantify reliability, and may result in real reduced availability.

ABB prefers to work with systems that are designed to keep redundancy on a system level to a feasible maximum. Having clear lines with minimal interdependencies and cross couplings makes it easier to design and analyze the system with less risk of hidden failure modes. And even more important, it makes it possible for crew and service engineers to more logically understand the redundancy philosophy of the design in order to take the right operational actions and to correctly repair and test after a service job to ensure system integrity.

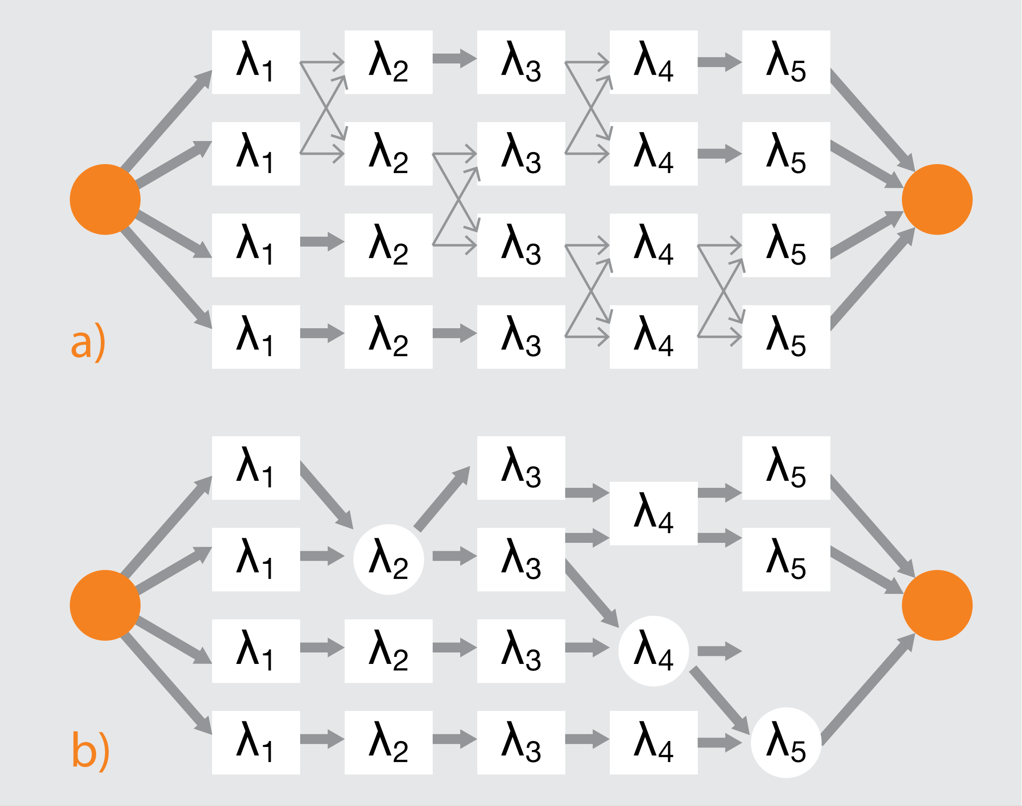
From these simple examples, it is clear that availability will be increased by:

- Using components with high reliability (MTTF)
- Increasing the number of redundancy segregations, represented in the diagram as independent paths
- Avoiding interdependencies between the redundancy segregations and, where cross connections are necessary, avoiding common failure modes for two or more of the paths shown in Figure 4b.

Computerized control and IT

The continuously more advanced systems for control and monitoring, navigatation and reporting make computerized systems and IT necessary installations

4 An apparent high availability by cross connections is shown in a), while b) may actually contain common failure modes.



and working tools for the crew and fleet management. Modern control and IT systems offer huge advantages in terms of running the vessel and installations at optimal and safe conditions. Gundersen's article (see page 127) on the emergence of IEC61850 and GOOSE communication in the protection of power generation and distribution systems is a good example of how modern IT solutions both simplify the hardware installations and, at the same time, pave the way for the improved protection of power plants, eg, with closed bus transfers.

Automation systems are also used to perform safety critical monitoring and control of process plants, and Hansen and Duran's article on SIL systems (see page 112) shows, with reference to the oil and gas industries, how such systems may be used to adopt a systematic approach to set safety targets.

From land-based industries, and computers at home and in the workplace, the precautions taken against virus attacks, or cyber security, are already well understood. However, while shipping industries and ship installations have so far avoided larger interference from cyber pirates, there is still work to be done to increase awareness and implement protection against cyber attacks. Hansen and Rahman (page 106) discuss how cyber security issues are handled by ABB in offerings of systems and support to the industries.

The human factor in safe operation must not be underestimated. Even with a high degree of automated control and safety functions, the user of the system, whether on the bridge or in the engine control room, will have to make decisions and interact with the system in both normal and failure situations, based on information provided by the system. The human machine interface (HMI) is the communication portal for the user of the system and it is essential that it is designed to meet the user's need for information and control input under both relaxed as well as stressful conditions. The computer systems may have access to thousands of events, alarms and dates.

Safety and availability are not ensured by one-off or simple means alone.

The importance of providing useful data to match the situation is obvious, although difficult. Azhar et al discuss the design process and fundamentals derived from it, in the design of the HMI for automation systems (see page 118) while Jehkonen and Matilainen describe the Intelligent Maneuvering Interface (IMI) for Azipod® propulsion systems (see page 122).

Redundancy for availability

With the entrance of dynamic positioning (DP) in the offshore fleet, a set of guidelines, rules and regulations have evolved that aim to define acceptable designs and procedures to obtain safety and availability. In order to understand the challenges, it is useful to learn from the past. Giddings, technical advisor of the International Marine Contractors' Association (IMCA), presents statistics collected over years on the failure of DP vessels (see page 148).

A fundamental requirement for such installations is the performance of FMEA analysis during the design, and continuous verification from sea trial through the lifetime of the vessel. Bhattacharya and Steven Cargill give their views on how FMEA processes should be done and how hardware-in-the-loop testing (HIL) can complement the traditional FMEA to make a faster, safer, and wider test footprint of automation system (see page 171). Adegeest presents the Octopus advisory system that extends the static DP capability plots and failure effects analysis with forecasting the vessel's behavior based on dynamic modeling and weather forecasting and is able to monitor and forecast vessel movements (see page 144).

As technologies evolve, and energy efficiency also becomes a competitive factor in the offshore fleet, there is increasing interest in solutions that give reduced fuel consumption, without compromising the safety and availability of the plant. DP operation, up to class 3, with closed bus transfers and ring connection on the main electric distribution system is a good example. Oil companies see the benefits of lower fuel bills and more stable voltage supply, and classification societies follow up with notations for enhanced reliability to permit such designs. Wendt shows in his article on page 154, how the use of IEC61850 communication, and autonomous systems helps to meet such requirements; while Hjukse's article (see page 161) on extended diesel-generator monitoring presents a solution for detecting power plant failures that were previously considered undetectable by traditional protection systems and hence could lead to a cascading failure of the power plant.

Also for vessels with single shaft propulsion, the concept of redundancy may be feasible by optimizing the design; where the additional cost of redundancy should be balanced with the reduced cost of main engine and fuel consumption. Vänskä (see page 185) shows how ABB has approached the in-line shaft booster/generator system for container vessels, where waste heat is converted to usable energy and, together with auxiliary power, can supply booster and take-home redundancy, giving the opportunity to optimize the propulsion design for reduced CAPEX and improved OPEX – to find the most cost effective balance.

Improving reliability and availability

Reliability and availability may not only be built at the system level to increase reliability of components and sub-systems and to use control methods to reduce the disturbing effects on the power plant that do not necessarily show up in the reliability diagrams. They may also have a significant impact on the final safety of operation.

Eriksson presents the solution for drilling drives and their control systems (see page 175). Although this is often regarded as a separate system to the DP installation, they are directly dependent through the common power plant and their safety aspects are coinciding. Design of the two systems should be well coordinated, with both physical and functional integration, to avoid mutual disturbances.

The use of Liquid Natural Gas, is expected to grow significantly this decade. LNG is a competitive energy source, with less environmental emissions, provided that proper solutions become available for transportation and tanking, as well as controlling the engines for optimized combustion process to avoid methane slip and large frequency fluctuations. Pestana presents an article on how electric propulsion fits well with the use of LNG engines (see page 175) and how electric propulsion allows for much more precise load control with lower load variations and more stable network voltage and frequency.

Reducing down time and MTTR

No technical installation lasts forever, and maintenance and upgrades are necessities. Instead of considering maintenance to be a non-deterministic cost over the years, Pajala's article (see page 190) points to ways to predict lifetime and plan maintenance at more practical and less painful times, such as during scheduled dry docking. Maintenance should be carried out in cooperation with suppliers, and the workload may be shared between the crew and supplier's service engineers to find the right balance of costs and resources for the ship operator.

ABB has implemented a remote diagnostics and support system, which allows our specialists to connect to the onboard installation and perform diagnostics similar to what used to be possible only by sending a service engineer on board. In combination with adequate spare parts storage on board, remote diagnostics already has numerous examples of how faulty systems can be made fully available through remote guidance of the crew.

A broad approach

Safety and availability are not ensured by one-off or simple means alone. The process of learning from experience and improving functions, solutions, and operational behavior is necessary. The articles in this issue of *Generations* give a broad overview of various approaches to make operations safer and more available for their intended work by reducing downtime. The overview is by no means a full picture of methods and solutions, but hopefully it will increase awareness and inspire designers, operators, and maintenance personnel towards even more improvements.

In conclusion, I thank all the authors of these articles for their contributions to this very important topic in the marine industries of today.

Alf Kåre Ådnanes
LBU Manager Marine and Cranes, ABB Singapore
Editor: *Generations* Technical Insight
alfkare.adnanes@sg.abb.com