Reliability Engineering and System Safety 169 (2018) 18–31

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis

Børge Rokseth*, Ingrid Bouwer Utne, Jan Erik Vinnem

Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ARTICLE INFO

Keywords:
Risk
Verification
STPA
Maritime systems
Maritime Safety

ABSTRACT

The process applied for verification of maritime systems lacks the ability to properly examine complex networks of interconnections. Verification is mainly focused on single failures of components, not properly accounting for the complexity emerging through interactions between human operators, computer systems and electro-mechanical components. The problem apparently resides in the supporting studies, or the lack thereof, for the development of test cases. A new methodology that can be introduced to the current verification process for these systems is proposed in this article. It employs Systems-theoretic process analysis (STPA) to generate verification objectives and related hazardous scenarios. These specify or extend the scope and provide acceptance criteria for verification activities, and may further serve as input to test case generation. The method is used in a case study to identify verification objectives for an automated module in the power management system of a maritime vessel. The results show that the method is able to reduce the number of context variables that verification results depend upon, and to highlight remaining context dependency, to allow for an integrated system view. It will help capture accidental scenarios with more complex causal relations than what is currently considered during verification of these systems.

1. Introduction

During recent decades, maritime vessels have evolved from assemblies of electro-mechanical components into complex systems featuring advanced automation such as dynamic positioning (DP) systems. Today, integrated software control systems are essential parts of all maritime vessels [1]. This evolution has enabled new types of operations, such as deep-water hydrocarbon exploration, which are both more complex in execution and associated with more severe consequences in the event of accidents. Loss of position for a dynamically positioned mobile offshore drilling unit (MODU) may, for example, result in a subsea blowout [2]. Therefore, risk management and system verification have become not only more challenging, but also more important. Skjetne and Sørensen [3] point out some characteristics and trends that contribute to the increased challenges of verification and testing of maritime vessels. Some of these are the increased use and dependence on computer-based systems, extended use of off-the-shelf technology, a drive towards low-cost solutions and the increased level of integration and system complexity.

A DP vessel is able to maintain its position and heading and to maneuver along a predefined track exclusively by means of automated thruster force [4]. Examples of typical applications of DP systems are positioning of MODUs, and positioning and maneuvering of crane vessels, shuttle tankers, cable and pipe layers, platform support vessels and diver support vessels. The consequences associated with loss of motion control for DP vessels can be, for example, blowouts, collisions and drowning of divers. Currently, the design requirements for DP systems address robustness against loss of position in the event of single failures by enforcing redundancy. Consequently, the main effort in verification is currently to verify technical redundancy.

The need for new methods for testing, verification and validation of advanced maritime systems was stated in a joint industry project documented in Skjetne and Sørensen [3] in 2004. The main reason for this need is the increased system complexity introduced by computer control systems, such as DP. The same year, Spouge [5] published a comprehensive review of the current methods for verifying redundancy in DP systems. Spouge concludes that failure mode and effect analysis (FMEA) may be a suitable tool, provided that sufficient guidance is given and that appropriate objectives for the analysis are formulated [5]. Some of the weaknesses identified in the report are that the current verification methods only consider technical failures, not human operators and onshore management, and that the methods may be unsuitable for some systems that are typically brought in by external vendors such as the DP control system and the power management system (PMS). The report does not discuss computer control systems or software in particular. A relatively recent method being employed in the maritime industry, and

* Corresponding author.
E-mail address: borge.rokseth@ntnu.no (B. Rokseth).

http://dx.doi.org/10.1016/j.ress.2017.07.015
Received 16 March 2017; Received in revised form 26 July 2017; Accepted 28 July 2017
Available online 1 August 2017
0951-8320/

that addresses computer control systems and software, is HIL testing [6–8].

Guidelines and standards for software development and verification processes have during recent years appeared in the maritime industry [9]. In particular, the classification societies DNV-GL and ABS have developed class notations for software verification processes (see DNV-GL [10] and ABS [11]). Both these class notations focus on hardware in the loop (HIL) testing in order to provide a higher degree of certainty that systems meet applicable requirements and function as intended. DNV-GL addresses the verification challenges by publishing a recommended practice [12], introducing a specialized version of FMEA, aimed specifically at verifying redundancy in the DP system. In addition to the classification societies, organizations such as the International Maritime Contractors Association (IMCA) provide guidance on vessel design, on conducting FMEA for verification purposes, and on conducting sea-trials [13–15].

The current verification activities (i.e., FMEAs to demonstrate technical redundancy and verification tests such as practical sea-trials and HIL tests) focus on specific system dimensions, such as hardware redundancy and computer control. Emergent properties such as safety, however, are not properties associated only with the individual components or system dimensions. They emerge through attuned interactions between these components and dimensions. As a consequence, the safety of, for example, a piece of software, cannot be evaluated and verified outside the context of the system in which it is operating [16]. And indeed, Skjetne and Sørensen [3] find that one of the main types of software-related problems is interaction problems between hardware, software and the human operator. This conclusion is also supported in Dong et al. [17], where a number of DP accidents and incidents are analyzed, and it is found that the majority are influenced by both technical and human/operational factors.

Even if the specialized version of FMEA proposed by DNV-GL [12] is an improvement for DP vessel applications, the weaknesses of the FMEA method is well known. The system perspective necessary to cope with the current level of system complexity is lacking. Furthermore, it is focused solely on verifying technical redundancy, which is inadequate from a safety perspective for complex software-intensive systems [18,19]. The FMEA process described in [12], is used as a tool to systematically going through the technical design of the system to ensure that it is designed according to certain requirements related to system redundancy, rather than as a traditional FMEA. An additional shortcoming with this is that it does not include any steps to ensure that the requirements themselves are safe for each particular system. The Systems-theoretic process analysis (STPA) is a relatively new hazard analysis technique based on the Systems-theoretic Accident Model and Processes (STAMP) [20–22]. The main idea in this accident causation model is that safety is a control problem, in accordance with the ideas presented in Rasmussen [23], and that accidents occur because of inadequate control and enforcement of safety constraints. The system is modeled as a hierarchical control structure, where each layer of control enforces control on the next layer. The objective when performing an STPA is to identify potentials for inadequate control, how inadequate control may occur in a system and to impose constraints on the control.

STPA has been successfully applied to a number of systems during recent years. Examples are safety analysis of defense systems such as a missile defense system [24], medical devices such as a radiation therapy system [25], air traffic control systems [26], security analyses where STPA is used in order to identify vulnerable system states [27], and hazard analyses for space craft [28]. Two applications for DP systems can also be found in the literature. Abrecht and Leveson [29] apply STPA to analyze a DP platform support vessel, and compare the results to independently conducted FMEA and fault tree analysis (FTA). Several safety concerns were identified in the STPA that were not identified in the other analyses. Rokseth et al. [19] present a case study for selected parts of the system of a generic DP vessel, and evaluate whether it is beneficial to replace the currently conducted FMEA with STPA or to combine the two methods. The conclusion is that a combination is most beneficial, but that FMEA alone is not sufficient to ensure safety. Rokseth et al. [19] also conclude that robustness against single point failures is not adequate in order to ensure the safety of DP systems, and that it would be beneficial to employ STPA to develop safer DP systems.

A safety engineering process that employs STPA for software development has been developed [30]. This process includes verification of software by building a safe behavior model based on results from an STPA. Software is verified against the safe behavior model by using formal software verification approaches. Although this method takes an integrated system view by applying STPA, only software is subject to verification.

The objective of this article is to present a methodology for systematically deriving verification objectives and determining the necessary scope of verification activities for complex maritime systems. The methodology can be used as input to improve the current verification activities, such as the FMEAs required by the classification societies to demonstrate redundancy, sea-trials and HIL tests, to better handle the complexity in the systems. A case study is performed to demonstrate the methodology, focusing on important functions in a marine diesel-electric power system.

When the proposed methodology is used as input to the specialized FMEAs required for DP vessels, the verification objectives will help ensure that sufficient guidance is given and that appropriate objectives for the analysis are formulated. Additionally, the verification objectives may help define more specific acceptance criteria than “No single failure shall result in loss of position”, and similar high-level criteria. When used as input for test activities such as practical sea-trials and HIL tests, the verification objectives will serve as input to the test case generation process. In this case, the verification objectives may define a suitable scope and specific acceptance criteria, and highlight relevant context.

The methodology, which is rooted in STPA, considers all system dimensions (such as human factors, software and physical components) as an integrated whole to capture potential safety concerns related to interactions between these dimensions, and to handle complexity. This means that the focus of the proposed methodology in this article is much wider than the current verification activities aiming to ensure that “No single component failure shall result in loss of position” . This is important not only because accidents can happen without the occurrence of component failures [19], but also because it is difficult to evaluate the consequences of events (such as a component failure) at a global system level during current verification activities. When observing outcomes of low-level tests at the system level, the outcome becomes too dependent on the circumstances in which the test is conducted, (i.e., too context-dependent), meaning that small variations in the context variables describing the circumstances (or test conditions) can potentially have a significant impact on the outcome of the tests. Thus, when testing a sequence of component failures in a random context, and observing the results at system level, it is not necessarily clear whether a successful outcome can be ascribed to system safety or to a favorable set of context variables. The proposed methodology both reduces the dependency of test results on context variables, and highlights and provides insight into the remaining ones. This is achieved by deriving verification objectives that can be observed and evaluated at a local level, while also examining how observations may be affected by the context. In other words, if we think of a scenario taking place during a test as a complex causal path that may result in some defined system loss, our objective is to enable observation of test results near the initiating event, rather than at the end of the causal path, while substituting the remaining causal development with the STPA.

The following section gives a brief overview of the currently employed verification process for DP systems along with a discussion of the requirements that this process aims to verify. In Section 3, the proposed methodology is described in detail, including a description of STPA. The case study is presented in Section 4. In Section 5, the methodology is dis-