Necessity of New Framework to Support Social Implementation of Maritime Autonomous Surface Ships

— Construction of a vulnerability database and consideration of its use in risk assessment —

Tomoaki YAMADA*, Noriyuki KAJITA**

1. INTRODUCTION

The development of MASS (Maritime Autonomous Surface Ship) is progressing worldwide. For example, in the fully autonomous ship program "MEGURI 2040 [1]" of the Nippon Foundation, five consortiums are conducting demonstration tests on actual commercial routes by a tourist ship, coastal container ships, large coastal ferries, etc. Berth-to-berth automated navigation was also carried out with shadowing by the crew, and the vessels were successful in automatically avoiding other ships and fishing ships engaged in commercial activities.

Active discussions on the development of international regulations for MASS are also underway in the International Maritime Organization (IMO). At IMO MSC105, a roadmap for developing a goal-based MASS Code was endorsed, in which non-mandatory MASS guidelines will be developed in 2024 and a mandatory goal-based MASS Code will be developed targeting enforcement in 2028.

When using autonomous navigation technologies for purposes (e.g. labor saving and unmanned operation) that exceed the support tools of existing ships, it is important to conduct appropriate safety evaluations for autonomous navigation systems, and risk assessment is attracting attention as a method for this purpose. The interim guidelines issued by IMO [2] and guidelines issued by some flag states [3)-5)] specify the implementation of risk assessment. Guidelines for MASS have already been issued by multiple classification societies [6)-9)], and risk assessment is also emphasized in all of them. For example, in the ClassNK guidelines [6], it is necessary to carry out risk assessments depending on the development phase of the autonomous ship system.

When performing a MASS risk assessment, the key points are how to exhaustively extract the risks of unproven new technologies and how to accurately estimate those risks. Although there is no alternative to accumulating experience and knowledge through demonstration tests, etc., new technologies will inevitably have aspects that cannot be understood until they are used. When considering the social implementation of MASS, it is necessary to allow some degree of imperfection and consider how it should be operated. While implementation of MASS is premised on thorough pre-verification, it is also necessary to create a process for updating MASS safety-related knowledge and improving safety evaluations after implementation.

Although the principle is to create robust rules [10)], it is important that those responsible for rule development and safety evaluations, such as classification societies, take the perspective that incompleteness (i.e., vulnerability [11)]) will remain in the rules and standards created for new technologies with no track record, and adopt a stance of flexibly reviewing those rules in the product life cycle. To this end, it is necessary to construct a framework for timely reporting of information (particularly failure cases) that is discovered after actual use to the rule development and safety evaluation side. Moreover, if public institutions can create a database of such information and appropriately disclose it not only to technology developers but also to the rule development and safety evaluation side, further improvement in the safety of MASS by building a PDCA cycle can be expected.

2. CONCEPT OF VULNERABILITY

2.1 What Is Vulnerability?

The word "vulnerability" is often heard in everyday life, for example, in connection with information security involving personal computers. It is well known that vulnerability is difficult to completely counteract, and the current situation is that new vulnerabilities are being discovered one after another. Even if a vulnerability is blocked once, there is a possibility that a new

* Research Institute, ClassNK
** Digital Transformation Center, ClassNK

vulnerability will be discovered again, so it is always necessary to collect new information on OS and software and update them as quickly as possible. These are the characteristics of vulnerability that the authors would like to focus on in this paper.

Vulnerability is a concept adopted by the National Institute of Standards and Technology (NIST) in the United States, which publishes many security-related documents. For example, the Framework for Critical Infrastructure Cybersecurity Version 1.1 (April 2018) [12] describes not only the consideration of vulnerability when judging risk, but also the disclosure cycle of vulnerability information. The SP-800 series [13] also requires reuse of vulnerability information. It is interesting to note that vulnerability information is made available from a variety of public and private sources, including the National Vulnerability Database (NVD). In other words, since NIST assumes that information security is fragile and vulnerabilities will always be breached, the scope of security includes the response to cases where a vulnerability has been breached.

2.2 Safety and Vulnerability

ISO/IEC GUIDE 51: 2014 defines safety as “no unacceptable risk”. Safety includes intrinsic safety and functional safety. As systems become more complex, the concept of functional safety, which ensures an acceptable level of safety by installing functional devices (functions to ensure safety: safety functions), has been adopted in various industries. In MASS as well, safety is ensured by making full use of safety functions based on the concept of functional safety [14].

If vulnerability remains in this safety function, it poses a great risk, so it is necessary to quickly and accurately collect information on the vulnerability of this safety function.

3. EXAMPLES OF APPLICATION IN OTHER INDUSTRIES

3.1 Autonomous Vehicles Case in California, USA

In the United States, state governments have jurisdiction over road administration within their states, and state authorities are also in charge of licensing public road tests for autonomous driving. As part of the promotion of the introduction of autonomous driving, California revised the regulations regarding testing of autonomous vehicles (Article 3.7 – Testing of Autonomous Vehicle) on April 2, 2018 (the latest version took effect on April 13, 2022 [15]). The following are mandatory for developers of self-driving cars [16].

a) Prove that the developer of an autonomous vehicles has tested the controllability of the vehicle in an environment close to the real environment.
b) Prove that the vehicle can detect and respond to road conditions in accordance with state and local government vehicle operation regulations.
c) After notifying the local government of the autonomous vehicle test plan, monitor the test status via a two-way communication link.
d) Report to the state in the event of an accident or in cases where it is necessary to cancel the automatic driving mode.

In this paper, we would like to focus on d) above. From the public road test stage, there is an obligation to report within 10 days in the event of a collision accident (see § 227.48 [15]) and submit an annual report on cases where the automatic driving mode had to be canceled to the State of California even if no accident occurred. (see § 227.50 [16]). In addition, any identified defects that may pose an unreasonable risk to safety are subject to reporting requirements (see 3.8. Development of Autonomous Vehicle § 228.12 [17]). In this way, the fact that a framework for collecting data is incorporated from the stage of granting approval to conduct tests should be an extremely useful reference.

In California, trial operation of an autonomous driving delivery service and commercialization of robo-taxis have begun, and advanced efforts are being made in the field of autonomous driving vehicles. Since these efforts are supported by the aforementioned regulations, this may show the importance of timely sharing of vulnerability data with the rule development/safety evaluation side, which tends to be difficult to submit to those responsible for rule development/safety evaluation.

3.2 Examples from the Commercial Aviation Industry

The commercial aircraft industry, which achieved rapid development after World War II, has a history of improving safety by revising rules based on “accidents”.

As with the maritime industry, the International Civil Aviation Organization (ICAO), a subordinate organization of the United Nations, establishes international standards for the civil aviation industry, and member countries have introduced frameworks

which obligate them to develop domestic laws that comply with these rules. However, there are no third-party organizations similar to the classification societies in the maritime industry.

This rule was enacted as an annex to the Convention on International Civil Aviation (commonly known as the Chicago Convention) adopted in 1944, and it is a important feature that fields related to aircraft design, manufacturing, operation, etc. are inclusively covered under one Convention Annex.

Annex 13 [17] defines "Aircraft Accident and Incident Investigation". Its Chapter 3 GENERAL OBJECTIVE OF THE INVESTIGATION states that "3.1 The sole objective of the investigation of accident or incident shall be the prevention of accidents and incidents. It is not the purpose of this activity to apportion blame or liability".

It can be said that this expresses the idea that it is necessary to recognize that the enacted regulations are not perfect, and to learn from actual accidents and incidents in order to prevent future accidents and incidents which have the same cause, since accidents and incidents are unavoidable events in aircraft.

In fact, in the United States, a law has been enacted that does not impose criminal penalties except in cases of intentional or malicious negligence in order to enable accurate interviews for investigations of aircraft accidents.

Based on this spirit, in the commercial aircraft industry, a framework has been introduced for each industry stakeholder (including the government authorities of each country) to report, disclose, analyze, and formulate countermeasures not only for accidents and incidents but also for various failure cases, and a framework for improving aviation safety on a daily basis has been put in place.

The important parts of this safety activity can be summarized in the following two points.

(1) Taking countermeasures will lead to improvements in safety, as accidents and incidents will inevitably occur.

(2) Collecting and disclosing various vulnerability information representing accidents and incidents in order to take countermeasures.

This is an example showing that vulnerability, which is the theme of this paper, is very effective in improving safety. Fig. 1 shows an overview of the PDCA cycle based on vulnerability in the commercial aircraft industry.

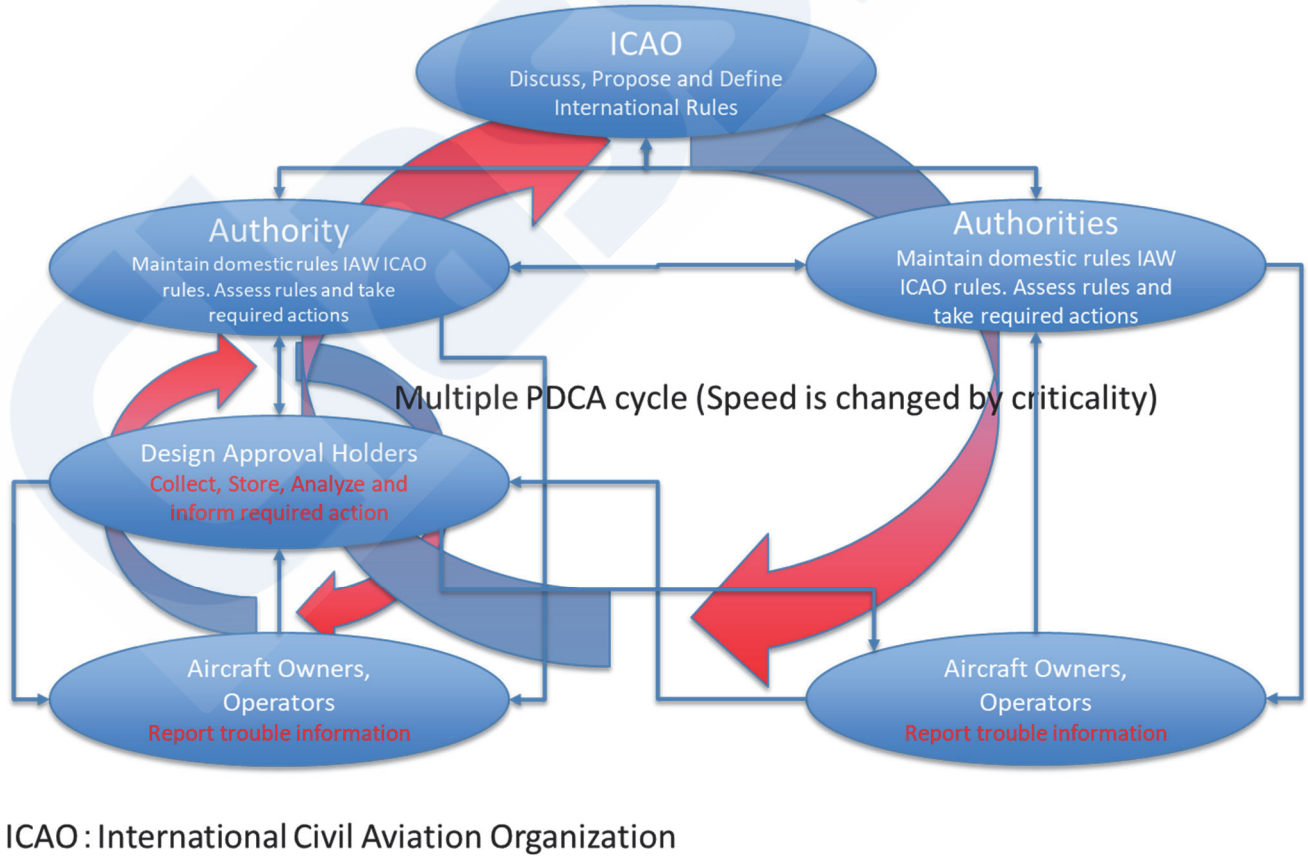

Fig. 1 Overview of the PDCA cycle based on vulnerability in the commercial aircraft industry

4. APPLICATION TO AUTONOMOUS SHIPS

4.1 Building a Vulnerability Database

As mentioned above, accepting a certain degree of imperfection and thinking about the optimum form of operation under this condition is a necessary way of thinking when confronted with new technologies. It is also necessary to create a framework for social acceptance of those technologies. The framework of collecting cases related to vulnerability, creating a database, and using it to improve the accuracy of safety evaluations has already been adopted in other industries, and we believe that it will also an effective approach for MASS.

In constructing a vulnerability database for MASS-related technologies, it is necessary to organize the classification and collection methods, but vulnerability has the property of decreasing as technology maturity increases. Therefore, we would like to propose that vulnerability levels be divided into two axes, that is, the status of the technology and the area of application [18], and that the reporting frequency be set according to the level. Tables 1 and 2 are shown only as examples. While setting the levels and reporting frequency according to the level of technical maturity at the time of social implementation, it is also necessary to consider conducting periodic reviews corresponding to improvements in the level of technology maturity.

Table 1 Example of vulnerability classification

		Technology Status		
		Proven	Limited field history	New or unproven
Application Area		SOLAS mandatory	On-shore ISO/IEC	Others
Known	On-market products	1	2	3
Unknown	On-market products	2	3	4
New	Development / Update	3	4	5

Table 2 Example of vulnerability reporting frequency

	Level of vulnerability				
	1	2	3	4	5
Defects that caused an accident	Immediately	Immediately	Immediately	Immediately	Immediately
Defects that caused disengagement of autonomous mode	Semi-annually	Quarterly	Quarterly	Quarterly	Monthly
Other defects found during operation	Annually	Semi-annually	Quarterly	Monthly	Monthly

4.2 Utilization in Risk Assessment

Risk assessment is also being carried out in the MASS demonstration project, and the safety of MASS is evaluated by analyzing the risks inherent in the new technology itself and the risks when the technology is installed on ships while verifying the differences with the existing technology. However, in the trial verification stage, it is very difficult to extract all the hazards of new technologies that have no track record and accurately estimate the risks that they may cause. Therefore, at present, evaluations are made in conjunction with the size of the safety margin set in the demonstration experiment.

On the other hand, for social implementation, it is necessary to optimize this safety margin. In this regard, we believe that incorporating the concept of vulnerability is one option. For example, use of a vulnerability database will ensure that risk assessments can always be performed based on the latest information. This will not only prevent the omission of verification of important risks, but also contribute to preventing excessive safety measures (rationalization of safety margins).

4.3 Build and Thoroughly Implement the PDCA Cycle

In the development phase, information and experiences such as failure cases and near-miss incidents should be shared with the rule development and safety evaluation side from the stage of demonstration experiments in order to prevent omission of verification when certifying the technology.

In the operation phase, considering that new technologies with little track record can be understood only after they are used, feedback from seafarers, who are the users, should be appropriately distributed to those responsible for technology development, rule development and safety evaluation. This will lead to improvements in technology, regulation and evaluation. Building a vulnerability database and appropriately using the PDCA cycle will lead to improvements in the safety of operation of MASS.

First, the vulnerability database is expanded, and the PDCA cycle is constructed based on vulnerability from the standpoints of technology development, rule development and safety evaluation. Then, this PDCA cycle must continue to be used effectively. We believe that such a framework is necessary for MASS, in which hardware failures, software defects, operation and management problems and other factors are interrelated in a complex manner.

5. CONCLUSION

As social implementation of MASS is now becoming a reality, the time has come to consider a new framework which supports the social implementation of truly new technologies and solutions that transcend the conventional framework, that is, a framework which can complement imperfect regulations and institutions. It is also necessary to incorporate concepts such as functional safety and systems engineering, which are new concepts for the maritime industry. As one of these methods, this paper proposed the concept of vulnerability.

To ensure that these new concepts take firm root, it is necessary to formulate the optimum approach and define the division roles within the industry. For this, a forum should be built, for careful discussion within the industry to determine who will assume the leadership position, what type of framework is needed to impose reporting obligations, and where the vulnerability database. In this regard, since classification societies have a neutral position, they should have a large role to play. We would like to work to stimulate discussions in the industry.

ACKNOWLEDGMENT

The authors wish to thank Professor Etsuro Shimizu and Ms. Ayako Umeda of Tokyo University of Marine Science and Technology for helpful discussions and comments on this paper.

REFERENCES

1) The Nippon Foundation: “The Nippon Foundation MEGURI2040 Fully Autonomous Ship Program”, https://www.nippon-foundation.or.jp/en/what/projects/meguri2040
2) IMO MSC.1/Circ.1604 (2019), INTERIM GUIDELINES FOR MASS TRIALS
3) Maritime Bureau, Ministry of Land, Infrastructure, Transport and Tourism: Guidelines for Safety Design of MASS (*Jidouunkousen no anzen sekkei gaidorain*) (2020) (Japanese)
4) VTMIS, EU OPERATIONAL GUIDELINES FOR SAFE, SECURE AND SUSTAINABLE TRIALS OF MARITIME AUTONOMOUS SURFACE SHIPS (MASS)
5) Norwegian Maritime Authority, RSV 12-2020: Guidance in connection with the construction or installation of automated functionality aimed at performing unmanned or partially unmanned operations
6) ClassNK: Guidelines for Automated/Autonomous Operation on Ships (Ver. 1.0) (2020)
7) DNVGL: Autonomous and remotely operated ships, DNVGL-CG-0264 (2018)
8) Bureau Veritas: Guidelines for Autonomous Shipping, Guidance Note NI 641 DT R01 E (2019)
9) ABS: ABS advisory on autonomous functionality (2020)
10) IMO Resolution A.1103(29): PRINCIPLES TO BE CONSIDERED WHEN DRAFTING IMO INSTRUMENTS
11) ISO 31073:2022, Risk management - Vocabulary
12) National Institute of Standards and Technology: Frame work for Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018
https://www.ipa.go.jp/files/000071204.pdf
13) National Institute of Standards and Technology: Computer Security Resource Centre

https://csrc.nist.gov/publications/sp
14) Yamada T: Safety Evaluation for Technologies related to Autonomous Ships, ClassNK Technical Journal No. 3, 2021(I)
15) California Department of Motor Vehicles (DMV): Article 3.7. Testing of Autonomous Vehicles https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/
16) California Department of Motor Vehicles (DMV): Article 3.8. Deployment of Autonomous Vehicles https://www.dmv.ca.gov/portal/file/adopted-regulatory-text-pdf/
17) International Civil Aviation Organization: Annex 13 to the Convention on International Civil Aviation, “Aircraft Accident and Incident Investigation”
18) IMO MSC.1/Circ.1455 “GUIDELINES FOR THE APPROVAL OF ALTERNATIVES AND EQUIVALENTS AS PROVIDED FOR IN VARIOUS IMO INSTRUMENTS”, Annex, page 9, Table 1: Categorization of new technology