No. 155 Contingency plan for onboard computer based systems

(Sep 2018)

1. Introduction

1.1 General

Computer based systems are vulnerable to a variety of failures such as software malfunction, hardware failure and other cyber incidents. It is not possible for all failure risks to be eliminated so residual risks always remain. In addition, a limited understanding of the operation of complex computer based systems together with fewer opportunities for manual operation can lead to crews being ill-prepared to use their initiative to responding effectively during a failure.

IMO and Classification Society rules contain many context specific examples of requirements for independent or local control in order to provide the crew with the means to operate the vessel in emergencies or following equipment failures. These requirements have generally been introduced when automation or remote control is introduced to individual pieces of equipment or functions and address concerns regarding its possible failure of the new features. The introduction of technologies which integrate different vessel's functions creates the opportunity for two or more systems to be impacted by a single failure simultaneously.

Where, due to high computer dependence, manual operation is no longer practical or where the number of systems simultaneously affected is too high for manual operation to be practical with existing crew levels then the value of local control as a form of reassurance is limited, however the crew will still need to be provided with practical options to try to manage threats to human safety, safety of the vessel and/or threat to the environment.

If the practical options are not considered during the design and installed during construction of the vessel then the vessel and its crew could be, due to the introduction of new technologies, exposed to risks which they cannot manage.

Practical options could include limiting the extent of potential damage so that manual control is still achievable or providing backup systems which could be used in a worst case systems failure. Whatever form of contingency is provided to address failures it is important that it is well documented, tested and that the crew is aware and trained.

Requirements related to preventive means, independent mitigation means, engineered backups, redundancy, reinstatement etc. are dealt with in the other relevant recommendations.

1.2 Objective

This recommendation is intended to clarify the need for developing contingency plans for the situation following a failure of onboard computer based systems and lays out expectations for the provision of systems and services that need to remain intact in order for the crew to be able to respond appropriately.

1.3 Scope

This recommendation concerns the need for policies and procedures to be applied in case of the failure or malfunction of onboard computer based systems which could lead to dangerous situations with respect to human safety, safety of the vessel and/or threat to the environment.

No. 155 (Cont)

In this connection, at least, the systems belong to Category III in accordance with UR E22 are considered as they are highly time critical. Category II systems are associated with a time element as they do not immediately lead to a dangerous situation. Each Category II system should also be reviewed to establish if specific provision for contingency needs to be available.

1.4 Exclusion

Navigation systems required by SOLAS Chapter V, Radio-communication systems required by SOLAS Chapter IV, and vessel loading instrument/stability computer are not in the scope of this requirement.

This Recommendation is not applicable to loading instrument/stability computer (Rec No. 48 may be considered).

2 Contingency Plan

2.1 General

The shipowner has overall responsibility of developing the contingency plan based on essential information which should be provided by the associated system integrators and suppliers to enable effective contingency planning. The Contigengy Plan should contain a set of predetermined instructions or procedures for how crews will detect, respond to and limit consequences of cyber incidents in a timely manner, and for how crews will recover the affected systems after securing the ship's safety by suitable response actions. In this context, the following response process in the event of a cyber incident should be taken into account:

.1 Detect a cyber incident and identify the failed system;

.2 Determine effective response options and take appropriate actions;

.3 Recover the failed system;

.4 Investigate and document the cyber incident;

.5 Evaluate the effectiveness of response options and update the contingency plan

The consideration of the full scope of a vessel's contingency plan will extend beyond the scope of class to include management systems and crew training. In the context of this recommendation, the use of the term 'contingency plan' is intended to capture the design, installation and documentation provided in order that the management systems and crew are provided with the facilities and information needed to support their response actions in the event of a cyber incident. The basis of the contingency plan and description of the documentation to be handed over on delivery of the vessel should be reviewed by the classification society at the initial stage.

The Contingency Plan should include the following information as a minimum:

.1 List of computer based systems covered by the Contingency Plan;

.2 System configuration and descriptions for systems covered by the Contingency Plan;

.3 Incident response plan;

.4 Recovery plan;

No. 155 (Cont)

.5 Periodic testing plan;

.6 maintenance procedure for the Contingency Plan;

During the preparation of the contingency plan, input should be obtained from the various stakeholders including ship operators, system integrator, system support vendors and IT/OT engineers.

When a cyber incident failure condition on computer based system on board is discovered, it is important that all relevant personnel are aware of the correct procedure to follow. It is vital that contingency plans, and related information, are available in a form which cannot be rendered ineffective by an onboard incident. A hard copy or an electronic device which is independent of the vessel's networks could be considered acceptable.

The contingency plan should be formatted to provide quick and clear directions in the failure event for use of onboard personnel unfamiliar with the plan or the system. A concise and well-formatted plan reduces the likelihood of creating an overly complex or confusing plan.

2.2 Developing the Contingency Plan

2.2.1 Identify computer based systems on board

At the initial stage of developing a contingency plan, it is very important to identify and to include all computer based systems on board. The provision of application scope of contingency plan among all computer based systems on board should be clearly defined based on their effects in a failure situation. At a minimum, all Category III systems according to UR E22 should be included in the plan. Category II systems should be also reviewed, if specific provision for contingency needs to be available, such systems should be included in the plan.

2.2.2 Incident Response Plan (IRP)

An incident response plan should contain a predetermined set of instructions or procedures to detect, respond to, and limit consequences of cyber incidents against computer based systems required for essential services according to UI SC 134.

Typically when a cyber incident is discovered, a quick assessment is performed to evaluate the consequence and the options to respond. For example, one possible response option is to physically isolate the failed or malfunctioning system and to use the redundant system, or if not available, independent or local control may be another response option. To assist crews to find effective response options quickly and to take response actions in a timely manner the provision of systems to facilitate an incident response plan for the identified systems on board should be developed in clear, concise, and easy format to implement in the event of a failure.

The incident response plan should, as a minimum, include the following information:

.1 System for response and breakpoints;

.2 Alarm indication or abnormal symptom caused by a cyber incident;

.3 Failure consequence;

.4 Effective response options which do not rely on either shut down or transfer to independent or local control, if any;

No. 155 (Cont)

.5 Independent or local control change over procedure;

Note:

1. The example template in Appendix 1 may be used for developing Incident Response Plan.

2. Appendix 2 Flow Chart/ Process which may assist in the process of developing Incident Response Plan.

3. Risk assessment report such as FMEA or FMECA may be considered to determine failure consequence.

4. Independent and local control should be capable of operating independently from the system that failed due to the cyber incident.

2.2.3 Recovery Plan (RP)

Recovery plans should be easily understandable by the internal personnel and potential external personnel, and include essential instructions and procedures to ensure the recovery of a failed system and how to get external assistance if the support from ashore is necessary. In addition, software recovery medium or tools essential for recovery on board should be available.

When developing recovery plans, it is important to specify the recovery objectives for the various systems and subsystems involved. There are two distinct types of objectives as below:

.1 System recovery: it involves the recovery of communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities.

.2 Data recovery: it involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential cyber incidents should be created and the recovery procedure developed and described. Recovery plans may be supported through access to the following information;

.1 Instructions and procedures for restoring the failed system without disrupting the operation from the redundant, independent or local operation.

.2 Processes and procedures for the backup and secure storage of information

.3 Complete and up-to-date logical network diagram

.4 The list of personnel responsible for restoring the failed system

.5 Communication procedure and list of personnel to contact for external technical support including system support vendors, network administrators, etc.

No. 155 (Cont)

.6 Current configuration information for all components

2.2.4 Review and onboard testing of the Contingency Plan

The contingency plan as well as appropriate onboard test procedures should be reviewed by Classification Society prior to the testing.

Onboard tests should be carried out according to the onboard test procedures after final integration of systems and witnessed by Classification Society. The testing enables deficiencies to be identified and addressed by validating and verifying the effectiveness of the plans. In this context, testing should be carried out in as close to an operating environment as possible, however, if impracticable, simulated test may be accepted. If any deficiencies are found, the relevant part should be reviewed and proposed solutions or alternatives submitted for consideration.

2.3 Onboard use of the Contingency Plan

The Contingency Plan should be kept at a position readily accessible to responsible personnel, who should be nominated by ship owner and be indicated in the plan.

The responsible personnel need to be familiar with the structure and contents of the plan in order that preplanned actions can be taken within the time required for them to be effective.

Note: Appendix 3 provides helpful information about the process to identify a failure event and quickly determine responses actions, including the provided or independent or local control means as appropriate.

2.3.1 Periodic testing on board

It is recommended that the contingency plans are tested periodically under the management of responsible personnel, for example using scenario exercises with all relevant personnel including management in order to verify that the anticipated response times are effective in the proper working of the plan.

2.3.2 Maintenance of the Contingency Plan

The contingency plan should be reviewed and updated regularly by responsible personnel to ensure that the plan is maintained in a ready state that accurately reflects the current information for onboard critical systems and the associated Response Plans.

Any proposed changes on the vessel that could have an impact on the effectiveness of the plan should be reviewed and if in the execution of the plan would be adversely affected then appropriate changes should be made, tested and documented. Significant changes or those with a potentially critical impact could include the inadvertent interconnection of systems or the exposure of systems to external networks

3 References

UR E22 (Rev.2 June 2016)
NIST Special Publication 800-34 Rev.1
NIST Special Publication 800-53 Rev.4
NIST Special Publication 800-82 Rev. 2
IEC 62443-2-1: 2010
The Guidelines on Cyber Security onboard Ships (Version 2.0: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)

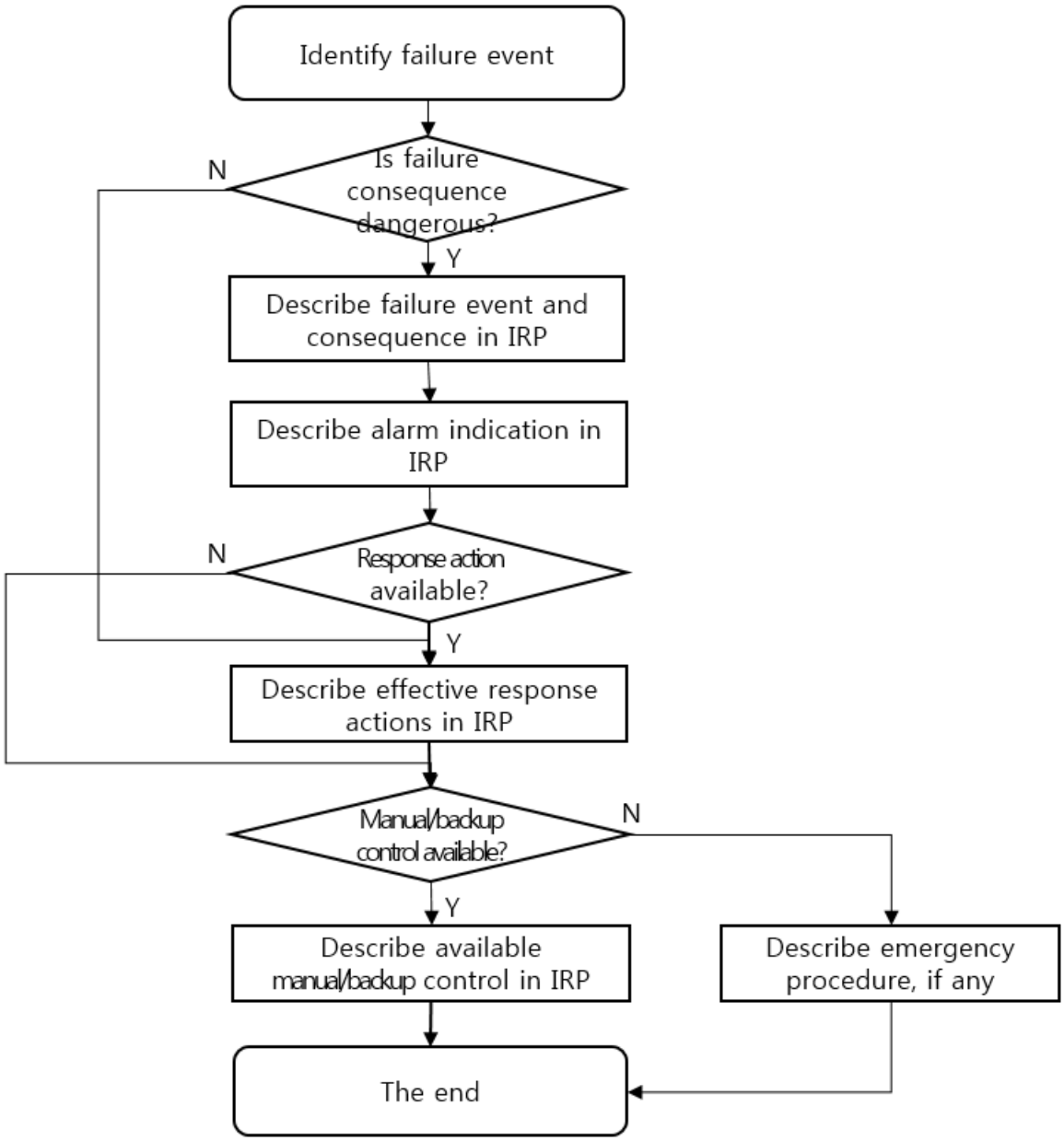
No. 155 (Cont)

Appendix 1 Example Template for Incident Response Plan

No.	Failure Event	Severity or Priority	Alarm	Consequence	Response Action
1	No.1 control failure	High	"control failure"	Loss of control of No.1 steering system	Switch from No.1 Steering Control to No.2 Steering Control by using control system selective switch on steering wheel stand.
2					
3					
4					
5					

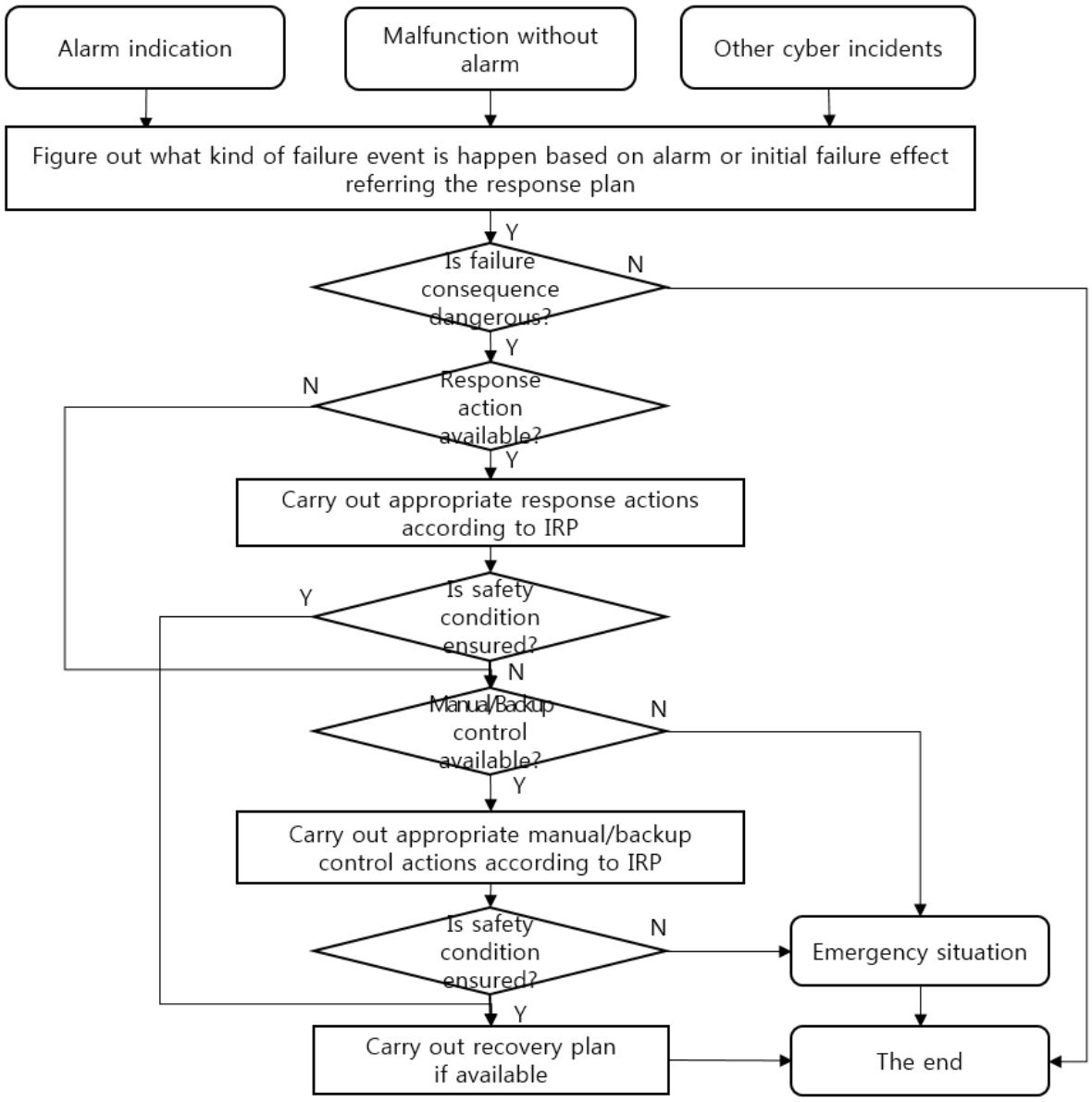
No. 155 (Cont)

Appendix 2 Flow chart for developing Incident Response Plan



No. 155 (Cont)

Appendix 3 Flow chart for response actions to a failure event on critical computer based system



No. 155 (Cont)

Appendix 4

Definitions.

Contingency Plan: Policies and procedures designed to maintain and restore essential services or operations in the event of a cyber incident which may result in the loss or malfunction of a computer based system.

Cyber incident: Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network or computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Computer Based System: The system based on computer technology which may be comprised of hardware, software and the associated interfaces for input and output.

Incident response plan: Documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of cyber incidents in computer based systems.

Recovery plan: Documentation of a predetermined set of instructions or procedures to restore computer based systems in the short and medium term and fully restore all capabilities in the longer term after a cyber incident.

End of Document