MISSION

WHITE PAPER

Standpoints for safety risk analysis of the MISSION Just-In-Time arrival system

Igor Kozin
Senior Researcher, PhD, Research Unit for Maritime Health and Technology (MHT), University of Southern Denmark

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor CINEA can be held responsible for them.

Table of Contents

For use only within the MISSION project consortium

1. Objective of the White Paper

This is an informational document that communicates the account of SDU participants of the MISSION project on how to prove whether the system being developed by the consortium improves the safety of ships in the port areas.

The methods suggested in this document are based on an overview of the state-of-practice guidelines and state-of-the-art methods in safety risk analysis. They are compliant with the Guidelines for Formal Safety Assessment (FSA) [1] and The Ship Inspection Report Programme (SIRE) [2].

Other accounts on the same issues may exist that are either complementary or preferred over the methods described in this paper. This document is intended to make discussions constructive by possibly benchmarking other views with those described here and by working out a clear methodology and guidelines for conducting a safety risk analysis of the system being developed; and for informing decisions on the system's acceptability or improvements needed to achieve the acceptability.

2. Scoping the study

A Just-In-Time (JIT) arrival system is an information and communication system binding ships and port services together. By collecting the needed data from port-bound ships and the availability of berth and port services, the JIT system processes the data and suggests ship arrival times. If properly designed, increased maritime safety is an important expected outcome. However, the enhancement of safety must be proactively proven by conducting an appropriate safety risk analysis.

The arsenal of safety risk analysis assessment methods is comprehensive, and the selection of the most appropriate tools is of utmost importance. The ISO 31010 standard on Risk Management – Risk Assessment Techniques and FSA [1] provide a list of different types of risk analysis methods and tools that may be used in the IMO rule-making process. However, they do not limit the risk analyses to the listed techniques, as the state-of-the-art in the field suggests a much broader set of available tools that may appear better fits for the case of our interest.

The system's definition and its nature (technical, man-machine, organisational, cyber-physical, etc.) are decisive in choosing the analysis method.

We argue that the JIT arrival system considered in its unity with port-bound ships and port services is a **Cyber-Physical System (CPS)**. The key features of a CPS imply that special safety risk analysis methods should be applied to firmly ground conclusions about the system's acceptability. A definition of a CPS and details on its key features are given in Section 3.

An important aspect of CPSs to take into account is their vulnerability to cyber threats and their potential to cascade into physical harm and safety issues. In other words, the security domain in CPSs can expand into the safety domain forming the sub-domain **Security for Safety** as visualized in Figure 1 [3].

A basis for a safety risk analysis of any potentially hazardous activity is a pictorial system model or representation. For example, for the systems of the process industry, these are Piping and Instrumentation Diagrams. Computer systems are represented by computer network diagrams (hardware system architecture) and/or unified modelling language diagrams. The control of industrial systems is represented by computer network diagrams complemented by information flow diagrams.

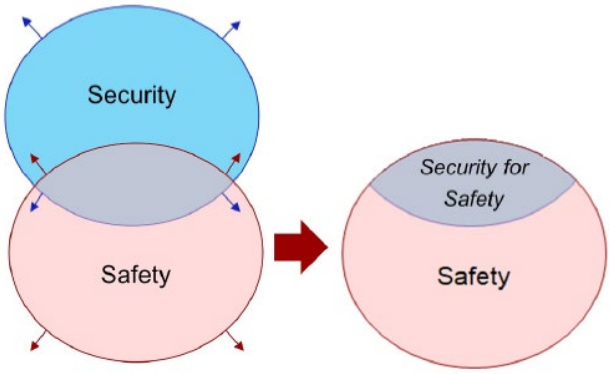


Figure 1. Expansion of the security domain into safety [3]

CPSs need a special type of system representation to cover to a degree possible the aspects influencing safety. Representation of CPSs in the form of **feedback control** loops and **multilayered diagrams** has proven useful for this purpose. Section 3 provides details on these two system's representations.

The role of **human factors** is crucial in the safe operations of a CPS. Its nature implies that humans are system units that can simply fail or make errors intentionally and unintentionally. Human failures and errors can make the whole system fail. The recognition of the significance of human factors for safe ship operations is stressed in The Ship Inspection Report Programme (SIRE 2.0) [2]. SIRE has been a cornerstone of the effort for the safe and efficient operation of vessels. Section 4 provides guidance on how to account for human factors in the safety analysis.

A lack of specific data on human reliability and the likelihood of system failures can be a cause of significant uncertainty in risk estimates. This may result in indecision on whether operating the system is acceptable from a safety point of view. (More details on acceptance criteria are given in Section 5.) To compensate for the lack of specific reliability data, **expert judgments** can be invoked. Even though expert judgment elicitation is thoroughly conducted, the residual uncertainty may not necessarily allow making conclusive statements on whether the designed system is safer compared to the existing one. In this case, an accepted decision-making strategy can be the **precautionary principle** that is applied to situations with high epistemic uncertainty. Additionally, and in case of failure of the developed JIT system, reliable **fall-back and recovery procedures** should be foreseen that allow bringing the system to a safe state that can, for example, be the existing system's set-up.

Having the fall-back and recovery procedures in place will make it possible to transfer the system to a **fail-safe mode** which will serve as a warrant for the avoidance of big economic losses and operation disturbances. It will give time to introduce improvements in the system's design, software, procedures, and other elements and activities that may influence system reliability and safety.

Several safety risk metrics can be estimated to compare with risk acceptance criteria. For the safety of maritime operations, individual risk per annum and societal risk appear appropriate risk metrics. However, for an existing operational system - the level of risk for which has been accepted - **a comparative safety risk analysis** can be sufficient. In this case, there is no need to carry out a full-scale analysis but to prove that the modified system is either safer or at least as safe as the existing one. This approach is much less resource-demanding compared to the full-scale risk assessment and well aligned with the **GAMAB risk acceptance criterion** (more details in Section 5).

The ultimate objective of the development of the JIT arrival system is to reduce waiting time in the anchorage area near ports. By achieving this objective, fuel consumption will be reduced as well as the traffic density. As known, the density of the traffic in a limited area is a major contributor to the likelihood of accidents (collisions and groundings) given other circumstances and conditions are equal. By reducing the density, the likelihood of the accidents is reduced and so is the potential to harm people and the environment, and to damage assets. In this view, the proof of enhanced safety can be focused on the proof of achieving lower ship traffic density in the anchorage area.

The expectation is that the implemented JIT system will make it true. However, the system's performance may deviate from its expected level. The contributing factors to impaired performance (yet to be identified) can be, for example, distrust between the navigators, failures of hardware and software, human errors, miscommunication, and cyber vulnerabilities. They can make the system so unstable and unreliable so that its continued operation may be halted.

The objective of the safety risk assessment is to prove the opposite.

3. Representation of the system for safety analysis

A CPS is widely defined as a system that integrates computational and physical processes [4]. In more detail, the generic key features of a CPS are the following: (1) real-time feedback control of physical processes through sensors and actuators; (2) cooperative control among networked subsystems; and (3) a threshold of automation level where computers close the feedback control loops in (semi)automated tasks, possibly allowing human control in certain cases [5].

Different references suggest different classifications of automation levels (see elsewhere in [6] and [7]). For our subject matter, the classification from level A to level C [8] appears most appropriate:

(A) Computer provides information or advice to human operator
(B) Computer interprets data and displays to the operator, who makes the control decisions
(C) Computer issues commands directly, but with human monitor of the computer's actions providing varying levels of input
(D) Computer completely eliminates the human from the control loop. The human only provides advice or high-level direction

We expect that the JIT port call system, which is being developed, will fall either into level A or B.

Figure 2 is the domain-specific mapping of the above-mentioned generic features of CPSs onto the feedback control loop corresponding to levels A and B.

The level of automation is the factor that influences the safety risks of a CPS. High levels of automation of the system design assign the computer the role of closing the feedback control loop, leaving the navigator a supervisory role. Such designs reduce the influence of operational human errors, while it is expected that lower levels of automation increase the likelihood of human error. However, this should not be taken for granted, as the irony of automation is that it "may expand rather than eliminate problems with the human operator" [9].

Despite being very simple system representations, diagrams A and B (feedback control loops) can serve as starting points for the identification of high-level hazards that will guide further detailed identification down to the level at which efficient risk prevention and mitigation measures can be suggested. Figure 3 [10] is again a feedback control loop but complemented with some of the general causes of why hazardous states might be generated. This model can assist in generating causal scenarios. However, it may as well appear too general to account for specific features of the

system under analysis. Leveson and Thomas [10] provide a good number of different cases that demonstrate how the model in Figure 3 can be extended to a level serving as an adequate basis for detailed hazard identification.

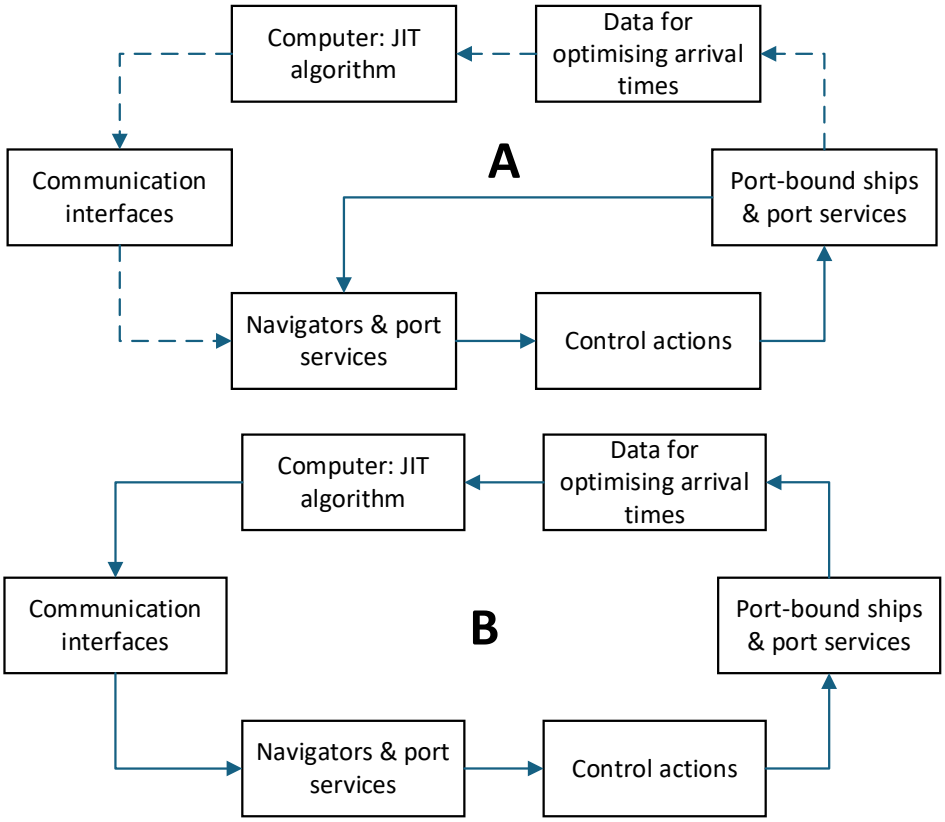


Figure 2. Roles of computers and humans in the control loops of the JIT arrival system

Appendix I shows a longer list of possible failure causes that can be attributed to the functioning of a control loop.

The model of a system in the form of a feedback control loop can be applied to the analysis of any controlled system, including organisational systems in which only people function in clustered organisational units. An extension of this system representation tailored to CPSs can serve as a richer basis for hazard identification.

The diagram in Figure 4 [5] is a generic CPS representation that was developed for the purpose of more detailed hazard identification, including the hazards caused by unintentional and intentional human actions. It is worth noting that the system representation in the form pictured in Figure 4 is in agreement with a comprehensive view stipulated in the FSA Guidelines (see Figure 3 in [1]).

Taking the basis of this master diagram, a detailed system representation can be developed to serve as a model for hazard identification of the JIT system being developed. Some examples of tailored master diagrams to specific CPSs can be found in [3] for a safety fan enclave and in [5] for an autonomous surface vehicle.

An important and specific aspect of CPSs, which is explicitly visualised on the diagram, is their vulnerability to cyber threats and their potential to cascade into physical harm and safety issues.

This is a common safety and security issue in transportation systems, robotics, critical infrastructures, and industrial control systems among others.

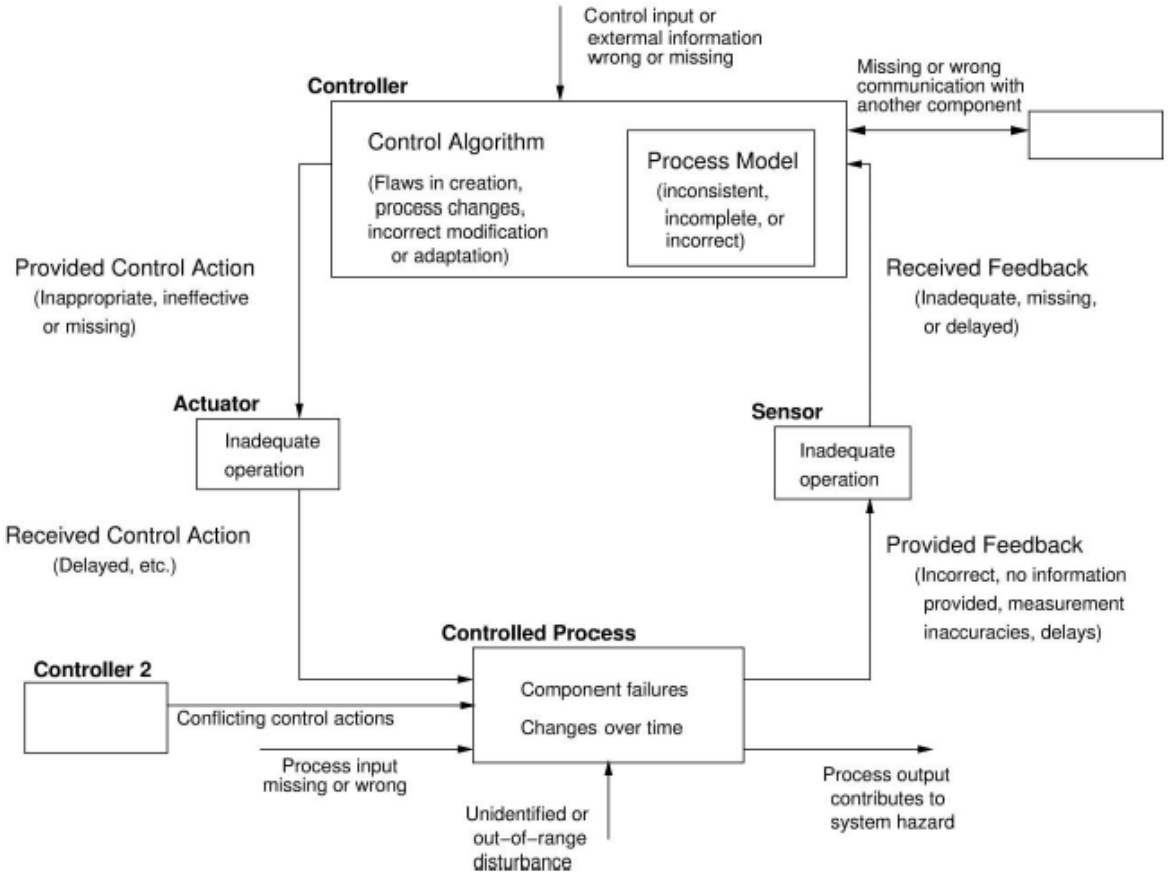


Figure 3. A general model to assist in generating causal scenarios [10]

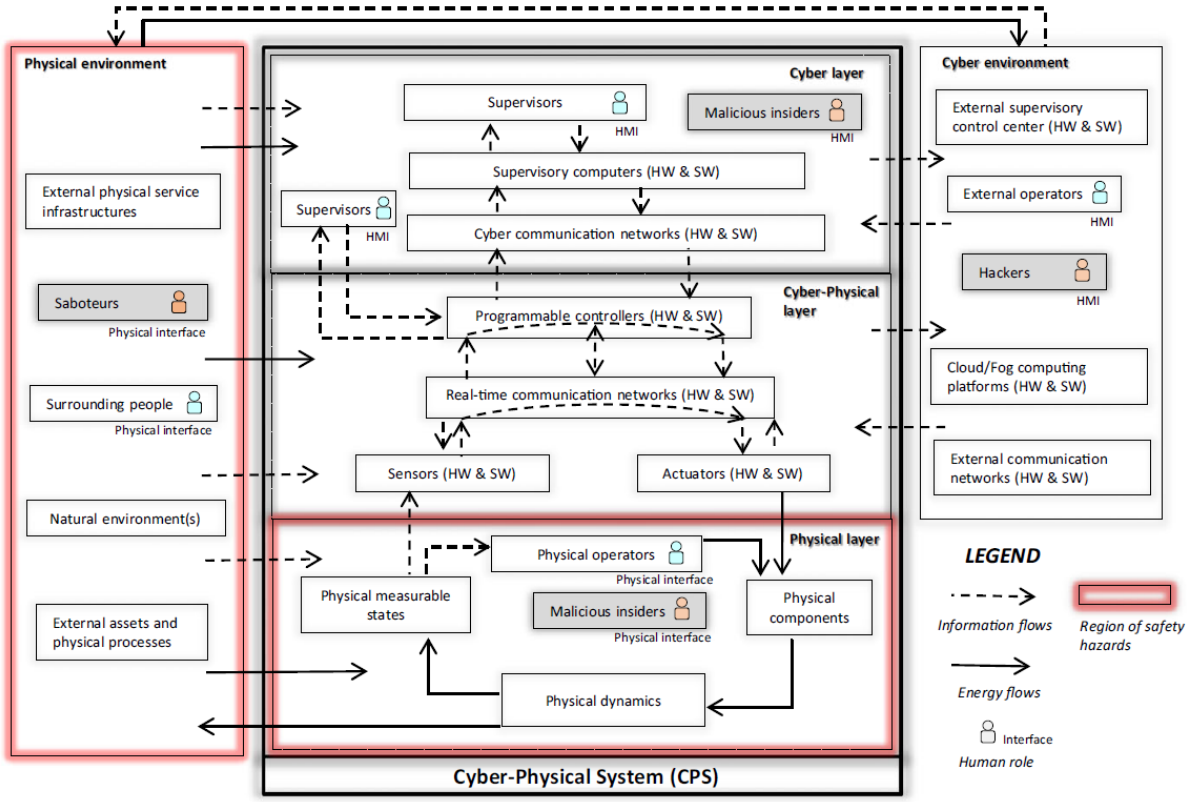


Figure 4. CPS master diagram: multi-layered representation of a CPS and environments with information and energy flows [5]

4. Human factors are crucial in safe operations

It is of utmost importance that human roles and actions are identified and potential deviations from expected actions are included as sources of risk in CPSs. Even if computers close the feedback control loops, humans could still perform complementary roles in cyber processes, such as data insertion, intermittent modifications, and parameter readings, among others [5].

The importance of the inclusion of human factors in the safety risk analysis of shipping operations is stressed in FSA [1] and SIRE [2]. However, these documents do not provide detailed guidance on how the analysis of human-machine systems should be carried out. A pictorial model of a specific CPS developed based on the master diagram will clearly indicate that human operators can be sources of risk for both unintentional motives and malicious acts of insiders and external cyber attackers. Malevolent activities can deliberately disrupt CPSs using acquired knowledge of the system's security vulnerabilities and the dependencies between its system layers [11, 12].

Table 1 [5] shows human roles in the possible malfunctioning of a CPS.

Table 1. Human roles as sources of risk at different system locations [5]

	System		Environment	
Risk motives	**Cyber**	**Physical**	**Cyber**	**Physical**
Unintentional	Supervisors using HMI	Physical operators	External Operators	Surrounding people
Deliberate	Malicious insiders	Malicious insiders	Hackers	Saboteurs

There exist a number of methods to analyse human reliability [13]. Arguably, the method of our choice for analysing human error in the system being designed is an Action Error Analysis (AEA). It has proven efficient in many applications, is recommended by the UK Health and Safety Executives (HSE) [14], and – which is decisive – can be well extended to the analysis of the whole CPS of our interest.

The starting point of AEA is to make an analysis of actions performed during the execution of a certain task. For example, the task "Undocking" of a ship consists of a number of consequent actions such as "activating forward-facing thrusters", "unmooring", "activating rear thrusters", etc. Different errors can be committed while executing an action, or even an action can be omitted. To exhaustively identify possible human errors, a list of error modes (akin to guidewords in Hazard and Operability Analysis (HAZOP)) is applied (Table 2 [1]):

Table 2. Generic list of human error modes

Generic error modes			
1.	Omission	9.	Wrong object
2.	Too early/too late	10.	Wrong substance
3.	Too fast/too slow	11.	Wrong materials
4.	Too much/too little	12.	Wrong tool
5.	Too hard/too slight	13.	Wrong value
6.	In the wrong direction	14.	Extraneous action (one unrelated to the task but interfering with it)
7.	In the wrong sequence	15.	Wrong action
8.	Repetition		

A more extensive checklist of error modes is provided in [14] and summarised in Table 3. This can be applied to analyse man-machine, and information and communication systems. Section 5 provides an example of the checklist that can be applied to the cyber and cyber-physical parts of the JIT system.

A detailed description of how AEA can be found elsewhere in [16].

The identification of deliberate human-made threats that can exploit a known or previously unknown vulnerability is a necessary part of the safety risk analysis of any safety-critical CPS. This type of analysis (security for safety), which is the analysis of cyber risks that may propagate into the physical layer of the system, should be performed with the help of dedicated for this purpose approaches. To date, there is no one commonly accepted method and the analyst can choose from a set of alternatives that are briefly presented in [3].

Table 3. HSE's checklist of error modes for human error identification

Action Errors	**Information Retrieval Errors**
A1 Operation too long / short	R1 Information not obtained
A2 Operation mistimed	R2 Wrong information obtained
A3 Operation in wrong direction	R3 Information retrieval incomplete
A4 Operation too little / too much	R4 Information incorrectly interpreted
A5 Operation too fast / too slow	**Information Communication Errors**
A6 Misalign	I1 Information not communicated
A7 Right operation on wrong object	I2 Wrong information communicated
A8 Wrong operation on right object	I3 Information communication incomplete
A9 Operation omitted	I4 Information communication unclear
A10 Operation incomplete	**Selection Errors**
A11 Operation too early / late	S1 Selection omitted
Checking Errors	S2 Wrong selection made
C1 Check omitted	**Planning Errors**
C2 Check incomplete	P1 Plan omitted
C3 Right check on wrong object	P2 Plan incorrect
C4 Wrong check on right object	**Violations**
C5 Check too early / late	V1 Deliberate actions

A comprehensive and systematic analysis of threat events can be performed with the BITS key risk measurement tool for information security operational risks [18].

The FSA Guidelines [1] state that “the depth or extent of application of the methodology should be commensurate with the nature and significance of the problem.” As the objective of the study is to carry out a comparative safety risk analysis of the system being developed and the existing one, a detailed analysis of cyber-risks influencing safety is not necessarily needed. The analysis may be limited to screening the risks and attributing subjective scores to a representative sample of the risks identified by experts.

The degree of detail should become clearer after the mapping of the system on one of the system representations (feedback loop or multi-layered CPS diagram) and identifying a gross list of risks. Usually, the depth of risk analyses is determined either by the availability of failure data for the components of the lowest level, or the need to identify the most efficient means of system protection and failure prevention.

A consensus should be achieved between risk analysts and designers of the system, incl., software developers. Constraints on resources needed for the analysis may become a decisive factor in choosing the degree of detail.

5. Integrated framework for risk identification

To make the human error analysis an integral and consistent part of the system’s safety analysis, using a HAZOP-like method for identifying risks and failures attributed to different functions of the system being designed would be appropriate. The reason for practicing a HAZOP-like method is that it is applicable for both human error identification and other technology-related failures (hardware, software, information flows, etc.)

The basis for the analysis is a pictorial system model (system representation) that in our case can either be a control loop (Figure 2 and 3) or the CPS master diagram (Figure 4). To make any HAZOP-like method work, a checklist of deviations is needed, and this should preferably be well-formed and rooted in post-incident and predictive analyses. If the control loop representation is chosen, deviations of a higher level are listed in Figure 3 and Appendix I. As information flows between entities of a CPS can be of two types (signals and messages), the checklists can be extended to capture the specifics of the two. An example is given in Table 4. Deviations provided in this table are applicable to information flows depicted on the both representations of CPSs.

Table 4. Generic failure modes for information flows between entities in a CPS

Aspect	**Signals deviation**	**Messages deviation**
Content	High value	Parameter high
	Low value	Parameter low
	Out of range	Value conflict
	No signal	No msgs
		Repetitive msg
		Wrong msg
	Noisy signal	Corrupted msg
Timing	Premature start	Too early
	Late start	Too late
	Too short	Too long msg
	Too long	Too short msg
Continuity	Sporadic	Incomplete msg. stream
Stability	Drift high	Interrupted
	Drift low	
	Cycling	Channel overload
	Hunting	
Routing	Wrong connection Cross connection	Wrong address Unwanted broadcast
Validity	Spurious signal	Spurious msg

Given the CPS is presented by a diagram based on the CPS' multi-layered pictorial model (Figure 4), the hazard identification analysis should be carried out for all five "subsystems" of the overall system: cyber-layer, cyber-physical layer, physical layer, cyber environment, and physical environment.

As mentioned in the previous section, a consensus on the depth of the analysis should be achieved between risk analysts and subject matter experts. While a deep analysis is a feasible option, it may appear unnecessary to carry out to fulfil the objectives of the study.

The available comprehensive checklist of cyber threats that can propagate to physical risks in CPSs is published in [19] and can be alternatively accessed directly https://orbit.dtu.dk/en/projects/cyphass-prototype-cyber-physical-harm-analysis-for-safety-and-sec .

Not all threats and hazards can be predicted or reasonably anticipated. Experience in conducting risk analyses indicates that the application of several threat and hazard identification methods results in a greater number of identified risks. However, the decisive constraint is the availability of

resources for carrying out analyses rooted in different methods. For example, a HAZOP analysis can be complemented by a Failure Mode and Effect Analysis (FMEA), What-If, structured brainstorming, or some other.

6. Safety risk evaluation

On a general note, the debate on how to evaluate risks focuses on three major strategies [17]:

1. Risk-based approaches;
2. Decisions derived from the application of the precautionary principle;
3. Standards derived from discursive processes such as roundtables, deliberative rule making, mediation, or citizen panels.

Strategy 3 is not an option for the considered system, as there is no value ambiguity for the improved system.

The other two strategies, 1 and 2, are the candidates to be considered for the application. The FSA Guidelines [1] require the application of risk-based approaches to safety analysis. Strategy 2 does not contradict this requirement, as implicitly, it is also based on a risk-based approach that recognises the significance of uncertainties in risk estimates. Proper consideration and influence of uncertainties on the results of the analyses are particularly stressed in [1].

Among risk acceptance criteria the following two, which use as input the results of risk-based approaches, can be applicable: the **GAMAB** and **risk-benefit** principles.

Figure 5 is a decision tree that guides the application of one of the three principles of decision-making on the acceptance of the system being developed: the precautionary, GAMAB, and risk-benefit principles. Which principle to apply to the case in consideration will become clear during the course of the study evolvement.

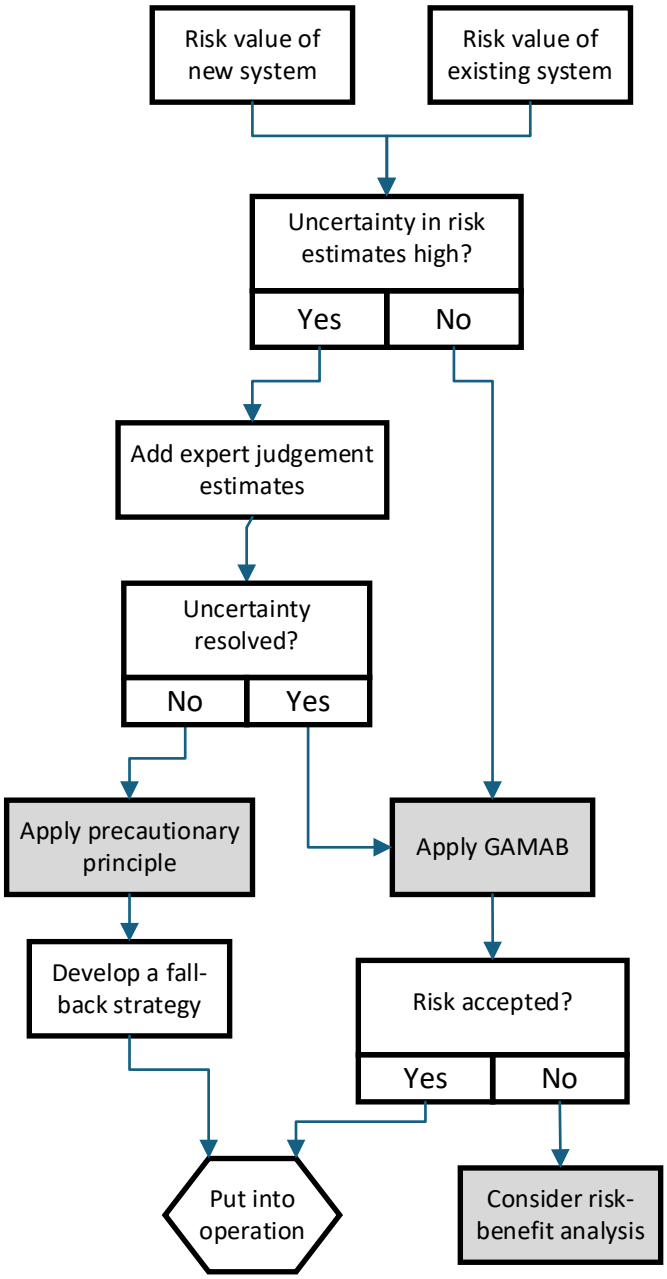


Figure 5. Risk acceptance approach for the MISSION JIT arrival system

7. Summary

As stated in the introductory part of this document, this is an informational document that communicates the account of SDU participants of the MISSION project. The methods described are compliant with the Guidelines for Formal Safety Assessment (FSA) [1] and The Ship Inspection Report Programme (SIRE) [2].

The cornerstone and the point of departure for scoping the current study on safety analysis is the recognition that the system being developed by the MISSION consortium is a *Cyber-Physical System*

(CPS). This implies that methods specially tailored to the analysis of the systems of this class should be applied.

Two pictorial system models are suggested which (if properly further extended to account for specific features of the system being developed) can be used as a basis for identifying hazards and threats that may propagate into operational and safety issues.

Because of *uncertainties*, which will inevitably convey the completeness of hazards and threats identification and the estimates of risk metrics (both qualitative and quantitative), crisp decision-making on the system acceptability may not necessarily be a justified option. A *precautionary principle* can be a better option to choose as an acceptance criterion. This in turn implies the existence of *fall-back and recovery procedures* that allow bringing the system to a safe state in case it fails to perform as expected.

The importance of accounting for the influence of human factors on safe ship navigation is particularly stressed and an *Action Error Analysis* is suggested as a method to identify unintentional human errors. Accounting for human factors is even more important for CPSs, as there is a greater number of human actors that can impact safety via cyber vulnerabilities.

An integrated approach to analysing the safety of the system being developed is suggested. It integrates the human reliability analysis into the safety analysis.

It is worth noting that it would be appropriate to perform an operational risk analysis of the system being developed, as it is not only safety risks that can result in poor performance of the system.

As a concluding note, no one risk identification method can exhaustively list all threats and hazards that can be attributed to a system. The use of several methods is beneficial for the completeness of risk identification. However, this is very resource-demanding, which is the constraint that is often difficult to overcome.

References

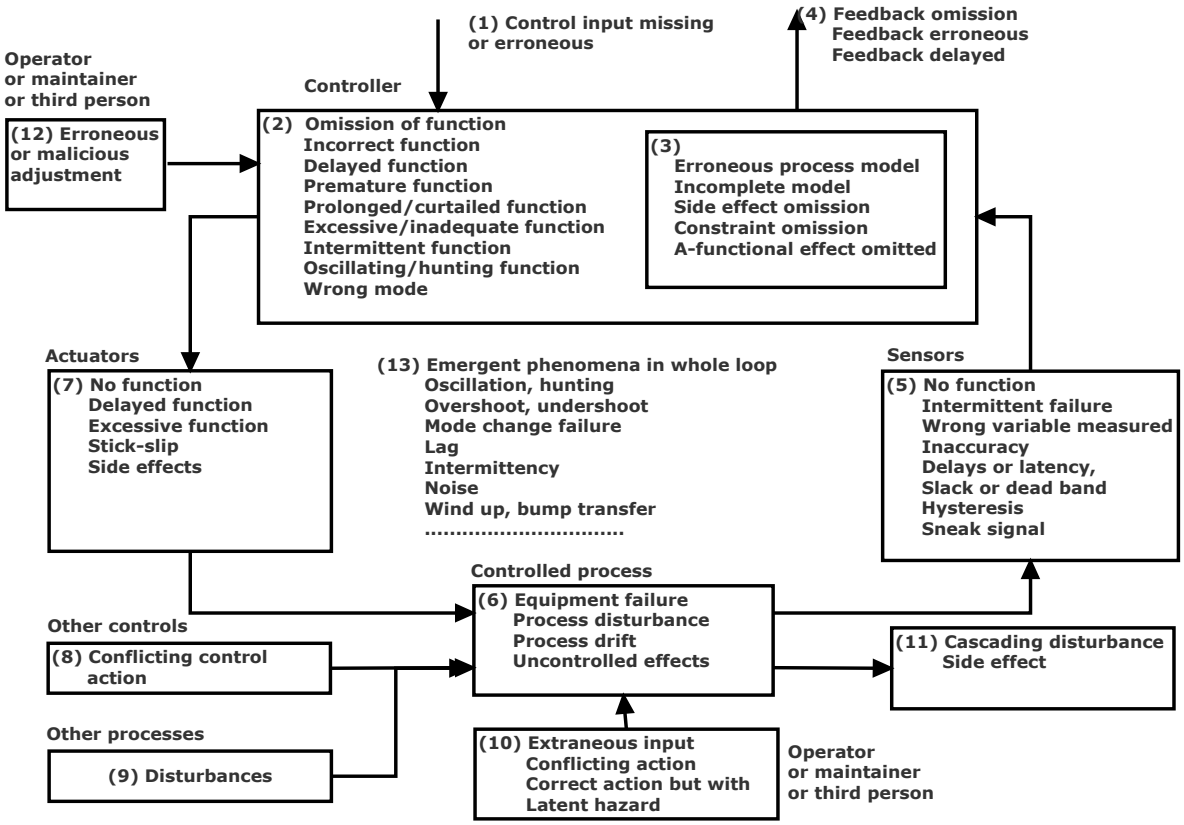
1. FSA: Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process. MSC-MEPC.2/Circ 12/ Rev. 2, 9 April 2018.
2. Simplifying SIRE 2.0 For Ship operators and Seafarers. (2024) MARINE INSIGHT LLP
3. Guzman, N.H.C., Kozine, I., Lundteigen M.A. An integrated safety and security analysis for cyber-physical harm scenarios. *Safety Science 144* (2021), 105458
4. Lee, E.A. Cyber physical systems: design challenges. In: 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing. Washington, DC: IEEE Computer Society; 2008:363-369.
5. Carreras Guzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2019). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, (23), 189–210. https://doi.org/10.1002/sys.21509
6. SAE Standard J3016, Levels of Automated Driving Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104
7. White paper, 2022.AUTONOMOUS SHIPS: TERMS OF REFERENCE FOR RULE DEVELOPMENT. One Sea, Autonomous Maritime Ecosystem

8. Leveson N. Safeware: System Safety and Computers. Boston, MA: Addison-Wesley; 1995
9. Bainbridge, L. Ironies of Automation. Automatica, V. 19-6, pp. 775-779
10. Leveson, N.G., Thomas, J.P. (2018) STPA Handbook.
11. Hahn A, Thomas RK, Lozano I, Cardenas A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. Int J Crit Infrastruct Prot. 2015;11:39-50
12. Orojloo H, Azgomi MA. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. Futur Gener Comput Syst. 2017;67:57-71. https://doi.org/10.1016/j.future.2016.07.016.
13. Taylor, J.R., and Kozine, I. Human Reliability Analysis. Chapter 11 In Practical Reliability Engineering, 6th Edition, Wiley, 2025. In press.
14. HSE. INSPECTORS TOOLKIT: Human factors in the management of major accident hazards. UK Health and Safety Executives (HSE), 2005. https://www.hse.gov.uk/humanfactors/assets/docs/toolkit.pdf Accessed on 20-02-2025
15. Taylor, J.R. (1994) Risk Analysis for Process Plant, Pipelines and Transport. London: E & FN Spon
16. Taylor, J.R. Human Error in Process Plant Design and Operations. A Practitioner's Guide. CRC Press, Taylor & Francis Group, 2016
17. A. Klinke and O. Renn. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis*, Vol. 22, No. 6, 2002
18. Kalculator: BITS Key Risk Measurement Tool for Information Security Operational Risks. BITS Financial Services Roundtable, 2004
19. Carreras Guzman, N. H. Identification of Safety and Security Cascading Risks in Cyber-Physical Systems. PhD Thesis. DTU – NTNU, 2020.

APPENDIX I. Failure modes in a simple control loop

(courtesy J.R. Taylor, unpublished work)

The list of failure modes shown in the figure is based on that of Leveson and Thomas (reference [10] in the list of references) and shows the failure modes for the individual system components. Two extensions have been made for the model analysis. The first is that side effects of disturbances in the loop, and interference from other loops or subsystems have been added. The other is that emergent effects in the loop have been added.



APPENDIX II. Sample inventory of threats

APPROACH TO INFORMATION SECURITY THREAT ANALYSIS

Actor (1): Human*

Access: Network

Actor (2) External

Motive

Deliberate	Accidental
➢ Unauthorized scans ➢ Unauthorized network or system access ➢ DDoS attacks ➢ Web defacements ➢ Malicious code ➢ Worms ➢ Viruses ➢ Trojan horses ➢ Network/application time bomb ➢ Network/application backdoor ➢ Virus hoaxes ➢ Social engineering ➢ Network spoofing ➢ War dialing ➢ Computer crime ➢ Lawsuits/ litigation	➢ Unintentional DDoS attack ➢ Unintentionally bad legislation

Actor (2) Internal

Motive

Deliberate	Accidental
➢ Unauthorized scans ➢ Network/application time bomb ➢ Network/application backdoor ➢ Social engineering ➢ Computer crime	➢ Human error

Access: Physical

Actor (2) External

Motive

Deliberate	Accidental
➢ War ➢ Terrorist attack ➢ Biological agent attack ➢ Bomb threats ➢ Bomb attacks ➢ Robbery ➢ Extortion ➢ Vandalism ➢ Civil disorder ➢ Sabotage ➢ "Dumpster diving"	➢ Automobile crash ➢ Airplane crash ➢ Chemical spill ➢ Radiation contamination ➢ Hazardous waste exposure ➢ Gas leaks

Actor (2) Internal

Motive

Deliberate	Accidental
➢ Work stoppage/ strike ➢ "Tailgating" to gain unauthorized access ➢ Shoulder surfing ➢ Embezzlement ➢ Sabotage	➢ Leaving doors unlocked ➢ Leaving sensitive documents exposed ➢ Leaving computer screen exposed or unlocked ➢ Discussing sensitive matters within earshot of those who don't have a need to know ➢ Lost or stolen laptops

Actor (1): Non-Human

Access: System

Actor (2) External	Actor (2) Internal
➢ Power failure ➢ Power fluctuation ➢ Telecommunications failure ➢ DNS failure	➢ Power failure ➢ Power fluctuation ➢ HVAC failure ➢ CPU malfunction / failure ➢ System software failure ➢ Application software failure ➢ Telecommunications failure ➢ Hardware failure ➢ Software defects

Access: Natural

Actor (2) External	Actor (2) Internal
➢ Floods ➢ Fire ➢ Seismic activity ➢ Volcanic eruption ➢ High winds ➢ Snow/ice storms ➢ Tornados ➢ Hurricane ➢ Epidemic ➢ Tidal wave ➢ Typhoon ➢ Solar flares ➢ Lightning	➢ Floods ➢ Fire ➢ Dust/sand ➢ Heat

***Human actors/threat sources:**

Outsiders, including:

Hacker	Cracker
Computer criminal	Terrorist
Industrial espionage	Customer
Computer user	Vendors/service providers

Insiders/employees, including:

End users	Developers
Database administrators	System administrators
Help desk staff	Security administers
Other personnel	Ex-employees
Disgruntled employees	

Kalculator: BITS (reference [18] in the list of references)