HULL INSURANCE OF AUTONOMOUS SHIPS ACCORDING TO NORDIC LAW– WHAT ARE THE CHALLENGES?

Trine-Lise Wilhelmsen[*]
Hans Jacob Bull[•]

1 INTRODUCTION

The topic of this chapter is the outlining of the challenges arising in relation to the hull insurance of autonomous ships under Nordic law. Nordic hull insurance is regulated by the Nordic Marine Insurance Plan (NP).[1] The concept of "autonomous" ships is defined in the introductory chapter to this book as containing three different elements, or levels, of ship automation: technical capability, manning, and autonomy. The three elements are closely interlinked and interdependent. The concept therefore encompasses a great range of ships, with different levels of technical capability, manning and autonomy.

Insurance means the transfer of risk to an insurance company (the insurer), against payment of a premium based on the insurer's assessment of this risk. Hull insurance covers the risk of loss of, or damage to, the vessel itself, as well as part of the risk of collision liability. By "challenges" in relation to hull insurance, we mean challenges for the parties to the insurance contract, i.e. for the insurer as the company that undertakes to grant insurance,[2] and for the person effecting the insurance[3] or the assured,[4] which in this case is normally the owner of the vessel.

We will in what follows first outline the risk factors tied to autonomous ships, in order to explain the object of the challenge in relation to the hull insurance contract. Thereafter, these risk factors will be analyzed in relation to hull insurance. Based on this, we will first look into the different methods for the insurer to handle the risk factors, and secondly into the extent to which the risk factors are covered and what tools the contract contains for the insurer to handle the risk. Generally, this raises three different types of legal question: to what extent is the risk connected to autonomous ships insured under NP, are there specific uncertainties in relation to this cover, and is there a need for changes in the provisions.

---

[*] Professor, Scandinavian institute of maritime law, University of Oslo
[•] Professor emeritus, Scandinavian institute of maritime law, University of Oslo

[1] The Nordic Marine Insurance Plan of 2013 (NP), Version 2019 available at <http://www.nordicplan.org/The-Plan/>. Reference to NP is to this version.
[2] See the no. 69 *Insurance Contract Act* 1989 [Norway] (ICA) § 1-2 (a), NP Cl. 1-1 (a).
[3] The party who has entered into the contract with the insurer, cf. ICA § 1-2 (b), NP Cl. 1-1 (b).
[4] The party who is entitled to compensation or the sum insured, cf. ICA § 1-2 (c), NP Cl. 1-1 (c).

2 THE RISK FACTORS TIED TO AUTONOMOUS SHIPS - CONCEPTS AND DELIMITATION

The question here is to what extent autonomous ships create new risk factors, compared to traditional shipping. Based on the conceptual framework set out in the introduction to this book, the key difference between traditional ships and autonomous ships is that the onboard machinery processes are automated and depend on systems rather than on manual operation, and/or that onboard manual operations are replaced by remote operations of systems. Further, we understand "automation systems" as referring to hardware consisting of computers and electronic devices and software consisting of all information processed by computer systems, programs and data. Traditional risks tied to the technology of machinery are thus replaced by risks tied to computers, programs, data and information, and the risk of human failure tied to navigational and other onboard tasks is transformed into risk of programming/construction errors that may be made by remote crew. Human errors in relation to onboard automated processes should not create any new challenges, but are included to the extent that it is artificial to distinguish between remote programming errors and such errors where made onboard.

We will therefore concentrate on onboard computer/program failure caused by human errors by remote or onboard crew, including programming errors, and computer/program failure where there is no such error.

An automated system can fail "by itself" because there is a technical error with some part or component of the system, or there can be a functional problem if the system fails to perform in the way it was designed to do. The system may also fail due to damage caused by an exterior cause, for instance fire or explosion. We use the term "system failure" as a common term for all these instances, unless there is a need to distinguish the failure in relation to its cause or to distinguish between the hardware (computer or electronic device) and software (program, data and information).

System failure may result in damage to the system, with the system then needing to be repaired or replaced. System failure may also result in damage to other parts of the ship, for instance the hull or machinery. The damage potential will depend on the type of automation, but in particular it seems that automated navigation carries a special risk. A failure in automated navigation can result in no speed, lower or higher speed than planned or in an altered course. If the ship drifts or sails on a wrong course, the result may be stranding, collision with another vessel or collision with installations in the port that is the ship's place of departure or destination. Collision may also be the result of a system that fails to recognize other vessels on a collision course with "our" vessel.

In addition to system failure, the system may be attacked or hacked by an outsider in order to use a virus program, or to manipulate or steal data and information. Such an attack will

normally have a malicious intent, but the purpose of the attack may vary. It may be a question of disruption of the system solely through loss of data and information, or it may be a question of disrupting the system in order to gain knowledge (industrial espionage), or using disruption as blackmail, or entering the system in order to capture the ship or cargo. This last scenario could be a matter of piracy or terrorism or be carried out by a foreign state.

3 AUTONOMOUS SHIPS AND THE REGULATION OF HULL INSURANCE

As a general rule, the Nordic Insurance Contract Acts contain few, if any, rules on marine insurance. Nordic hull insurance is instead regulated by the NP,[5] which is an agreed document that may in many ways be compared to private legislation.[6] This is a comprehensive set of provisions that covers the most commonly used types of marine insurance, apart from P&I insurance, and that also regulates such general issues as are regulated by the Nordic Insurance Contract Acts for non-marine insurance. The NP is a general set of provisions that is used by all the Nordic insurance companies, and also used by insurance companies in other countries.

Hull insurance mainly provides cover for loss of or damage to the vessel.[7] The insurance covers i.a. the vessel (hull and machinery) and "equipment".[8] The term "equipment" is defined in the Commentary as:[9]

> "a collective term for loose objects that accompany the ship in its trade, but which cannot be deemed to be part of it, e.g. radio and radar equipment, search lights, loose shifting beams, furniture and other fixtures and fittings. The prerequisite for covering equipment and spare parts under the ship's hull insurance is nevertheless that they are normally on board, cf. the term "on board", which indicates that the object in question shall be on board for an indefinite or prolonged period of time."

This must include onboard computers and electronic devices. It is more unclear to what extent "equipment" defined as a "loose object" includes programs, information and data. The term "object" seems to presume something "physical", and there is no specific reference to programs, data or information. However, the similar provision for hull insurance for Mobile

---

5 The NP is based on the previous Norwegian Marine Insurance Plan 1996, Version 2010 (NMIP). The NMIP 1996 was based on the previous NMIP 1964 and earlier similar agreed plans from i.a. 1930 and 1907.

6 See further T.-L. Wilhelmsen and H.J. Bull *Handbook on Hull Insurance* 2nd ed. (Gyldendal Juridisk, Oslo, 2017) 26 ff.

7 NP ch. 11-12.

8 NP Cl. 10-1 sub-clause 1 (a) and (b).

9 Commentary on the Nordic Marine Insurance Plan of 2013 (Commentary) – Version 2019 available at <http://www.nordicplan.org/Documents/Nordic%20Plan%202013/Commentary%20to%20the%20Nordic%20Marine%20Insurance%20Plan%20of%202013%20-%20Version%202019.pdf> at 252.

Offshore Units contains a specific exclusion in the cover for "blueprints, plans, specifications, logs, etc",[10] and the Commentary[11] on that point states that:

> The exclusion covers various documents and records which may be of considerable value (in particular the logs kept of drilling operations may contain very valuable information about the geological structure of the seabed and accordingly concerning the probability of finding petroleum in the area. The reason why the documents are nevertheless excluded from cover is partly difficulties in agreeing on their value in terms of money, partly the possibility which the interested parties have of continuously transmitting important data to shore. Much of the logs and data which used to be paper documents are now kept as digitally stored data. The exclusion is equally applicable to such digitally stored data/information; however, the hardware on which such data/information is stored on, including the software, is nevertheless covered but only for the cost of replacement. Costs or recovering digital data/information will thus not be recoverable under the insurance.

The Commentary here makes a distinction between "data/information" and "software", where the latter seems to be covered as part of the "hardware". The concept of "software" must then mean the programs. This is different from the definition of "software" used in this chapter, but in the context of hull insurance according to the NP, this implies that cover for hardware in the form of computers includes cover for software in the form of programs. Even if a program is, in itself, not a physical object, the cover for this can be explained by the fact that it is difficult to distinguish the program from the computer. On the other hand, it is not natural to characterize digital data and information as "objects" and this is therefore probably not covered according to Cl. 10-1, even if there is no specific exclusion. This is supported by the fact that hull insurance is a casualty insurance covering loss of or damage to objects, which does not include digitally stored data and information. Loss of data and information must thus be insured by a separate insurance.

Hull insurance is divided between ordinary hull insurance and hull interest insurance. The ordinary hull insurance covers both damage[12] to the vessel and total loss[13] of the vessel. Hull interest insurance only covers the risk for total loss.[14] Ordinary hull insurance is therefore the relevant insurance, in the case of damage to the computer/hardware and programs and if system failure or loss of data or information results in damage to the vessel. If the damage is so serious that it may lead to condemnation, or if disturbance of the system results in total loss of the vessel, the relevant insurances are hull and hull interest insurance.

By tradition, hull insurance also provides cover for one type of liability, namely liability for collision and striking.[15] However, the liability is limited by an extensive list of exclusions.[16]

---

10 NP Cl. 18-2 sub clause 2 (c).
11 Commentary, note 9 at 448.
12 NP ch. 12.
13 NP ch. 11.
14 NP Cl. 14-1. The system is explained in Wilhelmsen/Bull, note 6 at 378-379.
15 NP ch. 13.
16 NP Cl. 13-1 sub-clause 2 (a) – (j).

Also, this risk is, as a starting point, covered for an amount similar to the sum insured under hull insurance.[17] If the liability exceeds this amount, the hull interest insurance will cover the resultant liability within the sum insured under hull interest insurance.[18] Any amount exceeding this value is covered by P&I insurance.

If risk factors tied to autonomous vessels result in the vessel colliding with another vessel, the relevant insurance is, as a starting point, hull insurance as regulated by the NP, but if the liability amount is high, hull interest insurance and P&I insurance may also be triggered.

4 THE RISK FACTORS AND THE INSURER'S ASSESSMENT OF THE RISK

4.1 Methods for managing the risk

As mentioned, insurance means transfer of risk against a premium. The insurer must decide how to handle different types of risk factors when he decides whether he wants to insure the vessel and upon what terms.

In relation to hull insurance for ships, there is no duty to insure for the assured and no duty to contract for the insurer. The insurer is therefore free to refuse to effect hull insurance for autonomous vessels. However, this is an unnecessary and not very appropriate approach. It is the particular aspects of autonomous vessels that give rise to certain risk factors, rather than the vessels as such. Risk factors may be managed through the calculation of the premium, division of economic risk or different types of exclusions in the contract.

If the risk is extensive, an obvious method is to charge a higher premium than normal. The problem with this method today is the lack of statistics. The insurance premium is normally based on historical casualty records broken down into different types of risks, and as the concept of autonomous vessels is a new technical development, such statistics may not exist. This means that the risk assessment must be based on more subjective methods, depending on the insurer's attitude towards new types of risk. As a general starting-point, the insurer will protect themselves against uncertainty with higher premiums.

An alternative method is risk sharing through the use of deductibles. A high deductible tied to each casualty will both reduce the insurer's risk for the casualty and presumably also have a deterrent effect.[19] However, when the premium reduction for a raise in the deductible is to be calculated, the insurer meets the same problem as when the premium is to be calculated. In

---

17 NP Cl. 13-3.
18 NP Cl. 14-1 (b).
19 See further T.-L. Wilhelmsen "Deductibles as self insurance" (2011) *SIMPLY 2011* 157-193.

order to define a price for each level of deductible, the insurer needs historical records of previous casualties, which may not exist. But there again, a higher deductible may constitute a protection against uncertainty in the calculation of the premium.

If pricing of the autonomous risk factors is difficult, an alternative method is to manage this risk through exclusions in the marine insurance contract. This can be done either through exclusions directly aimed at system failure or cyber attack, or by providing the assured with special duties in relation to this risk. This is further discussed in the section below: "The NP - cover of autonomous risk factors and tools for risk management".

4.2 The significance of the reinsurance market

Reinsurance means that the direct insurer who has concluded an insurance contract, for example for the owner of a ship, then insures a portion of this risk with another insurer, the reinsurer.[20] Reinsurance as a commodity may be compared to liability insurance for the insurer, but is not regulated by the NP, and also falls outside the scope of the Insurance Contract Act.[21] The reinsurance market is highly international and based on agreements between the insurer as reinsured and the reinsurer. There is no contractual relationship between the assured under the direct insurance contract and the reinsurer.

Due to the high risks in marine insurance, the hull risk insurer is dependent on reinsurance. Even if the reinsurer normally accepts the insurance contracts as being agreed between the insurer and the assured, the reinsurance market may decide to refuse certain types of risk. The most illustrative examples of this over recent years are the requirements from the reinsurance market that the direct insurance contracts should insert the millennium clause in 1999 and the RACE II clause in 2003. Because of this pressure, the Norwegian Marine Insurance Plan 1996 (NMIP) Version 1999 included the millennium clause as a safety regulation to secure against the risk connected to "Failure to recognize the millenium date change".[22] It was removed in Version 2002 when the reinsurers no longer insisted on this clause. The RACE II clause was included in the NMIP Version 2007 as a response to i.a. the terrorist attack in New York in 2001, and excludes nuclear, biological and bio-chemical risks.[23] This clause is still included in the NP.[24]

---

20 Cf. Wilhelmsen, Bull, note 6 at 43-44.

21 No. 69 *Norwegian Insurance Contract Act* 1989 [Norway] § 1-1 sub paragraph 4.

22 The Norwegian Marine Insurance Plan of 1996, Version 1999 available at <http://www.nordicplan.org/Documents/Archive/Plan%201999/Norwegian%20Plan%20of%201996,%20Version%201999%20-%20English.pdf>, cf. § 3-24A.

23 The Norwegian Marine Insurance Plan of 1996, Version 2007 available at <http://www.nordicplan.org/Documents/Archive/Plan-2007/Norwegian%20Plan%20of%201996,%20Version%202007%20-%20English.pdf>, cf. § 2-8 (d) and § 2-9 sub-clause 2 (b).

24 NP Cl. 2-8 (e) and Cl. 2-9 sub-clause 2 (b).

It should be noted that at the same time as the reinsurance market introduced the RACE II clause in 2003, it also introduced the Institute Cyber Attack Exclusion Clause – Clause 380, with the following wording:

> "1.1Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
>
> 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile."

However, this clause was not included in the Plan, nor in the revision of 2007 or later, and was not discussed in the 2019 revision. The clause is included in some Nordic reinsurance contracts, but not all. Nevertheless, even without this exclusion in the reinsurance contract, the insurers often include this clause in the direct policies as a special clause, cf. below.

The direct insurers may also have excess of loss reinsurance, which means that the reinsurer is liable for losses that exceed an agreed (aggregated) amount. Such insurance may contain exclusions for Information Hazard,[25] but these clauses are apparently not used in the Nordic direct insurance marked.

5 THE NP - COVER OF AUTONOMOUS RISK FACTORS AND TOOLS FOR RISK MANAGEMENT

5.1 Introduction and overview

The purpose here is to outline some clauses that seem to be particularly relevant for insurance of autonomous risk factors, in order to see to what extent this risk is covered today and how the clauses may be used by insurers to manage this risk. The autonomous risk factors are, as mentioned, the risks connected to both automation systems (including computers, programs, data and information) and remote crew.

Two sets of provisions may be particularly relevant in relation to these risks. The first set is the regulation of the scope of cover. The second set is the regulation of duty of disclosure and due care.

---

[25] Cf. for instance the Information Technology Hazards Clause that was introduced in October 2017 in Joint Excess Loss Clauses (JELC) CL 432 for use in marine reinsurance contracts and XL2001/003 16/11/01, which appears to be used by Nordic marine insurers.

The expression "scope of cover" refers to four closely linked questions.[26] The first question is the defining of the perils covered under marine insurance, or the types of risk the assured is insured against. The second question is the defining of the "casualty", or the "insured event" through which the covered peril must materialize in order to trigger the insurer's liability. The third question is determining the type of loss that is covered. The fourth question is establishing what kind of connection is required between the peril insured against and the casualty, as well as between the casualty and the loss the insurer is liable for. This is the question of causation.

Within this framework, the main issue for autonomous vessels is the question of what perils are covered, i.e. in particular if there is cover for system failure and cyber-attack. The main provisions concerning perils being insured against are NP Cl. 2-8 and Cl. 2-9. Added to this, there are some provisions that may be relevant in relation to damage to the computer or the program itself, cf. Cl. 12-3 and Cl. 12-4. These provisions are addressed in the section on perils insured against.

The other set of provisions concerns rules on duty of disclosure and due care.[27] Whereas the rules on scope of cover regulate objective circumstances, i.e. circumstances where the acts or omissions of the assured have no influence, the rules on duty of disclosure and due care concern duties of the assured and the person effecting the insurance, and the consequences of a breach of these duties. Contrary to the objective scope of cover, the issue here is how the acts or omissions of the assured or of the person effecting the insurance, or of persons that may be identified with these, influence the right to compensation.

The duties of disclosure and due care concern two different situations: firstly, when the insurance contract is negotiated, and secondly, during the period when the insurance is running. The duty of disclosure is connected to the negotiations of the contract, whereas the rules of due care apply to the insurance period. The latter group may be divided into four sets of rules: rules concerning alteration of risk, safety regulations, duty of notification and to avert or minimize loss, and casualties caused negligently or intentionally by the assured. As a starting point, all these provisions may be relevant with regard to autonomous vessels, but we think the rules on duty of disclosure, safety regulations and casualties caused by gross negligence are the most important and we will therefore concentrate on these. However, it also seems necessary to provide some remarks on identification. All of these issues are discussed below, under the section on duty of disclosure and due care.

5.2 Perils insured against

5.2.1 The main regulation in NP Cl. 2-8 and Cl. 2-9

---

[26] Cf. Wilhelmsen/Bull, note 6 at 78.
[27] Cf. Wilhelmsen/Bull, note 6 at 146-148.

The regulation of perils insured against in the NP is divided between marine risks and war risks. The specific perils under an insurance against marine risks are defined in NP Cl. 2-8:

> **Clause 2-8. Perils covered by an insurance against marine perils**
> An insurance against marine perils covers all perils to which the interest may be exposed, with the exception of:
> (a) perils covered by an insurance against war perils in accordance with Cl. 2-9,
> (b) capture at sea, confiscation, expropriation and other similar interventions by own State power provided any such intervention is made for the furtherance of an overriding national political objective. Own State power is understood to mean the State power in the vessel's State of registration or in the State where the major ownership interests are located. Own State power does not include individuals or organisations exercising supranational authority,
> (c) requisition by State power,
> (d) insolvency or lack of liquidity of the assured or the operation of ordinary legal process to enforce payment of any fine, penalty, debt or right to security unrelated to a claim or liability covered by the insurance,
> (e) perils covered by the RACE II Clause:
> (1) onising radiations from or contamination by radioactivity from any nuclear fuel or from any waste or from the combustion of nuclear fuel,
> (2) the radioactive, toxic, explosive or other hazardous or contaminating properties of any nuclear installation, reactor or other nuclear assembly or nuclear component thereof,
> (3) any weapon or device employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter,
> (4) the radioactive, toxic, explosive or other hazardous or contaminating properties of any radioactive matter. The exclusion in this sub-clause does not extend to radioactive isotopes, other than nuclear fuel, when such isotopes are being prepared, carried, stored, or used for commercial, agricultural, medical, scientific or other similar peaceful purposes.
> (5) any chemical, biological, bio-chemical, or electromagnetic weapon.

It follows from the introduction to the clause that it is based on an all risks principle, meaning that the insurance covers all risks that are not specifically excluded.[28] The starting point is therefore that any risk in connection with automation systems or remote crew is insured under an insurance against marine perils. This will include programming, for instance in relation to navigation, both onboard and under remote operation. The marine risk insurance also covers cyber-attack and the use of virus programs, for instance in order to blackmail the owner. However, if such an attack constitutes a war peril, this will be excluded according to sub-clause (a).The other exclusions appear to be less relevant.

The cover for system failure and cyber-attack, including virus programs in the NP, means that if the insurer wishes to exclude these risk factors, he must insert an exclusion. This can be done either on a general basis following the revision procedures in the Nordic Plan Agreement,[29] or else through individual negotiations during renewals of the insurance. Two

---

[28] Cf. further Wilhelmsen/Bull, note 6 at 79-81.

[29] Cf. the Nordic Plan Agreement available at <https://cefor.no/globalassets/documents/clauses/nordic-plan/agreement-nordic-plan-03-11-2010---amended-09-12-2016.pdf>.

Nordic insurers inform us that they normally include Cl. 380, as referred to above, but that they may offer special solutions in such cases. In particular, the Norwegian Hull Club offers a "buy back" insurance covering the perils excluded by Cl. 380.[30] To avoid the problem of cumulative damages, such insurance is effected with a common yearly sum insured for all assureds. If the assured wants to buy back Cl. 380, he will be requested to cooperate with the insurer to lift the level of "cyber awareness".[31]

The Norwegian War Risk Association, which is a mutual insurance company that effects war risk insurance for most of the Norwegian fleet, offers in addition a limited cover for damage caused by "marine" cyber-risk, to the extent such risk is excluded from the marine cover:[32]

> This ALC Marine Cyber Attack covers total loss (including hull interest/freight interest) and physical damage directly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or computer process or any other electronic system.

Insurance against war risks is regulated in Cl. 2-9:

> **Clause 2-9. Perils covered by an insurance against war perils**
> An insurance against war perils covers:
> (a) war or war-like conditions, including civil war or the use of arms or other implements of war in the course of military exercises in peacetime or in guarding against infringements of neutrality,
> (b) capture at sea, confiscation, expropriation and other similar interventions by a foreign State power, provided any such intervention is made for the furtherance of an overriding national or supranational political objective. Foreign State power is understood to mean any State power other than own State power as defined in Cl. 2-8 (b), second sentence, as well as organisations and individuals exercising supranational authority or who unlawfully purport to exercise public or supranational authority,
> (c) riots, sabotage, acts of terrorism or other social, religious or politically motivated use of violence or threats of the use of violence, strikes or lockouts,
> (d) piracy and mutiny,
> (e) measures taken by a State power to avert or limit damage, provided that the risk of such damage is caused by a peril referred to in sub-clause 1 (a) - (d).
>
> The insurance does not cover:
> […]

This insurance is based on the named perils principle and thus only covers the perils that are listed in Cl. 2-9. System failure or cyber-attack are not listed as covered perils, and are thus not covered as such. Further, it does not seem very probable that technical or functional

---

30 Cyber – Clause 380 buy-back available at <https://www.norclub.com/products/special-risks/cyber-clause-380-buy-back-/>.

31 Cyber – Clause 380 buy-back available at <https://www.norclub.com/products/special-risks/cyber-clause-380-buy-back-/>.

32 Den norske krigsforsikring for skib – (The Norwegian Shipowners' Mutual War Risks Insurance Association), Conditions of 1 January 2019, Cl. 15.1.

system failure or programming errors will be used with malicious intent. A cyber-attack or hacking can however manifest themselves through a war peril, which is listed. Examples are if pirates, terrorists, saboteurs or foreign states use cyber-attack, such as virus programs, to destroy the vessel, blackmail the owner for money or capture the vessel. A cyber-attack as part of piracy, sabotage or terrorism must be considered part of the act of piracy, sabotage or terrorism, and must thus be covered as a war peril. The same appears to be true if a foreign state attacks the system to maneuver the vessel into its own territory, in order to capture it. If the insurer wants to avoid this risk, an exclusion is necessary.

The Norwegian War Risk Association effects war risk insurance without exclusions for cyber-attack. The practice among the other Nordic war risk insurers appear to be that they use Cl. 380 in a similar manner to its use for marine risk cover.

5.2.2 Exclusions for damage to the computer or program itself?

Even if the risks in connection with automation processes and remote operations are covered, there may be exclusions for damage to either the computer or the program itself. Two provisions may be relevant. The first is the exclusion for inadequate maintenance etc. in Cl. 12-3:

> **Clause 12-3. Inadequate maintenance, etc.**
> The insurer is not liable for costs incurred in renewing or repairing a part or parts of the hull, machinery or equipment which were in a defective condition as a result of wear and tear, corrosion, rot, inadequate maintenance and the like.

It should be noted that this exclusion only applies to the "part" of the "machinery or equipment" that was in a defective condition. If the provision is applicable to computer or program failure, any consequential damage to the vessel is therefore covered.

As already mentioned, it is clear that computers and electronic devices must be considered as equipment, and the same appears to be true for programs (but not data and information). The question then is whether the perils of "wear and tear, corrosion, rot, inadequate maintenance and the like" are relevant in this context. It may be argued that the updating of programs can be seen as "maintenance", and it may also be the case that other requirements tied to the programs can be seen in the same way. If so, damage to the computer and/or program that is defective will not be covered, but any consequential damage to other parts of the ship will be.

The other provision is Cl. 12-4 on error in design etc.:

> **Clause 12-4. Error in design, etc.**
> If the damage is a result of error in design or faulty material, the insurer is not liable for the costs of renewing or repairing the part or parts of the hull, machinery or equipment which were not in proper condition, unless the part or parts in question had been approved by the classification society.

The structure of this provision is the same as for Cl. 12-3; the exclusion applies only to the part that is not in proper condition. Further, if the part in question is approved by the classification society, the exclusion does not apply.

The concept of design is defined in the Commentary 2019 as referring to:[33]

> [T]he entire process of defining how the various parts of the vessel should be configured and assembled, how they should be manufactured and the exact nature and quality of the material to be used. Any defect arising as a consequence of any of these matters must be regarded as an error in design.

The concept of "error in design" refers to a failure in any of these processes, but does not say anything about what the design is to be compared to in order to establish that there is a "failure". It appears from the Commentary that "failure" cannot be given a clear definition, but instead depends on a concrete evaluation in each case, based on certain criteria. The discussion in the Commentary is summarized in Wilhelmsen/Bull as follows:[34]

> The concept of «error in design» is further developed in the Commentary p. 285 ff. It follows from these elaborations that the concept cannot be given a simple definition, but rather is based on a total evaluation of several circumstances. These circumstances may be divided into six different considerations: whether or not the defective part should be changed if the defect was discovered before the loss occurred; the degree of seriousness of the defect; whether the defect was unforeseeable; how much time it took before the defect materialized into damage; whether the defect developed over time or occurred suddenly; and whether the defect must be considered a business risk taken by the assured. These considerations are closely connected and have a certain degree of overlap.

From this, it appears that if the computer and/or program fails because it does not function as it was meant to function, there may be an error in design. It should be noted that malfunctioning is, in itself, not sufficient to trigger the insurance. What the insurer covers, according to the wording, is "damage". Damage caused by malfunctioning that constitutes error in design will therefore be covered, to the extent that the device and/or program is approved by the classification society. This includes the part that is defective and any consequential damage, but only the costs to repair damage. The costs needed to rectify the error in design are not covered.

5.3 Duty of disclosure and due care

5.3.1 Duty of disclosure

According to NP Cl. 3-1, the person effecting the insurance has a duty to disclose "all circumstances that are material to the insurer when deciding whether and on what conditions

---

33 Commentary, note 9 at 295.

34 Wilhelmsen/Bull, note 6 at 301. The reference is to the Commentary to the 2016 Version, but the text is not amended in the 2019 Version.

he is prepared to accept the insurance". As a starting point, it may be argued that the level of automation and remote crew are material for the insurer. However, the duty of disclosure must be seen in conjunction with several other provisions. First, there is a general condition in the NP Cl. 3-14 that the ship is classed in a classification society approved by the insurer. It must therefore be presumed that the level of automation or remote crew is approved by the classification society and thus within the generally accepted standards. In such cases, the relevance of the rules of duty of disclosure seems to be limited. Second, if the insurer knows about the level of automation and remote crew before the insurance is effected, he may not invoke a breach of the duty of disclosure.[35] It should also be noted that the insurer has a right to obtain particulars from the vessel's classification society.[36] If the risk factors are easily accessible through the Veritas Shipping Register or similar registers, or generally known in the shipping community, there is little room for a duty of disclosure concerning these circumstances.[37] For the ship-owner, this means that he is protected against casualties caused by system-failure, cyber-attack or programming/construction errors made onboard or by remote operation, regardless of not having informed the insurer about the level of automation or remote crew, if this is approved by the class and/or known within the shipping community.

5.3.2 Safety regulations

Safety regulations in the context of marine insurance mean that the assured has to comply with certain requirements aimed at reducing the risk for a casualty. Safety regulations are regulated by NP Cl. 3-22 to Cl. 3-28. Cl. 3-22 sub-clause 1 reads as follows:

> **Clause 3-22. Safety regulations**
> A safety regulation is a rule concerning measures for the prevention of loss, issued by public authorities, stipulated in the insurance contract, prescribed by the insurer pursuant to the insurance contract, or issued by the classification society.

If the assured negligently breaches a safety regulation and the breach results in a casualty, the insurer is free from liability.[38]

It follows from Cl. 3-22 that rules concerning measures for the prevention of loss issued by public authorities or by the classification society qualify as a safety regulation according to the NP. Even if the IMO Conventions[39] relevant for autonomous vessels are not directly binding for the ship-owners, these conventions are implemented within Nordic legislation

---

35 NP Cl. 3-5 first sentence.
36 NP Cl. 3-7.
37 Wilhelmsen, Bull, note 6 at 153.
38 NP Cl. 3-25, see further Wilhelmsen/Bull, note 6 at 195 ff.
39 See International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 7 July 1978, UNTS 1361 2, 1362 2 (STCW), Convention on the International Regulations for Preventing Collisions at Sea of 20 October 1972, UNTS 1050 16 (COLREGs), and the International Convention for the Safety of Life at Sea of 1 November 1974, as regularly amended, UNTS 1184, 1185 2 (SOLAS).

through the Nordic Ship Safety Acts. For instance, the Norwegian Ship Safety Act § 6[40] states that the owner has a duty to control the captain and others onboard following the rules, and also contain provisions with requirements to personnel onboard.[41] This means that the assured has to comply with any such regulations on the level of automation or remote crew, if they concern loss prevention.

The question has been raised of whether loss of navigational data may render the ship unseaworthy. Seaworthiness as a concept is not used in the NP, and the question is therefore whether loss of such data constitutes breach of a safety regulation. The relevant provision is the Ship Safety Act § 14, which states that:

> The navigation of the ship shall not result in risk for life, health, environment or material values.

If loss of data means that the navigation of the ship results in such risk, this will be a breach of a safety regulation. It may therefore be argued that the assured must secure the navigational data needed for safe navigation, or at least organize help if such data is lost.

NP Cl. 3-22 does not require that the sole purpose of the regulation is to prevent loss. If the regulation pursues several purposes, it will suffice if one of these purposes is to prevent casualties or mitigate their effect.[42] As most rules on these issues will have an effect on the risk for a casualty, it must be presumed that such rules are relevant in this context. Loss caused by a breach of the internationally accepted framework for ship safety will thus normally not be covered. Further, if the international/national safety regimes create difficulties for automation and the use of remote crew, the same difficulties will transfer to the insurance through the safety regulations. However, this challenge is created by the public rules, and not by the insurance conditions.

According to Cl. 3-22, a safety regulation may also be stipulated in the insurance contract. The reference to the contract includes both the special safety regulation in the NP itself and in the individual policy. There is no such regulation in the NP today. If the insurers find that the regulation by public authorities or the classification society is insufficient to protect against the risk caused by automation or remote crew, they may want to make special regulations in the NP.[43] Examples in our context would be requirements of systems to compensate for lack of human crew onboard, back up routines for securing data, and measures to protect against virus programs. Similarly to what is stated for Cl. 2-8, such safety regulations can be required in a general plan revision or during the individual negotiations for each vessel and inserted into the policy.

---

40 No. 9 *Ship Safety Act* 2007 [Norway] (Norwegian Ship Safety Act).
41 Norwegian Ship Safety Act §§ 15-20.
42 Wilhelmsen/Bull, note 6 at 187.
43 See as examples today Cl. 3-22 sub-clause 2 and 3 and previously NMIP 1996, Version 1999 § 3-24A.

5.3.3 Gross Negligence

If a casualty is caused by acts or omissions by the assured, but there is no breach of safety regulations, an alternative for the insurer is to invoke the ordinary rules on gross negligence in NP Cl. 3-33:

> **Clause 3-33. Gross negligence**
> If the assured has brought about the casualty through gross negligence, any liability of the insurer shall be determined based on the degree of fault and circumstances generally.

This provision may be relevant if the cause of the casualty is, for instance, a programming error in regard to navigation or failure to prevent a covered cyber-attack in the form of a computer virus, which does not constitute breach of a safety regulation. It should be noted that the insurer may not invoke ordinary negligence. And even in the case of gross negligence, there is no automatic freedom from liability.

5.3.4 Identification

The rules on safety regulation and gross negligence are directed at the "assured", who is the person entitled to compensation after a casualty.[44] This will normally be the ship-owner. The more detailed definition of the assured in relation to who acts on behalf of the company will depend on company law.[45] Added to this, the NP also contains rules on identification, i.e. to what extent the assured can be identified with other organizations or persons. The relevant rule in our context is the regulation of identification of the assured with his servants in Cl. 3-36:

> **Clause 3-36. Identification of the assured with his servants**
> The insurer may not invoke against the assured faults or negligence committed by the vessel's master or crew in connection with their service as seamen.
>
> The insurer may invoke against the assured faults and negligence committed by any organisation or individual to whom the assured has delegated decision-making authority concerning functions of material significance for the insurance, provided that the fault or negligence occurs in connection with the performance of those functions.

The provision makes a distinction between functions that constitute "service as seamen" and other functions of relevance for the insurance contract. The natural starting point is therefore that the expression "service as seamen" in sub-clause 1 must include all performance of functions undertaken by crew onboard the ship, whether the performance concerns ordinary machinery, computers, programming or using digitally stored data, provided the task has the same function onboard as that undertaken by the traditional seaman. If so, identification may not be invoked in case of errors in this respect.

---

44 NP Cl. 1-1 (c).

45 See further Commentary, note 9 at 138-140 and Wilhelmsen/Bull, note 6 at 211.

It is may be less natural to use the words "service as seamen" if the error is made by a remote operator. The result would then be that all such errors must be judged by sub-clause 2, which allows for identification. However, this interpretation seems to be contrary to the functional approach in Cl. 3-36. It seems more correct to follow this functional approach, even if the expression "service as seamen" does not fit well. If so, errors made by a remote operator that has the same functions as a traditional seaman should be judged under sub-clause 1. Examples are errors under remote control of cargo operations or navigation of the vessel. If sub-clause 1 is applied, there would be no basis for identification and the assured is then covered for any casualty occurring as a result of such error.

Aside from this, it may be argued that decisions in regard to levels of automation and remote crew in general concern "functions of material significance for the insurance", and therefore that the assured must be identified with any organization or individual that has decision making authority on such issues, according to sub-clause 2. However, identification may only be invoked against the person having the relevant "authority". Identification may not be claimed against an individual who is merely implementing decisions made by his superiors.[46] Thus, the assured will be identified with a person who is responsible for choosing the program or system or deciding procedures to secure or evaluate the program/system, but not with an employee who installs or operates the system according to instructions given by his superiors.

If the insurer includes special safety regulations in the insurance contract, he may also require a wider degree of identification, according to Cl. 3-25 sub-clause 2:

> If the breach relates to a special safety regulation laid down in the insurance contract, negligence by anyone whose duty it is on behalf of the assured to comply with the regulation or to ensure that it is complied with shall be deemed equivalent to negligence by the assured himself.

6 CONCLUSIONS

It appears to us that the insurance of autonomous ships does not raise many challenges for the parties to a hull insurance contract based on the NP. The insurance covers computers and programs, but probably not data, which must be protected by alternative cover. This is a natural consequence of hull insurance being a casualty insurance covering physical objects. However, in order to avoid uncertainty, this should be clarified. Further, the starting point is that system failure and cyber-attack that is not war related are covered by NP Cl. 2-8, and war risk cover is provided for cyber-attack by pirates, saboteurs, terrorists or foreign states. Some insurers use the cyber-attack exclusion in Cl. 380, but it is possible to buy back this exclusion and the Norwegian War Risk Association provides full war risk cover for cyber-attack, as well as a limited cover for marine cyber-attack. The ship owner must follow the rules on duty

[46] Commentary, note 9 at 143 and Wilhelmsen, Bull, note 6 at 215-216.

of disclosure and due care, but this is no different from insurance of other vessels. It may be that the regulation in the Nordic Ship Safety Acts, similarly to the international regulation, creates an obstacle to the level of automation and remote crew, but that problem is not caused by the insurance conditions. The only immediate problem we can see from the assured's perspective is the need for clarification on how the rules on identification apply to remote crew.

From the perspective of the insurer, the safety regulation regime will provide protection against losses caused by a higher level of automation or remote crew than that allowed by the international conventions and national legislation. If this is not sufficient, the insurer may request the inclusion of special safety regulations in the insurance contract. This regime seems to provide a flexible tool to handle the risks factors connected to autonomous ships. The insurer may also raise the premium or the deductible, but this approach may be difficult if there are no statistics on the casualty risk for autonomous vessels. If the insurer wants to exclude the risk of cyber-attack, the insurer may use Cl. 380. However, as it is possible to effect insurance against this risk in the market, this seems first and foremost to be a question of premium and confidence in the assured's data awareness routines.