Handling export, import and security constraints

Deliverable D2.3 - Version Final – 2021-12-21

Advanced, Efficient and Green Intermodal Systems

http://aegis.autonomous-ship.org/

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement Nº 859992.

Document information

Title	D2.3 Handling export, import and security constraints
Classification	Public

Editors and main contributors	Company
Anne Cecilie Rueness (ACR)	GC
Terje Krogstad (TK)	GC
Gjert Ingar Gjersund (GIG)	GC
Jarl Eirik Korsvik (JEK)	GC
Marianne Hagaseth (MH)	SO
Kay Endre Fjørtoft (KEF)	SO
Odd Erik Mørkrid (OEM)	SO
Kristoffer Kloch (KK)	DFDS
Jan-Jaap Kramer (JJK)	VH
Christina Louise Mayland (CLM)	VH
Kenneth Johanson (KJ)	NCL
Magnus Bakke (MB)	NCL
Peter Bjerg Olesen (PBO)	AAH
Rasmus Hededal (RH)	AAH
Terje Meisler (TM)	TRH

Rev.	Who	Date	Comment
0.1	MH	2021.10.18	Template
0.2	MH	2021.11.24	Added input from all partners.
0.3	MH	2021.12.02	Link to the deliverable sent to VH.
0.4	MH	2021.12.15	Added more on ISPS and Customs clearance related to use cases (Use Case A).
Final	MH	2021.12.21	Final revision to be submitted to EC

This publication has been provided by members of the AEGIS consortium and is intended as input to the discussions on and development of new automated and autonomous waterborne transport systems. The content of the publication has been reviewed by the AEGIS participants but does not necessarily represent the views held or expressed by any individual member of the AEGIS consortium.

While the information contained in the document is believed to be accurate, AEGIS participants make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. None of AEGIS participants, their officers, employees, or agents shall be responsible, liable in negligence, or otherwise howsoever in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing neither of AEGIS participants, their officers, employees or agents shall be liable for any direct, indirect, or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Table of contents

Executive Summary

This deliverable gives an overview of ISPS processes and documents, and also of customs and cargo clearance processes and documents. It is based on questionnaires and workshops held with the project partners. The answers were reported both written and by having tele conferences.

Further, the deliverable describes how the mother and daughter concept may affect the ISPS and customs clearance processes. This is relevant when transhipment is done between the mother and daughter vessels.

For ISPS, we need to distinguish between the case where both vessels and the facility are on the same ISPS-level and the case where all are non-ISPS. In both cases, some extra procedures may be needed. In addition, it is not yet defined how ISPS requirements will be handled for autonomous vessels.

Regarding the customs process for transhipment involving mother and daughter vessels, the conclusion is that there may be a higher risk of delay in the clearance process, since more steps are involved. However, autonomous ships and autonomous operations may also increase the flexibility of when to pick up and deliver the cargo.

The analysis done for Use Case A will also be relevant for Use Case B and C since focus is on transhipment of cargo.

Definitions and abbreviations

API: Application Programming Interface

CCU: Cargo Carrier Unit

COPARN: Container Announcement Message. Typically a pre-arrival message or an order to release an empty container (EDI)

CUSCAR: CUStoms CARgo report message. Details related to the consignee and the cargo inside CCUs (EDI)

DOS: Declaration Of Security

EDI: Electronic Data Interchange

ETA: Estimated Time of Arrival

FAL: Convention on Facilitation of International Maritime Traffic

FTP: File Transfer Protocol

IMO: International Maritime Organization

ISPS: International Ship and Port Facility Security

ISSC: Issuing of the International Ship Security Certificate

MSC: Maritime Safety Committee

MSW: Maritime Single Window

PFSA: Port Facility Security Assessments

PFSO: Port Facility Security Officer

PFSP: Port Facility Security Plan

RSO: Recognized Security Organisation

SMTP: Simple Mail Transfer Protocol

SSN: Safe Sea Net

SSO: Ship Security Officer

TOS: Terminal Operating System

UNECE: The United Nations Economic Commission for Europe

VGM: Verified Gross Mass

WCO: World Customs Organization

1 Introduction

This document is based on the results of two questionnaires that were published among the project partners to get a state-of-the-art view on the processes and documents related to the ISPS Code and cargo clearance. One questionnaire for ports (Annex A) and one for shipping companies (Annex B) were distributed. The answers were collected both as written text and through several teleconferences during the autumn of 2021. The involved ports were Trondheim Havn, Vordingborg Havn and Aalborg Havn, while the shipping lines NCL and DFDS also provided input to this work. In addition, input already collected through the interviews in WP5 as part of deliverable *D5.1 System design specification* were used as a starting point for this work.

The purpose of this analysis is to describe the current situation regarding ISPS and cargo clearance and next, to be able to improve the efficiency in transport systems involving autonomous functionalities as covered by the use cases. This deliverable also relates to D5.5 on Methodology for safety and security analysis, since safe and secure communication is a requirement when introducing autonomy to the ports.

Chapter 2 summarizes the responses on the questionnaire regarding ISPS handling, while Chapter 3 does the same for customs and cargo clearance. Chapter 4 gives an analysis of Use case A with respect to the overall ISPS requirements regarding mother and daughter vessels, and Chapter 5 describes how the cargo clearance process will be affected by transhipments between mother and daughter vessels.

2 ISPS

2.1 Introduction

The International Ship and Port Facility Security Code (ISPS) entered into force under SOLAS chapter XI-2 on 1 July 2004 [1]. The code forms the basis for a comprehensive mandatory security regime for international shipping. The code is divided into two sections. The mandatory Part A outlines detailed maritime and port security-related requirements which SOLAS contracting governments, port authorities and shipping companies must adhere to, in order to be in compliance with the code. Part B of the code provides recommendatory guidelines on how to implement measures to meet the requirements.

The main objectives of the ISPS code are [6]:

1. To prevent any unauthorised entry into port facilities, ships and other related restricted areas.
2. To prevent the passage of unauthorised weapons, incendiary devices or explosives to ships and port facilities.
3. To detect the different security threats onboard vessels and in ports.
4. Establish security plans for ship, company and port facilities in order to respond and implement necessary actions according to different threat situations.
5. Determining the respective roles and responsibilities of all parties concerned with maritime security.
6. To ensure that there is early and efficient exchange of maritime security-related information.

The ISPS code defines three security levels according to the risk for security incidents [6]:

- Security level 1: Minimum security measures should be implemented
- Security level 2: There is a heightened risk for security incidents and additional security measures should be implemented. Commercial activity can be continued with increased security restrictions
- Security level 3: The strictest security level. Commercial activity can be suspended, and security response transferred to governmental organisations.

2.2 Main ISPS Documents

2.2.1 Ship Security Plan

In international waters, all passenger ships (including high-speed passenger craft) and cargo ships (including high-speed vessels) with a gross tonnage of 500 or more, and mobile offshore drilling units with their own propulsion are subject to ISPS-code [6].

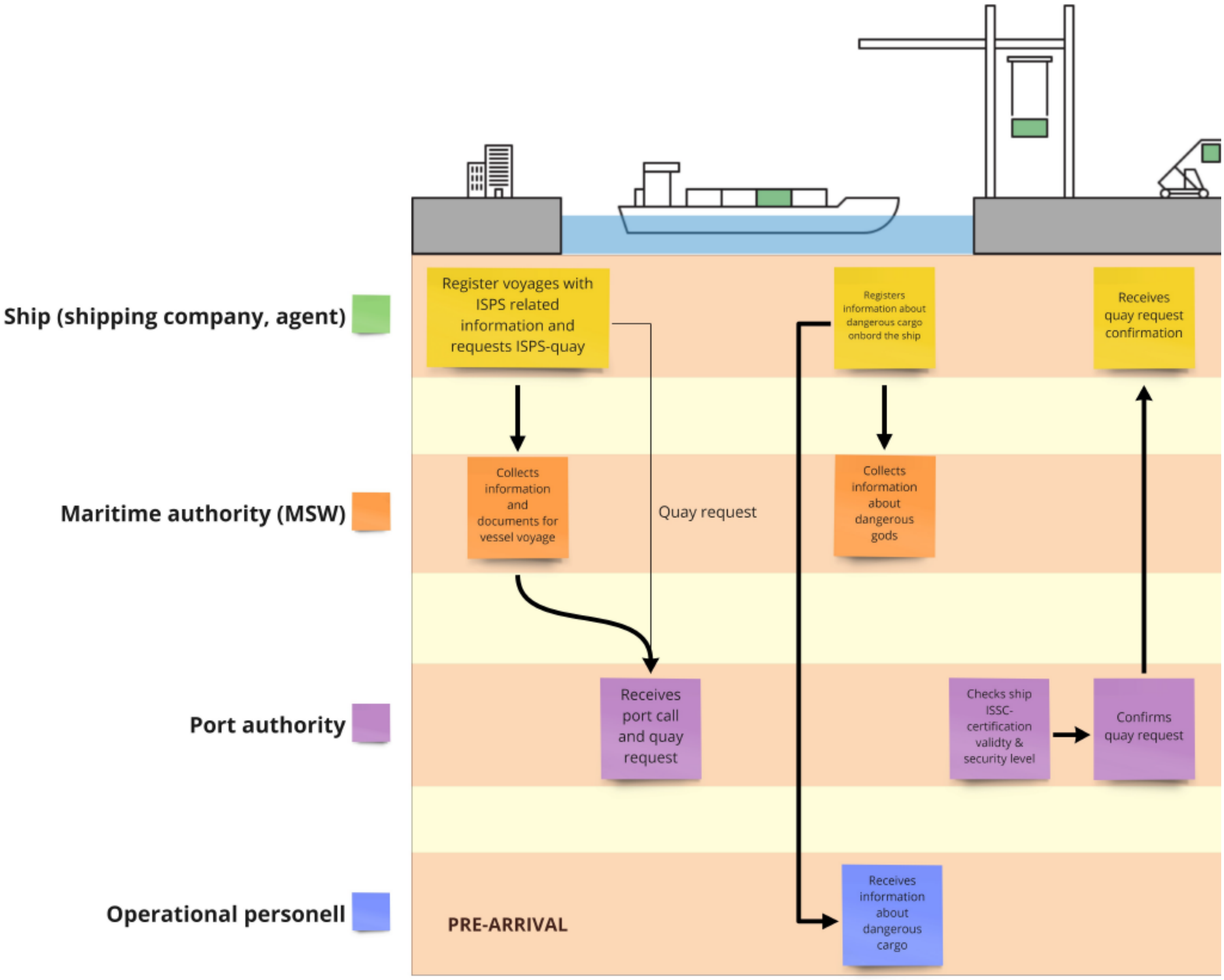
All ships subject to the ISPS-code are required to carry on board a ship security plan (SSP) approved by the administration where the ship is registered. The SSP is developed to protect ships, persons and cargo onboard from the risk of security incidents. The shipping company security officer (CSO) has the responsibility for development and revision of the SSP. The ship security officer (SSO) is responsible for the security of the ship including implementation and maintenance of the security plan. The plan should define actions to be taken for all the three security levels defined in the ISPS-code [6].

In order to visit ISPS quays the ships must have an approved SSP and be issued a valid international ship security certificate (ISSC). The certificate states that the ship complies with the requirements in SOLAS chapter XI-2 and the ISPS code.

2.2.2 Port Facility Security Plan

Port authorities are required under the ISPS code to have Port Facility Security Plans (PFSP) for each of its Port Facilities. The PFSPs should be based upon Port Facility Security Assessments (PFSA) of each of the Port authority’s port facilities. PFSA contain vulnerability assessments and suggest corresponding security measures for the specific Port facility. PFSA’s are carried out by either a country's designated authority or by a recognized security organisation (RSO). The governing body of a PFSP is the port authority’s Port Facility Security Officer (PFSO) [4]. PFSP’s can be developed by the PFSO or by an RSO. A country's designated authority must approve the final PFSP in order to fulfil the ISPS code’s formal requirements.

The port authority will then submit its ISPS facility status to the MSW which maintains a register of all available ISPS facilities. ISPS facilities can be activated and deactivated based on the ISSC certification of ships requesting a quay visit with the port authority. The activation/deactivation status is not submitted to the MSW, and it is a general industry practice that an ISPS quay is up to the security standard of the ISPS-code upon arrival. When activating an ISPS quay, the Port authority is responsible for preparing the quay according to the regulations of the ISPS-code and the PFSP, this process is referred to as quay cleaning.


Ship (shipping company, agent)
Maritime authority (MSW)
Port authority
Operational personell
Register voyages with ISPS related information and requests ISPS-quay
Registers information about dangerous cargo onbord the ship
Receives quay request confirmation
Collects information and documents for vessel voyage
Quay request
Collects information about dangerous gods
Receives port call and quay request
Checks ship ISSC-certification validty & security level
Confirms quay request
PRE-ARRIVAL
Receives information about dangerous cargo

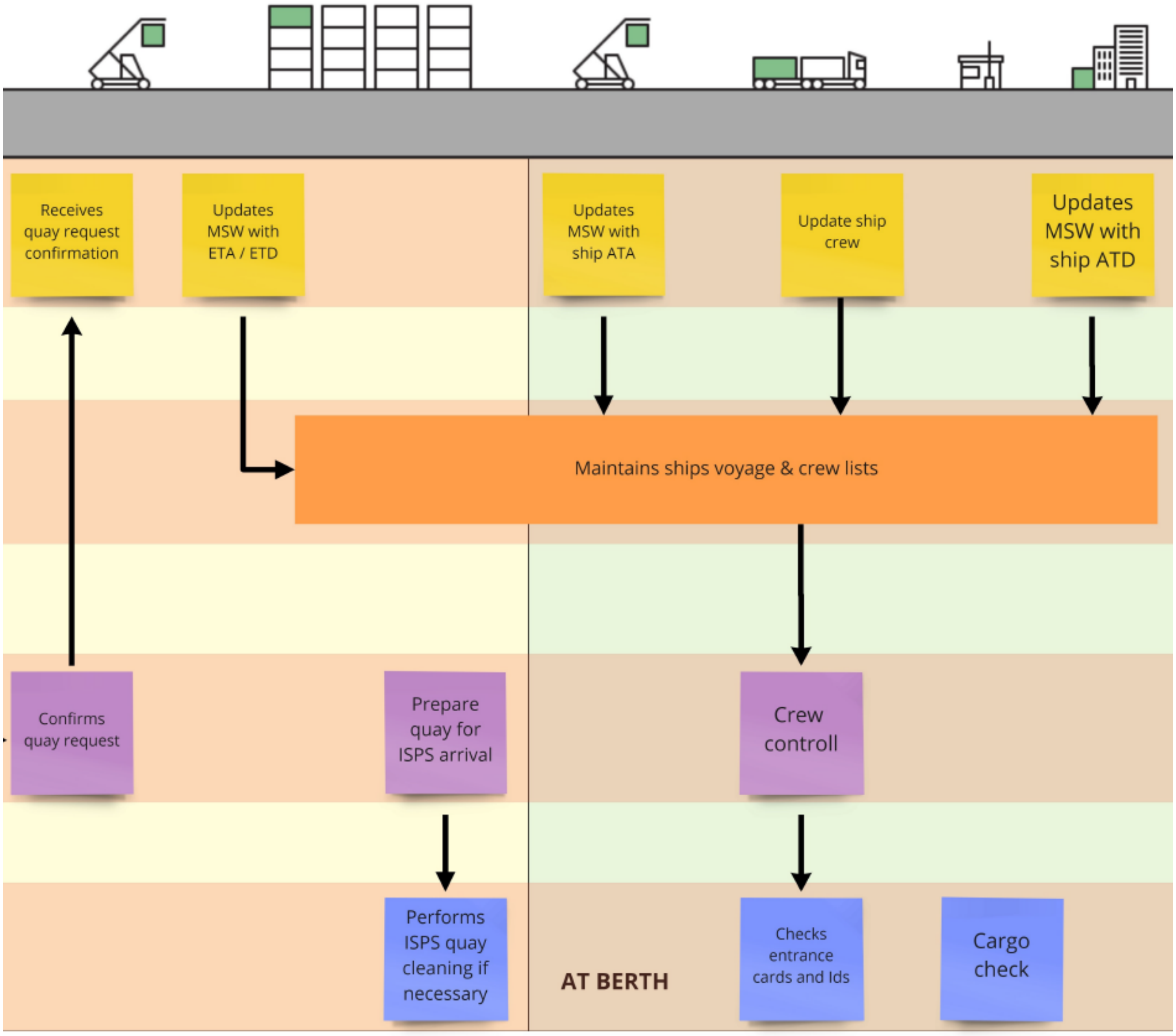

Receives quay request confirmation
Updates MSW with ETA / ETD
Updates MSW with ship ATA
Update ship crew
Updates MSW with ship ATD
Maintains ships voyage & crew lists
Confirms quay request
Prepare quay for ISPS arrival
Crew controll
Performs ISPS quay cleaning if necessary
AT BERTH
Checks entrance cards and Ids
Cargo check

Figure 1: Port Call ISPS Processes

2.3 Continuous ISPS Processes

Figure 1 (divided on two pages for convenience) shows a typical port call ISPS process.

2.3.1 Pre-arrival

Prior to the arrival the vessels register voyage and ISPS-information in the maritime single window (MSW). Each country has their own implementation of the maritime single window and the information and functionality in the systems can vary. In the description we have focused on the security related information reported to Danish and Norwegian maritime authorities through Safe Sea Net (SSN), where we use SSN-N and SSN-D for the Norwegian and Danish version respectively. Ships subject to the ISPS-code must report their arrival at least 24 hours before arriving at the port. In SSN-N the ship has the possibility to request a specific ISPS-quay, but the communication about the specific ISPS-quay to use is often done through direct contact between the ship and the port authority.

The following ISPS-related documents are registered by the ship in SSN:

- ISSC-certificate and expiration date.
- Security related matters. If there are particular security related matters to be reported for a particular voyage this can be entered and necessary actions can be agreed between the ship and the port authority (see description of declaration of security (DOS) in [3]).
- Ten last port calls. The ship should keep records of the information provided for the last 10 port calls. The information includes all DOS the ship has agreed in addition to the security levels the ship has been operating on. Any ship-to-ship activity for the last ten port calls should also be registered.
- Crew list. In case of crew change, both incoming and outgoing crew are registered in the crew list. There is no specific overview of crew changes.
- Passenger list
- Dangerous cargo. This includes classification code, amount and location onboard the ship.

Before arrival the ships ISSC-certificate is collected from the MSW by the Port authority and is validated against third party sources. The ship's ISPS security level is also checked. If the security level of the ship is lower than that of the port facility for the requested quay, the quay request will have to be automatically rejected [2]. If the vessel's security level, however, is higher than that of the port facility, security measures can be agreed upon by the SSO and the PFSO and should be documented in a declaration of security (DoS) [3]. Once the ship security matches the security requirements of the Port or a DoS has been issued, and the Port has done its final adjustments, a quay confirmation is issued to the ship/agents via the MSW or directly depending on the MSW support for handling quay requests.

Prior to the ship's arrival, the ship will continuously update its ETA in the MSW. Some time ahead of arrival the port will prepare the ISPS quay for arrival. If the quay is no longer fulfilling the security requirements of the ISPS-code, the Port must perform necessary quay cleaning tasks, meaning actions must be taken to secure the port according to the Port Facility Security Plan (PFSP). This could involve operations such as securing the ports infrastructure, e.g. closing gates to prevent access, patrol the area for suspicious activities, and internally document the security efforts. In practice, it is expected that the quay is ISPS ready by the time the ship arrives, and little to no communication occurs between the ship and the Port at this stage. Communication usually occurs by email/phone/radio when there are exceptions to this practice, e.g. security level has changed or a DOS needs to be drafted.

2.3.2 At berth

As the ship arrives at the Port, the relevant ISPS documents should already be filled out and submitted to the MSW. In the case of dangerous cargo, relevant information is also submitted to the relevant MSW before arrival. The Port will act according to the Port Security Facility Plan (PSFP) for the dangerous cargo being transported, but in practice this usually does not involve direct handling of the cargo. Dangerous cargo is usually handled by terminal operators according to the severity of the dangerous cargo, the PSFP and the stowage plans received by the ship. Handling of dangerous cargo begins once the ship has issued a notice of readiness.

Some port authorities exchange ship specific documentation such as ISSC-certificates, tonnage reports and ship particulars for first-time visiting ships. Further validation of ISSC-certificate is usually also carried out at this stage.

Ship crew members are validated against the crew lists in the MSW, and usually identifies themselves with identification provided by the shipping companies/ship and/or by access provided by the Port. During crew changes the ship and/or the shipping company will inform the Port about the changes and update the crew list in the MSW accordingly. For MSW’s that does not support crew changes, the crew list tends to contain both the embarking and disembarking crew members during a port call.

2.3.3 Departure

There are no directly ISPS related communication between the port and the ship after departure. Some information regarding the finalized stowage plan, which could include detailed information regarding dangerous cargo in some cases, are sent to the next Port, or the relevant terminal operators. The general practice for Port authorities is to maintain the ISPS facility active until the next port call.

2.4 Implementation in New Transport Systems

2.4.1 ISSC-certificate verification

It is expected that all ISSC certified vessels have a valid ISSC-certificate added to the MSW. Currently this is a self-governing system, and it is not guaranteed that the ISSC-certificates added by the ship is in fact valid. ISSC-certificates provided by the MSW usually has to be validated by the Port authority by looking up the certificate number and validating it against third party sources.

Having a central authority, e.g. MSW, IMO (the International Maritime Organization) or a body representing IMO, for validating ISSC-certificates and the ships security level would make it possible to automate the validation process, and implement automatic notifications when certifications and/or security levels don't conform to the ISPS-code requirements.

Work is ongoing in IMO Convention on Facilitation of International Maritime Traffic (FAL) through the Correspondence Group on "Developing Guidelines on Electronic Signature Systems and Operational Port Data for the Purpose of Digital Information Exchange" to define a system for electronic signatures that can be used for certificates as well, and in this way ease the validation of the ISSC certificates. At the same time, the IMO Reference data model is now being extended with data elements to describe important parameters related to certificates. Thus, using data models that implement the IMO

Reference data model will ease the exchange of certification statuses among the different stakeholders.

2.4.2 On/Off port facility process

For Port facilities of type “On/Off”, there is a manual process to do 1 – 2 hours before the ISPS ship arrives. Logging of check lists and other related documentation are often done in a paper-based system, or in a document that are stored in a file share.

An improvement would be if information about the Port Facility can be shared with all stakeholders, and available to all at the moment the Port facility is “turned On/Off”.

2.4.3 Uploading dangerous cargo information several times

The shipping companies are uploading dangerous cargo documents to MSW, and they send the exact same to the terminal. An improvement would be to integrate with their own system to automate this process.

2.4.4 Crew change

Crew on board when vessel is arriving, and crew on board at departure is reported and available in SSN-N. But when a crew change is planned, all the dialogue about incoming crew is done between the ship and the port, and not via SSN-N. This leads to a lot of e-mails, and not standardises formats of incoming crew lists, in order for the port to grant access to the port facility for them.

It will be a great improvement if crew changes also were reported to SSN, and available for the port authorities there. Also, if this information will be included in the SSN-N API, the port security system could get this information automatically.

The IMO Reference data model defines data elements that cover the information need for crew lists as requested by IMO FAL. These data elements are implemented in both ISO 28005-2 on Electronic Port Clearance, in the World Customs Organization (WCO) data model and in the The United Nations Economic Commission for Europe (UNECE) data model covering trade processes. Also, work is ongoing to define a code list covering all crew ranks and ratings onboard ships (and offshore installations).

2.4.5 Changed security level information exchange

In response to a change in security level by the countries designated authority, the PFSO gets notified of the change. It is the Port authority's responsibility to notify any arriving vessels of these changes as by the ISPS-code regulation [5]. Exceptions to the expected validity of the ISPS facility is usually resolved by direct communication and drafting up a DOS between the PFSO and SSO via email, phone, or radio.

Automatic notification of all involved parties in the port call as provided in the MSW during security adjustments would decrease the amount of proxy communication between the countries designated authority, PFSO and the SSO.

2.4.6 E-mail communication

It seems that the ISPS process is quite well functioning because all the documents are collected by MSW, and the authorities find their information there. All other communication between the shipping company and the port are in general very cumbersome. Most of the dialogue is still via e-mail.

3 Customs and Cargo Clearance

3.1 Introduction

Customs and cargo clearance involves the processes related to validating and approving the state of cargo carrier unit (CCU) and cargo passing through a port. There are different levels of validating and approving the cargo, such as validating and approving internally, towards mercantile stakeholders and/or towards formal stakeholders.

Mercantile stakeholders in this regard can be port, terminal operator, shipping company, hinterland transport company and cargo consignee. Formal stakeholders are typically state government formalised by national regulations and international regulations.

Although we will touch into different levels of clearance in this document, the most relevant to discuss is the formal process of validating and approving cargo towards state government, i.e. customs clearance.

3.2 Customs Clearance Processes

3.2.1 Introduction

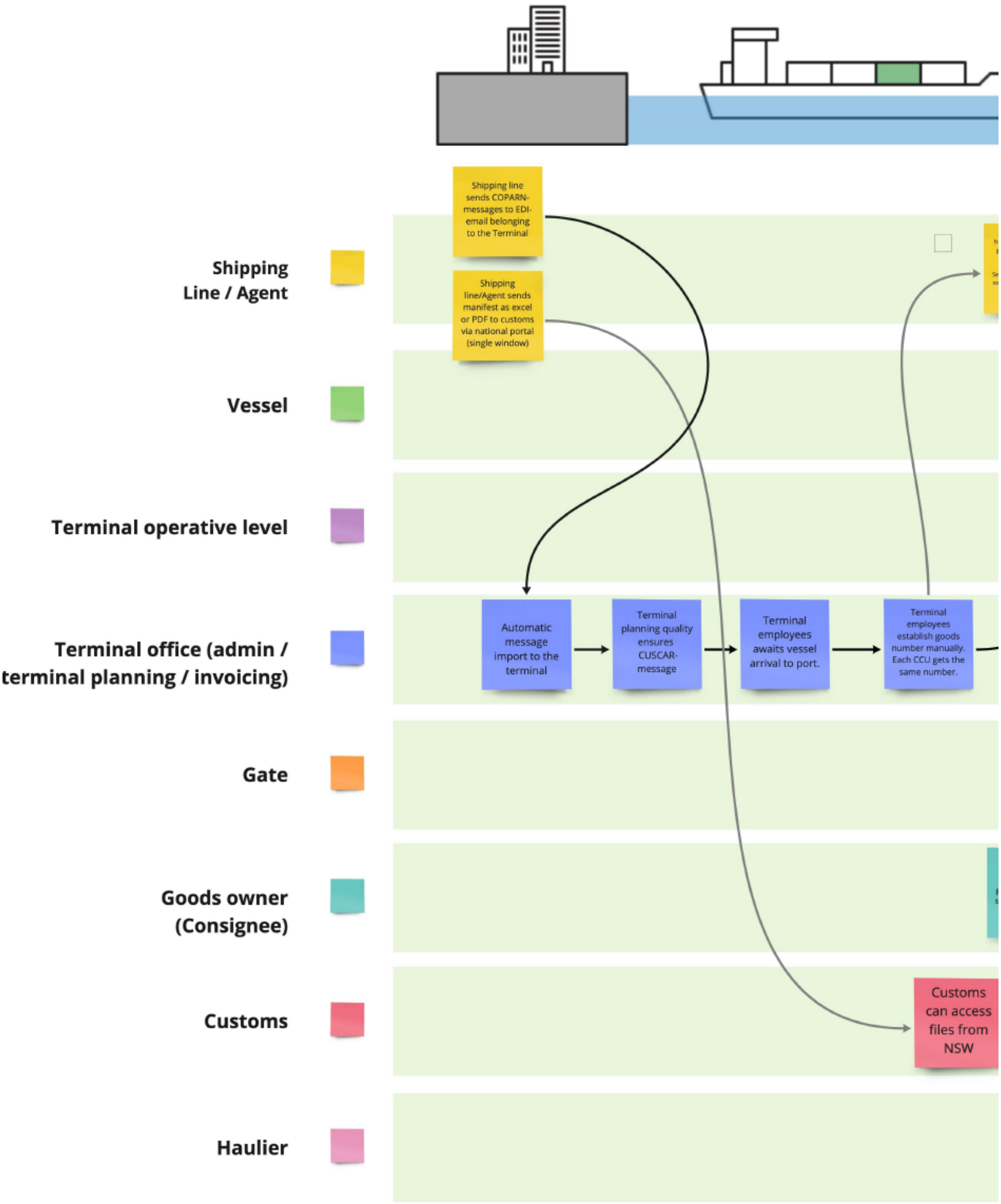
This section describes the customs clearance process as neutral as possible, but most of the information is gathered from Norwegian ports and terminal operators, and thus some of the assets involved (i.e. exchange documents, data and formats) are specific for the Norwegian customs clearance process. An overview of the customs clearance process is given in Figure 22 (divided on four pages for convenience).

The interviews uncover a high diversity in the degree of digitisation and automation in this process. This means that the internal routines for processing assets may vary. We will describe this in detail in those sub-processes where the diversity is of significance.

It is worth mentioning that this process is only relevant for what is commonly called import terminals. These are terminals approved by the government to handle import of goods through a cargo import flow. A port call may involve both discharging cargo and loading cargo, but we will only consider the former as discharging cargo arriving from a foreign port constitutes an import flow.

Customs

A graphical view of the concept flow



Shipping line sends COPARN-messages to EDI-email belonging to the Terminal

Shipping line/Agent sends manifest as excel or PDF to customs via national portal (single window)

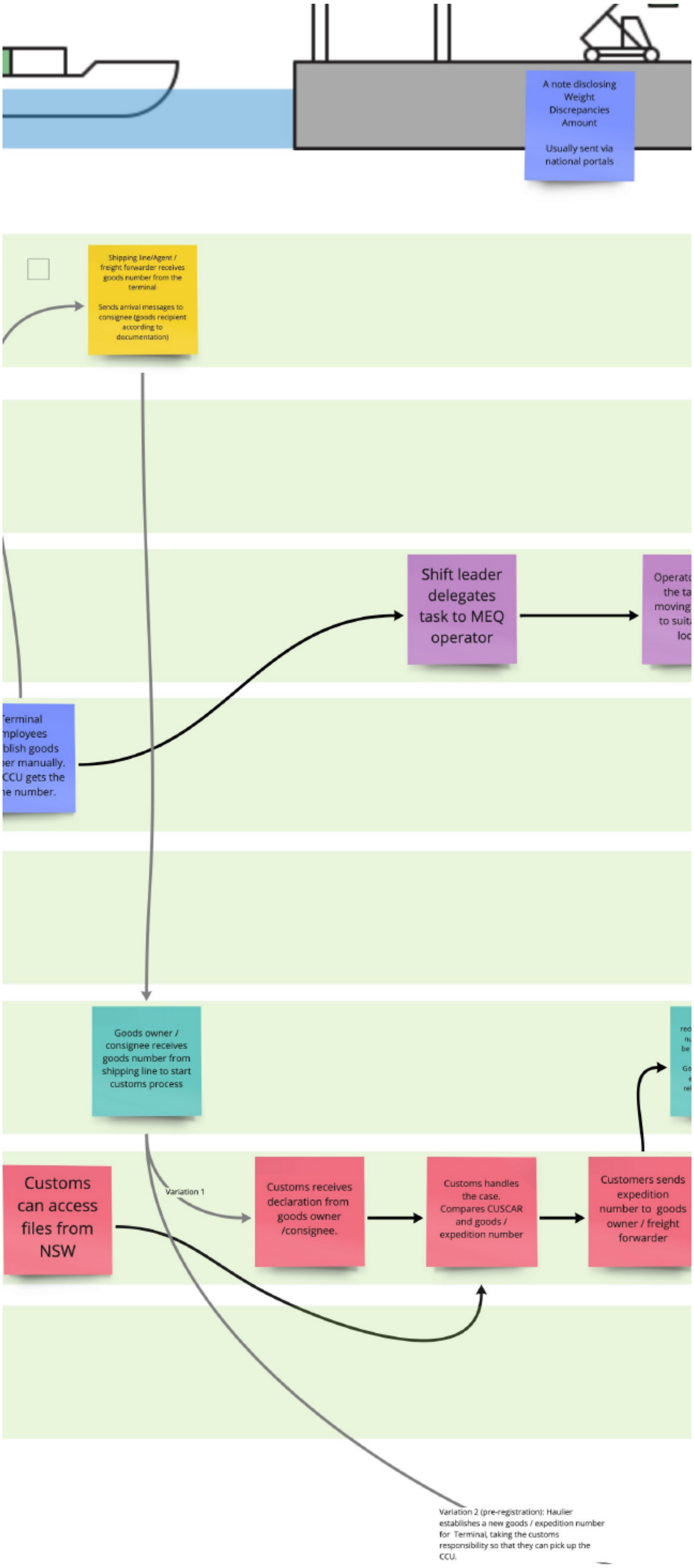
Automatic message import to the terminal

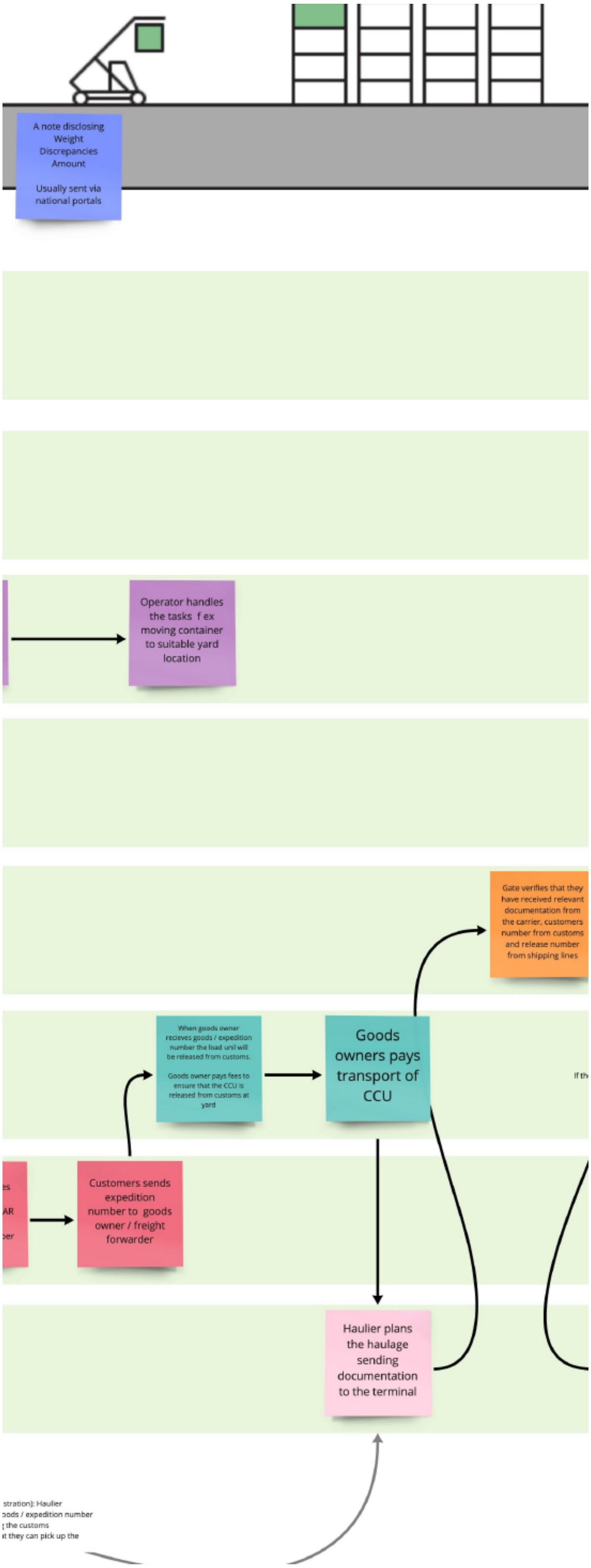
Terminal planning quality ensures CUSCAR-message

Terminal employees awaits vessel arrival to port.

Terminal employees establish goods number manually. Each CCU gets the same number.

Customs can access files from NSW


A note disclosing Weight Discrepancies Amount
Usually sent via national portals
Shipping line/Agent / freight forwarder receives goods number from the terminal
Sends arrival messages to consignee (goods recipient according to documentation)
Shift leader delegates task to MEQ operator
Operato the ta moving to suita loc
erminal mployees blish goods er manually. CCU gets the e number.
Goods owner / consignee receives goods number from shipping line to start customs process
rec nu be
Go e rel
Customs can access files from NSW
Variation 1
Customs receives declaration from goods owner /consignee.
Customs handles the case. Compares CUSCAR and goods / expedition number
Customers sends expedition number to goods owner / freight forwarder
Variation 2 (pre-registration): Haulier establishes a new goods / expedition number for Terminal, taking the customs responsibility so that they can pick up the CCU.


A note disclosing Weight Discrepancies Amount
Usually sent via national portals
Operator handles the tasks f ex moving container to suitable yard location
Gate verifies that they have received relevant documentation from the carrier, customers number from customs and release number from shipping lines
When goods owner recieves goods / expedition number the load unil will be released from customs.
Goods owner pays fees to ensure that the CCU is released from customs at yard
Goods owners pays transport of CCU
If th
es
AR
per
Customers sends expedition number to goods owner / freight forwarder
Haulier plans the haulage sending documentation to the terminal
stration): Haulier
oods / expedition number
the customs
it they can pick up the

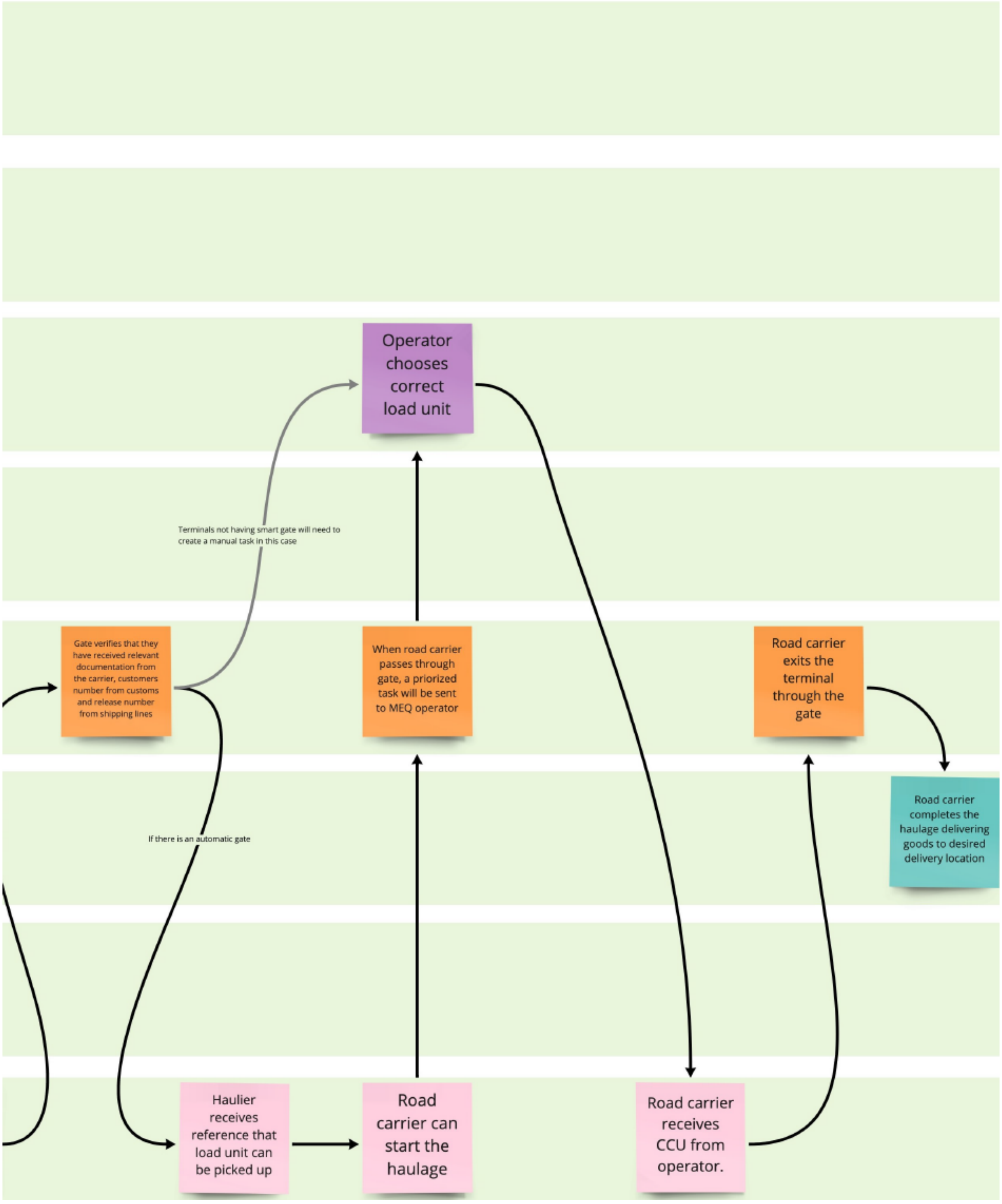

Operator chooses correct load unit
Terminals not having smart gate will need to create a manual task in this case
Gate verifies that they have received relevant documentation from the carrier, customers number from customs and release number from shipping lines
When road carrier passes through gate, a priorized task will be sent to MEQ operator
Road carrier exits the terminal through the gate
Road carrier completes the haulage delivering goods to desired delivery location
If there is an automatic gate
Haulier receives reference that load unit can be picked up
Road carrier can start the haulage
Road carrier receives CCU from operator.

Figure 2: Customs Clearance Process

3.2.2 Pre-arrival

It is useful to view the process and interactions from the terminal operator's perspective. The terminal operator is either an organisational department of the port or an autonomous organisational unit solely responsible for its own operation and only being a tenant of the port. The mercantile relationship in the latter scenario is regulated through regular tenancy contracts as well as other monetary models (i.e. invoicing based on the amount of CCUs passing the port)

The planning of a cargo operation in an import flow is initiated by the shipping company or an agent on behalf of a shipping company when sending a cargo announcement to the terminal operator. The cargo announcement document exchange varies from documentation through excel or pdf files to the established Electronic Data Interchange (EDI) exchange format COPARN [15]. The shipping company simultaneously associates the cargo manifest as excel, pdf or a text-based description to a port call in the national single window portal from which customs authorities can access the same documentation [16].

Information regarding customs clearance is of relevance for the terminal receiving the cargo. This information is either exchanged manually in an excel document or a pdf by e-mail or delivered as a CUSCAR EDI message [14] distributed through suitable channels, i.e. FTP (File Transfer Protocol) or SMTP (Simple Mail Transfer Protocol), for automatically parsing and registration of the information in the Terminal Operating System (TOS).

The terminal administration starts planning the forthcoming discharge operation upon receiving the cargo announcement and the customs clearance information. One step is to assign a goods number to the arriving cargo. The terminal operator assigns one goods number per port call and communicates this goods number back to the shipping company.

Upon arrival, the shipping company sends an arrival message alongside the cargo and the goods number to the goods owner/consignee of the cargo. This communication is to a large extent done by e-mail and is thus naturally prone to errors.

The consignee registers the incoming cargo and the goods number in a portal provided by the customs authorities. The customs authorities validate the information received. Typically, the consignee also orders transport hinterland from a haulier company at the same time.

3.2.3 During Discharge Operation

The discharge operation is executed as planned by the terminal operator and the stevedoring crew and the CCUs are moved into the terminal yard and stacked while awaiting pickup by road carrier.

In Norway, import terminals are obliged to maintain a goods journal with the CCUs and associated goods numbers and expedition number. It is important for the terminal to register any deviations at the very moment they take over the responsibility for the CCU to avoid liability related to cargo missing or being damaged.

Typically, the reach stacker has weighting mechanisms and registers the weight of the CCU when moving it to the desired location. The operator also inspects the CCU for any damage that may expose the cargo inside and that the accompanying seals are valid and not broken. Any deviations are reported in the terminal customs journal.

3.2.4 Post Discharge Operation

Usually, the customs authority's validation is merely a formality, and the consignee receives the needed expedition number to prove that the cargo is cleared, but in some cases the authorities may stall this expedition to perform an inspection of the goods within a CCU.

When the consignee receives the expedition number, it communicates to the haulier that the cargo is ready for pickup and sends this expedition number to the terminal. There are variations of expedition number interchange; in some cases, the consignee communicates it to the haulier which then again registers it in the terminals systems or communicates it directly in the gates upon which the terminal confirms the information with the customs authorities through the customs portal.

When the road carrier from the haulier company arrives at the gate, the necessary information (goods number and expedition number) is validated, and the release of the cargo is verified by the terminal personnel. The gate personnel register a task to cargo handling personnel, such as a reach stacker operator, who clarifies and loads the CCU on the road carrier.

In some cases, the terminal has an automatic gate. In these cases, the haulier typically pre-announces their arrival through registering a work-order with a CCU number. The terminal operating system sends a message when the CCU is ready for pickup after receiving the necessary clearances, such as the customs expedition number.

3.3 Implementation in new transport systems

3.3.1 Administrative overload

The ports involved in the interviews typically reported bureaucratic overload related to manual processes in information exchange where they knew the involving data was registered digitally in other systems. The problem they pointed out was missing interaction between these systems.

One example is the manual labour involved in reporting the number of CCUs passing the port. Some of the terminals and ports had established exchange of documents that was automatically parsed and thus making this process quite effective, but others reported that these numbers were punched in documents and passed on to the port, who punched it in their economy and invoicing system.

The relevant question here is: If this information is already digitised in MSW and manifests, how can it be exchanged automatically?

3.3.2 E-mail interaction

For those shipping companies and terminals that had not established an EDI-interchange, the communication was based on e-mail and telephone. This was highly ineffective and error prone.

It is also worth to note that the protocols upon which the EDI interchange is established, are not suitable for secure and robust communication. Typically protocols such as ftp and smtp are used, both of which do not ensure the kind of security-level one would seek to implement between systems interchanging business critical data, although most of the parties reported having moved or moving to secure alternatives such as sftp. Still the protocol does not ensure the transactional robustness of business-critical systems due to its “fire and forget”-type of nature.

4 ISPS Related to the AEGIS Use Cases

Here, we look at ISPS in relation to the concept of mother and daughter vessels. We have focused on use case A (“Short sea and rural terminals in Norway”), but it will also be applicable to the other uses cases in AEGIS where cargo is reloaded between mother and daughter vessels on the way to its destination.

In case A, the mother vessel will primarily be used to transport containers between main ports along the Norwegian west-coast and Rotterdam, while daughter vessels will be used between smaller ports/terminals inside fjords in the Trondheim region. Daughter vessels will feed containers to/from mother vessels either directly or through a transit terminal.

Case A has defined two scenarios that is well described in “D8.1 Cargo Volume Analysis – Case A” [7]:

1. The transport between Rotterdam, Netherland and Hitra Kysthavn (Sandstad), Norway
2. Transport within the Trondheimsfjorden region, Norway. Different scenarios for visiting facilities in the area with daughter vessels are discussed.

The map in Figure 3 displays one of the scenarios where containers are loaded/discharged by mother vessels at Sandstad, while daughter vessels perform the local transport between Sandstad and other facilities in the area.

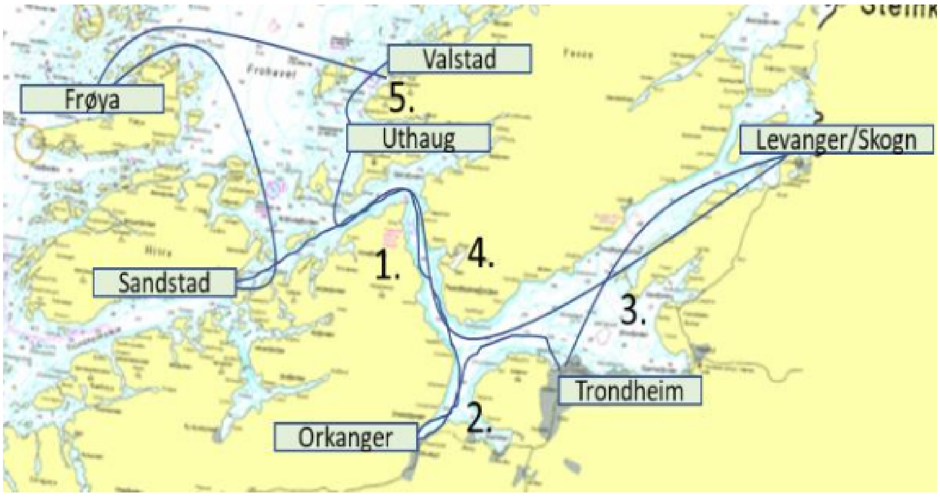


Figure 3: One possible daughter scenario in Trondheimsfjorden, from D8.1

Table 1 shows the current ISPS status of the facilities in the Trondheimsfjorden region:

Table 1: Current ISPS status of the facilities in the Trondheimsfjorden region

Facility	ISPS status
Orkanger	ISPS, permanent
Hitra Kysthavn, Sandstad	ISPS On/Off
Frøya	ISPS On/Off

Trondheim	ISPS On/Off
Stjørdal	ISPS On/Off
Frosta	ISPS On/Off
Levanger/Skogn	ISPS On/Off
Verdal	ISPS On/Off
Steinkjer	ISPS On/Off
Verran	ISPS On/Off
Inderøy	Not ISPS
Uthaug	ISPS On/Off (outside of Port of Trondheim)
Valstad	ISPS On/Off (outside of Port of Trondheim)
Rørvik	ISPS On/Off (outside of Port of Trondheim)

In order to tranship containers directly between mother and daughter vessels, we consider the following scenarios:

- ISSC vessel with transhipment to ISSC vessel via ISPS facility
    - This is ok
- ISSC vessel with transhipment to non-ISSC vessel via ISPS facility
    - The facility must document the activity in their risk assessment and Port Facility Security Plan (PFSP). The vulnerability that affects the facility must be handled with adequate measures, both for the non-ISSC vessel and also describe how the transhipment will be handled.
- ISSC vessel with transhipment to non-ISSC vessel via non-ISPS facility
    - Not allowed
- ISSC vessel with transhipment to ISSC vessel via ISPS facility where final destination is non-ISPS facility
    - Not allowed to visit the non-ISPS destination facility with ISSC vessel

Requirements for ISSC certification of vessels are described in the ship security plan section. The mother vessels are above 500 gross tonnage and in international trade and must have valid ISSC. The daughter vessel will also be able to have ISSC certification as long as they apply to the criteria. In this case, the daughter vessels must be at least 500 gross tonnage and be certified for international trade. Barges do not have their own propulsion and will not qualify for ISSC certification.

In order to satisfy the ISPS requirements, there are currently two possible options, as described in the following two sections.

4.1 Option 1 – ISSC Daughter Vessel and ISPS Facilities

In this case, both mother and daughter vessels are ISSC certified, and all facilities visited are ISPS. In order to utilize the quay areas as good as possible, most of the facilities will be ISPS-On/Off. Prior to arrival of ISSC vessels, security procedures must be followed to switch the ISPS status of the facility to

"On". In case of arrival of ISSC daughter vessels, this narrows down the time window when the daughter vessels can pick-up/deliver the containers. Some of the terminals in the region are currently non-ISPS facilities. These will have to perform risk assessment and formulate and endorse a Port Facility Security Plan (PFSP) in order to accept port calls by ISSC-certified daughter vessels.

It is not yet defined how ISPS requirements should be handled for autonomous vessels. A scoping exercise for autonomous vessels was performed by the Maritime Safety Committee (MSC) of the International Maritime Organisation (IMO) in May 2021. ISPS is one of the topics that must be investigated further for autonomous vessels [8].

In case of autonomous vessels, remote control of the vessels must be performed from shore-based control centres. IMO has traditionally avoided regulating shore-based matters, but in case of autonomous vessels, a uniform standard in this area would be important [9].

4.2 Option 2 – Non-ISSC Daughter vessel and non-ISPS Facilities

In this scenario, the daughter vessels are non-ISSC and can only visit non-ISPS facilities. The containers must then be picked up/delivered at non-ISPS areas of the facilities.

For import cargo, transhipment of cargo from the mother vessel to a non-ISSC vessel will be possible given that the ISPS facility has documented the procedure in their risk assessment and PFSP as described above. As long as the destination facility is non-ISPS, this scenario will be similar to a truck picking up the container and leaving the ISPS facility for delivery to another non-ISPS facility.

For export cargo, security check and cargo cleaning of the containers must be performed at the transhipment hub before the containers are sealed and transported to the ISPS area for pickup by mother vessels. When the transport companies deliver cargo to an ISPS facility, they are responsible for the cargo they are bringing, and the receiver (operator/ship/facility) are responsible for checking the cargo when received at the ISPS facility. In the current scenario with non-ISPS daughter vessel and non-ISPS facility, one will not utilize the same procedures.

Even on a non-ISPS facility, monitoring and securing of the containers at enclosed areas of the terminal will be important to avoid access by unauthorized persons.

For export cargo, this scenario seems unlikely to be realistic.

5 Customs Clearance related to the AEGIS use cases

In this section, we will discuss the customs clearance process in the scope of use case A as it is described in deliverable “D8.1 Cargo Volume Analysis – Case A” [7] (“Short-sea and rural terminals in Norway”). The work is kept on a general level, meaning that most of the assumptions are applicable for e.g. use case B as well.

5.1 Transit Processes

The transport of goods from one customs territory (e.g. geographical areas under the jurisdiction of countries such as Norway or regions such as the EU) to another through a third or more customs territories is called transiting of goods.

It is also possible to transit goods within a customs territory, which in practice means that the declaration process through the nodes in the transhipment chain is delayed. This is typically called forwarding.

Both processes need to be considered in the context of use case A. The processes resemble each other and is quite equivalent between customs territories by the following characteristics [10][11][12][13]:

1. Transit processes need to be carried out by a party with forwarding license (Licensed agent) issued from the customs territory judiciary.
2. The goods are under the judiciary customs unit control throughout the transit.
3. The forwarder needs to apply for a permit for transiting the goods, a process that typically is more lenient than that of declaring the goods.
4. The consignee of the goods cannot utilise the goods before the goods is declared at a transhipment node within the specific customs territory.
5. In transit processes, the judiciary customs unit may require the consignee to give a form of security which will be refunded once the goods have been cleared.

5.2 Use case A and Transit Processes

Use case A describes a scenario in which the mother vessels feed CCUs to daughter vessels either directly or through a transit terminal. We will discuss these transhipment techniques further in detail.

When the transhipment is carried out directly between the vessels, we need to consider whether or not this transhipment is done between the same freight forwarder or between two different parties. In both scenarios, a formal transhipment is done, and this needs to be described in the information exchange with the judiciary in the customs clearance process. For one party carrying out this operation, this is merely a matter of supporting keeping the required data within its own systems. Exchange between freight forwarders probably means that the original freight forwarder needs to have a contractual agreement with the freight forwarder of the daughter vessels and autonomous exchange of required data in a standardised format for further interchange with the judiciary.

If the transhipment is done through a transit terminal, the forwarding process is complicated further. The transit terminal needs to register the transactions of the goods (discharge and load operations) and provide a new goods number acquired from the next port of discharge through the consignee of the goods. This implies that all the involved parties are able to interchange the required information in a standardised manner [10].

5.3 Use case A and Clearance Processes

The specific process of clearance is the interchange of information between consignee, shipping company/forwarder, terminal and government as described in Section 3.2. The transit processes described in the previous section would lead up to a specific clearance process. This means that a transit-process will always be superseded by the actual clearance process. The transit process is as described in Section 5.1, while the clearance process is described in Section 5.4.

As long as the infrastructure and standards for information exchange is present in a customs clearance process and the parties involved supports these standards, the steps in the process would not stand in the way of automation. The network of information interchange is of course complex due to the relatively high number of stakeholders, but informatics-wise this flow could be represented in a manageable state diagram based on Figure 22 and thus represent a solvable problem.

5.4 Customs Clearance Process Options in Use Case A

Use case A represents a scenario that may or may not involve transit processes (The clearance process is always involved). The presence of transit processes is of importance related to the complexity of the entire clearance process as described in Section 5.2.

For sea-based transit, the terminal involved in the clearance is typically the terminal of the first port of arrival within a customs territory, but in a forwarding context it may just as well be the second or third terminal in which the goods arrive. Considering that transit processes introduce higher complexity, handling the customs clearance in Hitra would lay the grounds for a less complex information interchange with fewer involved parties. This is because two extra stakeholders will participate in the information exchange at each node and transit point. These stakeholders are the authorities and the sub-contractor for freight, that is, the freight forwarder that takes responsibility for the cargo into a terminal that have customs functionalities. However, if early declarations are done instead, this is not needed.

But still, these considerations are based on the premise of an effective clearance process. There are steps in this process that could halt the process of clearing specific CCUs/goods (e.g. deviations or customs authorities controls) and thus this halt would perpetuate through the rest of the logistics chain. If this is a recurring problem, centralising the customs clearance process on the first transit node could be a potential risk of hurting the logistics chain flow.

In a dynamic logistics chain with autonomous vessels of a more reactive nature, this would probably not be of any great importance for the effectiveness of the logistics network. In such a network, the halted CCUs would anyway be picked up as soon as they are cleared, and thus, this would not affect the effective transit of other CCUs.

6 Cost Benefit Analysis

The costs and benefits of adopting the ISPS and customs clearance processes to the transhipment will be further analysed in WP7.

7 Summary and conclusions

Currently, ISPS is an important barrier to reduce the possibility of having a hazard leading to a security related event during a port call. The regulatory requirements are based on the ISPS Code [13], and this is implemented for terminals and ships. This document has described ISPS related processes and the information that is exchanged related to this, in addition to the roles that each of the actors have. When autonomous functionalities are introduced, both related to autonomous ships, auto-mooring systems and autonomous loading and discharge equipment, technical barriers can and must be built into these systems. This means that the introduction of autonomous functionalities will increase the importance of building technological barriers. This is related to the information exchange and the safety and security of the communication between ship and shore. This is further handled in work package 5, task 5.3 on Communication safety and security analysis.

References

[1] SOLAS XI-2 and the ISPS code. https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

[2] Veileder til forskrift om sikring av havneanlegg. Veileder til forskrift om sikring av havneanlegg

[3] Example of a Declaration of Security. Decleration of Security Template Kystverket

[4] Port Facility Security / ISPS. https://www.kystverket.no/en/sea-transport-and-ports/port-facility-security--isps/port-facility-security-isps/

[5] ISPS Code, part B, 4.11

[6] Guide to the maritime security and the ISPS code 2021 Edition. International Maritime Organisation (IMO).

[7] AEGIS D8.1 Cargo Volume Analysis – Case A

[8] Autonmouns ships: regulatory scoping excercise https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx

[9] Henrik Ringbom (2019): Regulating Autonomous Ships—Concepts, Challenges and Precedents, Ocean Development & International Law, DOI: 10.1080/00908320.2019.1582593

[10] Norwegian customs, Completion of a Transit declaration - https://www.toll.no/en/corporate/transport-and-customs-warehouse/transit-declaration/completion-of-a-transit-declaration

[11] Norwegian customs, Import guide for beginners - https://www.toll.no/en/corporate/import/import-guide-for-beginners

[12] EU customs, What is customs transit? - https://ec.europa.eu/taxation_customs/business/customs-procedures-import-and-export/what-customs-transit_en

[13] UK customs, Using common or union transit to move goods into, through and out of the UK - https://www.gov.uk/government/collections/using-common-or-union-transit-to-move-goods-into-through-and-out-of-the-uk#bringing-goods-into-great-britain-using-common-transit

[14] CUSCAR: https://service.unece.org/trade/untdid/d21a/trmd/cuscar_c.htm

[15] COPARN: https://service.unece.org/trade/untdid/d21a/trmd/coparn_c.htm

[16] ITIGG - Guide to UN/EDIFACT Container Messages: https://unece.org/fileadmin/DAM///cefact/cf_plenary/plenary97/docs/97g109.pdf

Annex A. Questionnaire to Ports

A.1. ISPS

We have started to document the process related to arrival of ISPS vessel and getting an overview of documents in use and other routines. This is still incomplete, and this questionnaire will help is fill in the gap.

1. Quay requests and documents
    a. Does the shipping company/agent make a quay request for a specific ISPS quay when planning a port call?
        i. How, via SafeSeaNet and/or email?
    b. Which ISPS related documents does the shipping company or agent have to deliver to the Port and when? E.g. crew list, 10 last ports, dangerous cargo.
        i. pre-arrival
        ii. at berth
        iii. after departure
    c. How do you receive the documents? Via SafeSeaNet, email, or other?
    d. Are you checking/using any of these documents actively for port call? Which ones, and in what situations?
        i. pre-arrival
        ii. at berth
        iii. after departure
    e. Is there other ISPS related information shared from the shipping company/agent/vessel to the port? E.g. vessel ISSC certificate number and expiration date
    f. How is passenger information reported for an ISPS port call? Only numbers, or detailed lists?
    g. How is crew information reported to the port for an ISPS port call? Only number, or detailed lists?
        i. crew on board
        ii. crew changes
    h. How is dangerous cargo information documented and what are the procedures related to it?
        i. pre-arrival
        ii. at berth
        iii. after departure

iv. Do you communicate with any authorities related to dangerous cargo? Who, how and when?

2. Confirmation of quay request
    a. What do you check prior to confirmation of a quay request to an ISPS quay?
    b. How do you confirm the requested quay to the shipping company/agent?
        i. Via SafeSeaNet, email, phone, other?
    c. Does the port give any information to the vessel about the ISPS quay pre-arrival, e.g. instructions to the ship security officer (SSO)/captain/crew?
3. Before arrival
    a. Do you perform any routines prior to the arrival? E.g. check lists, securing the area
        i. How many hours prior to the arrival?
        ii. What is the routine?
        iii. What documents/ICT systems are in use?
4. During the port call
    a. Is there any communication between port and vessel related to ISPS during the port call?
5. After the port call
    a. Is there any communication between port and vessel related to ISPS at or after the departure?
6. ISPS roles
    a. Which roles in the port are dealing with the ISPS related documents and routines?
7. Pain points
    a. Have you identified any pain points in today's processes?
    b. Anything that is cumbersome and time-consuming?
    c. Do you see possibilities for making the ISPS process more efficient?
    d. Do you see any showstoppers for automatic handling of the ISPS process?

A.2. Cargo Clearance

This section is mainly relevant for ports that incorporates terminal services (Cargo transit services) as a part of their responsibility and organisation.

We are also in the process of gathering insights from stakeholders in the cargo clearance process and need to validate some of the process documents that have been created in this regard. This is also still incomplete, and this questionnaire will help us validate and/or extend this information.

1. Before arrival

   a. What documents related to customs clearance are you obliged to exchange with other stakeholders / parties before arriving with cargo?
      i. Exchange with the shipping company
      ii. Exchange with customs authorities
      iii. Exchange with consignee
   b. How do you exchange these documents? E.g. through a national Single Window portal, through agents etc.

2. During the port call
   a. What kind of information do you record during and shortly after discharging cargo from a vessel?
      i. Do you weigh containers? How?
      ii. Is it relevant to gather information regarding other anomalies for purposes related to the customs declaration process? (E.g. damages to a CCU compromising the cargo in a container)

3. After the port call
   a. Are you in any way liable in situations where there are remarks or dispute regarding status of the cargo during the customs declaration process? E.g. remarks or disputes regarding verified gross mass (VGM) documented in manifest versus that of the weighed VGM in the terminal upon discharge.
   b. If a is true, when does your liability end?
      i. E.g. does it end according to specific events or time schedules manifested in formal contractual agreements?
      ii. When is the inland carrier responsible for the cargo? As soon as it is loaded to the truck or when the truck has passed the gate?
   c. How do you know that the cargo is cleared by the customs authorities and ready for release? How is this communicated to you?
   d. What kind of documents / information do you exchange with other stakeholders / parties?

4. Pain points
   a. Have you identified any pain points in today’s processes?
   b. Anything that is cumbersome and time-consuming?
   c. Do you see possibilities for making the customs clearance process more efficient?
   d. Do you see any show-stoppers for automatic handling of the customs clearance process?

Annex B. Questionnaire to Shipping Companies

B.1. ISPS

We have started to document the process related to arrival of ISPS vessel, and getting an overview of documents in use and other routines. This is still incomplete, and this questionnaire will help is fill in the gap.

1. Quay requests and documents
    a. Do you make a quay request for a specific ISPS quay when planning a port call?
        i. How, via SafeSeaNet and/or email?
    b. Which ISPS related documents do you have to deliver to the Port and when? e.g. crew list, 10 last ports, dangerous cargo,…
        i. pre-arrival
        ii. at berth
        iii. after departure
    c. How do you deliver the documents? Via SafeSeaNet, email, or other?
    d. Are you getting any response from the Port related to these documents? Which ones, and in what situations?
        i. pre-arrival
        ii. at berth
        iii. after departure
    e. Do you share any other ISPS related information with the port? e.g. vessel ISSC certificate number and expiration date
    f. How do you report passenger information to the port for an ISPS port call (if relevant)? Only numbers, or detailed lists?
    g. How do you report crew information to the port for an ISPS port call? Only number, or detailed lists?
        i. crew on board
        ii. crew changes
    h. How do you report dangerous cargo information to the port? Do you get any response from the port related to this?
        i. pre-arrival
        ii. at berth
        iii. after departure
        iv. Do you communicate with any authorities related to dangerous cargo? Who, how and when?
2. Confirmation of quay request

   a. Do you get a response from the port to you quay request related to missing ISPS information?

   b. How do you get the confirmation for the quay request from the port?

      i. Via SafeSeaNet, email, phone, other?

   c. Does the port give any information to the vessel about the ISPS quay pre-arrival, e.g. instructions to the ship security officer (SSO)/captain/crew?

3. Before arrival

   a. Does the vessel perform any routines prior to the arrival related to ISPS?

      i. What is the routine?

      ii. What documents/ICT systems are in use?

4. During the port call

   a. Is there any communication between port and vessel related to ISPS during the port call?

5. After the port call

   a. Is there any communication between port and vessel related to ISPS at or after the departure?

6. ISPS Roles

   a. Which roles at the shipping company/agent/vessel are dealing with the ISPS related documents and routines?

7. Pain points

   a. Have you identified any pain points in today's processes?

   b. Anything that is cumbersome or time-consuming?

   c. Do you see possibilities for making the ISPS process more efficient

   d. Do you see any show-stoppers for automatic handling of the ISPS process?

B.2. Cargo Clearance

We are also in the process of gathering insights from stakeholders in the cargo clearance process and need to validate some of the process documents that have been created in this regard. This is also still incomplete, and this questionnaire will help us validate and/or extend this information.

1. Before arrival

   a. What documents related to customs clearance are you obliged to exchange with other stakeholders / parties before arriving with cargo?

      i. Exchange with the port

      ii. Exchange with the terminal

      iii. Exchange with customs authorities

iv. Exchange with consignee

b. How do you exchange these documents? E.g. through a national Single Window portal, through agents etc.

2. After the port call

   a. Are you in any way liable in situations where there are remarks or dispute regarding status of the cargo during the customs declaration process? E.g. remarks or disputes regarding VGM documented in manifest versus that of the weighed VGM in the terminal upon discharge.

   b. If a is true, when does your liability end? E.g. does it end according to specific events or time schedules manifested in formal contractual agreements?

3. Pain points

   a. Have you identified any pain points in today's processes?

   b. Anything that is cumbersome and time-consuming?

   c. Do you see possibilities for making the customs clearance process more efficient?

   d. Do you see any showstoppers for automatic handling of the customs clearance process?