CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING (CIISE)

INSE-6311, Summer 2022

Sustainable Infrastructure Planning and Management Systems

Project Report on

"Analysis of Automation in Ports and Terminals"

Submitted to: Professor Amin Hammad, Ph.D.

Submitted By:

Student ID	Name	Tasks Performed
40221227	Priya Meghana Raavi	Introduction, Case study- rotter dam port
40219221	Jagadeesh Bavineni	Port automation analysis and yard management
40195824	Pavan Koushik Nellore	Internet of things in ports
40189233	Sai Chandra Sekhar Reddy Dwarampudi	Automation in port transportation and logistics
40161606	Gokula Rani Vallabhu	Cybersecurity in ports
40203239	Manoj Narayana Katragadda	Case studies, Future Scope & conclusion

TABLE OF CONTENTS

List of Figures

List of Tables

ABSTRACT

In these modern times every country's economy, growth and development are completely dependent on coastal regions and more specifically on marine ports. Ports are the main exchange points for the trade of daily commodities that a country is dependent on. With the advancement of technology, A lot of ports and container terminals around the world are moving towards automation. While automation of the ports can reduce the operating costs and improve the overall performance of the terminal, automating the conventional way of doing things can bring a lot of challenges, for example, the establishment of a fully automated port requires a completely different terminal layout than a traditional operating one, which will be a huge financial burden to the port authorities and interaction of all the automated systems can bring a lot of integration loopholes too. This report provides an overview of the current state of automation in ports, Port automation analysis and yard management, examines how Internet of Things (IOT) can be used for automating the port, explores the technical and security challenges of port automation. This report briefly examines case studies of ports which have implemented the innovative technologies and discusses the future of port automation.

1. INTRODUCTION

Automation is currently applied in a broad spectrum of activities in shipping and transportation. The development of autonomous ships in a commercial and military operations is already underway. The future also sees new uses of computer-controlled robot arms and unmanned air vehicles, which are increasingly used in many industrial and military fields. Automation has proved itself as a powerful tool for increasing efficiency and productivity in all areas of transportation, cargo handling, and shipbuilding. The purpose of the first part of this study is to review and provide an overview of the existing automation solutions and how they have been implemented in ports and terminals around the world. The study reviews a variety of topics related to automation in ports and terminals, including modern technologies, the role of computers in the field of automation, the level of automation, control systems, automation systems, the potential for further developments, security threats and future opportunities [1].

An attempt has been made to identify potential applications of automation in ports and terminals. The potential uses of computer-controlled automation systems include improving the working environment, enhancing the quality of service, reducing human exposure to hazards, streamlining processes and systems, improving safety, and achieving more effective and efficient use of energy. Although many of these possibilities are already realized in individual ports and terminals, more advanced technologies are under development and will significantly improve the efficiency of maritime operations [2].

Since the beginning of navigation, the ports, and terminals that facilitated the exchange of goods and people have played a vital role in the globalization of society. At the beginning of the 20th century, a shipping line could have a fleet of around 100 vessels, but now, even a single container ship can have several hundreds of containers. To continue with the process of globalization, the world's ports, terminals, and shipyards must continue to develop and evolve. This requires an improved understanding of the ports and terminals to develop efficient and effective methods of logistics that ensure that the global economy is as efficient as possible. To be more precise, technology and automation are playing an increasingly key role in the development and improvement of maritime commerce and the shipping industry [3].

Over the last decade, computers and automation have become increasingly applied in all areas of transportation, including port and terminal operations, warehousing, ocean freight, and air transport. Autonomous navigation (semi-autonomous and autonomous operations) is already taking place on both ships and aircraft. Autonomous vehicles are under development in several industries and are

used for military purposes in the field of surveillance, transportation, and event logistics. The use of robots is continuously increasing, especially in the field of industrial automation [4].

Port and terminal automation is a modern business model. The need for the rapid introduction of new business models is created by continuous dynamic changes in the global economy. The main factor that significantly contributes to the development of new business models is the continuous growth of the shipping trade. The shipping market is characterized by the diversity of vessels and a wide variety of cargo. According to several sources, there are about 30 million vessels in the world that carry about half of the world's trade. The total value of cargo shipped by ships accounts for about 40 percent of the world's trade. Therefore, shipping accounts for a major part of international trade and the leading part of the world economy [5].

Automated ports are also characterized by the variety of technologies used in different facilities. The range of technologies includes fully automated terminals and automated ports. The introduction of automation to ports and terminals has led to the development of new concepts. The new port and terminal business models are based on a greater level of cooperation, higher volumes, and larger throughputs. The increased volume of the port and terminal activity makes it necessary to optimize the utilization of the available resources. This is necessary because the increase in volumes requires the development of new terminals that will provide enough capacity to handle the ever-increasing volumes of cargo and vessels. The increase in the volumes of traffic also requires the development of terminals that can be used to handle both containers and bulk cargo. Furthermore, the increase in traffic volume and the range of containers requires the use of technology that will allow faster and safer procedures for unloading and loading [1].

In the present day, the introduction of automated and unmanned ports has become a widespread trend. The main factors in favour of the introduction of automation in ports and terminals are:

A) The growth of containerization and the development of innovative technologies.
B) The increase in volumes of cargo and containerized trade.
C) The use of containerization and the introduction of innovative technologies (automation) [6].

Ports and terminals are also characterized by a diverse range of operations and technologies. Automation will allow port operators to drastically cut operator burden and the amount of person-hours spent on port and terminal operations. This will aid in the improvement of working conditions and the protection of employees. Furthermore, the implementation of automation will provide an opportunity to improve port and terminal safety. The implementation of automation in ports and terminals will allow operators to boost their productivity dramatically. Automation will contribute to

the restructuring of the port and terminal operation's organisation, in addition to greater efficiency. As a result, available resources will be better utilised, and operators will have the potential to grow their volume of business. [2].

Operators will be able to greatly boost their throughputs thanks to automation. As a result, better operational methods will be developed, and existing technologies will be better utilised. Finally, the implementation of automation will aid in the creation of novel technologies. Terminal automation is an innovative business approach that will appeal to potential customers. The terminal owners or terminal operators are potential customers of automated terminals. Automated terminals will allow terminals to be used more efficiently. Additionally, terminal owners will be able to expand their activities and improve their business volumes by using automated terminals. [7].

1.1 Port and Terminal Automation

Port and terminal automation are computer and communication technology-based facilities. A terminal automation system can significantly improve efficiency and safety, reduce operating costs, and ensure security in a terminal or port. However, a well-designed, mature, and well-implemented automation system can mitigate the potential for incidents.

In the traditional ports, it was particularly important that the ship crew, and in most cases, their entire crew, was fully occupied in handling the vessels and containers. With the development of technology, containerization, and globalization, it became possible to have one, or in some cases, two teams of workers who would assist the ship crew in the process of handling the cargo. This process usually includes the manual stacking of containers, the processing of entries into the container, the processing of cargo into ships, the processing of documents, and the storage of goods for loading into the vessel. These procedures could often be performed by teams of operators with little or no supervision. However, to achieve greater efficiency, it is necessary to have a supervisor who could oversee the entire process. in the shipping industry [1].

Automation in the traditional port started with the development of the automatic container crane. Although it is still a challenge to maintain a 100% reliability rate for container cranes, it is expected that shortly the container crane will have a 100% automation rate. The automation of container cranes will probably enable the increase in safety by reducing the operator workload and increasing the safety of container cranes in port operations. Container cranes are used to stack containers and move them to the containers that will be loaded into the vessel. Containers are usually stacked in such a way that they are vertically aligned along the side of the ship. This means that the height of the container stacks depends on the width of the ship [2].

The second part of automation in the traditional port is related to the handling of containers. Because the height of container stacks depends on the width of the ship, the handling of containers is a very time-consuming process. The first attempts to automate container handling were made in the early 1980s. The main objective of those first attempts was to reduce the time needed to unload and load containers onto trucks. This could be done by automatically moving the containers to trucks and vice-versa. Although the automation of container handling has significantly reduced the manual labour, the process was never completely automated, and manual labour is still required to move the containers into the containers on the ship, move the containers out of the trucks onto the rail yard and store them in the container yard. Container cranes used to stack and move containers are often referred to as automated container cranes. These cranes are used to move the containers onto and off the ships. Since they cannot move any containers that are on the ship, the automation of container cranes requires the automation of containers as well [4].

The latest automation in the traditional port is mainly related to the introduction of innovative technologies. For example, some port terminals, such as Korean ports, have already introduced fully automatic terminals for container handling, but to achieve this goal, the container cranes must be automated. Also, the fully automated terminals will reduce the manual labour involved in the container handling process. Containers will only be handled by automated cranes. The automation of containers also creates opportunities for the automation of cargo processing and the storage of containers. This is because most cargo in ports is containerized, and with the recent introduction of fully automated container cranes, the process of container handling and storage will remain fully automated [5].

Automation is also applied in many other areas of transportation, including container handling, port operations, and air traffic control. In container handling, the only areas where automation is not applied are stacking and the handling of individual containers. The main reason for this is the physical distance of the containers and the fact that the container cranes can only move containers at an extremely low speed, which is not enough for automated container handling. Other areas that could benefit from automation are air traffic control, container cranes, and other types of transport systems. The automation of container cranes is more time-consuming since they require the automation of containers as well. This is not a problem for fully automated terminals, but the automation of other container handling systems requires the automation of container cranes [1].

Concerning the development of automation in the container industry, container cranes are probably the most advanced systems in the field of automation. However, there are many other areas of the container industry that could benefit from the automation of container handling. For example, the development of automated docks, automated containers, fully automated container yard storage, and

warehousing, automated terminals, container storage, and transport systems, semi-automated terminals, fully automated container yard storage, and transportation, and automated containers are examples of the areas of the container industry that require the development of technology [2].

Automation in ports and terminals could be seen as a part of the broader automation trend that is observed in almost all industrial sectors. The recent growth of the service sector and the fact that manufacturing has become increasingly digitized are contributing to the ongoing spread of automation. In addition, the development of low-cost robotics is enabling the use of such technology in many sectors. These two factors together make a significant contribution to the trend of automation [1]

The port sector, for its part, has been an early adopter of automation. This is, at least in part, because ports have a relatively unique and distinctive position in the transport sector. Two key areas contribute to this: firstly, ports must operate with little capacity for spare parts or extra crew, so they are constantly required to be on the lookout for new and innovative technologies. This is further compounded by the fact that they are an intermodal transport hub, meaning that they serve as an interchange point for goods going in and out of the country. Therefore, when a new transport technology comes along, it is important to check that the impact on its business model and operations is not negative [2].

The growth of the port sector and the development of automation, which includes the use of the latest innovations in robotics, also provide an opportunity for a whole new sector to develop. This can be beneficial for several reasons. The port sector and the port administration are heavily dependent on port and terminal automation. So, if the port industry becomes more automated, it will allow the port sector to use its automation more effectively, which means it can save money and it could potentially allow other sectors to expand as well [4].

Automation in port operations is having a disruptive effect on many areas of port activity, such as labour, scheduling, and the management of ships and port terminals. Transportation workers, as stakeholders, are often affected by the changes taking place in port operations and may be required to take on additional duties

The Role of Computers in The Field of Automation

In general, automation is a process in which the human is removed from some part of the process to achieve greater efficiency, productivity, and quality. By eliminating manual labour, it is possible to increase the speed and efficiency of the process. The increase in the speed and efficiency of the processes is always a challenge to the operator of the process. In ports, the first opportunity for automation is in the operation of the crane. The traditional cranes were operated by human operators,

who could manually control the movement of the container cranes and operate the winch. Because human operators were very mobile, it was a challenge to supervise them and ensure that they operated safely. The development of automated cranes (both in the traditional and semi-automated versions) removed this problem and ensured a safer operation. This development led to an improvement in the productivity and quality of the operations in port terminals. The increase in the speed and the efficiency of the process has increased the automation of the traditional port terminals [6]

Another area of automation is the introduction of innovative technologies into port operations. One of the main obstacles to the introduction of innovative technologies in port operations is the cost of introducing innovative technologies. It is not possible to introduce innovative technologies without affecting the existing system. This process may affect the cost, performance, and quality of the existing system. In most cases, it is possible to introduce innovative technologies by reducing the amount of manual labour in the existing process. With the automation of container cranes, the amount of manual labour required to stack, move, and store containers could be significantly reduced. In the case of other areas of automation, it is important to develop a process and design that reduces the amount of manual labour required in the existing process [3]

1.2 Automation Process

The automation process is a multiphase process. The ports or terminals use a port and terminal design framework to develop an automation system. The port and terminal design framework include the following components:

- **Design Process**: The design process requires the development of the conceptual automation system and the specification of design constraints [7].
- **Constraint Checking Process:** Constraint checking processes ensure that automation systems comply with the design criteria [8].
- **Installation Process:** The installation process involves the installation and testing of the automation system and its associated controls.
- **Monitoring And Maintenance Process:** The monitoring and maintenance process includes the monitoring, maintenance, and optimization of the automation system [10].

1.2.1 Elements

The automation system consists of the following elements:

1. **Control Systems:** The control systems perform a generous portion of the automation operations. These operations can be described as tasks. For example, the control system can transfer containers from a warehouse to a cargo hold [5].
2. **Computer Workstations:** The computer workstations communicate with the control system and allow the human operators to perform tasks [7].
3. **Interface Devices:** The interface devices enable human operators to perform control functions. For example, the interface device can be a human-machine interface device.
4. **Peripherals:** The peripherals allow the operators to view, process, and interpret data. For example, the operator can view the status of the automation system [9].
5. **Tables And Other Equipment:** The tables and other equipment support human operators. For example, the operator can load and unload goods from containers [10].

1.2.2 Automation System Design

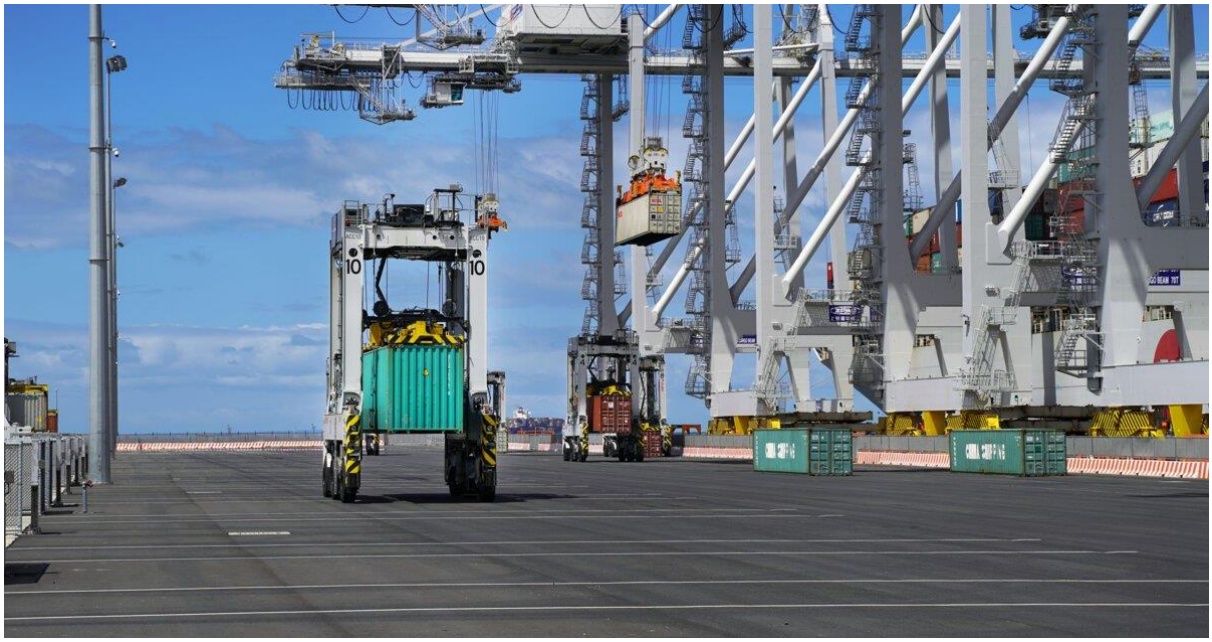

Figure 1: Automated Stacking [10]

The port and terminal design framework helps port and terminal authorities develop a conceptual automation system and the specifications for the systems. The conceptual automation system provides a high-level specification of the functions and the structure of the automation systems. The port and terminal design framework must meet certain design criteria. Design criteria include the following components:

- **Safety-Related Criteria**: The design criteria for safety-related criteria include the design standards for ports and terminals [8].

- **Performance Criteria:** The performance criteria include the design standards for port and terminal automation.
- **Reliability Criteria:** The reliability criteria include the design standards for automated ports and terminals [2].
- **Security Criteria:** The security criteria include the design standards for port and terminal automation [4].

1.3 Automation Levels

The port and terminal automation industry is already one of the most important industries in many economies and is expected to increase in importance in the coming decades as container volumes and trade volumes increase, with a consequent demand for efficiency, reliability, safety, and connectivity. The port and terminal automation industry is already one of the most important industries in many economies and is expected to increase in importance in the coming decades as container volumes and trade volumes increase, with a consequent demand for efficiency, reliability, safety, and connectivity. It is also an area in which technology and innovation play a key role, as technologies such as IoT, robots, drones, and autonomous vehicles are increasingly common in the economy at large. In addition, the industry is a major employer, providing employment for many thousands of people around the world. Therefore, the automation of ports and terminals is of great interest, both for the port and terminal operators themselves, and for companies that want to access the ports and terminals for trading and other activities, including transport, logistics, and related industries.

The various levels of automation in ports and terminals are described below: [3].

- **Level 0: Manual Tasks**

The automation level has no robots or automation whatsoever. Level 0 refers to tasks where human input is needed for the most part. It may also be used in cases where automation is impractical because of the complexity of the task. Examples include the loading and unloading of ships, the hand-stowing of containers, or the unloading and stacking of trucks [5].

- **Level 1: Some Automation**

Tasks such as the stacking of containers, hand-stowing of containers, and dock crane operation all fall within level 1 automation. These are tasks where the machine performs only a limited part of the task. There is more automation for level 1 than for level 0, as it involves human intervention. This is likely to be the case in the short- to medium-term, as the automation levels increase. However, it is expected that the number of tasks within level 1 automation will decrease, with the most common

tasks for level 1 automation likely to be tasks that were previously carried out by level 0 automation. For example, the robots that perform dock crane operations are often used in manual tasks such as loading and unloading of ships, although these are not considered to be automated tasks [2].

- **Level 2: High Automation**

  Level 2 refers to automation where some or all of the task is automated. Tasks that require level 2 automation include handling containers by robots. This automation may occur before loading and unloading ships or unloading and stacking trucks. It may also occur at warehouses and other locations in port and terminal operations and can be used in the loading and unloading of trucks, trains, or planes. Tasks that require level 2 automation include:

  Handling of containers by robots – the robots that handle and load/unload containers are often used in level 0 tasks such as loading and unloading ships and trucks. The robots that do this do not necessarily require human intervention, as they often follow pre-programmed paths. However, their work is not necessarily 'automatic' in the sense that it is undertaken without any human input [6].

  Robot-assisted automation – the use of robots to assist with manual tasks. For example, a person may perform the handling of containers and pallets manually, but a robot may assist with the work. Robots may also be used for the loading and unloading of ships or trucks [8].

  Robot-driven automation – the use of robots to perform work that was previously performed by humans. In some cases, this work is not even required, as it is done automatically, for example, in the loading and unloading of trains.

- **Level 3: Complex Automation (Multiple Robots and Other Forms of Automation)**

  Level 3 refers to automation where multiple robots and other forms of automation work together to carry out the task. Robots and automation use AI and machine learning to ensure that the task is performed safely and efficiently. The use of multiple robots and automation is likely to increase in coming years and is more likely to occur in the short- to medium-term, as the development of multiple diverse types of robots and automation becomes increasingly feasible. It is important to note that many 'automation machines' are not always level 3 automation, as tasks may be carried out manually with the occasional use of robots [1].

1.4 Automation Process Risks, Challenges and Advantages

1.4.1 Automation Process Risks

Automation systems may fail due to a variety of reasons. These reasons can include system software and hardware defects, human error, cybersecurity, or mismanagement.

A failure or malfunction in the automation system can cause a human operator to be at risk [6].

An accident can occur in a port or terminal. An automation system is designed to improve the performance, safety, and security of a terminal or port. However, the automation system cannot eliminate all the potential for accidents in ports and terminals [1].

1.4.2 Automation Process Challenges

The automation process has significant challenges. The automation system must be designed to mitigate the potential for potential accidents in terminals and ports. The design of the automation system should consider the following components.

The design standards for the human-machine interface include the design standards for the interaction of the automation system and the human-machine interface. For example, if an automation system uses an offline interface device, the human-machine interface should allow for the use of the device. The automation system must also comply with the design standards for other human-machine interface devices [7].

The automation system must comply with the design standards for port and terminal security. The safety standards may include the design standards for safety-related components of the automation system. These components include the human-machine interface. The automation system must meet the design standards for performance in the port and terminal. For example, the performance standards must ensure that the automation system can perform the required functions [3].

The automation system must comply with the design standards for reliability in the port and terminal. The reliability standards include the design standards for the components of the automation system. These components include the human-machine interface [10].

The human-machine interface must provide high data security. The design standards for the human-machine interface must include the human-machine interface security standards. The human-machine interface should also comply with the design standards for the human factors of the human-machine interface. The security standards may include the design standards for the human factors of the human-machine interface. For example, the design standards for security should ensure that the human factors of the human-machine interface are reliable and that they provide a safe and secure interface for the operators of the terminal and the automation system [8].

The automation system must comply with the design standards for security in the port and terminal. The security standards may include the design standards for the design of the automation system and

the human-machine interface. The security standards may also include the design standards for the human-machine interface.

The human-machine interface design standards should support the design criteria for the human-machine interface. For example, the design standards for the human-machine interface should also comply with the design standards for security.

1.4.3 Advantages of Automation:

- Automatic control of the whole or part of the port process means that fewer people are required to take care of processes, equipment, and workflows.
- The use of automatic control can contribute to the creation of increasingly efficient equipment, which allows reducing the cost of equipment purchase and installation and reduces personnel expenses [2].
- The implementation of automation in terminals allows for reducing the risks associated with the human factor. In the case of accidents, they are not directly related to the human factor, but to the operation of equipment [7].
- It is difficult to say exactly when automation is applied in ports and terminals. Automation is used in a lot of container terminals as well as general cargo terminals.

1.5 Economic considerations

For large vessels, the total costs of both the capital and operating costs are a much smaller proportion of the cost of the cargo than for smaller ones. The operating costs for smaller ships are also proportionally higher.

Thus, smaller vessels benefit more from the use of automated machinery than large ones, but the increase in capital costs for the larger ships is more than offset by the benefits. Even so, automation does not make it necessary to lower the rate of automation.

Another example of the benefits of automation is that it becomes possible to load vessels with containers that could not be loaded in a reasonable amount of time otherwise. In the case of the container vessels, it has become possible to load containers weighing two tons, and with a standard capacity of containers (20 ft by 8 ft by 8 ft, or a volume of 5,880 cubic feet). At present, it takes a human being about 10 minutes to load a typical container ship with a cargo of standard 20-foot containers [4].

It takes only about 20 minutes to load a container ship with a cargo of 2-ton containers. This is still a small portion of the total amount of time required to load a large cargo vessel, however, and many other container ships that have more space (or less to load) could be automated. In fact, in the ports,

in the main, two-thirds of the time is spent taking up space in the container and moving the containers to the final location. It would be possible to automate the whole of this part of the work if necessary [1].

For larger ships, the benefits are considerable. The use of the machine can reduce the crew from 20 to 10, and a reduction of the load of about 10% is possible, saving 5% of the cost of the cargo. The capital costs will therefore be higher, but only by an additional 1-3% (that is, 0.5-1.5% of the cargo value), for the first 10% of the fleet. Similarly, for passenger ships, there will be a similar effect of increasing the automation rate, but in this case, it is not possible to increase the number of passengers loading or unloading because of the space constraints [7].

1.6 Key Characteristics

The key characteristics of automated port terminals are as follows:

- Containers can be stored, loaded, and unloaded at a terminal at specific time intervals. This means that no container will be left to wait around for any length of time before being loaded, hence an overall increase in productivity.
- An increase in production as it is a fast and cost-effective method of managing containers. Container storage can be monitored by the operator and the system can alert the operator when a container is about to be removed.
- Increased security levels as access to containers can be restricted by the operator to only authorized personnel [4].
- A variety of technologies can be implemented in a single automated port terminal to ensure that it can operate continuously without any disruption.
- The container terminal can be monitored from any location and hence any potential problem can be detected immediately [1].
- Container handling and storage are more flexible as an automated terminal allow access to/from almost all areas of the container terminal.

2. PORT AUTOMATION ANALYSIS & YARD MANAGEMENT

2.1 Types of automated ports:

After the commissioning of the ECT Delta Terminal in the Port of Rotterdam in 1993, the phrase "automated terminal" was coined to describe the terminal's activities relating to yard operations, storage facilities, and quay–patio interconnection. The terminals are categorised as automated, semiautomated, or manual depending on the degree of automation of the primary movements (yard, dockyard). A semiautomated terminal is one that has automated storage or connectivity equipment. However, the word "semi automatization" can refer to the administration of equipment by supported control or the systematisation of certain of the equipment's tasks through minimal or partial automation [12]. The below image shows all the automated and semi-automated ports in the world.

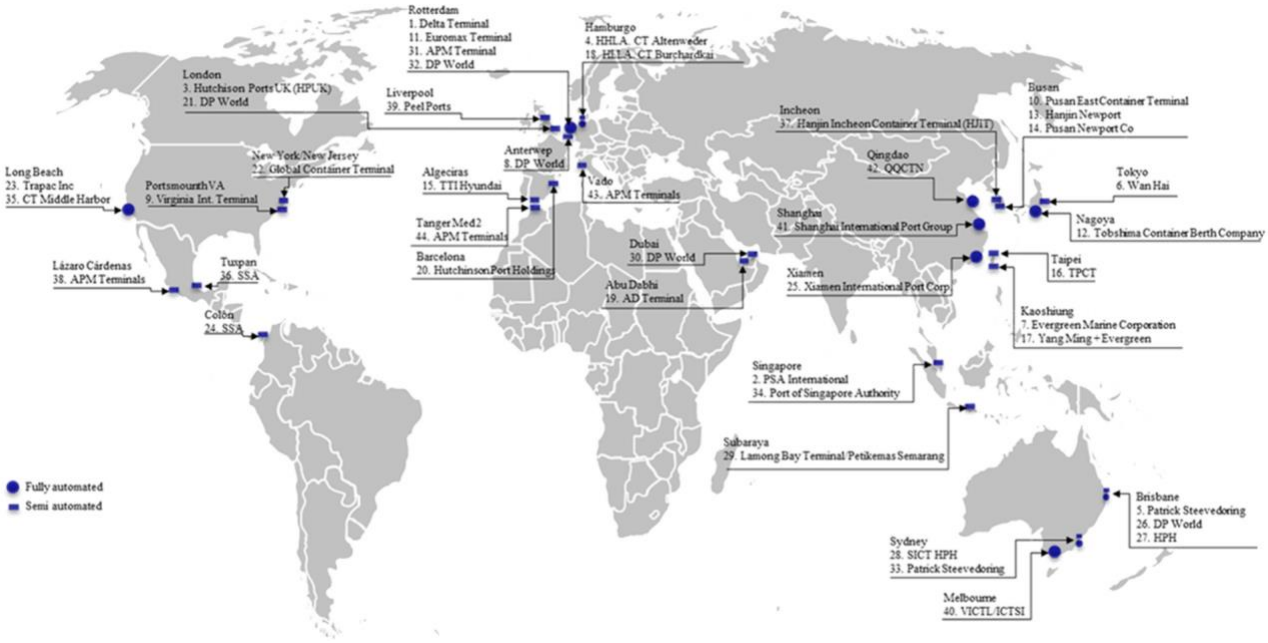

Figure 2 : Automated and semi-automated ports around the world [12]

2.2 Trends in port container terminal automation

Automation in ports is a complex process which involves bringing all the sub systems of the port and container terminals to work together. In order to proceed with this level of complexion in automation we need to consider the whole workflow instead of the of the individual components involved in it, so a proper analysis and planning is required. Ana, Martin et al, [11] suggested a model of automation implementation in ports:

In general, this broader development encompasses: Gate automation; Yard automation; and the automation of dock cranes. In reality, the most advanced automation systems on the market today

are based on the earliest automations developed in PCTs (port container terminal) are those that have to do with the processes that occur at the terminal gates. Efforts are still being made in this regard. In the terminal-logistics chain interface, improvements of data collection systems are the best example for this. The desire to automate data collection is growing. Inland and maritime gates are both frequent in data collection, though the former captures more data due to its larger size. Secondly, the yard automation. The most visible and evident trend in PCTs is yard automation. As a result, these terminals with fully or partially automated yard movements are referred to as automated or semi-automated terminals, respectively. The automated technology of storage and transfer equipment is identical, and it automates the inventory of the yard's stock of containers as well as real-time equipment monitoring. It is progressing toward the development of handling systems that are increasingly self-sufficient in terms of operation and cost. Finally, automation of dock cranes, these are the operational elements with the least developed automation, despite the fact that they are expected to be the equipment with the most technical advancement in the coming years. To date, efforts to automate quay cranes have resulted in limited automations that, when applied in factories at the time of manufacture or retrofitted, can mechanise some of the duties that previously relied on crane operators' ability.

2.3. Functional approach for automation

The automation solutions designed for the PCTs (port container terminals) usually concentrates from a systematic point of view and detailing the practical parts of systems and their primary responsibilities, as well as their interfaces and interconnections. This systematic approach, on the other hand, limits the design of solutions and hinders terminal operational departments, who are thought to be the primary users of such solutions, from comprehending how they fit into the PCT's operations. A methodology for the automation of PCTs is proposed to circumvent this problem as a state-of-the-art advance [11]. It takes a functional approach to process automation and re-engineering as a work discipline and applies it to the problem at the same time. This combination provides a detailed and integrated view of PCT operational problems, detecting bottlenecks and identifying improvement ideas, allowing the solution formulation process to be thorough and adaptable to real-world operational needs, as well as expandable to other possible improvements unrelated to automation.

The functional approach of automation addresses the goal of removing the human intervention in port operations. [11] Human resources are involved in three aspects of operations: (1) the physical movement of containers through facilities; (2) the corresponding information flow; and (3) the planning and management of operations. So, the automation of ports should concentrate on (1) the

automation of the container handling, (2) the automation of information flows or (3) the automation of the decision-making process.

The automation of handling tasks entails lowering the intervention of equipment operators in handling movements, allowing infrastructure and equipment to become more autonomous. Even if it is not totally eliminated, modest equipment automation brings aid systems for handling activities, enhancing productivity and operational safety and security. In terms of information flow automation, this is based on the use of interface, communications, and information management software systems to reduce human resources in the acquisition, transmission, and administration of information processes that allow for activities to be carried out. The automation of information flows in real-time information systems necessitates an innovative approach to managing PCTs, one that is based on reliable and timely data, removing uncertainty in response times, and allowing for decisions that are in sync with the operations being carried out at any given time. Finally, automation of the decision-making process entails removing human intervention and the human aspect from the strategic, tactical, and operational planning processes. To do this, software tools that work with the TOS must be implemented, as well as decision rules at the planning and management levels of operations, as well as mechanisms to handle exceptions. Mathematical algorithms or simulation-emulation techniques can be used to define these criteria. In any case, it is worth noting that a PCT with partially automated equipment can work with manual information flows, and vice versa. Similarly, the level of automation of the decision-making mechanism may be unrelated to the extent of automation of equipment or data flows.

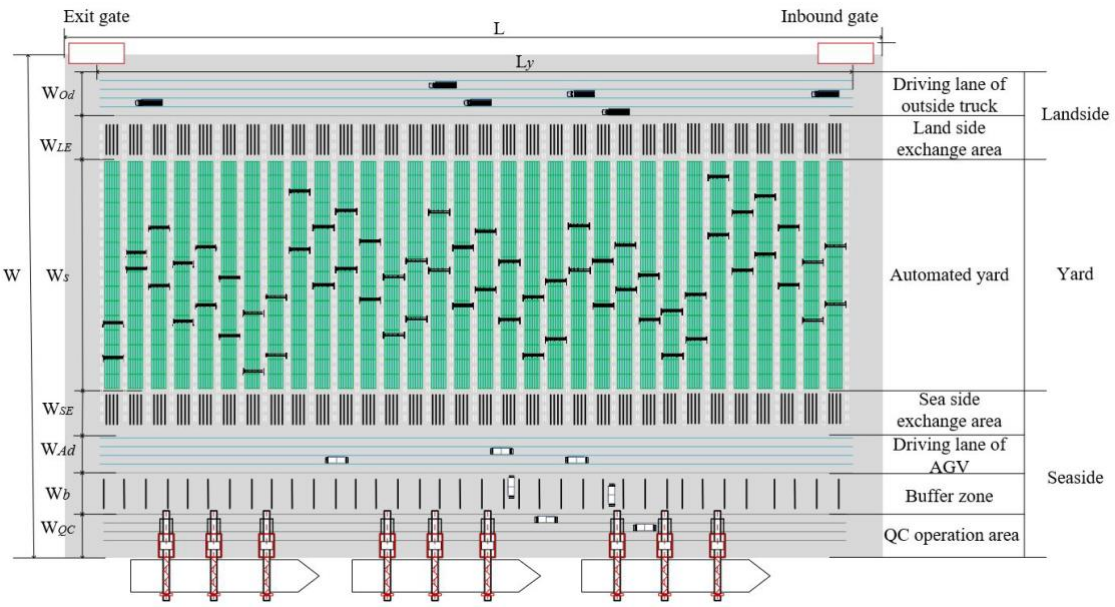

Figure 3: Layout of typical automated container terminals [19]

Orive and Santiago et al.,[12] proposed the implementation of the port with a different approach with a model called BOT analysis (Business observation tool). The concept is based on the creation of four key scenarios: Motivations and Capacities (resources) to advance, Establishment of the working group, Characterize and understand the development environment, and Macro-environment analysis, it enables the establishment of the current scenario on which to operate in order to ensure proper port terminal implementation, taking into account both micro and macro environmental factors. BOT is a tool that is frequently utilised in the business world, but it can be used to any industry if the BOT approach is followed appropriately. As a result, it can be used in the port sector when terminal operators decide to automate (to a greater or lesser extent) their terminals.

The results of Orive and Santiago et al., summarise the following with respect to the previously

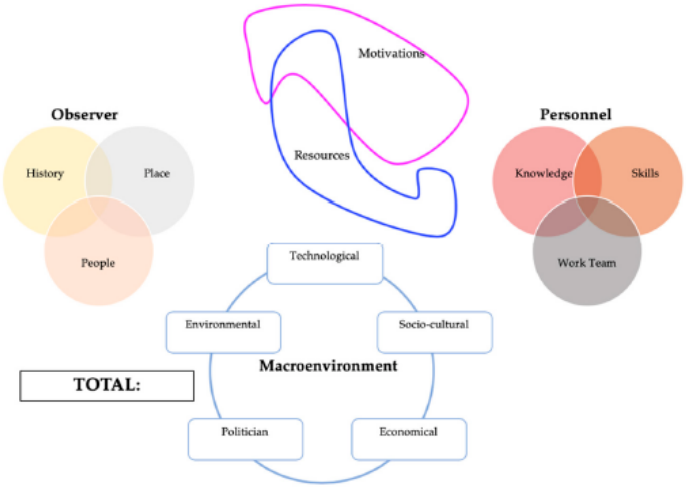

Figure 4: Business observation tool (BOT) analysis [12]

mentioned four key scenarios Ports are subject to new sustainability, financial, safety, and efficiency regulations. They must grow and advance towards the notion of Port 4.0 in order to meet these needs and sustain their competitiveness. The benefits achieved from this process, such as a reduction in operating costs (OPEX), primarily leads to a decrease in the workforce, an increase in terminal safety, as well as environmental benefits, since these are terminals with a greater density of containers that produce effective use of space and operate with less electrical equipment, motivate the automation of port terminals. Institutional support, as well as the desire of the Port Operators and national and international entities required to implement, are available to carry out the automating of the procedures. With regard to the establishment of the working group, the success of the objectives depends on the participation of a large number of agents, both public and private, in the fluidity of data transfer between them, as well as the processing and treatment of this data. Because the staff do not have the appropriate qualifications and expertise for the new technical advancements, a reconversion of the workforce network is required. Results of Characterizing and Understanding the Development Environment states that the transformation from smart ports to ports 4.0 (Ports that are

connected and have an elevated level of digitization and sensorization) demands increased transparency and collaboration between the concerned agents and begins with accepting and internalising the necessity for change and regeneration. Macro-environment Analysis concludes that the vitality of the technological industry necessitates the creation of operational mechanisms that allow for the incorporation of new instruments and adaptation to new research advances, such as the incorporation of autonomous ships. Socio-cultural aspects, the automation of terminals produces a social tension in a sector with a strong trade union presence, as it indicates a reduction in the traditional required worker force.

2.4 Yard management in automated Port container terminals

As it connects the berth and the hinterland, the storage yard plays a significant role in the overall performance of the container terminal, acting as a buffer for storing containers.

Yard space management can be separated into four sub-problems for conventional container terminals, including storage strategy design, storage space allocation, location assignment, and re-marshalling. Most of the current research methods regarding Container terminal talks about the block layout when maximising yard space, storage techniques for allocating containers, and re-marshalling handling that result in additional expenses. So, our main focus in this analysis is on yard layout, storage strategy planning, Re-Marshalling [13].

2.4.1 Yard Layout

The yard plan serves as the framework for managing and scheduling equipment. Appropriate and optimal yard plan is vital not only for increasing yard area utilisation, but also for facilitating interaction between different sub-systems. The effect of yard layout and automation on container terminal performance is proven by a simulation model, as proposed by Liu et al. [14].

Abbreviation
QC (Quay Crane)
AQC (Automated Quay Crane)
A-SHC (Automated SHuttle Carrier)
IT (Internal Truck)
AGV (Automated Guided Vehicles)
IAV (Intelligent and Autonomous Vehicle)
ALV (Automated Lifting Vehicle)
SC (Straddle Carrier)
ASC (Automated Straddle Carrier)
YC (Yard Crane)
AYC (Automated Yard Cranes)
RMG (Rail-Mounted Gantry cranes)
ARMG (Automated Rail-Mounted Gantry cranes)
ARTG (Automated Rubber Tyre Gantry)
RTG (Rubber Tyre Gantry)
XT (eXternal Truck)

Figure 5: Main equipment used in automated container terminals [13]

The performance of parallel and perpendicular layouts with and without automation activities is compared in their study. The research has shown that, when compared to manual processes, the use of AGVs can significantly increase the terminal's throughput. Meanwhile, the research demonstrates that for the same number of AGVs, a perpendicular layout has a higher throughput than a parallel layout.

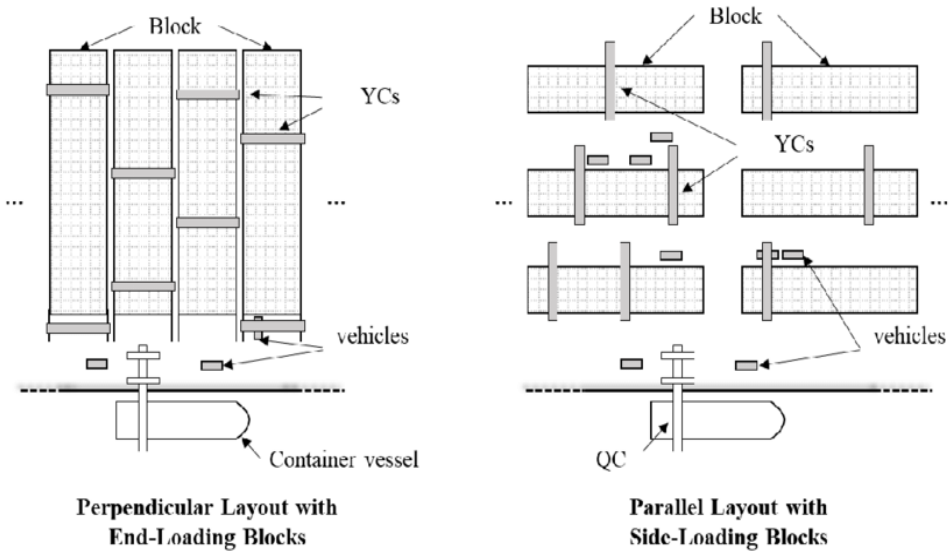

Figure 6: perpendicular and parallel yard layouts [16]

The key benefits of this layout are that horizontal transportation equipment's running distance is considerably reduced, and the number of horizontal transport vehicles in the ACT is reduced.

A lot of study has been done on the classic yard plan based on Straddle Carriers (SCs), Rail-Mounted Gantry (RMG) cranes, and Rubber-Tired Gantry (RTG) cranes for traditional container terminals. However, current ACT yard layout research is focused on a more practical discussion rather than the implementation of next-generation technologies.[15] The majority of automation equipment used in current ACTs has been converted from traditional equipment to automated control systems. As a result, for most ACTs with AQC+ARMG+AGV, AQC+ARMG+A-SHC modes, the standard yard arrangement has proven to be suitable. Current talks on yard layout in ACT are mostly focused on horizontal growth (additional bays) and horizontal orientation (parallel or perpendicular), rather than vertical expansion, in order to determine the appropriate layout for ACTs in operation (higher tier, etc.).

2.4.2 Storage Strategy Planning

The storage strategy is a set of criteria for managing yard space, with each export (import) container's allocation calculated by taking into account the operations of all linked equipment. Ku et al. [17] presented an optimisation model called the weekly yard templates, as a standard storage planning

technique for ACT. Because the liners consistently call for every week, the yard's allocation requirement is predictable. As a result, the weekly yard template, which is made up of sequential bays (ranges), is effective in terms of space management. The primary uncertainty impacting yard management, however, is the unpredictable vessel arrival, which constantly generates traffic congestion and re-handles. Ku et al. [17] suggest a more resilient yard template planning for ACT, where the storage strategy is easy to adjust when uncertainty arises.

[13] To locate each incoming container, a dynamic change of container stacking policy is made. Due to the perpendicular layout, containers from the same group do not have to be assigned to adjacent bays. Rather, the AYCs' moving speed during loading and unloading is a greater concern for stacking. propose the space allocation method for three different segregation strategies for the inbound containers. Their research reveal that the non-segregation strategy is more suitable for a congested terminal, which is efficient in reducing the possible re-handles. The most significant goal of the storage strategy planning for ACT is to reduce additional movement, same as it is for regular container terminals. As a result, numerous researchers have looked into the re-marshalling problem in the ACT yard, as follows.

2.4.3 Re-Marshalling

Due to the uncertainty of vessel arrival, it is possible that the order of container picking up is not consistent with the beginning stacking position, necessitating re-marshalling. Since import and export containers are always held in separate blocks at typical container terminals, most terminal managers prefer to concentrate on synchronising space management with yard crane planning to prevent re-marshalling and lower the expense associated with it. Although the import and export containers are mixed and kept in the same block, the normal perpendicular yard management of ACT requires the yard cranes to transfer the import or export containers from the end of the block to a handshake area and re-marshal afterwards for the loading or retrieving [13].

Choe et al. [18] suggest using a simulated annealing (SA) approach to create the re-marshalling configuration in order to identify a re-marshalling plan for an intra-block in ACT. They assess various re-marshalling configurations in accordance with the target quay crane's initial configuration in order to produce an intra-block reloading plan that minimises interference from stacking cranes and re-handles during the loading and unloading operation. Re-marshalling is crucial for minimising the time that external vehicles must wait to receive the import containers.

As earlier study has shown, it is difficult to prevent re-marshalling because of the yard layout and mixed storage of exports and imports containers at ACT, which also needs to take into account the unpredictability from the arrival of ships and external trucks. The next section also extensively covers

contemporary issues related to organising yard equipment scheduling based on yard space management.

2.5 Advantages and challenges of the automation of PCTs:

The automation of PCTs is a major initiative that addresses the three strategic needs that any terminal's strategy must address in order to consider the modern business concept of sustainable development of an activity: improved operational performance, increased safety and security, and ability to contribute to environmental sustainability. [1] However, the lack of flexibility that comes with standardising automation procedures has an impact on the planning and operational administration of automated PCTs. Planning activities makes it tough to plan and manage new scenarios that have never been addressed before, as well as exceptions that must be handled methodically and efficiently.

Simultaneously, automation leads to increasing human and port facility safety and security. Automation procedures not only improve safety by minimising human errors in operation, but they also lessen the effect of potential accidents by separating humans from the area where activities are physically carried out. In terms of environmental sustainability, while automation was primarily designed to increase PCT productivity, it also has a significant impact on the global energy use of PCTs. From the standpoint of energy efficiency, automating a PCT is one of the most effective management enhancements that can be made. Automation aids in the optimization of operations in all areas, reducing equipment travel, empty runs, container shuffling, and so on, resulting in a reduction in energy consumption.

On a societal level, automation in PCTs have an effect that is not always viewed positively. The inescapable loss of employment that a large automation entail produces problems with port employees or dockworkers, who perceive how their employment circumstances and stability are jeopardised, leading in labour conflicts with difficult outcomes and lengthy discussions with trade unions. In any case, while automation does reduce direct human participation in processes, it also greatly raises the level of training required to do the functions of the job roles involved. As a result, because the automation of PCTs necessitates a complete shift in the working system and management in comparison to the operations of a standard PCT, it must be supported by a workforce plan.

In keeping with previous statements, PCT automation provides significant benefits over manual procedures; however, this procedure also faces numerous problems in terms of planning, business, and operational management, which may jeopardise the viability of such projects.

3. AUTOMATION IN PORT TRANSPORTATION & LOGISTICS

3.1 Container Transport Infrastructure - Sustainability & Advancements

Container Transport and logistics is one of the main components in the port and shipping industry. The containers have to be carefully handled and sent to the destined location so that they are delivered to the right customer. After the removal of the containers from the ships using the cranes are transferred to different modes of transport to distribute the containers to the destined locations. Strong maritime logistics sector had a significant contribution to the economic growth. The careful design and implementation of a proper logistics plan to minimize the human and material power is crucial. The concept of port let development is an idea of development of Special Economic Zones (SEZ) in which logistics part is given a high priority. Port connective to rail, road, air as well as river connection with the hinterland. The main vision is to lower the logistics costs set by both import and export with a very less investment in the port logistics sector. Consider the following image which shows the steps in the priority to achieve sustainable port development [20]. Hinterland connectivity development which is the logistics part is the second most important thing in achieving the sustainable port development.

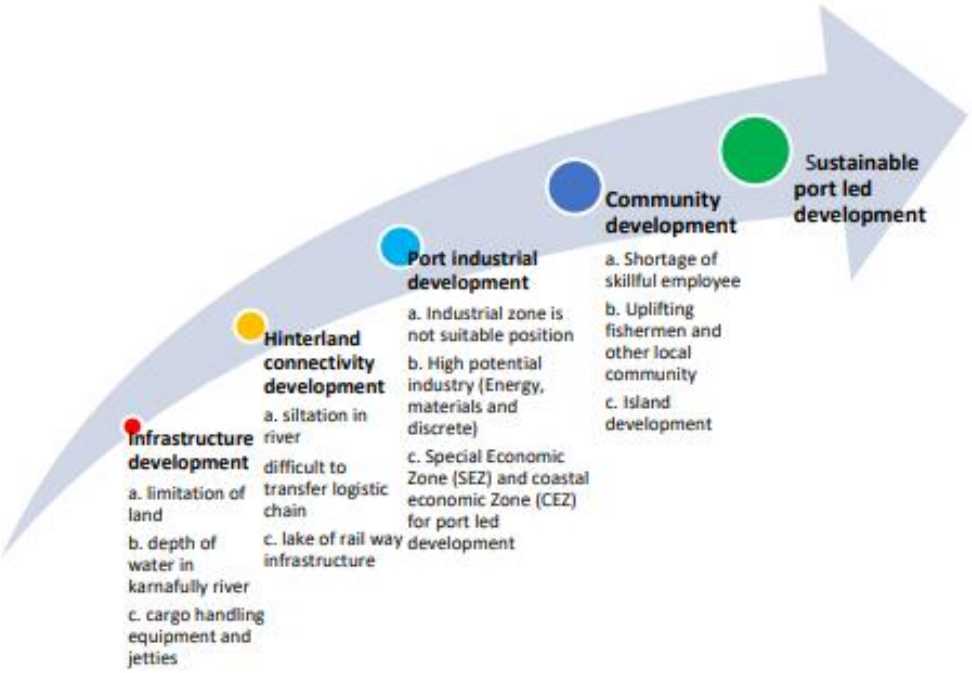

Figure 7: Various Stages that lead to Sustainable port development [20]

The logistics parts include two major components one is the machinery used to transport the cargo and the other is the medium on which it is transported. Here the mediums specify the road, water, and

air. Development of high-speed rail network with dedicated freight corridor is necessary for cargo to travel in rail in a cost effective and fuel-efficient manner [21]. The Governments should invest in improving the roadways by designing new high-speed expressways to remove traffic congestion and decrease the time to deliver the cargo.

With the emerging technologies there are several new advancements in the machinery used for the transportation [21].

- The use of autonomous vehicles (AVs) from the movement of container from unloading cranes to the container storage area.
- The usage of drones to provide last mile delivery Service to the cargo.
- Self-driving and remote-control container lifting equipment's for the movement of containers in the port.
- Most cost-effective freight movement is achieved through trains, and these should be made driver less.
- Improvement in trucks so that they can carry container stacks one above the other.

Not only from the hardware, but there should also be an effective software technology to be used for the freight control, collaboration [21]. Secure storage area with RFID tracking and Digital signalling systems for the movement of autonomous vehicles. The following table specifies the impact of usage of various methods of above stated machinery on the safety, congestion, delivery time, efficiency, cost, and human intervention.

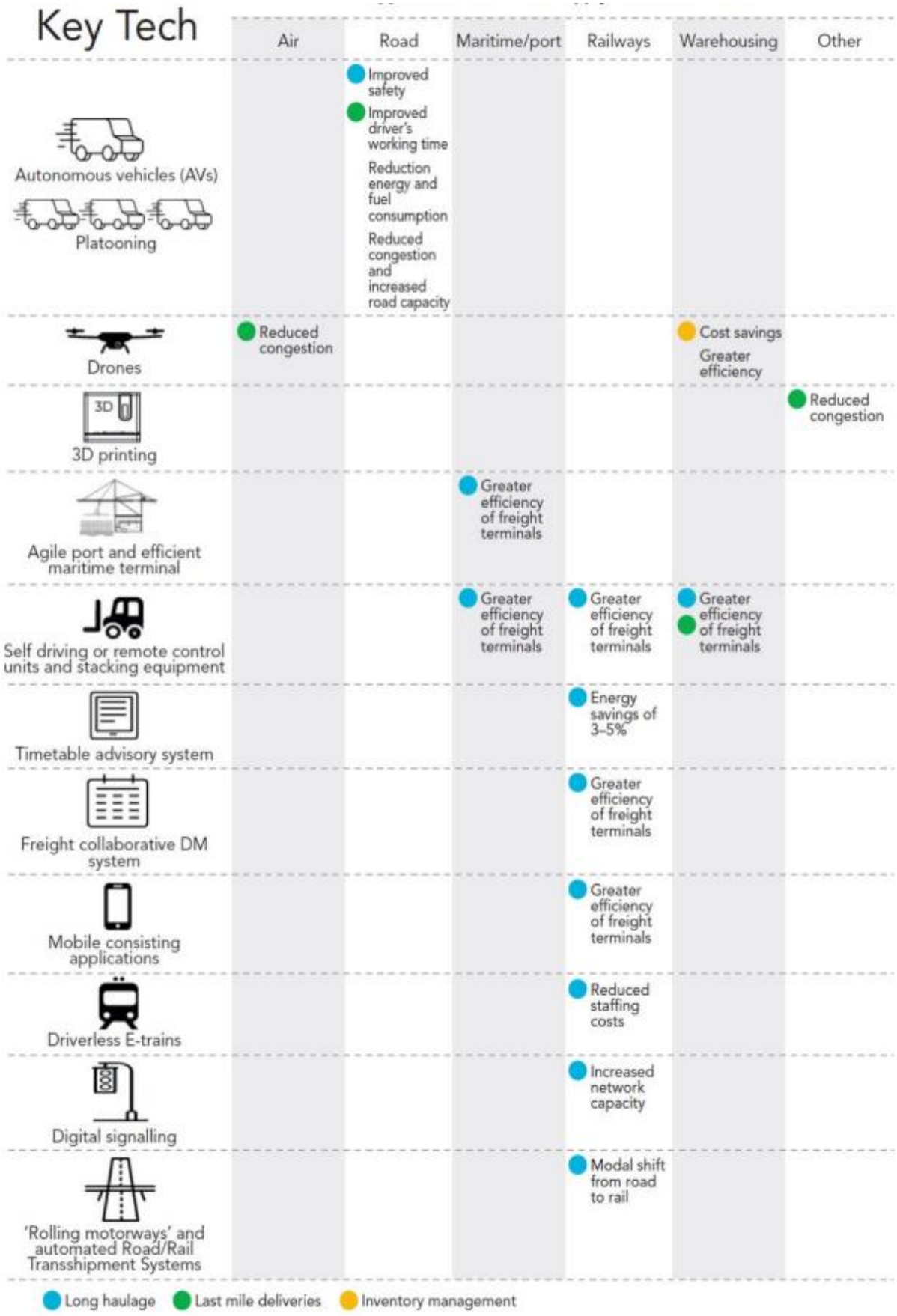

Figure 8: Impact of modern port logistic machinery on several factors [21]

3.2 Automation in logistics:

A container port is often representing a break point in the supply chain. Being a crucial exchange point between exports and imports to a country it is affected by difference in arrival and departure time of the vessel, any lack of information often leads to time inefficiencies. Automation in the terminal can overcome these issues as they are programmed to follow a predefined pattern with high accuracy. If the order of the truck arrivals is known beforehand, yard planning can be more efficient by using the automation [21]. In the idea of agile port management system, the marine terminal and the intermodal interface centre are connected through a dedicated line of railway. The main idea of Agile port system is:

- Shift as many cargo containers as possible from the vessels on to the trains so that the storage of the container can be minimized at the terminal.
- Move the containers as quickly as possible to the intermodal interface centre by train.
- Sort the containers between the trains as per their final delivery point.
- Load and unload the trucks quickly at the intermodal interface centre

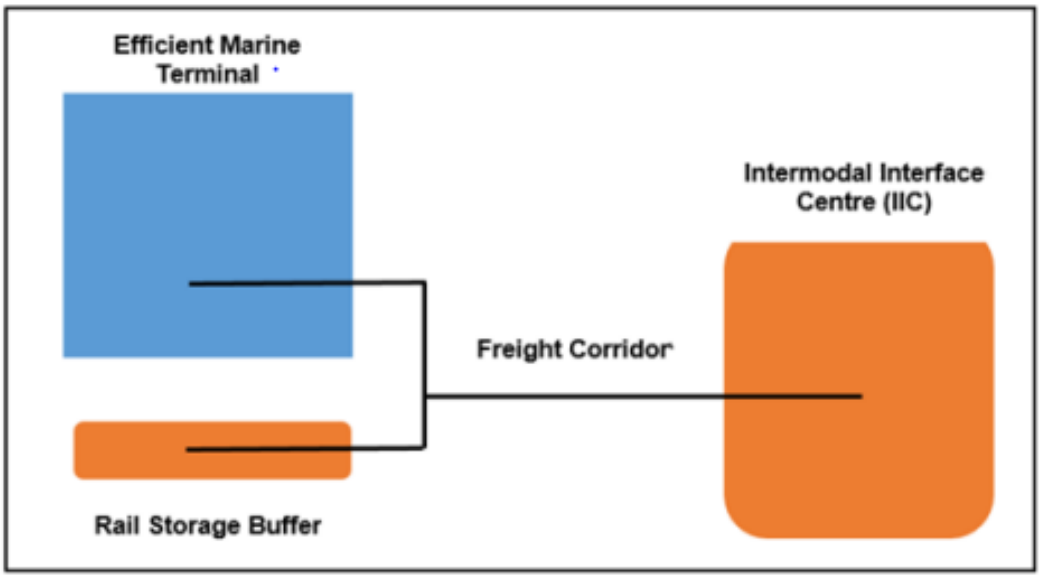

Figure 9: Agile port concept [21]

Agile Port concept is a combination of improved semi-automated equipment that allows that transfer of the containers between the vessels and the train and vice versa Here the efficiency, performance and the utilization of the storage place is improved. The containers units are also stored extremely near to the customer instead at the terminal. The port of Hamburg acts as a good example for the agile methodology, here 360 container boxes are transferred on the trains in one hundred minutes. The two main benefits of efficient marine terminal are reduction in machinery and labour costs mainly due to

the decrease in number of yard transfer vehicles [21]. It is combination of improved semi-automated, ship-to shore cranes, semi-automated cantilevered and rail –mounted gantry cranes, a rail box mover

Figure 10: Intermodal ship to rail transfer in California [21]

and shuttle cars with automation technology.

The turnaround time for the ships in the ports is greatly reduced by the automation which would in turn leads to the advantage of shipping companies. The cost of investing in the automation technologies would easily be reverted within few months and the benefits gained because of automation are exceedingly high [21]. Automated rail mounted gantry systems are found to be much cheaper when compared to the rubber tyre or semi-automatic gantry system. Automated guided vehicles (AGVs) and Automated stacking cranes (ASCs) are found to have to number of advantages when compared to the drawbacks or weakness.

AGV's are capable of rotating their wheels independently with precision in loading and unloading. They are able to deal with containers of different lengths and work at high speed and with less noise. They can move safely as they are equipped with laser detectors that identify the obstacles in their path and take necessary deviations. AGVs are able overtake each other and can refuel by themselves [21]. Similarly, the ASC's Automated Stacking Cranes also have several strengths like they are able to stack boxes in one and five layers deep and can move at 21 kmph on tracks. The save space and are able to avoid collisions. They are able to work in extreme conditions and can load the boxes very accurately. These automated systems provide a complete automation solution to the stack yard and the software's running on them can be integrated with other terminals [21].

Figure 11: Automated Gantry Vehicle and Automated Stacking Crane [21]

3.3 Self-driving unit's and Stacking equipment:

Automated vehicles can be used in moving the container boxes to different areas in the port. With automated vehicles we can reduce the number of empty trips, shortening the routes, human errors thus achieving optimal utilization of resources [21]. Truck arrival times at the loading / unloading dock is uncertain and loading of a container is dependent on other container and the truck responsible for first container might not arrive. This may create unexpected delays in the supply chain. To avoid this problem

Figure 12: Automated vehicles in Singapore port [21]

Truck platooning can be used, here the order of the trucks and the trucks are loaded continuously depending on the order. Even though as of now there is not much research in truck platooning, major automobile companies are investing a lot of amounts in this field. The trucks are equipped with high end cameras, various sensors to detect obstacles, Global Position System GPS, and various artificial intelligence software's to detect the movement of other vehicles [21]. Till date there are a few vehicles which have partial automation which requires a driver to operate and guide at some point of time. For full length driverless autonomous trucks which can platooning requires time and research.

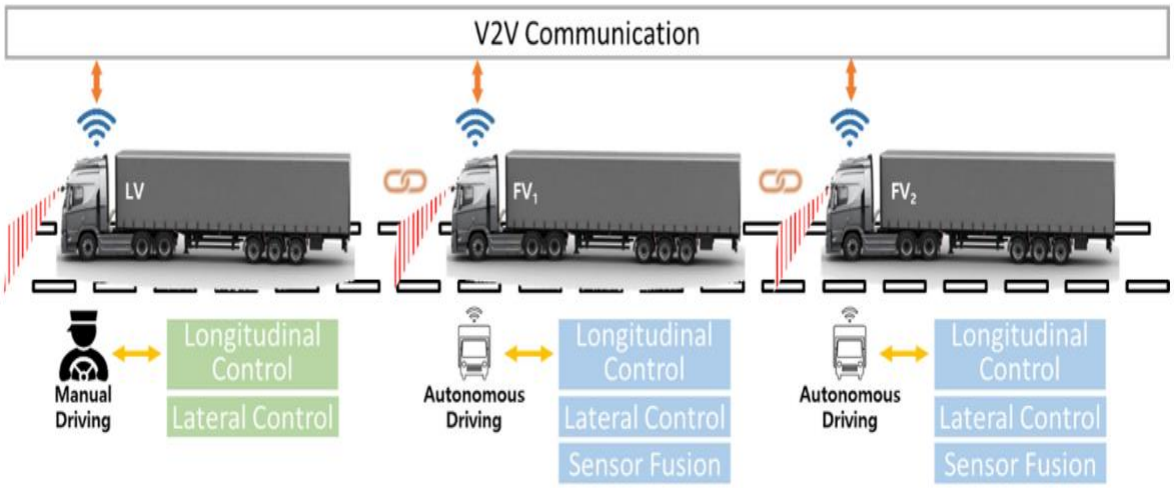

Figure 13: Trucks Platooning Railway System Automation [21]

Trains are the cheapest and most efficient form of freight transportation on land. The automation in the trains is huge boom to logistics department of the port industry. The Smart Automation of Rail Transport (SMART) project is researching on the obstacle detection and automation, braking systems that offer a short distance of wagon recognition. There are three innovative technologies that are currently used by freight rains in UK one is Timetable Advisory System used for tracking the progress of the train [21]. The other is Freight Collaborative Decision Making System which gives the real time information of the freight terminals, the arrival times of the freight services. Mobile Consisting Application is the third technology which is used log the details of the train and the freight it is carrying. Currently the techniques like increase in the length of the train, high power engines and double stacking one container on the top of another are being used to transport the containers in a cheap way.

Figure 14: Double Stack Freight Train [21]

3.4 Automation in Air Transport and last mile deliveries:

Aviation industry grew very rapidly in the rapidly in the recent years. There are several innovative technologies like drone, autopilot, unmanned aircraft for military applications. Drones are ow being repeatedly used in warehouses, making the tasks perfectly accurate and cheaper. Drones can be used in the last mile deliveries as they can escape the traffic congestion, road collision. They also help in delivery of the cargo in a cheap and fast manner while causing less impact on the environment [21]. Various solutions have been put forward to reduce the impact of urban population density on the delivery service. One of them is drone delivery and the other is using small, automated vehicle which can travel autonomously on the roads avoiding obstacle and delivering the products to the customer at their address. FURBOT is one such concept used by the DHL to deliver the packages.

It can automatically load or unload the goods and the deliver them to the right person by scanning the name and QR code of the package [21]. Amazon uses drones to deliver their packages. There are a few limitations for the drone due to the limited carrying capacity.

3.5 Digital platforms to manage transport logistics:

As a part of digitalization, everything in the world is getting digitalized. Several software's were designed to shift the manual work to a work that computers can perform. Since the vehicles are autonomous, they require a central authority to identify the working of each autonomous machine. Through digitization the cost can highly be reduced and parallelly efficiency can be improved [3]. Digitalization simply refers to adopting the use of computer to organize or monitor the work. There are several digital technologies used in the shipping industry like RFID, Big data, Cloud, Artificial intelligence, and other latest generation technologies in information technologies.

RFID, Big data and Digital camera and sensors technology is mostly used in the automation of logistics department [23]. The RFID tags are assigned to each container and autonomous vehicles AV's. The RFID reader which are placed near the dock doors or in any other region where the container movement can be quickly tracked [24]. Software integration between both to get a user interface view of presence of each container or AV.

Technologies like Big data are highly used in storing large volumes of data which is coming from the containers and the autonomous vehicles. AVs are equipped with Global positioning system GPS sensors; their movement is continuously tracked from the control panel of the port [23]. There are variety of software's used in the port logistics department like Arviem, netSuite, Logiwa WMS, Rose Rocket [25]. There Software's are used to track the movement and location of the containers. The following image is control unit of the world second largest Shanghai port.

Figure 16: Control Panel where all the port operations are monitored [23]

Environmental Impacts of port logistics: Two to Three percent of the global greenhouse gases emissions are due to the marine shipping and they are predicted to increase to 17 percent by 2050. Intermodal transportation of cargo in trucks, trains and smaller ships also results in release in CO2, Sulphur dioxide, black carbon, and other environmental dangerous greenhouse gases.

3.6 Modal Shift in Freight transport:

Ports on one hand providing the economic growth for the country on the other hand these ports are causing severe environmental concerns in the local areas. Emissions from the vessels have caused severe health issues to the local people [22]. More than 80 percent of intermodal transport or hinterland transport is done by the trucks, these cause high amount of pollution when compared to the other means of transport like trains or ships. Several analyses were made in which shifting of the cargo from roads to less environmentally damaging modes of transport is good for the environment. One such analysis is made in the Europe considering different agencies like port authorities, Regional Institutions, National Institutions and Private firms. They have analysed various inputs from different sectors and made a goal to shift 30 percent of the freight transported on road to rail or waterways by 2030 and more than 50 percent by 2050 [22]. The people are more inclined towards shifting the freight to railways by 51 % while to waterways by 27 % and 22% for both.

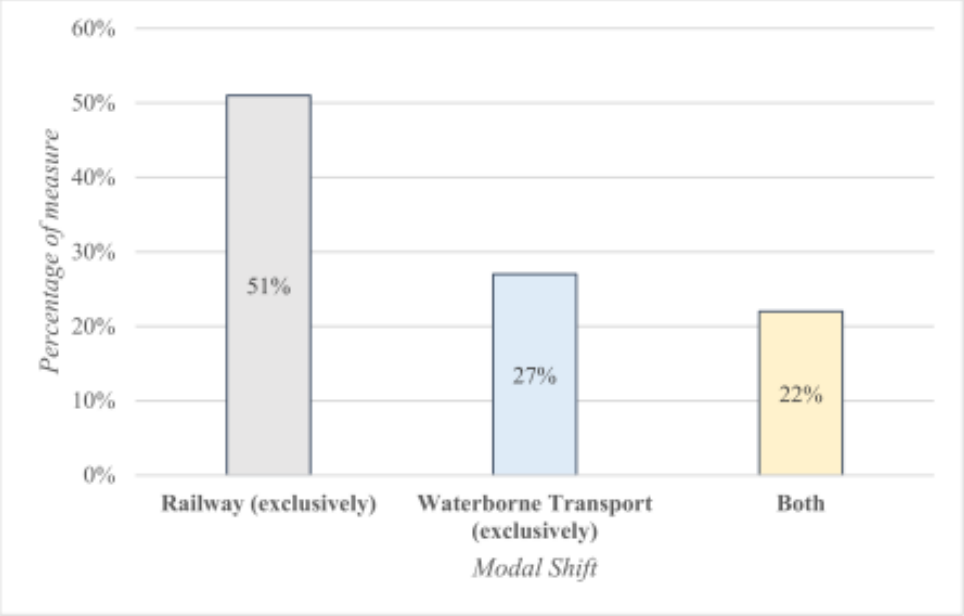

Figure 17: Modal shift Railways vs waterways [22]

3.7 Cost Analysis:

Cost of the freight delivery completely depends on the distance it would travel from the port, the more it travels the less the cost per mile. The handling cost of the amount to 35% to 40% of the cargo for long distance transport and 45% to 50% of the cargo for short distance transport [27]. In the olden days, the cargo needs to be packed specially before loading it on to the ships but now the container itself acts as packaging material to the cargo [27]. Coming to the implantation of automation in the logistics, the AVs are mostly in prototypes stage and are costly. The cost is expected fall rapidly once

tested and mass produced [21]. The following table shows the cost of automation different load carrying trucks.

Table 1: Investment and benefit of automated systems in different cases [21]

	Optimistic (£)	Baseline (£)	Pessimistic (£)
Cost of automation			
38-tonne trailer truck	12,500	15,000	20,000
18-tonne trailer truck	12,000	14,500	19,000
7.5-tonne trailer truck	11,500	14,000	18,000
Taxi	9,400	11,400	15,000
Private car	9,400	11,400	15,000
Driving time benefits:			
Commercial driver salary reduction	80%	60%	60%
Private car productive use of time	60%	40%	25%
Fuel-efficiency benefits	10%	5%	5%

The following figure shows the future likelihood of cost for fright transport by different modes. Autonomous trucks would be significantly more competitive when compared to others. The following analysis is made in the US. The same would repeat even if the study is made in the Europe as the cos of rail system is more in the Europe when compared to the US [21]. The effective solution for most economic mode of freight transport is by autonomous vehicles with platooning when compared other modes of transport. Railways are also as efficient as AV's with just minute higher price. The Air mode is the costliest which is beneficial only in urban areas and last mile delivery situations.

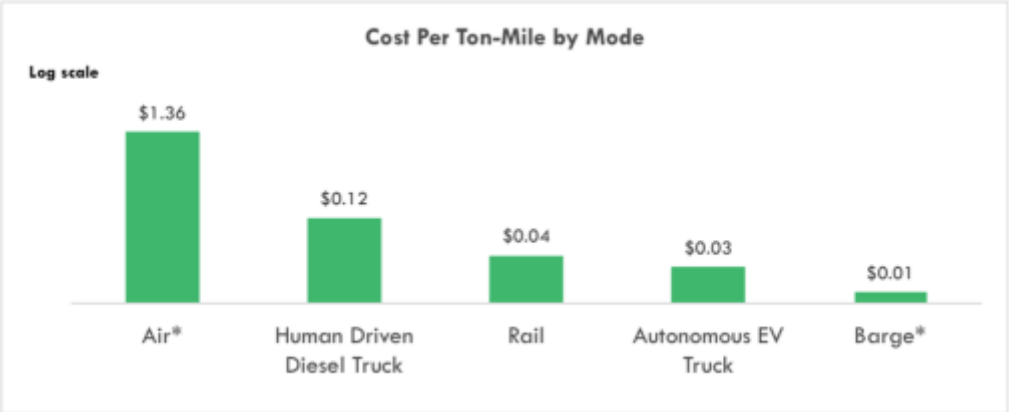

Figure 18: Cost per ton mile by various mode of transport [21]

4. INTERNET OF THINGS IN PORTS

The Internet of Things (IoT) is now widely regarded as a significant technological revolution in smart city, smart home, smart factory, and smart port installations. Different operation sectors are now working in automatic mode as the presence of smart sensing systems in ports becomes a reality. From Europe to Asia, Australia, and North America, there are examples of complex projects related to smart ports in the IoT era; sensing technologies play a significant role in all of these new architecture implementations. Internet of Things (IoT), as defined by the IEEE, is a network of items including sensors and embedded systems which are connected to the Internet and enable physical objects to gather and exchange data. Sensors are playing an increasingly vital role in assessing the physical features of items and turning them into numerical data that can be read by another device or by the user as the Internet of Things grows in popularity. The global sensor market has been growing at a rapid pace in recent years, and it is projected to continue to do so in the future. When we look at future-oriented projects from various governments, such as Germany's Industry 4.0 and China's Made in China 2025, the data produced by sensors is the key to these projects. Smart power grids, smart buildings, smart industries, smart cities, and smart ports are just a few of the areas where sensors are used [28].

The Internet of Things (IoT) is the first step toward port automation. The internet will connect all the different sections of the supply chain in the IoT environment that will be relevant for container handling. Heavy Machines, Terminal vehicles and containers, as well as humans or inland freight transporters, will be involved. They make it possible for devices to become smart, link with other devices, and gather and provide data on their operating conditions and status. Older machinery and devices must be replaced with new ones in order to adopt IoT solutions, and where new devices cannot be brought in due to cost or feasibility, new sensors must be installed. A single port is home to thousands of tiny and large machines and equipment. Until now, humans have had to manually check for proper operation, accuracy, and maintenance of these equipment. A wide range of scenarios can be implemented with IoT such as Predictive and prescriptive analytics, as well as automation of operations and workflows such as loading and unloading goods and containers from vessels and trucks. Data is essential for performing predictive and prescriptive analytics. All of this information comes from IoT devices and sensors. They generate or collect data without interfering with the operation of machines and equipment, and then send it to a cloud platform for further analysis [29].

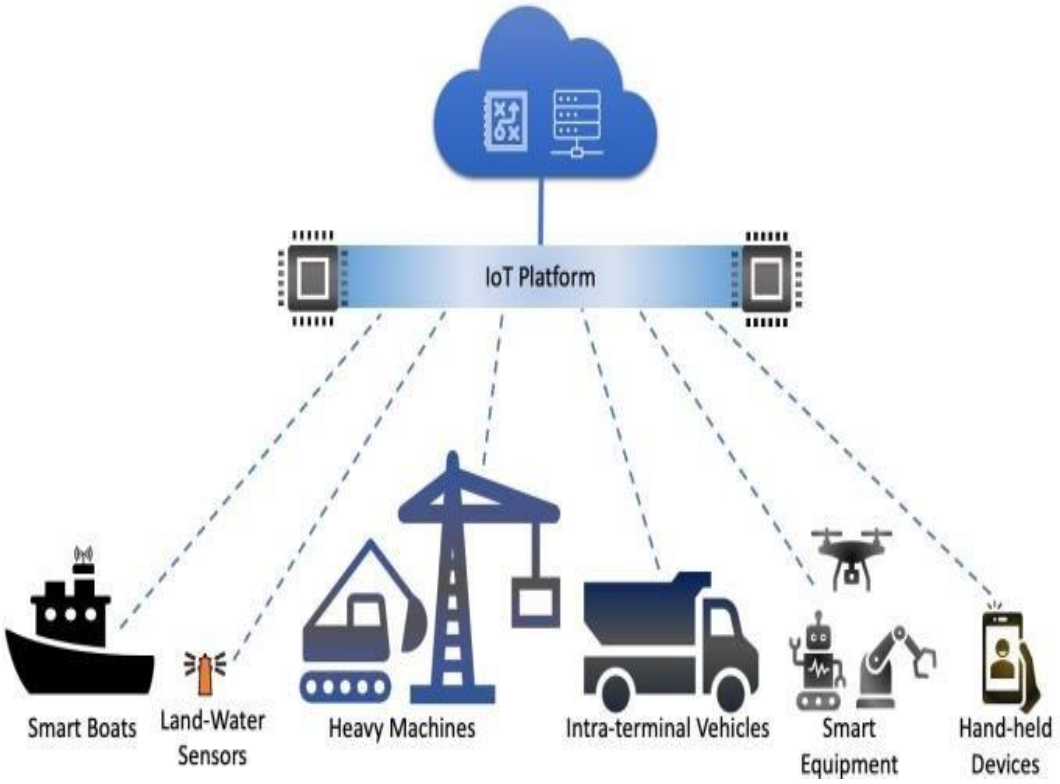

Figure 19: IoT and Device communication at Sea Port [29]

4.1 Sensing Systems for Smart Ports:

Sensing systems are used in tasks such as quayside crane structural health monitoring, container position detection and handling, AGV localization, navigation, and control, and so on. Current developments in the fields of optical fibre sensors, extremely sensitive magnetic sensors, and MEMS inertial measurement units that enable interoperable wireless protocols, including the latest developments in 4G and 5G that will allow the extension of the Internet connectivity of sensing systems, represent significant opportunities for smart port development. Contact and distant sensing solutions are used in new smart sensing architectures for container identification and management, vehicle identification and management, location and navigation services, and the safety of port terminals equipment connected to structural health monitoring [28].

4.1.1. Structural Health Monitoring:

The goal of structural health monitoring (SHM) is to determine whether or not damage exists based on measured dynamic or static properties of the system being monitored. The contents of SHM in smart ports are focused on identifying stress and strength reserves of metal structures in cranes and RMG, as well as flaws detection, such as microcracks, weld cracks, and plastic deformation, in the process of structural failure where the stress under load is clearly beyond the allowable value. The

SHM must be implemented throughout the equipment's life cycle. The oblique rods of QCs, for example, are subjected to substantial force, and their installation symmetry must be verified using strain monitoring equipment at the production stage. Table 2 lists the main sensor technologies utilised in smart ports for SHM. The strain gauge is the most often used sensing element among these technologies. The gauge that converts structural strain to resistance change is low-cost and reliable. FBG is a more expensive long-term monitoring device than the strain gauge for sensing the influence of strain through a frequency shift and magnitude change of the reflected beam. In addition, two on-line defect detection devices include eddy current probes and ultrasonic probes. Cracks and other imperfections in electric conductive materials that are detected using eddy current probes that include exclusively coils or coils and magnetic sensors such as gigantic magneto resistors will alter the size and shape of the eddy current in the electromagnetic field. The presence of faults in the uniform material causes discontinuity in the material, which can result in uneven acoustic impedance for the ultrasonic sensor. The ultrasonic wave will be reflected at the interface of two different acoustic impedances, according to the reflection theorem, and the magnitude of the reflected energy is proportional to the difference in the acoustic impedance of the interface, as well as the orientation and size of the interface. As a result, by analysing the signal obtained by inductive eddy current sensors and ultrasonic sensors, a crack situation in the metal structure of QCs and RMG can be determined [28].

Table 2: Main sensing technologies used for structural health monitoring in smart ports [28]

Type	Parameter			
	Relative Cost	Working Range	Environmental Adaptability	Applications
Strain gauge	$	Long-term monitor	Sensitive to water, humidity and electromagnetic interference	Stress and strength reserve of the metal structure in cranes and RMG
FBG	$$$	Long-term monitor	Resistant to dust, water, humidity, and electromagnetic interference	Stress and strength reserve of the metal structure in cranes and RMG
Inductive eddy current sensor	$$	Short-time monitor	Resistant to dust, water, and oil interference; Sensitive to surface roughness, surface coating and material	Flaws detection, such as micro-cracks, weld cracks and plastic deformation
Ultrasonic sensor	$$	Short-time monitor	Sensitive to reflection problem, noise with the same frequency and cross problem	Flaws detection, such as micro-cracks, weld cracks and plastic deformation

4.1.2. Distance Measurement:

The proximity, level, and distance measurement sensors are mostly used in smart ports for anti-collision monitoring and location applications of cranes, RMGs, and AGVs, and ultrasonic, inductive, laser, and infrared sensors being the most prevalent, as shown in Table 4.

Table 3: The comparison between the distance measurement sensors in smart ports [28]

Type	Parameter			
	Relative Cost	Effective Range	Environmental Adaptability	Applications
Ultrasonic sensor	$$	High	Sensitive to water, humidity and wind interference; Long response time	Anti-collision of quayside crane and RMG in track
Laser and Lidar	$$	Very high	Sensitive to dust, water and oil interference; Very short response time	Anti-collision of spreader, main trolley, portal trolley, quayside crane, AGV and RMG
Electromagnetic induction sensor	$	Very low	Resistant to dust, water, humidity, wind and oil interference; Short response time	Anti-collision of quayside crane and RMG in track
Infrared radiation sensor	$	Low	Sensitive to sun and reflector interference; Short response time	Anti-collision of spreader, main trolley and portal trolley in quayside crane

4.1.3. Navigation:

RFID-based navigation systems (HF and UHF RFID solutions), differential GPS systems, laser-based navigation systems, inertial navigation systems, and encoders are the common navigation sensors for AGVs and autonomous container trucks, which are the main container handling equipment in smart ports from the coastal area to the container terminal, as shown in Table 5

Table 4: The comparison between the navigation sensors in smart ports [28]

Type	Parameter			
	Relative Cost	Accuracy	Measurement of the position	Environmental adaptability
HF and UHF RFID solutions	$$	High	Absolute position	Sensitive to foundation settlement
Differential GPS systems	$$$	Very high	Absolute position	Sensitive to metal and other shelter
Laser- based navigation systems	$$$	Very high	Absolute position	Sensitive to dust, water, humidity, oil, sun and reflector interferences
Inertial navigation systems	$$	High	Relative position	Sensitive to cumulative error, vibration and slip
Encoders	$	Low	Relative position	Sensitive to cumulative error, vibration and slip

4.2 Changes due to the Internet of Things:

The Internet of Things has the potential to have an impact on the amount of data sent via the PCS. The data collection and processing of accessible data are the two key areas where the Internet of Things will enhance things. This will have an impact on port efficiency, security, and transportation monitoring capabilities [32].

4.2.1. Port Efficiency:

IoT-enabled efficiency gains can be realised at many levels of the supply chain. For instance, knowing where actors are in real time improves planning and reliability. This will benefit all actors in the supply chain, resulting in increased time efficiency and efficient use of available facilities during container transportation. The real-time positioning of container ships that are scheduled to dock at the port provides further information about the ships' expected arrival time. The physical group, such as terminal operators, can prepare for the anticipated arrival and ensure that everything is in place to unload a ship as needed. This information will be used if something goes wrong enroute. This early insight into supply chain delays allows terminal operators to free up handling capacity, resulting in an up-to-date list to align supply and demand for their facilities. Other barges can use the extra space created by the delay, resulting in a more efficient use of terminal resources and, as a result, less costly downtime. The status updates will also be beneficial to the hinterland transporters. They can also adapt their timetables sooner to accommodate changes, reducing unplanned waiting time. The level of congestion will be affected by real-time information exchange. Congestion is a side effect that might arise when the port processes an increased quantity of TEU. More ships can call at the port as a result of increased efficiency, producing more congestion. However, the expanded capabilities for making a dependable plan also present opportunities to avoid traffic congestion [32].

4.2.2. Security benefits:

The authorization's handling is where the fourth efficiency gain is found. This boost will most likely come from customs, which can save a significant amount of time by providing better information. Almost all information forms used by firms situated in the port are now transferred via Port base. This saves time and paper while also increasing the documentation's dependability. The PCS allows the loading and unloading lists to be sent to customs before to entering the port, eliminating the need to hand them in in person. This not only saves time, but it also increases the reliability of the forms because they are written in a language that the PCS understands. Not only will the Internet of Things improve the efficiency of customs processing, but it will also improve security. The use of E-seals can provide information on whether a container has been opened. Data from an E-seal is useful information for bespoke services when combined with its location path. When this information is

provided, the authorisation group may make more accurate assessments of hazards and the need for additional inspections. Customs, for example, can detect potentially dangerous occurrences during a container's journey. The loading and unloading of containers, as well as a container on hold during its journey, are the riskiest events. E-seals and GPS trackers can provide information to identify these dangers, resulting in a safer and time-efficient container environment [32].

4.2.3. Monitoring benefits:

The database is the PCS's third most important feature. The data that has been implemented in the PCS is stored in this database. In addition, real-time updates will keep the data current. There are two methods to profit from this circumstance. Governments can have access to all of the information communicated on the PCS by simply joining the system. Previously, data had to be collected separately from each company, making it a time-consuming procedure to gain a fair picture of port performance. The CBS takes up to six months to provide useful information about the Port's performance. They can reduce this time to one month by accessing the PCS database (Rook, 2015), and the data is more trustworthy due to fewer inaccuracies. Governments can intervene at a shorter notice if necessary, and hence intervene more reliably, because the delay is shorter. The database storing of information benefits more than just governments. Companies have access to information that allows them to see what is going on in the process. The sixth efficiency benefit of the Internet of Things is that they can search for more efficient modes of transportation. However, not all businesses are willing to be so open about their confidential company information [32].

4.3 Cold chain logistics:

CCL has an impact on every step of the process, from the manufacturing of a temperature-sensitive product to its storage in the manufacturing site, transportation to the warehouse, and storage at the customer's location. Temperature requirements vary depending on the product. Every setting necessitates unique consideration when it comes to temperature monitoring. According to Cargosense.com, 20 percent of pharmaceuticals are harmed as a result of CCL failure. According to the BCG, 1.6 billion tonnes of food are damaged or discarded each year, and this figure is expected to rise by 1.9 percent per year between 2018 and 2030[3].

4.3.1 Internet of Things (IOT) enabled Cold chain:

The IoT-based CCL monitoring system's overall framework is depicted in the diagram below. Cloud technology, as well as internal and exterior mechanical hybrid positioning technologies, are all part of the system. The components that make up the developed system are as follows:

(1) detecting the status of different environmental and internal positioning devices, as well as the WSN gateway, in relation to products in the container and in the port area and measuring the sender's ambient temperature.

(2) CCL in an RFID system for identifying sensitive items.

(3) transmitting collected data to a distant server WSN, RFID reader, and hardware and software interfaces with the GSM communications gateway [30].

RFID technology has advanced significantly in recent years, and it is currently successfully utilised to identify and monitor perishable commodities in the food business. It is a viable alternative to existing barcode and other traditional systems for tracking cold chain products, and it offers significant benefits. Standard wireless communication methods such as RFID, GPS, and ZigBee are used to collect data. In a variety of scenarios, data can be synchronised, transferred, and exchanged. IoT sensors are employed during storage and shipping, while RFID is used to track and trace foods in the port. A smart tag and a commercial reader are the most basic components of this system. Light, temperature, and humidity sensors, a microcontroller, a memory chip, low-power electronics, and an antenna for RFID transmission are all included in tags attached to cargoes with objects to be tracked. It consists of an RFID reader that can read and write data on the smart tag from a short distance [30].

The following is a more detailed description of how the system works. The sensors can communicate with each other through satellite, cellular network, or radio-based Wireless Personal Area Network. Sensors integrated in containers and other IoT-enabled monitoring solutions collect data on the status of the products in the container as well as ambient factors. The collected data is sent to the cloud server through 3G/4G/5G or LAN networks, where it is processed and, if necessary, fast alarms are sent. The aggregated data is then sent to management tools that help maintain a consistent monitoring network. MongoDB is the database that the proposed system uses to process big data applications. A web service receives the RFID and sensor data and transfers it to a MongoDB database, where a JSON-based document is constructed. The event time, recording time, IoT device ID, and IoT device name, as well as the reading point, temperature, and humidity, are all included in this sensor document. Authorized users in the cold supply chain can be accessible with suitable information sharing between information systems. Each authorised participant has real-time access to and monitoring of containers through this platform. This guarantees that the appropriate point in the cold supply chain is fully

visible. This approach is more cost-effective, effective, and efficient than standard manual tracking systems like as barcodes [30].

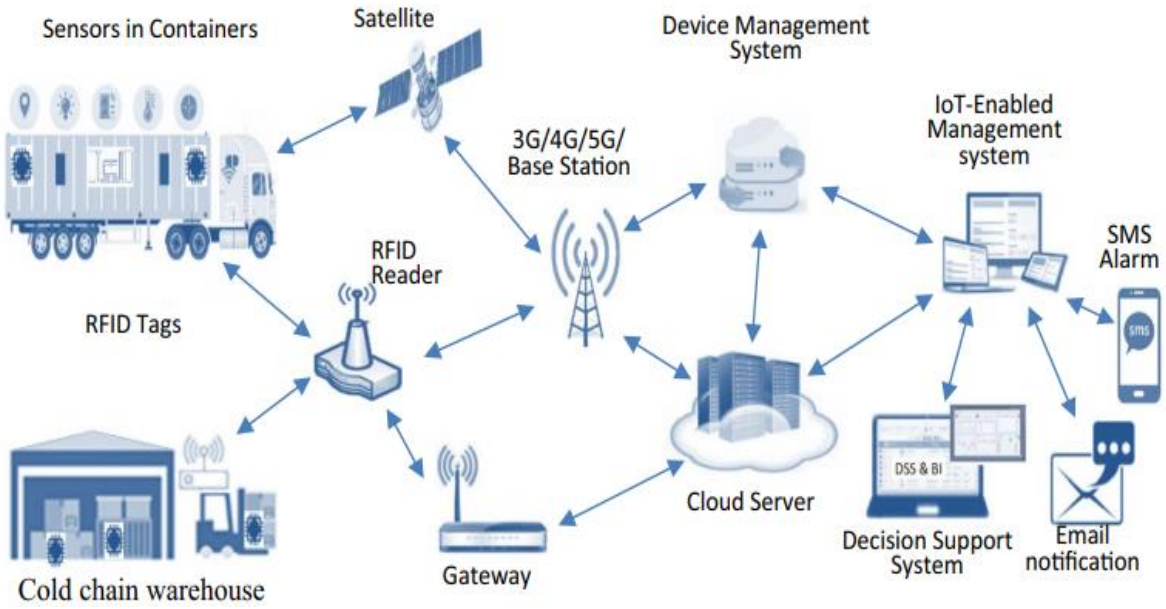

Figure 20: IoT-enabled CCL system framework for container operations at a port [30]

4.4 Container Seal and RFID Technology:

Every container going for export must be equipped with a seal that acts as a lock to safeguard the contents. Container seals come in a variety of styles, and their use is typically dictated by the value of the items being transported in the container. For example, for less expensive goods, a steel bend seal, a bolt type that consists of a metal bar with a lock, is the most widely used type at a fair price, and for the most expensive goods, a high-quality container seal or even an electronic seal is employed (e-seal). Every mechanical or electronic seal on a container has a unique number as an identity seal ID. The types of seals are depicted in Figure 3. Figure 3(a) shows the most typical mechanical bolt seal used in container terminals, while Figure 3(b) shows an electronic seal with a passive Ultra High Frequency (UHF) RFID tag EPC Gen2 and packaging constructed around it. Figure 3(c) shows another electronic seal design that uses UHF RFID but has a broader anticipated reader to make retrieving information from the tag easier. Figure 3(d) depicts an electronic seal based on a 2.4 GHz active RFID system with a mechanical bolt seal for easy container locking. The final decision on the system design is to use an active RFID e-seal in the container for effective reading of tag information. Other considerations include the fact that an active RFID e-seal can store more information, making

Figure 21: Container seal (a) mechanical bolt (b) RFID e-seal passive tag bullet (c) RFID e-seal passive tag lay (d) RFID e-seal active tag 2.4 GHz [31]

the tag stand alone, and the information can be queried on a mobile device using a handheld reader [31].

Because the location of RFID tags and e-seals on a vehicle affects reading performance, several scenarios and testing are carried out to establish the ideal location, such as driver tags for driver information, vehicle tags for truck or prime mover information, and e-seals for container information. The top of the windshield and the dashboard are among the places where the driver tag is checked. The optimal place to hang the driver's tag on the vehicle's rear-view mirror was discovered. The top of the dashboard was discovered to be the optimal location for the car tag. Note that vehicle tags are permanent and must be attached to the vehicle, whereas the driver tag varies depending on who is driving the car [31]. The position of RFID tags on the truck is shown in the below figure.

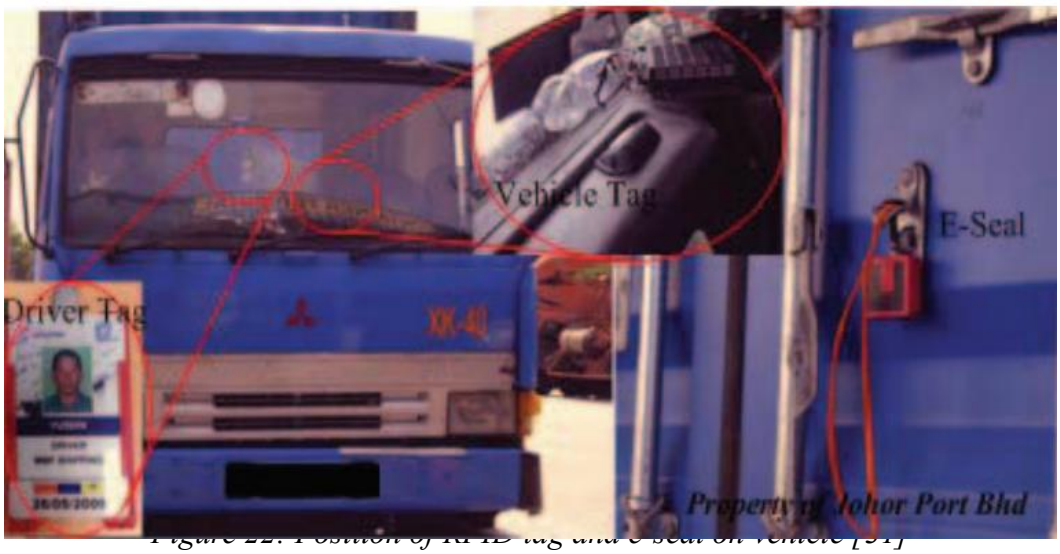

Figure 22: Position of RFID tag and e-seal on vehicle [31]

4.5 Types of RFID Tags:

RFID tags can be active, passive, or semi-passive, depending on the asset type and application needs.

4.5.1. Active Tags:

There is a battery in active tags. They either broadcast their encoded data on a fixed periodic basis (beacon type) or when polled by a reader and asked to do so. Depending on the tag power, antenna type, and surrounding environment, these tags can be read from hundreds of metres away. Embedded batteries provide the necessary power to send data. Active tags are the most expensive due of the battery expense and additional functions [33].

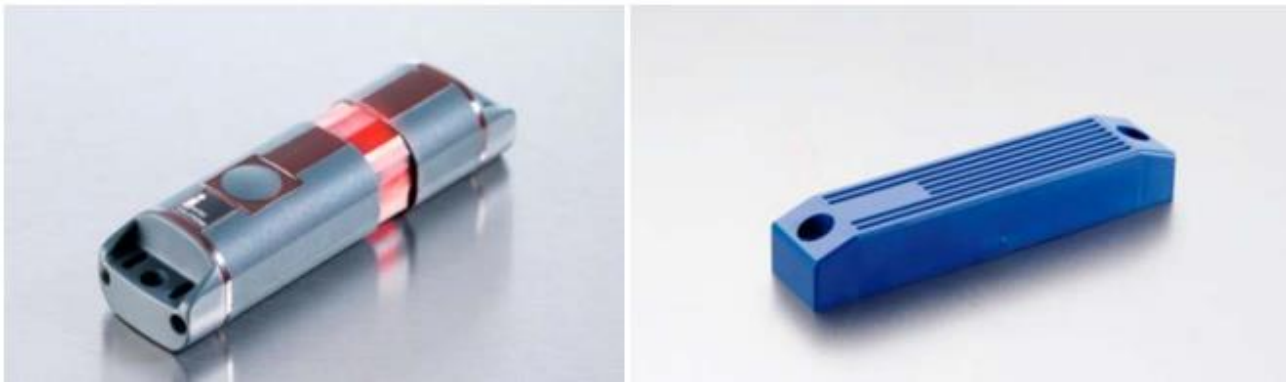

Figure 23: RTLS active RFID tag (left) and active beacon-type tag (right) [33]

4.5.2. Passive Tags:

When passive tags are within the reader's field of view, they have more force. The passive reader activates the tag's electronic chip, and the tag replies to the reader. While they are less expensive than active RFID tags, they have a much shorter read range, with most having a maximum read range of ten metres (30 feet). This is frequently less than one metre in the case of access cards [33].

4.5.3. Semi passive Tags:

Semi passive tags have a battery but operate in the same way as passive tags, transmitting only when triggered by a reader. The battery extends the transmission's range [33].

4.6 Tag frequency:

Each tag sends its data out at a set frequency. These frequency bands are shared by both active and passive devices. The following are the four most popular ranges used in ports today:

1. ***Low frequency (LF):*** For access cards, this is the 125 KHz band (HID, MiFare etc.)
2. ***High frequency (HF):*** This is commonly utilised for access purposes.

3. Ultrahigh frequency (UHF): Range of frequency is 433 MHz to 950 MHz the most popular frequencies for active tags are 433 MHz and 868-915 MHz for passive and active tags, respectively.

4. Microwave or ultra-wide band (UWB): This is 5.6 GHz frequency and utilised only for active RFID systems [33].

The frequency selection is critical since each frequency has its own set of data transmission speeds, distances, and cost/benefits. It is also worth noting that the frequencies are heavily regulated by local governments, with guidelines based on certain frequency bands. The LF range of 125 KHz, for example, is widely utilised and highly standardised. Although UHF is the industry standard, the amount of power that can be broadcast is limited on a local level. As a result, a port must check that the proposed technology from a vendor complies with national and/or local regulations [33].

4.7 IOT Challenges:

There are a number of risks associated with the installation of the Internet of Things and the transformation of the Port into an information hub.

4.7.1. Security Risk:

When setting up an IoT ecosystem and constructing an information hub, it is important to think about the security threats. The data that will be transferred is classified as confidential company information. This information could pose a major security risk if it falls into the wrong hands. Criminals can exploit stacking and destination information, for example, to open containers at terminal facilities. Falsified e-seals would be a great technique to smuggle products without incurring further customs scrutiny. There is also the possibility of a port closure, which would have far-reaching economic effects. In 2012, criminals hacked Antwerp's port community system, which served as an example of these concerns. The port's actors are aware of the potential security dangers. If a port relies on an internet-based network, it must ensure that it is safe. This will persuade the system's users that it is functioning well and will not cause any problems. Creating an information hub, on the other hand, increases the amount of data transported while also making it more difficult to protect [32].

4.7.2. Support:

To some extent, the Port can impact modifications, but the willingness of actors to alter port can make or break implementation. These players must deploy the services and make the necessary investments to make it happen. Because the port culture is a conservative one, this can be challenging. Many businesses are hesitant to make changes to systems that are already in place. Furthermore, not every outcome will be favourable to them. Increased supply chain transparency, for example, eliminates the

option of exploiting free time for transportation. This reduces the operating margin, which is especially important in the event of delays or unanticipated events. These developments in container transportation will very certainly alter supply chains in ways that will not be welcomed by all port stakeholders. Certain businesses may be forced to work more quickly as a result of the transparency. Customers will not accept this; thus, they are unable to keep extra time. Most port stakeholders will have to be persuaded to adopt the modern technology. Showing customers, the increased value of the services is the simplest method to convince them to make new investments. The usage of working pilots can demonstrate this enhanced value. When a small trial is effectively implemented, it is simpler to persuade port stakeholders and get support for the move to new development. However, the financial situation of the actors must be considered. Deep-sea carriers are often larger than barge carriers. To make the system truly operate, they must make the same adjustments. However, the financial condition of both modalities differs, with the hinterland shipping actors paying higher fees. When establishing new systems, this changing proportion of income spent on investment must be considered [32].

5. CYBERSECURITY IN PORTS

Shipping, like any other significant sphere of activity, evolves in lockstep with technological advancement: ships grow while crews shrink as increased procedures become automated. Some onboard systems now receive updates while sailing, and the teams have access to the Internet. With the increased reliance on automation, the risk of external interference and disruption of critical systems is dramatically increased; hackers can interrupt ship operations or navigation systems, cut off all external communications, or steal confidential data. As a result, effective cyber security is required to protect against such hostile attacks.

Cyber security can be defined as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user’s assets. The motivations of cyber threat actors to participate in a cyber-attack on a port system can be varied, including state-sponsored espionage, the pursuit of greater kudos amongst hackers, or simply perverse curiosity. [34]

Figure 24: Cyber Security Threat Actors [36]

Cyber espionage: Cyber espionage is defined as attempting to get unlawful access to sensitive information such as intellectual property, business information, corporate strategy, personal data, lifestyle patterns, and disruption of state or commercial objectives [36]. Cyber espionage attempts to acquire competitive benefits instead of creating pressure and commercial disruption. [34] As a result, there can be five different losses [43]:

A) Loss of intellectual property, business, and customer information
B) Extra costs due to interrupted business plans and competitive exercises
C) Loss of profits and efficiency.
D) Damage to company reputation
E) Increased IT-related security costs

Hacktivism: Hacktivism is obtaining attention or applying pressure in support of a specific goal or cause, such as preventing the handling of specific cargo or delaying the development of a new port facility. The port, the operator of a port facility, or a third party, such as the cargo's source or recipient, could all be targets.[36]

Cyber Criminality*:* The term "cybercrime" refers to criminal behaviours that are regarded to be harmful to the public good and are therefore illegal. The motivation for cybercrime is usually to take advantage of human or security flaws to steal passwords, data, or money directly, such as by sending fraudulent emails requesting security information and personal information. It may be used to achieve

financial gain, cause human injury, jeopardize the confidentiality and availability of data and systems, or destroy a company's reputation and brand.[34]

Cyber criminality can be divided into four categories [43]

1. Actions endangering confidentiality, integrity and availability of data and systems
2. Forgery or Identity thefts
3. Illicit gambling or spreading false information
4. Copyright or brand violations

Cyber terrorism: Cyber terrorism is a politically motivated attack carried out by cyberterrorists, who could be international groups or secret agents, who use a variety of tools such as computer viruses, computer worms, phishing, and other malicious software to compromise the information, computer systems, computer software, and databases of important organizations or global networks in order to achieve political or ideological goals. Cyber terrorism usually has catastrophic ramifications, such as massive damage to government networks and national security initiatives, as well as loss of life or serious bodily harm.[34]

Cyber warfare*:* Cyberwar relates to a military operation aimed at disabling a military target using malicious software, viruses, and other technologies. Apart from the military, state-sponsored actors such as terrorist groups, corporations, and political, or ideological extremist groups may use cyber warfare to attack the opponent's computer networks. Hacktivism, espionage, denial-of-service attacks, and disruption of the electrical power grid have been identified to be the most common attacks in the cyber war over the years, however, these activities could pose a variety of risks to a nation. Computers and satellites could be used in cyber war to disrupt key water, power, fuel, communications, and transportation infrastructure, resulting in catastrophic effects.[34]

Table 5: Characteristics of cyber threats [34]

Cyberthreat category	Objective	Cyberthreat
Hacktivism	■ To invade web pages and computers to create pressure	■ Hack by malware ■ Hack by ransomware ■ Credential theft ■ Privacy violation
Cyber criminality	■ To gain financial benefits ■ To inflict personally motivated harm	■ Revenge or bullying ■ Criminal damage ■ Robbery of cargo ■ Identity theft ■ Data breach ■ Data damage ■ Illicit gambling or spreading false information ■ Copyright or brand violation
Cyber espionage	■ To gain competitive advantage and intellectual property of other business ■ To interrupt business operations ■ To damage company reputation	■ Illegal access to secret and delicate information such as company strategy, private information or intellectual capital ■ Cyber extortion ■ Information stealing ■ Insiders gaining unauthorized access to information systems ■ Intruder having direct physical access to systems and the network ■ Cross contamination ■ Cyber fraud
Cyber terrorism	■ To politically attack information, computer systems, computer software and databases	■ Outage and information system failure ■ Website defacement ■ Subversion of security control Sabotage
Cyber war	■ To fight against opponent countries by damaging or disabling their rivals' computer networks, especially relevant to military affairs	■ Sabotage at national level ■ Disruptive attacks by state actors

5.1 Cybersecurity Attributes of Ports

The port environment encompasses a wide range of existing and emerging technology, and the cyber security approach taken will differ from building to building and system to system. It will be determined by the supply chain's complexity, ownership, and use in the design, construction, operation, and occupation of each structure and its use. In the port environment, cyber security is best addressed by considering a set of security qualities, allowing for the adoption of appropriate solutions based on the type of the building, facility, or system, as well as potential threats. The following are the key characteristics of cyber security as they apply to cyber-physical systems. [36]

- **Confidentiality:** The port data should only be accessible to those who are permitted. To prevent unauthorized access to information such as sensitive financial, security, commercial, or personal data, port systems and associated processes should be created, deployed, operated, and maintained. All personal data should be overseen in compliance with the General Data Protection Regulation (GDPR), and due to the aggregation of data, information, or metadata, additional safeguards may be required to preserve privacy.[36].
- **Possession or control:** Unauthorized control, manipulation, or interference must be avoided in the design, implementation, operation, and maintenance of systems.[44]
- **Integrity:** Maintaining the consistency, coherence, and configuration of information and systems, as well as preventing unauthorized alterations, is what integrity is all about. To prevent unauthorized modifications to assets, processes, system state, or system configuration, port systems and associated processes should be created, deployed, operated, and maintained. Physical changes to a system, such as the unlawful connecting of a Wi-Fi access point to a secure network, or a defect, such as the corruption of a database or file owing to media storage problems, can cause a loss of system integrity.[36]
- **Authenticity:** Authenticity is ensuring that system inputs and outputs, as well as the state of any connected processes and data, are authentic and have not been tampered with or modified. [44]
- **Availability:** Availability is ensuring that asset information, systems, and associated procedures are always available and used in a timely and suitable manner. To achieve the desired availability, each of these may need to have a level of resilience that is suitable and reasonable. A loss of availability could result from a system component failure, such as a disc crash, or from a malicious act, such as a denial-of-service assault that inhibits the usage of an internet-connected machine.[36]
- **Utility:** The utility is ensuring that asset information and systems are useable and helpful throughout the port asset's lifecycle The utilization of port assets should be maintained

throughout their existence by designing, implementing, operating, and maintaining port systems and associated activities. A case where a port system has been modified or improved and the file format of old data is no longer intelligible to the system is an example of loss of utility. The data is unusable, but there has been no loss of availability.[36]

- **Safety:** The ports should prevent the formation of dangerous conditions that may result in injury or loss of life, as well as inadvertent physical or environmental damage, through the design, implementation, operation, and maintenance of port systems and related activities. Malware could cause a failure to show or communicate the alert states of port systems, posing a safety risk. The failure of a motion or proximity detector or other sensors could result in property damage or even death.[36]
- **Resilience:** Resilience is the ability of asset information and systems to adapt, renew, and recover quickly in the case of a disaster. Cascade failures should be avoided in the design, implementation, operation, and maintenance of port systems and associated operations. If a system or associated process is disrupted or impaired, or if an outage occurs, it should be possible to quickly restore a normal operational condition or a satisfactory business continuity state.[36]

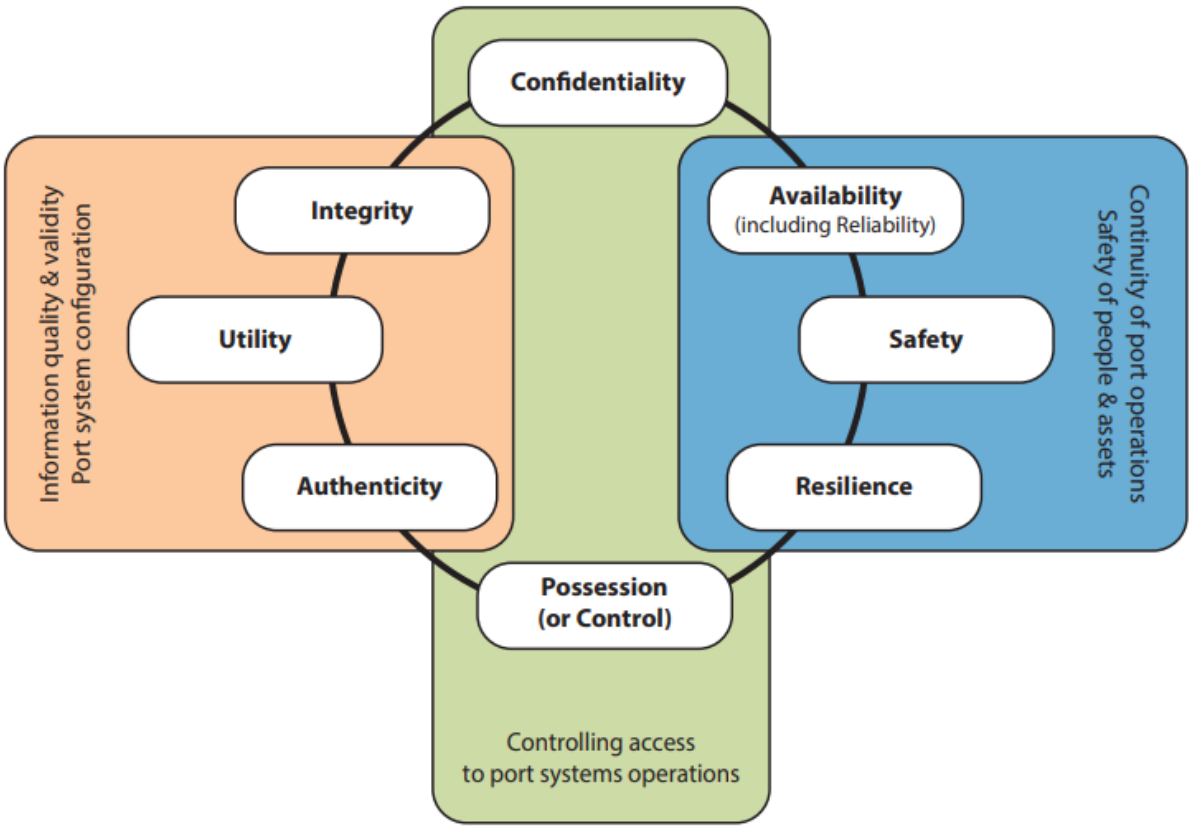

Figure 25: Cybersecurity attributes of ports [36]

5.2 Recent Maritime Cyber-Attacks

Cyber-attacks on the industry are taking place. Exploiting banking records, gaining access to logistical software, and taking control of a ship's navigation and engine controls are all examples of cyber risks and weaknesses. Many of the world's largest ports and shipping companies have been hit by cyber threats, which have cost them millions of dollars in lost revenue and system recovery.

- **The Port of Houston, August 2021: Hackers exploit a software flaw**

One of the major US ports, The Port of Houston was hit by a cyber-attack. It was attempted on ManageEngine ADSelfService Plus, a password management program [5]. According to the Coast Guard investigation, the unnamed hackers used a previously unknown vulnerability in password management software to break into a web server located at the complex around 2:38 p.m. UTC on August 19, 2021. After that, the intruders put malicious code on the server, allowing them to get access to the IT system. The hackers acquired all the log-in credentials for a type of Microsoft software that enterprises use to manage passwords and network access starting 90 minutes after the initial intrusion [37].

- **South Africa, July 2021: a case of cyber-force Majeure**

Transnet Port Terminals (TPT), a branch of the state-owned freight corporation that runs container terminals at the country's major ports, including Cape Town, Port Elizabeth, Ngqura, and Durban, declared force majeure late in July 2021 after its IT systems were disabled by a large cyber-attack. The disturbance reverberated throughout Africa's most industrialized economy, especially since Transnet's Durban port handles 60% of the country's shipments. Shippers from landlocked African countries such as the Democratic Republic of Congo, Zambia, and Zimbabwe relied heavily on the ports. After the devastation created by violent riots that shut down companies in two provinces in July, a protracted impact on container port operations dealt a further blow to South Africa's fragile recovery from the epidemic and a series of lockdowns.[40]

- **Port of Kennewick, November 2020: Digital Ransomware Attack**

The Port of Kennewick was the target of a digital ransomware attack in which fraudsters exploited the port's systems, installed a sophisticated encryption lock on the port's computers, and demanded $200,000 in ransom to regain access to the port's servers and files. This was a unique cyberattack that employed sophisticated, military-grade encryption to lock the port's servers and keep them captive in exchange for a ransom.[41]

- **Port of Shahid Rajaee, May 2020: a cyberattack**

Shahid Rajaee port received a cyberattack on 9 May, where shipping movement at Iran's busy Shahid Rajaee port terminal came to a screeching halt for no apparent reason. Computers that control the movement of ships, trucks, and commodities all went down at the same time, causing major bottlenecks on the canals and highways leading to the facility.[42]

- **Port of San Diego, September 2018: Ransomware Attack**

The Port of San Diego in the USA was subjected to a cyberattack on 25 September 2018. This incident, which was recognized as a ransomware attack known as SamSam, impacted over two hundred people, including hospitals, towns, and government institutions, as well as the port itself, causing $30 million in losses. The attack was coordinated by two Iranians, who demanded a Bitcoin ransom. [45]

- **Maersk NotPetya Attack, 2016: Ransomware Attack**

The Maersk NotPetya Attack got its moniker from its resemblance to Petya, a ransomware that made its debut in 2016 and extorted victims to pay for a key to release their information. NotPetya's ransom messages, on the other hand, were only a ruse: the real purpose was to cause havoc. It cost AP Moller-Maersk, which was not even the intended target of the attack, at least USD 300 million. A worm (virus) was used in the attack to permanently encrypt computers' master boot records, which tells them where to look for their own operating system. Any ransom payment made by victims was fruitless because there was no key to reorganize the contents of their computers. The publication of NotPetya was a cyberattack, and it has been classified as a terrorist/war threat actor.[45]

- **Danish Maritime Authority, April 2012-2014: Critical Cyberattack**

In April 2012, the Danish Maritime Authority was subjected to a critical cyberattack, though the cyberattack was not officially announced until September. The cybersecurity breach under discussion was discovered in 2014 after an American IT specialist reported it. Investigations revealed that when a Danish Maritime Authority employee opened a PDF file containing the virus that was sent as an e-mail attachment, the virus corrupted the employee’s computer and infected the attached network. the attackers wanted confidential information regarding Danish shipping companies and the merchant fleet.[45]

- **Port of Antwerp, 2011-2013:**

From 2011 to 2013, the Port of Antwerp was subjected to an attack in which drug traffickers intercepted and controlled container movement and position, allowing them to conceal illegal substances among the lawful cargo. The organization used a phishing attempt to send malicious

software to the personnel via e-mail, allowing them remote access to the port's data. Even though the first attempt was detected, and a security system was erected to prevent additional attacks, the hackers were able to gain access to port facilities and install key-logging devices on genuine machines. They were able to get wireless access to keystrokes typed by employees and screenshots from their computers in this way.

5.3 Cyber Attacks Methods

Cyber-attacks are criminal acts that aim to compromise, destroy, or access information technology systems or cyber assets, as well as operational technology systems, physical systems, computer networks, or personal computer devices [44]. Malicious people, groups, or state-sponsored organizations use a variety of tactics to conduct cyberattacks. The techniques employed by attackers in the maritime industry are:[45]

- **GPS Jamming**: Global Positioning System (GPS) jamming is also called brute force jamming. GPS jamming is an attack in which radio noise is broadcast on the GPS frequency, preventing the use of GPS, and potentially rendering a vessel's ability to navigate safely disabled.[45]
- **Global Position System Spoofing**: By receiving a bogus GPS signal, a GPS spoofing attack leads the targeted GPS to display the incorrect position. This form of attack is more harmful than a GPS jamming attack since an officer on a ship's bridge might not see it. A ship's safe sailing is jeopardized by an undetected attack of this type.[45]
- **Spear Phishing:** The attacker sends an email to the victim's account in this type of attack. The target could be a person, a department, or a firm. The malicious e-mail, which looks to be issued from a respected entity such as a bank, e-mail provider, or university, frequently asks the recipient to click a link. Personal data theft is the goal of this assault, which requires the victim to enter the required information on a pop-up screen, which could include passwords, personal information, and credit card numbers. A customized e-mail may also be sent, which may include the victim's name, logo, or personal information.[45]
- **Distributed Denial of Service (DDoS):** DDoS (Distributed Denial of Service) attacks are illegal. By overloading the network with heavy traffic and limiting access to its sites, the port information system is jeopardized. As a result, maritime services and cargo tracking are endangered.[46]
- **Malware:** Malware, often known as malicious software, is software that is meant to gain access to or damage a computer, server, or network without the victim's knowledge. Malware syphons resources from a computer and takes advantage of network flaws such as obsolete or unpatched software [45][44]

- **Ransomware:** It is a type of malware that encrypts contents on a computer and holds it hostage, compelling victims to pay money to get their files back. Ransomware has grown in popularity and has become a lucrative industry.[44]
- **Social Engineering:** Social engineering is a non-technical method of persuading employees within a company to violate security policies. Email, web, phone, and USB drives are only a few examples of social engineering strategies and means of application. Social engineering is exemplified through phishing.[44]
- **Virus:** A virus is self-replicating computer software that can infect a computer without the user's permission or knowledge. A virus can corrupt or delete data on a computer, propagate to other computers by attaching itself to an active host program or an already-infected application, and then execute code when a user runs these programs.[44]
- **Worms:** A computer worm copies itself as many times as possible from computer to computer. It can self-replicate without the need for human involvement and does not require the attachment of a program to inflict harm. Worms could change and remove files, as well as introduce more software into a machine. Unlike viruses, which proliferate by infecting an already-infected host file, worms are standalone malware that does not require a host software or a human to spread.[44]
- **Port Scanning:** Attackers use the traditional technique of scanning to verify the most vulnerable network ports. The purpose is to determine the status of services, establish the best database access method, and determine which users monitor services. As a result of the attacker's use of IP fragmentation to mislead the security system, the packet filters are bypassed, and the attacker can deliver incorrect data to ports.[46]

5.4 Key Cyber-Attack Scenarios

In this section, we will describe the key cyber-attack scenarios with the sources of threats and the possible impacts on port assets

1 Compromising critical data to steal high-value cargo or allow illegal trafficking through a targeted attack:

This is a sophisticated and targeted attack on port systems (Advanced Persistent Threat). On one hand, attackers seek out and retrieve authentication data (credentials) to gain access to valuable systems. Attackers use social engineering to collect information on port systems. Then they identify the targeted cargo and container management systems, as well as the personnel who use them. Once

attackers have discovered systems and their operators/users, they execute phishing assaults to obtain credentials to enter those systems. [47]

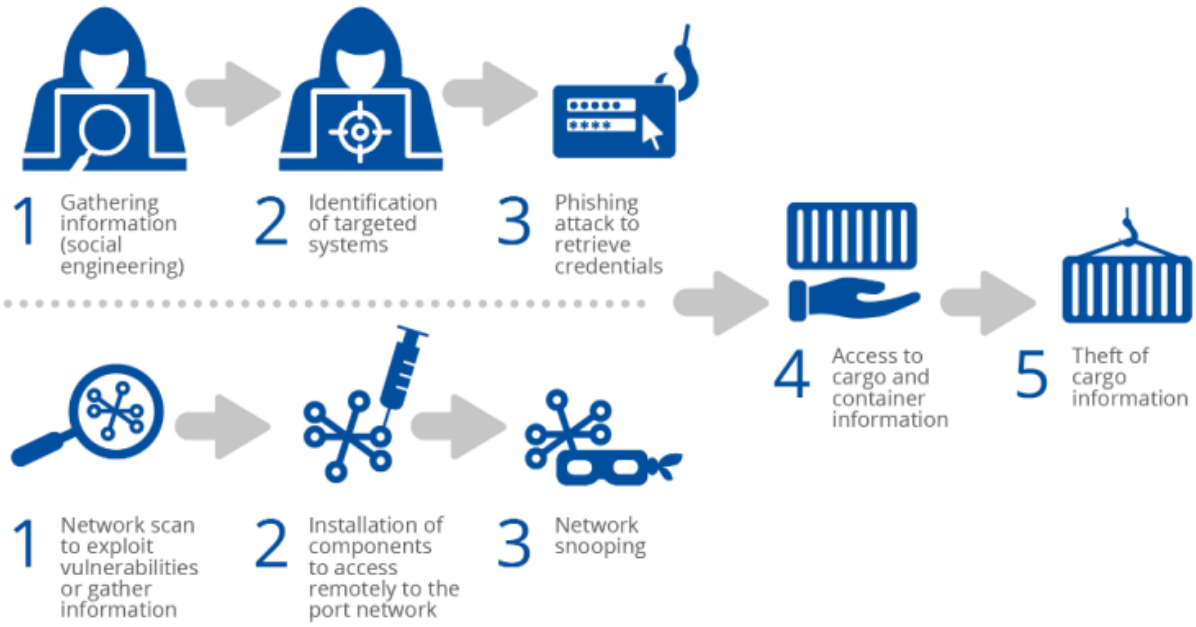

Figure 26: Compromise of data to steal high-value cargo or facilitate unlawful trafficking [47]

Attackers, on the other hand, install components to get remote access to the port network and circumvent network security. Attackers scan port networks for weaknesses that can be exploited, and information gathered. They install components that provide remote access to port networks, such as wireless access points if required through physical infiltration. They spy on networks to maintain constant access and to react to network and infrastructure changes over time. [47]

Attackers now have access to freight tracking systems and other relevant port systems, and they can access critical information on containers they want to steal from outside the port facilities, such as localization, content, pick-up code, and so on, and steal the cargo before the official pickup date. [47]

5.4.2 Propagation of ransomware leading to a total shutdown of port operations:

This scenario can be a targeted or non-targeted attack, such as collateral damage from a targeted attack on other companies via ransomware propagation. The large-scale event affecting Maersk's operations was an example of a damaging ransomware-like malware attack. [47]

Using social engineering, the attacker installs a ransomware-infected update on the port data via one of its servers. Using various unpatched vulnerabilities and a lack of network segmentation, the ransomware spreads over the port's network. The ransomware infects the port's systems and devices, stealing the credentials stored on them. The ransomware uses a way to elevate privileges by exploiting a flaw in the segregation of highly privileged accounts and then spreads throughout the port's network using the same mechanism. The compromised systems and gadgets have been encrypted and are no longer usable. While all systems and gadgets are down, a ransom is requested. [47]

5.4.3 Compromise of Port Community System for manipulation or theft of data:

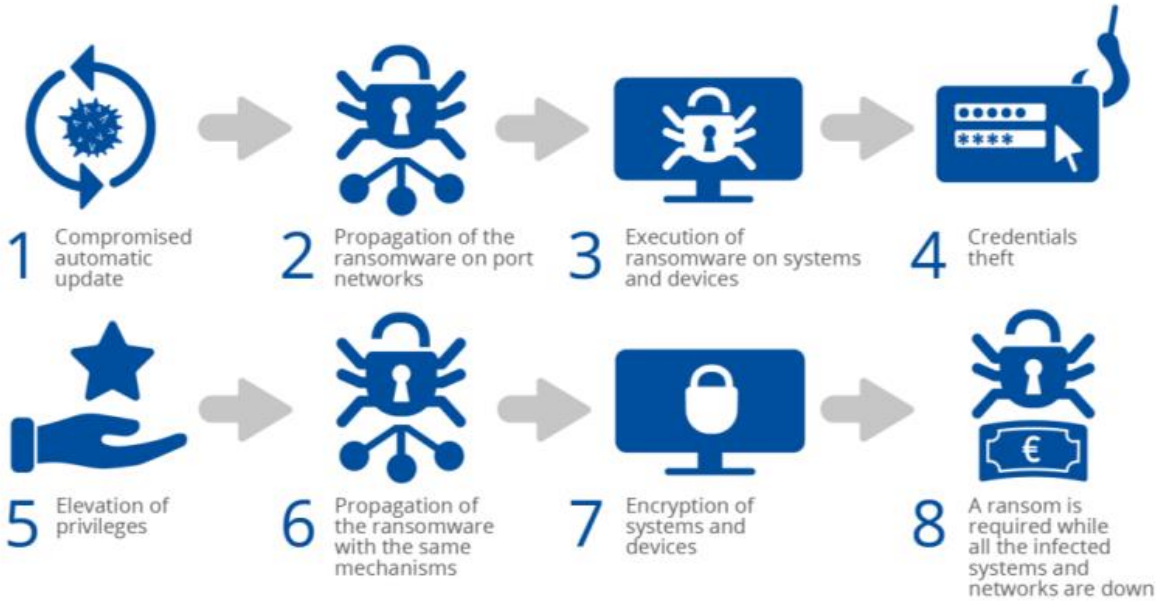

Figure 27: Propagation of ransomware leading to a total shutdown of port operations [47]

This scenario involves a targeted attack on the systems that allow all stakeholders to communicate, usually the Port Community Systems. The goals are to fake information about port services to interrupt operations or affect specific system activities, such as assuming an economic loss for the port. Because those systems are exposed to all port stakeholders in several ways, this situation is plausible.[47]

Because these mechanisms differ from one port to the next, this assault can be set up in a variety of ways: If the Port Community Systems are exposed through a web application, for example, the attacker can exploit common web application vulnerabilities; if the application is developed internally

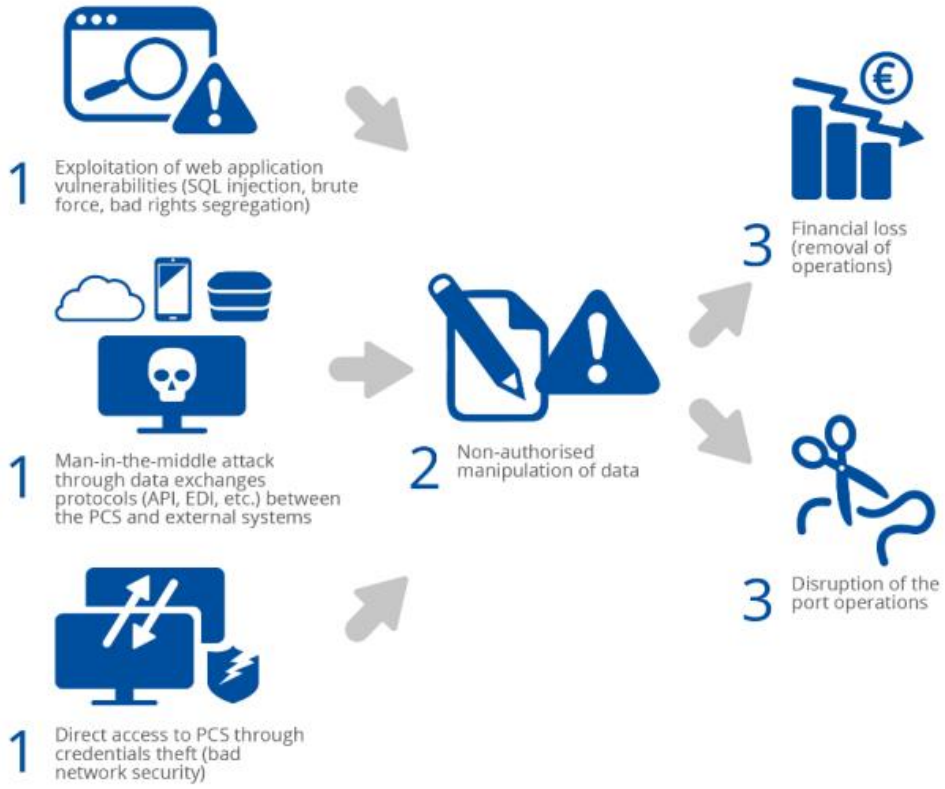

Figure 28: Compromise of Port Community System for manipulation or theft of data [47]

by port developers and standard security development rules are not followed, specific vulnerabilities can be exploited; and so on.[47]

Depending on the architecture of the PCS and the network's exposure: If the PCS is accessible to third parties via a specialized online interface, the attacker can get access to the PCS by using SQL injection, brute force attacks, exploitation of improper access rights segregation, and other standard web application vulnerabilities. If the PCS is automatically connected to external systems via data exchange protocols like API or EDI, the attacker can launch a man-in-the-middle attack by intercepting and manipulating data exchanges if they are not sufficiently secure. If direct access to the PCS is feasible outside of the port network, the attacker can take advantage of flaws in network security to get direct access to the system and utilize credentials he may have obtained through social engineering. [47]

Once the attacker has gained unauthorized access to the PCS and has sufficient access permissions, they can change data directly on the PCS, such as changing port operations, stealing important data, deleting data on certain actions, and so on. The loss of PCS data integrity has a number of consequences, including chaos in port operations, potential economic loss for the port as it loses information on operations, preventing it from billing for those operations, and even an accident if data related to dangerous goods is manipulated or made unavailable. [47]

5.4.4 Compromise of OT systems creating a major accident in port areas

A port contains a variety of operational technology networks, systems, and end-devices that are used for various services and operations and are owned, managed, and maintained by various stakeholders: cranes for vessel loading and unloading in port terminals, bridges at the port's entry to get vessels in and out, systems in refrigerated warehouses to keep fragile foods at a safe temperature, sensors and systems for transporting, storing, and monitoring dangerous goods, and so on. [47]

A malicious code is installed on a maintenance laptop that accesses OT control systems, either by a compromised USB drive or email or through the download of malicious software from the Internet. When the laptop connects to it, the malicious code spreads to the OT networks and eventually to the OT systems. If the Industrial Control Systems (ICS) are complex, attackers can use remote command mechanisms to control them. If this is not the case, the ICS code is updated to run predetermined commands from the malicious code. Cranes and bridges are examples of OT end-devices that move irregularly or unpredictably. This could result in a security and safety incident, resulting in port infrastructure damage or destruction, injury, death, and so on.[47]

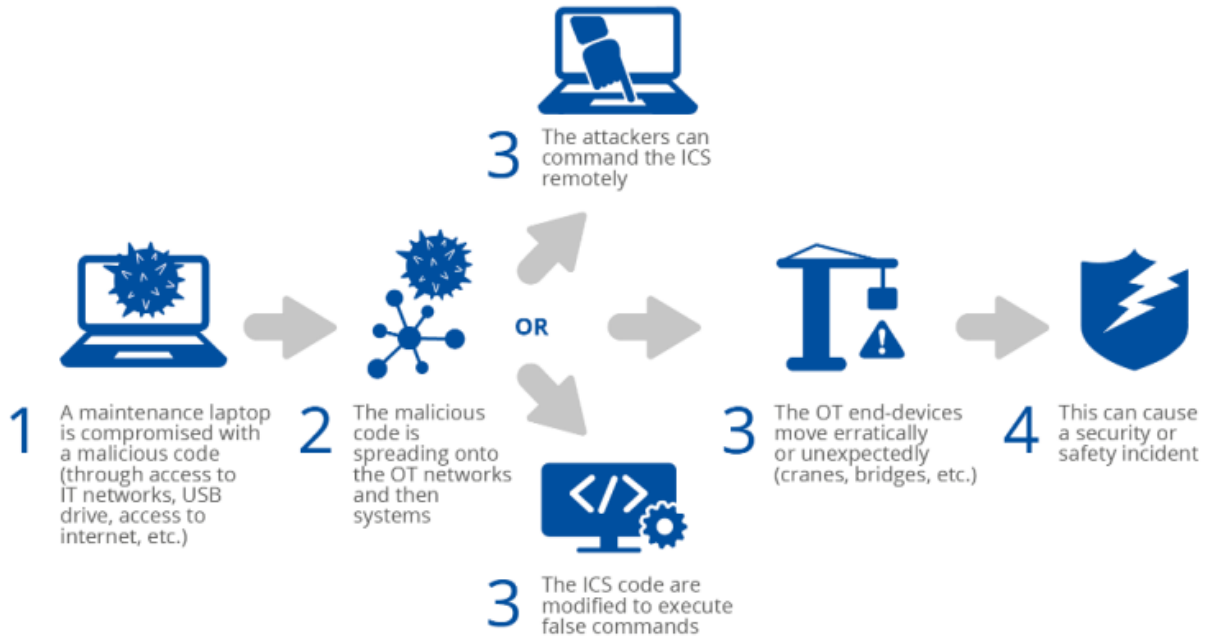

Figure 29: Compromise of OT systems creating a major accident in port areas [47]

5.5 Impacts of Port Disruption

Disruption refers to a disruption in which material flows are completely stopped, whereas delay refers to a disruption in which material flows are hindered. Both delays and disruptions will cause cargo to arrive later than expected, posing a risk to ports. Port disruption has a cascading impact, with costs

and benefits for adjacent ports. It is worth remembering that ports compete for cargo, so a well-timed disruption at a rival port may be beneficial. Five-day closure of a US West Coast port, for example, would cause ships to be rerouted to East Coast ports. These ships, most of which are too huge to pass via the Panama Canal, would have to transit the Suez Canal to reach the US East Coast, delaying their arrival by over a week. In this scenario, the Suez Canal suffers owing to unanticipated congestion, while US East Coast ports benefit from increased shipments. The level of coordination that goes into cargo flow emphasizes ports' interdependence and means that any disruption has a broad impact. The five potential hazards of port interruption are described here: congestion, economy, environment, geopolitics, and safety. [44]

5.5.1 Congestion

Port activity is becoming increasingly necessary to fit seamlessly into larger organization chains, yet congestion might prohibit ports and their networks from matching. When a port is overcrowded, it is assumed that ships are waiting in line for a berth. The higher the imposed expense, the busier the traffic. Time loss, additional fuel consumption, inconvenience, and potentially even accidents are all costs associated with traffic congestion. However, the most significant contributing element is time lost, which is passed on to others. Hapag Lloyd, a shipping firm, claims that its liners visit more than a dozen ports on each journey. Operations may be harmed because of delays, and congestion may be felt across the logistics chain.[44]

5.5.2 Economy

Ports are a significant economic multiplier for the success of a state. Ports handle about 80% of the world's trade volume and 70% of the world's trade value. Ports are crucial to trade, and their disruption would harm trade flows, economies, and numerous parties involved, in addition to port operations. Many stakeholders, from governments to businesses and individuals touched by marine trade around the world, are concerned about the economy [44]

5.5.3 Environment

Another potential hazard of port disruption is environmental degradation. The bulk of such accidents involves tanker vessels, barges, platforms, and petroleum shore stations, making oil and gas tankers one of the worst dangers in a port environment. Furthermore, unlawful human activities such as tanker cleaning contribute to some polluted locations. Every year, harmful chemicals such as diesel, oil, and petrol are dumped into the water, harming species, habitats, and ecosystems. While unlawful dumping is not always unintentional, it can have disastrous consequences for the ecosystem. Minimizing the risk of accidents requires actively working to guarantee port and ship security, including the cybersecurity of their physical systems, which can be exploited by enemies if they are weak.[44]

5.5.4 Geopolitics

Critical infrastructure protection has long been at the forefront of homeland security. You do not have a country if you do not have food, water, energy, power, or communication. Ports are strategically and politically vital to a state as critical infrastructure. "Ports are the main target in each campaign, for the enemy knows well the devastating impact on his opponent of seizing, or even putting out of service, the ports through which supplies, arms, and troops reach the battle zone," says the enemy. By jeopardizing states' capabilities, port disruption poses a geopolitical risk.[44]

5.5.5 Safety

Both dockworkers and sailors operate in dangerous environments, and they must undertake intensive safety training to avoid workplace mishaps. Fatigue, stress, teamwork, communication, and safety culture are all elements that influence maritime safety. Port interruption can have an impact on these elements, sometimes interfering with essential services like communication and putting people in danger. Furthermore, the loss of Critical Information Infrastructures may have an influence on safety. Furthermore, significant incidents can cause port disruptions and are harmful to the port's growth and efficiency, as well as its reputation.[44]

5.6 Mitigation Measures

- Regularly scan the network for unauthorized and malicious networks, such as WIFI, as well as end-devices that operate as bridges between two segregated zones, such as interfaces between two network zones.[47]
- Implement multi-factor authentication for accounts that have access to essential applications and data, such as personal information, sensitive operational data, and specific information on ships, dangerous items, and cargo.[36]
- Define installation and configuration policies and guidelines, as well as security baselines, to ensure that only necessary services and functionalities are installed, and that only essential equipment is authorized for the security and operation of port systems.[47]
- On all port systems, including PCs and servers, make that anti-malware, anti-spam, and anti-virus software is installed and up to current.[47]
- Define a cloud security assessment technique that considers applicable rules and regulations to assess the impact and risks of using cloud solutions.
- Implement mechanisms to secure machine-to-machine exchanges, such as EDI messages and APIs, which are mostly used with external stakeholders like shipping companies, and to provide mutual authentication, integrity, and confidentiality with port systems, use encryption,

PKI or digital certificates, integrity checks, digital signatures, and timestamping when exchanging information over the Internet.[43]

- Implement cryptographic methods and mechanisms in port systems to safeguard data secrecy, authenticity, and integrity.[47]
- Define an update management approach to keep port IT and OT assets current, as well as compensatory measures such as network segregation and account hardening for legacy systems.[47]

5.7. Cybersecurity challenges

the main challenges currently faced by ports to implement cybersecurity measures are the following:

- **Lack of digital culture in the port ecosystem:** latest trends, such as automation and IoT projects, are colliding with the marine industry's conservative attitude and are increasingly being implemented. Investors that are only interested in technology adoption sometimes overlook the cyber security concerns and best practices of these efforts. [47]
- **Lack of awareness and training regarding cybersecurity:** Previously, the ports ecosystem relied solely on safety and physical security to handle threats; however, IT and OT introduce additional cybersecurity issues that port stakeholders frequently fail to anticipate and grasp. [14]
- **Lack of time and budget allocated to cybersecurity:** As a result of a lack of understanding, adequate time and money is not invested in cyber security. [47]
- **Lack of human resources and qualified people regarding cybersecurity matters:** The ports need sufficient information technology and operational technology personnel to supervise all initiatives, particularly cybersecurity programs. Furthermore, cybersecurity skills are highly specialized and in short supply, making it difficult for small businesses to acquire appropriately qualified personnel. [47]
- **Complexity of the port ecosystem due to the number and diversity of stakeholders taking part in port operations**: A port's stakeholders might be numerous. This ecosystem is made up of businesses of varied sizes and cybersecurity capabilities, and some of them may even be direct competitors. Because of the disparate levels of control within the port, overall cybersecurity control at the port is difficult. [47]
- **Need to find the right balance between business efficiency and cybersecurity**, especially by ensuring service continuity while maintaining information technology and operational technology security, such as by disconnecting essential systems and updating systems without disrupting company operations [47]

- **Legacy of some systems and practices:** Especially when it comes to systems that manage navigation data and operational technology (OT) systems, which might be very outdated and susceptible, necessitating additional cybersecurity measures.[47]
- **Lack of regulatory requirements regarding cybersecurity:** The Network Information System Directive is a good starting point for implementing cybersecurity measures, although it only applies to specific marine stakeholders. This is insufficient to maintain a sufficient level of cybersecurity throughout the entire port ecosystem and to release sufficient money to meet the needs.[47]
- **Difficulty to stay up to date with the latest threats,** especially given the wide range of stakeholders who operate in ports, the processes, and systems that are deployed and used, and the quick expansion of innovations in the port ecosystem.[47]
- **Technical complexity of port information technology and operational technology systems:** Different systems are used by port stakeholders, which are built, managed, and maintained by different teams or groups. They can, for example, be built by port IT teams, third-party vendors, or IT services. They can also be based on a variety of technologies. Finally, the teams in charge of the security of IT and OT systems can differ. As a result, it is challenging to specify and maintain the mapping of all port systems over time.[47]
- **IT and operational technology convergence and interconnection:** Usually OT systems, more vulnerable than IT systems, are protected because they are separated from IT systems and networks. But, increasingly, IT and OT systems and networks, become increasingly dependent and interconnected, exposing OT systems to higher risks; [47]
- **Supply chain challenges.** The supply chain faces several cybersecurity challenges, including a lack of cybersecurity certifications for port products and services, security risks associated with supplier remote access to port networks/systems, long patching cycles for certain types of systems, heterogeneity and a large number of suppliers, and difficulty changing supplier services. Contractors have little control over their suppliers' cybersecurity and, as a result, the cyber dangers they expose themselves to (supply chain attacks).[47]

6. CASE STUDIES

6.1 PORT OTAGO LIMITED

Port Otago is 100% owned by the Otago Regional Council. In line with the company's Statement of company intent, Port Otago's main goal is "to perform as a a hit and sustainable enterprise that can provide price to our shareholders in the form of each monetary and non-monetary returns on investment". Port Otago employs approximately three hundred people and paid $32.2 million in wages and salaries at some stage in 2020/21. Just over $46 million turned into spent on substances and offerings and capital projects. The company's $five billion shipping-associated shipment throughput price (i.e. excludes Chalmers Properties) turned into made up of $4.6 billion exports and $0.four billion imports, reflecting the export nature of our country and region.[56]

Figure 30: A manual straddle crane at work on port [56]

As a part of the zero-damage tradition POL desired to become aware of troubles and tendencies in the safe operation of the Container Handling Equipment (CHE) earlier than ability injuries occur. This allows them to take proactive movement primarily based totally on actual measurable metrics with measurable benefits.[56]

6.1.1. Optimised Operational Control with Live Data Visualisation

The PORTSPECTIVE Management Suite and PORTAUTOMATION Mobile Systems supplied POL with a rich suite of systems that integrated seamlessly with every different and additionally offer external connectivity to third party systems. The POL integration includes sub systems for driver identification, device monitoring, GPS tracking and complete management operational visualization [56]

Figure 31: PortSpective Management System [56]

6.1.2 Key operational advantages:

1. Visualize the live operation, follow it, and report on it.
2. keep an eye on live surgeries and bottlenecks.
3. Keep an eye on the status of the equipment.
4. Quickly identify and fix problems.
5. Performance graphs, charts, graphs, time spent doing nothing, etc.
6. Analyze the tools safety.
7. Analyze current and historical KPIs incidents.

6.1.3 The PORTSPECTIVE Management Suit Includes:

- A live map display and an equipment status view.
- Alarms and errors are presented.
- Replays of historical data.
- Replay and analysis of a snail path.
- For large data analysis, a database with second-by-second data is required.

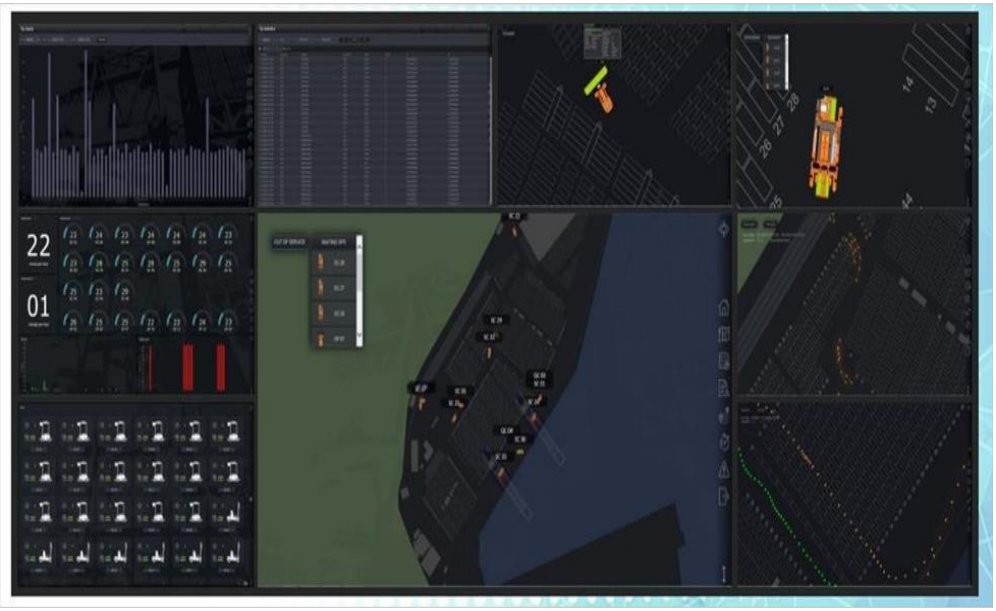

Figure 32: interface of port automation mobile system [56]

6.1.4 Features of Port Automation Mobile Systems:

- Tracks equipment in real-time operations.
- Collects equipment and safety data automatically.
- Operator pre-shift inspections on a touch screen.
- The PortSpective system receives real-time reporting.
- A reader for access cards has been installed.

6.1.5 D-MON features of access control:

1. Checks the operator's card and authorization levels.
2. Unauthorized usage is prevented.
3. Identifies and logs who is driving automatically.
4. PORTSPECTIVE will be updated in real time.

6.2 ROTTER DAM PORT

Rotterdam is a world-magnificent port, and Europe's biggest port via way of means of far. Anything you could believe passes via here. Rotterdam is the gateway to Europe. A crucial logistical hub for the complete planet. Goods pass through Rotterdam in their manner to and from destinations for the duration of the world. From pineapple juice to paper, from computer systems to chemicals. The port of Rotterdam stretches over a place of approximately forty-two kilometers, from the coronary heart of the town to the North Sea. Many docks are so deep that they can accommodate even the biggest vessels with a draught of as much as 24 meters, getting rid of the want to by skip through locks and permitting the vessels to moor quickly on the quay. Rotterdam is more than only a transit port. Numerous items are processed into various products here. The listing of sports is stunning: from the refining of oil to the production of plastics, from the unpacking of packing containers to the packaging of fruit into the portions required with the aid of using wholesalers, and so on. The items and services produced withinside the port and industrial vicinity have a complete introduced price of about 45.6 billion euros annually. [54]

Many human beings' paintings withinside the port itself, or at businesses which might be related to the port in exceptional ways. From oil buyers to chandlers. From tugboat crews to the folks who write laptop packages that manipulate all the delivery flows smoothly. From builders of cranes for unloading ships to caterers on visitor boats. From truck drivers to manner engineers withinside the chemical industry. In all, 385,000 human beings' paintings are in and round the port.

Port of Rotterdam Facts biggest European port rolling out shore-primarily based totally electricity for sea vessels by 2030 one of the most secure ports in the global with a mobile degassing station that doesn't launch petrol vapors into the air carried out by laws, together with banning smoking close to petroleum or oil terminals represents 6.2% of Dutch GDP welcomed deliver HMM Algeciras, on June third 2020, 20 meters deep, forty three meters brief of the duration of the Empire State Building.[54]

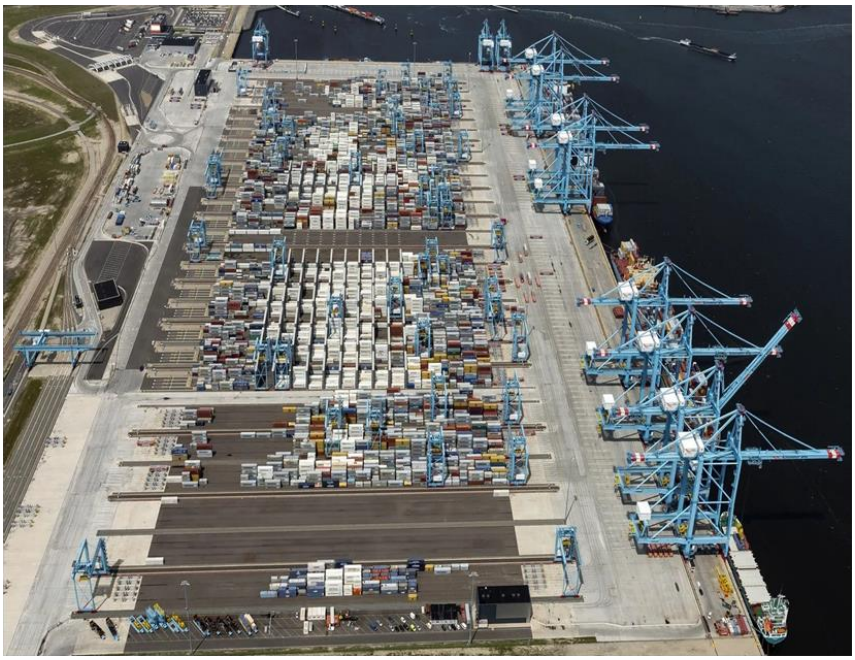

Figure 33: Port of Rotterdam [54]

Smart Port Initiatives Of Rotterdam

They have a Digital Twin. A Digital Twin is a completely virtual model in their port, giving them insights to how gadget withinside the port operates with one another. This additionally enables them to carry out real-time tracking of all operations. There are IoT (Internet of Thing) sensors measuring water movement, turbidity, and strain to make certain their sports are complying with environmental water standards. HavenLeerWerkPlaats is a constructing that has been built for port employers, employees, and process seekers to discover exertions possibilities on the port, combining network into the port They are operating to transition to renewable electricity reasserts and inexperienced electricity reasserts, hoping to impress their ports.[53]

What is a digital twin? A digital twin is a digital representation of a physical object or gadget throughout its complete lifecycle. It makes use of virtual equipment and real-time records to without a doubt create, test, construct and display a product or process – remaining the remarks loop among layout and operations. It is a resourceful technique that allows transformation without risking operations. And it is one which the Port of Rotterdam, Europe's biggest and busiest port, enthusiastically embraces. The assignment changed into a collaborative attempt that blanketed Rotterdam Port Authority, Axians, Cisco, IBM® and plenty of others.[52]

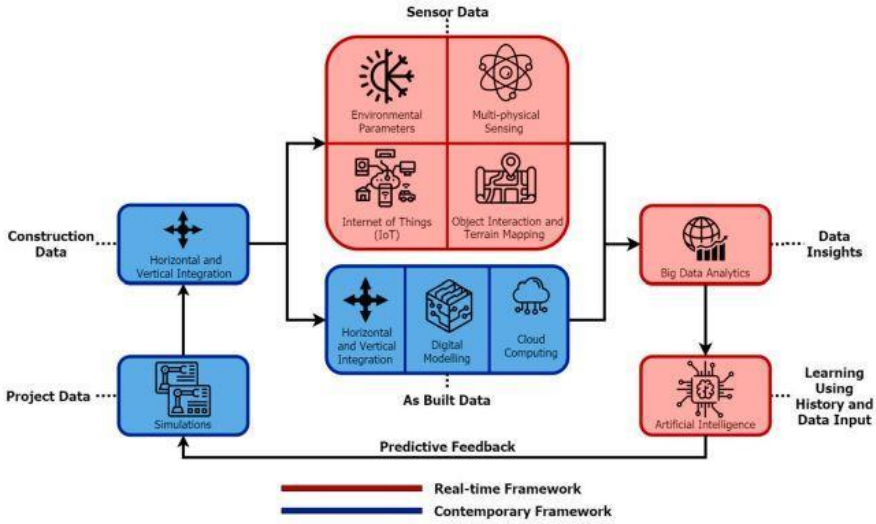

Figure 34: Smart Port Initiatives Of Rotterdam [52]

Very cleverly the usage of Watson IoT and artificial intelligence (AI). And with the cooperation of a global atmosphere of delivery companies, generation firms, and others inside their delivery chain. Sensors all through the expansive dock facility to constantly collect real-time facts air temperature, wind speed, (relative) humidity, turbidity, and salinity of the water plus water glide and levels, tides, and currents. The port even has "Digital Dolphins," clever quay partitions and sensor-ready buoys. Among the extra precise and modern components of the transformation is a sensor-packed experimental physical container, Container 42. This sophisticated research tool is journeying to associate centers all through the arena to gather geophysical readings. It returns the fact that this is consolidated into the ever-increasing pool of information [53]

Figure 35: Rotterdam Port Container 42 travels the world to gather research [53]

Using artificial intelligence to investigate all the data collected, it is viable to expect extra correctly what the excellent time is to moor and depart. This reduces ready instances and costs. For example, let us say a vessel must first sell off a part of its shipment in the deeper part of the port on the way to be capable of preserving sailing. With a virtual dual of the port, it is viable to calculate precisely how an awful lot of shipment desires to be unloaded there. This permits the vessel to sail faster and with extra shipment to its very last destination. Of course, to have dependable measures of intensity and draught, could be particularly important, each for safety, and commercially. Using a virtual dashboard that makes operations seen with 100$ curacy, transport agencies and the port can also additionally keep up to 1 hour in berthing time, that can quantity to approximately USD 80,000 in financial savings for deliver operators and permit extra ships to pass via the port every day.[53]

6.3 SHANGHAI YANGSHAN PORT

Shanghai Yangshan port is the second largest shipping port after the Singapore port. It is the deepest water port on the earth with 20 km key, 50 births and 30 km out into the sea [23]. It is connected to the mainland China with the world's second longest bridge on the sea which is 20 km shaped in the form of 'S' to reduce the tidal push on the bridge and the ships.

At the beginning before the port being developed, the phase 3 of the Shanghai port is on the bank of the river Yangtze where it meets the ocean. With the increasing demand of imports and exports and size of the ships, the phase 3 of the port cannot hold the on growing demand. The Shanghai port saw yearly 30 percent increase in the imports and exports, so a new port was built [23]. The Yangshan port is an artificial port with ten square kilometres of area. The cranes are immensely powerful that they can lift up to fifty containers per hour.

The port adopts fully automated terminal, intelligent production management control system with complete coordination of the hardware on the software system. It is employed with advanced green protection technology, which makes it a green and low carbon emission terminal. Various digitals technologies like 5G and intelligent driving were employed in the port. The intelligent heavy truck of Shanghai automotive industry is combined with the intelligent driving control system to produce autonomous vehicles which are used in the port [23]. The port is constantly developing both in size and digitalization making it the most advanced, largest, and deepest port in the near future.

Table 6: Digital technologies in Shanghai port [23]

Technology	Application
IOT	IOT platforms, data acquisition from the underwater, IOT sensors in logistics
BigData	Huge data processing and digital data platform
Cloud	Data storage on cloud about the containers and AV's
Blockchain	Paperless port, various platforms such as electronic EIR platform, process collaboration and data penetration between customers
Automation	Terminal is fully automated including AGV
Digital Camera and Sensors	Advanced CCTV cameras and sensors are installed

Figure 36: Shanghai Port phase IV [23]

7. FUTURE SCOPE

The future of port automation is promising, but it will be difficult. The future Port automation shouldn't merely run old processes with new automated equipment. The solutions should focus on adjusting to the actual working environment. The system and automated procedures must allow for the implementation of new methods and ideas, as well as respond to changes in the current working environment. The system, automated procedures, and actual working conditions must all be linked and be adaptable to new ideas and methodologies. The automation infrastructure must include a dynamic database structure and be able to handle the dynamic situations flexibly [52]

A solid project-governance and communication plan must be established, as well as a disciplined execution plan. Terminal operations, technical engineering, software engineering, and systems integration are just a few of the skills required for automation projects. Early feedback from stakeholders like as customers, shareholders, labor representatives, operations executives, the technical team, vendors, and external experts is critical in a collaborative project environment.[51]

With the upcoming 5G, or the fifth generation of cellular network technology, which is considerably faster than the old standard, supporting greater bandwidth for data throughput it can track and interact with roughly a million devices. For port terminals looking to enact broad automation efforts across their entire operations, this extreme device density means significantly more granular control over port operations and data collection. [55]

Blockchain, the technology that produced and allowed Bitcoin and other cryptocurrencies, is moving out of the financial sector and into a variety of other fields. The port industry is investigating the possibilities of blockchain to improve port connectivity, data security, and transparency. In a trial initiative aimed at improving the safety and efficiency of vital document flows, the Antwerp Port Authority is already experimenting with this technology. To transfer phytosanitary certificates, for example, the system uses blockchain technology. These are documentation that ensure the safety of produce being exported. These vital documents are rendered unalterable by blockchain technology, preventing document tampering. Port operators would benefit from full transparency of the document's history if blockchain was employed from the moment these phytosanitary certificates were generated, confirming their accuracy and legitimacy with perfect confidence.[55]

Given the speed of technological progress and that the construction of new terminals lasts between ten and twenty years, the ones we will see in 2040 could have the following features: Automated dockside gantry cranes, Automated container yard with bays, Automated horizontal transportation, Automated mooring system, Automated terminal access gates, Track & Trace for containers and Infrastructure to accommodate both automated and manual trucks simultaneously[52]

8. CONCLUSION

Automation developments in ports and terminals, focusing on new developments that offer the potential for new business models and enhanced trade flows. New business models may be realized using 'open' automation that does not need to rely on proprietary solutions, a trend that is accelerating for many sectors of the economy. New developments in automation require greater integration between multiple types of technology, e.g., systems such as the Internet of Things (IoT). These developments will enable the seamless flow of data throughout the entire container supply chain. They will also create new opportunities for port operators in the areas of logistics, automation, digital services, data analysis, and more. Such opportunities are more likely to arise as the level of automation increases, which is expected to be the case in the short- to medium-term, because of the rapid development of autonomous trucks, unmanned vessels, and drones. Therefore, opportunities for ports and terminals are likely to be affected in the short- to medium-term by new developments in automation [49].

Automation has also enabled other changes in the terminals, such as a switch from manual to autonomous containers. The introduction of automated systems has meant that container terminals will no longer need to have human labor involved in the process of storing and sorting the containers. In this case, the terminal is automated from the moment that the container arrives until it is processed. This means that the container is handled by a robot, without any human intervention. This is done to ensure that the container is stored safely since no person is supervising it during the storage. Automation and IoT are gradually making a mark on logistics and supply chain management, with their increasing use in ports and terminals. While the role of automation is still primarily in the field of handling, the role of IoT is more obvious when it comes to information collection [51].

REFERENCES

[1] Braidotti, L., Mazzarino, M., Cociancich, M., & Bucci, V. (2020, July). On the Automation of Ports and Logistics Chains in the Adriatic Region. In International Conference on Computational Science and Its Applications (pp. 96-111). Springer, Cham.

[2] Camarero Orive, A., Santiago, J. I. P., Corral, M. M. E. I., & González-Cancelas, N. (2020). Strategic analysis of the automation of container port terminals through BOT (business observation tool). Logistics, 4(1), 3.

[3] Ghiara, H., & Tei, A. (2021). Port activity and technical efficiency: determinants and external factors. Maritime Policy & Management, 48(5), 711-724.

[4] Iris, Ç., & Lam, J. S. L. (2019). A review of energy efficiency in ports: Operational strategies, technologies, and energy management systems. Renewable and Sustainable Energy Reviews, 112, 170-182.

[5] Park, S. H., Hwang, J., Yun, S., & Kim, S. (2022). Automatic Guided Vehicles Introduction Impacts to Roll-On/Roll-Off Terminals: Simulation and Cost Model Analysis. Journal of Advanced Transportation, 2022.

[6] Ma, N., Zhou, C., & Stephen, A. (2021). Simulation model and performance evaluation of battery powered AGV systems in automated container terminals. Simulation Modelling Practice and Theory, 106, 102146.

[7] Mansouri, F. S. A. A. K., Allal, A., Mansouri, K., & Qbadou, M. (2021). A model for analyzing capacity of ports to accommodate autonomous ships using k-means cluster analysis: a case study. International Journal on Technical and Physical Problems of Engineering, 13, 68-75.

[8] Wang, N., Chang, D., Shi, X., Yuan, J., & Gao, Y. (2019). Analysis and design of typical automated container terminal layout considering carbon emissions. Sustainability, 11(10), 2957.

[9] Yao, H., Xue, T., Wang, D., Qi, Y., & Su, M. (2021, March). Development direction of automated terminal and systematic planning of smart port. In 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE) (pp. 708-712). IEEE.

[10] Yu, H., Deng, Y., Zhang, L., Xiao, X., & Tan, C. (2022). Yard Operations and Management in Automated Container Terminals: A Review. Sustainability, 14(6), 3419.

[11] Martín-Soberón, A.M.; Monfort, A.; Sapiña, R.; Monterde, N.; Calduch, D. Automation in Port Container Terminals. *Procedia Soc. Behav. Sci.* **2014**, *160*, 195–204.

[12] Orive, & Santiago, & Corral, & González-Cancelas, (2020). Strategic Analysis of the Automation of Container Port Terminals through BOT (Business Observation Tool). Logistics. 4. 3. 10.3390/logistics4010003.

[13] Yu, H.; Deng, Y.; Zhang, L.; Xiao, X.; Tan, C. Yard Operations and Management in Automated Container Terminals: A Review. *Sustainability* 2022, *14*, 3419. https://doi.org/10.3390/su14063419

[14] Liu, C.-I.; Jula, H.; Vukadinovic, K.; Ioannou, P. Automated guided vehicle system for two container yard layouts. Transp. Res. Part C: Emerg. Technol. **2004**, 12, 349–368.

[15] Ku, L.P.; Chew, E.P.; Lee, L.H.; Tan, K.C. A novel approach to yard planning under vessel arrival uncertainty. Flex. Serv. Manuf. J. **2012**, 24, 274–293.

[16] Zhou, Chenhao & Lee, Byung & Li, Haobin. (2020). Integrated optimization on yard crane scheduling and vehicle positioning at container yards. Transportation Research Part E: Logistics and Transportation Review. 138. 101966. 10.1016/j.tre.2020.101966.

[17] Ku, L.P.; Lee, L.H.; Chew, E.P.; Tan, K.C. An optimization framework for yard planning in a container terminal: Case with automated rail-mounted gantry cranes. OR Spectr. **2010**, 32, 519–541.

[18] Choe, Ri & Park, Taejin & Oh, Myung-Seob & Kang, Jaeho & Ryu, Kwang. (2011). Generating a rehandling-free intra-block remarshaling plan for an automated container yard. Journal of Intelligent Manufacturing. 22. 201-217. 10.1007/s10845-009-0273-y.

[19] Wang, Nanxi, Daofang Chang, Xiaowei Shi, Jun Yuan, and Yinping Gao. 2019. "Analysis and Design of Typical Automated Container Terminals Layout Considering Carbon Emissions" *Sustainability* 11, no. 10: 2957.

[20] Rakibul Hasan, K. M. (2020). Port led development in Developing Countries for Effective and Efficient. *North America Academia Research*.

[21] Parkhurst, P. D. (2018). *New Technology and Automation in Freight Transport and Handling Systems.* Bristol: University of the West of England.

[22] Gonzalez-Aregall, M., Cullinane, K., & Vierth, I. (2021). A review of Port Initiatives to promote freight modal shifts in Europe: Evidence from Port Governance Systems. *Sustainability*, *13*(11), 5907. https://doi.org/10.3390/su13115907

[23] Xuyuan, S. (2021). Digitalization in the port industry from the perspectives of bibliometric analysis. Malmö, Sweden: World Maritime University

[24] Ab&r®. (2020, December 29). *HOW RFID can simplify your Container Verification System*. AB&R. from https://www.abr.com/how-rfid-can-simplify-your-container-verification-system/

[25] Logistics software. Best Logistics Software - 2022 Reviews, Pricing & Demos. (n.d.). Retrieved June 15, 2022, from https://www.softwareadvice.com/ca/scm/logistics-comparison/

[26] Dmitriev, A., & Plastunyak, I. (2020). Digital platforms for managing transport and logistics systems in the context of sustainable development. *E3S Web of Conferences*, *208*, 01007. https://doi.org/10.1051/e3sconf/202020801007

[27] Barlas, L. Y. (2000). The cost and efficiency of Port Container Tranportation. *International Symposium Marine Technologies and Managment.*

[28] Yang, Yongsheng & Zhong, Meisu & Yao, Haiqing & YU, Fang & Fu, Xiuwen & Postolache, Octavian. (2018). Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine. 21. 34-43. 10.1109/MIM.2018.8278808.

[29] Donepudi, Praveen. (2014). Technology Growth in Shipping Industry: An Overview. American Journal of Trade and Policy. 1. 137-142. 10.18034/ajtp.v1i3.503.

[30] Cil, Ahmet & Abdurahman, Dini & Cil, Ibrahim. (2022). Internet of Things enabled real time cold chain monitoring in a container port. Journal of Shipping and Trade. 7. 10.1186/s41072-022-00110-z.

[31] E. A. Kadir, S. L. Rosa, and H. Gunawan, "Application of RFID technology and e-seal in container terminal process," 2016 4th International Conference on Information and Communication Technology (ICoICT), 2016, pp. 1-6, doi: 10.1109/IcoICT.2016.7571926

[32] Sander van Kersbergen,"THE INTERNET OF THINGS IN THE PORT OF ROTTERDAM" ERASMUS UNIVERSITY ROTTERDAM, Erasmus School of Economics, Department of Economics, https://thesis.eur.nl/pub/31064/BA-thesis-Sander-van-Kersbergen-v1.pdf.

[33] A PEMA INFORMATION PAPER "RFID IN PORTS AND TERMINALS" https://www.pema.org/wp-content/uploads/downloads/2011/06/PEMA-IP1-RFID-in-Ports-and-Terminals.pdf

[34] Chalermpong Senarak, "Port cybersecurity and threat: A structural model for prevention and policy development", The Asian Journal of Shipping and Logistics, Volume 37, Issue 1,2021, Pages 20-36, ISSN 2092-5212, https://doi.org/10.1016/j.ajsl.2020.05.001.

[35] Ahokas, Jenna, et al. "Cybersecurity in ports: a conceptual approach." *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23*. Berlin: epubli GmbH, 2017.

[36] "Cyber Security for Ports and port systems code of practice," 16-Aug-2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf. [Accessed: 08-Jun-2022].

[37] Hackers breached computer network at key US port but did not disrupt operations, Aug 2021 [online] Available: https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html

[38] Port of Houston target of suspected nation-state hack, Sept 2021, [online] Available https://www.nbcnews.com/tech/security/port-houston-target-suspected-nation-state-hack-rcna2249 [39] South Africa port operations halted and workers reportedly put on leave after major cyberattack, July 2021, [online] Available: https://www.cnbc.com/2021/07/27/transnet-halts-port-operations-in-south-africa-after-major-cyberattack.html

[40] Disruptions from Cyber Attack Force S. Africa Port Operator to Declare 'Force Majeure' July 2021, [online] Available https://www.insurancejournal.com/news/international/2021/07/27/624407.htm

[41] Washington's Port of Kennewick hit by cyberattack, Nov 2020, [online] Available https://professionalmariner.com/washingtons-port-of-kennewick-hit-by-cyberattack/

[42] Iran says ports hit by cyberattack this week, but flow of goods unhindered, May 2020 [online] Available https://www.timesofisrael.com/iran-says-ports-hit-by-cyberattack-this-week-but-flow-of-goods-unhindered/

[43] Ahokas, Jenna; Kiiski, Tuomas; Malmsten, Jarmo; Ojala, Lauri M. (2017): Cybersecurity in ports: A conceptual approach, in Hamburg International Conference of Logistics (HICL), Vol. 23, ISBN 978-3-7450-4328-0, epubli GmbH, Berlin, pp. 343-359, Doi:10.15480/882.1448

[44] Kuhn, Kristen & Kipkech, Jeptoo & Shaikh, Siraj. (2021). Maritime ports and cybersecurity. 10.1049/PBTR030E_ch2.

[45] Oruc, Aybars. (2020). Claims of State-Sponsored Cyberattack in the Maritime Industry. 10.24868/issn.2515-818X.2020.021.

[46] Ben Farah MA, Ukwandu E, Hindy H, Brosset D, Bures M, Andonovic I, Bellekens X. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*. 2022; 13(1):22. https://doi.org/10.3390/info13010022

[47] “Port Cybersecurity - good practices for cybersecurity in the maritime sector,” ENISA, 26-Aug-2021. [Online]. Available: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector. [Accessed: 08-Jun-2022].

[48] Braidotti, L., Mazzarino, M., Cociancich, M., & Bucci, V. (2020, July). On the Automation of Ports and Logistics Chains in the Adriatic Region. In International Conference on Computational Science and Its Applications (pp. 96-111). Springer, Cham.

[49] Camarero Orive, A., Santiago, J. I. P., Corral, M. M. E. I., & González-Cancelas, N. (2020). Strategic analysis of the automation of container port terminals through BOT (business observation tool). Logistics, 4(1)

[50] Ghiara, H., & Tei, A. (2021). Port activity and technical efficiency: determinants and external factors. Maritime Policy & Management, 48(5), 711-724.

[51] Iris, Ç., & Lam, J. S. L. (2019). A review of energy efficiency in ports: Operational strategies, technologies, and energy management systems. Renewable and Sustainable Energy Reviews, 112, 170-182.

[52] Park, S. H., Hwang, J., Yun, S., & Kim, S. (2022). Automatic Guided Vehicles Introduction Impacts to Roll-On/Roll-Off Terminals: Simulation and Cost Model Analysis. Journal of Advanced Transportation, 2022.

[53] Boyels, R. (2019, August). How the Port of Rotterdam is using IBM digital twin technology to transform itself from the biggest to the smartest [web log]. Retrieved from https://www.ibm.com/blogs/internet-of-things/iot-digital-twin-rotterdam/.

[54] Witschge, L. (2019, October 7). Rotterdam is building the most automated port in the world. WIRED UK. from https://www.wired.co.uk/article/rotterdam-port-ships-automation

[55] leahy, E. (2020, August 12). 2020 state **of Port Automation (Part Two): The future is now. Tideworks. Retrieved from https://tideworks.com/2020-state**-port-automation-part-two-future-now/

[56] Chu, F., Gailus, S., Liu, L., & Ni, L. (2021, November 10). The future of Automated Ports. McKinsey & Company. Retrieved June 16, 2022, from https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/the-future-of-automated-ports