ClassNK MAGAZINE

June 2019 - 85th Edition

- *IoS-OP data sharing initiative goes global*
- *A systematic approach to cyber security*
- *NAPA adds catalyst to the ship data mix*

An ever-changing era

Welcome to the 85th edition of the ClassNK Magazine

We are in the midst of a paradigm shift soon to be in full swing. Digital technology has become widespread in our lifestyles and industry and is now changing the world. The ability to estimate actual conditions through data, analyze risk and set an acceptable range is essential; thus it is becoming more evident that those who actively utilize digital technology and data will succeed in the next era.

The methods of verification conducted by classification societies will drastically change in the future with the introduction of new technology. The use of AI, condition monitoring and data analysis through big data, remote monitoring, robotics and more will likely allow the classification process to develop further and enable real time assessment. ClassNK is also advancing its R&D initiatives in this field with its excellent human resources, experience, and vast intellectual property containing massive amounts of data which we have accumulated through many years of ship classification.

This year, we have released the ClassNK Cyber Security Approach followed by our Guidelines for Designing Cyber Security Onboard Ships for newbuilding designs as the first part of the ClassNK Cyber Security Series which incorporates requirements for taking onboard cyber security measures. In addition, we published the Cyber Security Management System for Ships which provides guidance on ensuring, implementing, maintaining and continuously improving the cyber security management system of companies and ships with the goal of safe navigation. A more in-depth look at all of these is provided within this special issue.

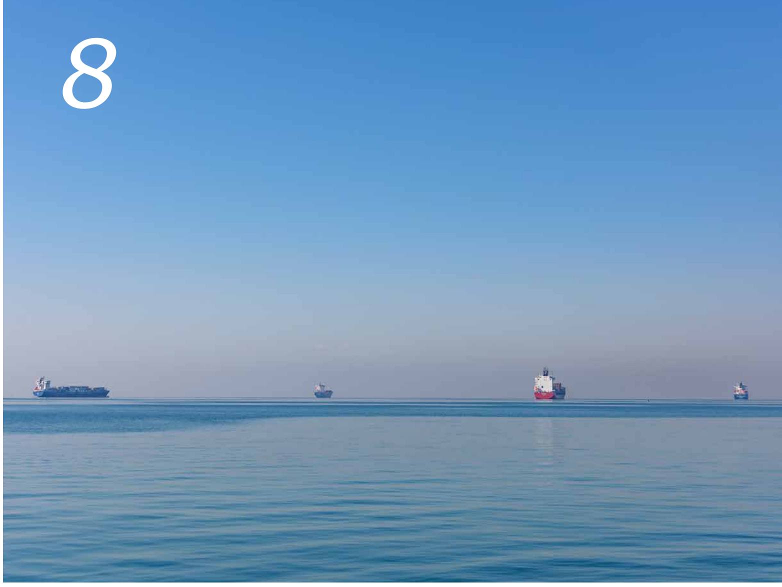
This edition features the various digital initiatives underway at ClassNK, such as the recent establishment of our Data Transformation Center. We are working together with our subsidiaries, such as Ship Data Center and NAPA, and other notable companies to further advance the Internet of Ships Open Platform (IoS-OP) initiative and digitalization overall.

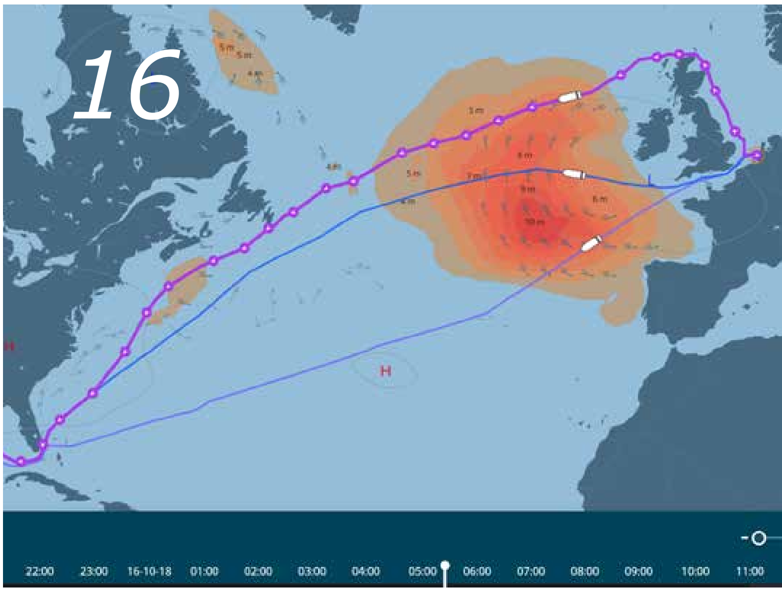
ClassNK is always ready to provide unrivaled support to the maritime industry during the constantly changing era.

I hope you enjoy this edition of the ClassNK Magazine.

Koichi Fujiwara, President & CEO

ClassNK





ClassNK

ClassNK Public Relations Team
4-7 Kioi-cho, Chiyoda-ku, Tokyo 102-8567, Japan
Tel: +81-3-5226-2047 Fax: +81-3-5226-2039
E-mail: eod@classnk.or.jp

ClassNK Magazine
85th Edition

Published by JLA media

ClassNK news

Carbon Trust partnership on climate change

06 December 2018 - The Carbon Trust and ClassNK Consulting Service Co., Ltd. signed an agreement to work together to develop a commercial partnership for offering climate change and sustainability services. The partnership will initially involve the two organizations exploring collaborative opportunities to deliver advice and consulting projects for businesses in Japan, as well as in selected markets across Asia more broadly. As a result of this partnership, corporates in the region will be able to access world-leading technical advice and support across areas, such as setting ambitious climate change targets, accurately reporting on environmental impacts, and developing strategies for achieving reductions. It will also be possible for companies to access independent environmental assurance and certification services, in line with internationally recognized standards. Japan's Ministry of the Environment has encouraged the nation's businesses to show leadership on climate change issues.

AIP for LNG-fueled KHI bulker

31 January 2019 - ClassNK granted an Approval in Principle (AIP) based on its Rule Part GF which adopts IGF Code (regulation for ships using low-flashpoint fuels) to Kawasaki Heavy Industries (KHI) for its project on the concept design of an LNG-fueled 207,000 DWT bulk carrier. Speaking on the occasion, ClassNK Corporate Officer and Director of Technical Solution Department Hayato Suga said "The maritime industry has been setting its sights on LNG as an energy source for ships as it is an environmentally-friendly alternative to fossil fuels. Kawasaki Heavy Industries is taking full advantage of this opportunity as well with its new bulk carrier design. We have carefully confirmed the safety of the design and are proud to contribute to this project." Kawasaki Heavy Industries has let it be known that it plans to widen its application of LNG propulsion technology in commercial vessels and to increase its focus on building LNG-fueled vessels.

New PrimeShip-Hull (HCSR) software

12 February 2019 - ClassNK released the latest version of its design support software PrimeShip-HULL (HCSR) Ver.6.0.0, developed in response to the IACS Common Structural Rules for Bulk Carriers and Oil Tankers (CSR BC & OT). The new version incorporates the latest rule amendments to CSR BC & OT including amendments based on feedback from the industry. In addition, various functions were added or improved in the PrimeShip-HULL (HCSR) prescriptive calculation software and direct strength assessment software. The enhanced calculation report function found in the prescriptive calculation software makes it possible to create reports for multiple sectional data all at once. The update also allows users to change output settings in detail, enabling the sorting of reports by section, evaluation item and more. Additionally, the enhanced data linkage function with 2D CAD data enables users to load the sectional data of outside cargo parts. It is now possible to load the sectional data of all ship parts.

2020 Sulphur cap support

02 April 2019 - ClassNK developed 'Guidance for onboard use of Compliant Fuel Oil with SOx regulation from 2020' and an implementation plan sample for switching to compliant fuel oil in order to support the industry in complying with the sulphur cap which will be enforced starting on 1 January 2020, requiring sulphur emission amounts to remain under 0.50%. ClassNK will also provide related appraisal services for the 2020 Sulphur Cap. Compliant fuel oil is anticipated to include more low-sulphur blendstocks than ever before in addition to light distillates. ClassNK has identified five properties of compliant fuel oil that should be taken into consideration with its use: Compatibility; Low viscosity; Cold flow properties; Cat-fines; and Ignition/Combustion quality. ClassNK released its guidance which explains the basic characteristics of each property, and the potential safety implications associated with them. ClassNK has also published the 'SOx PM regulations' section of its website.

New ClassNK Senior Executive Vice President

12 March 2019 - Effective 12 March 2019, Mr. Hiroaki Sakashita was appointed as Senior Executive Vice President as well as Executive Director of ClassNK. Mr. Sakashita graduated from the Division of Naval Architecture and Ocean Engineering, the Faculty of Engineering, Yokohama National University in 1980. Mr. Sakashita began his career at Japan's Ministry of Transport (now Ministry of Land, Infrastructure, Transport and Tourism) in 1980. During his period at the government he has played vital roles in maritime administration including regulatory oversight and industry development. He assumed the position of Director-General of the Maritime Bureau in 2015, and Deputy Minister for Technical Affairs, Minister's Secretariat in 2016. He joined ClassNK in 2018 as Executive Consultant and has been appointed to the current position overseeing ClassNK's expansion of its business portfolio and digital transformation.

Mr. Hiroaki Sakashita
ClassNK Senior Executive Vice President

ClassNK releases its Cyber Security Approach

29 March 2019 - ClassNK has released the ClassNK Cyber Security Approach which outlines its basic approach to ensuring onboard cyber security for ships. It was released alongside its Guidelines for Designing Cyber Security Onboard Ships for newbuilding designs as the first part of the ClassNK Cyber Security Series which incorporates requirements for taking onboard cyber security measures.

In the ClassNK Cyber Security Approach, ensuring navigational safety is regarded as the most important goal of onboard cyber security. To achieve it, high priority is given to availability of systems in terms of operation technology (OT) as well as information technology (IT) systems, which support operation of ships.

To mitigate cyber risks in both IT and OT, the Society will propose measures based on a balanced combination of physical, technical, and organizational approaches, such as designing ships and onboard equipment with security by design, constructing management systems during service, etc.

Specifically, ClassNK will classify cyber security controls into different layers, and clarify what each stakeholder should do for each layer by adopting requirements from the existing standards on cyber security that are considered applicable to ships.

ClassNK Cyber Security Management System for ships

15 April 2019 - ClassNK has released its Cyber Security Management System for Ships. As part of the ClassNK Cyber Security Series, ClassNK regularly releases guidelines and standards that outline cyber security measures based on the recently-released ClassNK Cyber Security Approach that outlines ClassNK's basic approach to ensuring onboard cyber security for ships.

The Cyber Security Management System for Ships provides guidance on ensuring, implementing, maintaining, and continuously improving the cyber security management system of companies and ships with the goal of safe navigation. It includes management measures regarding protection against cyber risks in not only the navigation stage, but also in the construction/design stage of ships through Security by Design. The standards focus on the Information Technology (IT) and Operation Technology (OT) that support ship navigation and were created with reference to the latest IACS recommendations and ISO27001(*1) and ISO27002(2*) Information Security Management System global standards. "In the meantime, ClassNK's new Guidelines for Designing Cyber Security Onboard Ships acknowledge measures from the NIST SP800-53(*) compiled for the US Government that can apply to ships, and the latest IACS recommendations."

For further information see pp. 12-15.

Digital drive

ClassNK is spearheading the development of new digital services

A wave of digitalization is currently sweeping through the maritime industry that could dramatically change the face of commercial shipping. New technology promises to transform almost every aspect of vessel operation and management. It will also have an impact on classification societies. To prepare for this digital future, ClassNK has initiated multiple initiatives spanning all of its departments and business areas.

These various efforts, some of which are described below, are being overseen and coordinated by a newly established Digital Transformation Center (DXC) so that the outcomes generated can be applied as widely as possible throughout the society and to ensure that our customers gain maximum benefit.

Vessels transmit ever larger quantities of data concerning overall operational status and the condition of onboard machinery and equipment by satellite back to shore-based datacenters, where it can be combined with the latest weather information.

The next step is to merge that data with a virtual model of the ship – the so-called 'digital twin' – based on the design and technical specification data. Instead of providing a snapshot at a single moment, these 'digital twins' will allow owners to track a vessel's condition and performance through her life taking into account operational information as well as any modifications made since it entered into service.

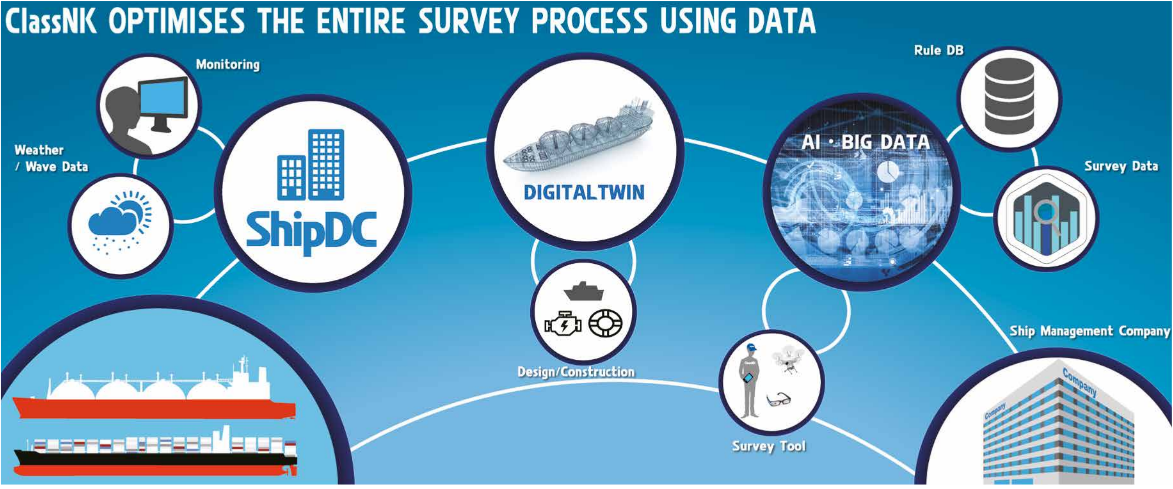
Flexible survey scheduling

Such innovations may eventually trigger a rethink on how surveys are planned and carried out. Typical class surveys are conducted at fixed intervals. Utilizing innovative technologies (including artificial intelligence) can realize more flexible intervals or condition based surveys based on the outcomes of previous surveys, a vessel's current condition and the demands imposed by regulatory requirements. Moreover, such developments would let surveyors concentrate on the onboard systems or parts of the vessel that need most attention.

The fact that a growing number of vessels are collecting data from equipment and using condition-based monitoring indicates the industry is already moving in that direction. In fact, some owners have already started experiments with a predictive diagnosis system capable of analyzing data to predict faults before they happen.

Naturally, many questions will need to be answered as the industry transitions from a survey regime based on conventional regulations to one based solely on data collection and analysis. To meet this challenge, ClassNK has initiated a study into what types of data should be collected and what sort of analytical methods would be necessary for a condition-based approach to ensure the same safety level as a conventional inspection.

If eventually class surveys can be implemented according to condition diagnosis, surveys will become more efficient for ship management companies and maintain – or perhaps even increase – the overall level of ship safety.



ClassNK OPTIMISES THE ENTIRE SURVEY PROCESS USING DATA

It is worth noting that today the use of sensors and data analytics is predominantly focused on managing the condition of onboard machinery and equipment. However, ClassNK is looking further ahead and researching the possibility of adapting the technology for monitoring the integrity of hulls and other structural elements.

Assisting the ship manager

In the nearer term, ClassNK is working on developing a service that harnesses algorithms to assist ship management companies optimize when they send a ship for a survey. Currently they have to decide the scheduling for themselves.

The envisaged service would take into account vessel operation data, weather, harbor traffic, surveyor locations and other relevant data points to calculate and propose a suitable date and place as well as recommend survey items.

Another effort is aimed at bringing plan approval for newbuilds fully into the digital age. While some progress has been made, for example, allowing shipyards to supply plans for approval as PDF documents instead of physical paper, the fundamental approach is the same as ever. This is because the acceptable digital formats are paper-equivalents; they are not pure data. Currently, ClassNK is exploring the options that would allow approvals based on data taken directly from CAD systems.

Switching to a fully data-driven process would not only reduce the manhours spent on vessel design by decreasing the time taken to review plans, but would likely improve quality by ensuring consistency and preventing the errors that can sometimes occur when proposed corrections or modifications are fed back. ClassNK's efforts towards realizing a truly digital approval process are focused on developing a viewer with appropriate functionality and digitalizing its rules for the survey and construction of ships that form the basis of the approval process.

Various initiatives to unlock the full potential of digitalization are currently underway in the marine industry. In addition to the future-oriented work described above, ClassNK is proactively enhancing certification services through means such as by developing guidelines that assume certification of hardware and software solutions intended to support more efficient vessel operation as well as cyber-security certification services, and it makes possible to promote these initiatives relating to digitalization.

These are just portions of ClassNK initiatives on digitalization, and we plan to provide other services that will facilitate our clients to realize their innovation with digitalization.

IoS-OP data sharing initiative goes global

ShipDC invites the industry to step up to its Internet of Ships Open Platform

The Internet of Ships Open Platform (IoS-OP) initiative from ClassNK subsidiary Ship Data Center Co., Ltd. (ShipDC) is the transparent architecture for data distribution that the Society believes delivers the new type of maritime cluster needed in the digital era.

Even in anonymized form, vessel data analytics can provide guidance on: ship speed reductions in stormy weather; optimized engine outputs over given routes; energy-saving device evaluation; pre- and post-dock performance after a given procedure; offshore waiting times by port; etc.

At a time when drone-based inspection, sensor-based condition monitoring and product design using digital twins are bringing gains of an ever-more precise nature, the IoS-OP seeks to reap cumulative benefits of sharing data across software, equipment and operational parameters. In this way, the full safety, maintenance and efficiency benefits available from shipping's digitalization can be unlocked.

ShipDC MEMBERS

Shipping Company	**9%**
Shipyard	**18%**
Marine Manufacturer	**42%**
ICT	**20%**
Others	**11%**

55 companies

ClassNK established ShipDC as a subsidiary business in 2015 to provide a focus for the rising volumes of IoT data generated by vessels. Its role has quickly blossomed, with the subsidiary tasked with orchestrating plans for diverse and increasingly digitalized industry players to access and use data in a safe and secure manner.

The result has been an initiative for the IoS-OP to bring clarity to rights over data, find a sharing strategy that is satisfactory for shipowners, ship managers, shipyards, marine manufacturers, etc., and develop solutions that can be deployed in reality.

Its combination of the IoS-OP Common Rules and the ShipDC system infrastructure as a data center provides the basis for neutral data governance, where each player is free to develop competitive services separately through data driven innovation.

Initially established as a membership consortium overseen by ShipDC at the end of May 2018 and including 46 companies, the IoS-OP Consortium had expanded to 55 members by the end of last year. Its diverse stakeholders include shipowners, ship managers, shipyards, ship design companies, marine manufacturers, classification societies, insurers, weather information providers, trading companies and research institutes, but also ICT companies from outside the maritime industry.

From the practical point of view, the Consortium holds Plenary Meetings

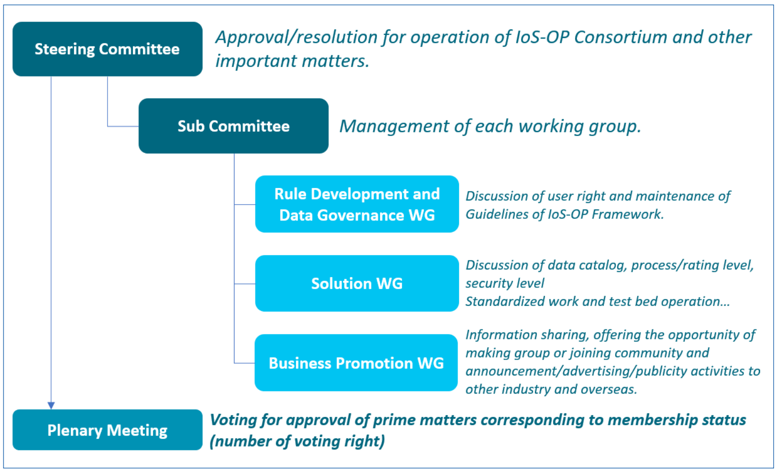
The IoS-OP seeks to reap cumulative benefits of sharing data across software, equipment and operational parameters

for all members and is served by a Steering Committee of platinum/elected members, a practitioner-level Sub Committee and working groups (WG).

Speaking at the global launch of the new IoS-OP at Sea Asia, Singapore in April 2019, Mr. Yasuhiro Ikeda, President of ShipDC said: “We have prepared a platform where everyone could make data driven innovation under the agreed rules. Now, it is time to invite everyone to join the initiative to create an innovative solution in the maritime industry.”

Digitalization is clearly benefiting shipping’s operational efficiency - for example through the sensor-based condition monitoring that enables remote and predictive diagnostics services, but rigor is needed in an industry supported by a patchwork of software solutions and fragmented data capture. Lack of harmonization – between marine manufacturers, management cultures and ship operations – make data difficult to collect and difficult to use. With shipping’s commitment to shipboard sensors highly variable and its monitoring practices inconsistent, it is also fair to question data quality; even data that has been collected successfully may be hard to draw common conclusions from.

To date, even though the IMO’s Energy Efficiency Design Index (for example) depends on information exchange and benchmarking, there has also been no framework of regulation governing data ownership, and lack of consensus on the rights of stakeholders to share or use data.



Steering Committee

Approval/resolution for operation of IoS-OP Consortium and other important matters.

Sub Committee

Management of each working group.

Rule Development and Data Governance WG

Discussion of user right and maintenance of Guidelines of IoS-OP Framework.

Solution WG

Discussion of data catalog, process/rating level, security level
Standardized work and test bed operation…

Business Promotion WG

Information sharing, offering the opportunity of making group or joining community and announcement/advertising/publicity activities to other industry and overseas.

Plenary Meeting

Voting for approval of prime matters corresponding to membership status (number of voting right)

One of the first tasks of the IoS-OP Consortium has therefore been to develop rules for data utilization that will ensure transparency and data ownership. Its Rule Development and Data Governance WG has defined the roles and rights of each stakeholder, and reviews guidelines for the quality of data and the needs/methods for anonymization and statistical analysis, and on definitions for the role and rights of each stakeholder prepared by the Solution WG.

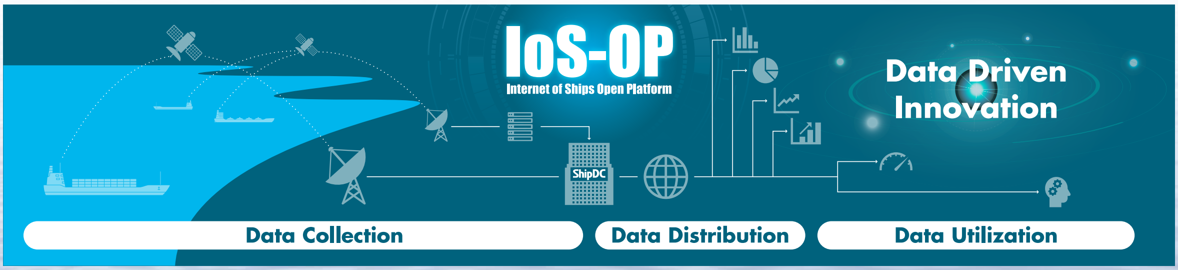
As data is not creative and is not subject to copyrights, the IoS-OP Consortium identifies the data usage right as an ownership principle conferred by the cost of owned equipment for data collection and data communication to shore. Data owners should keep observing efforts for data quality improvement and fair, orderly data sharing.

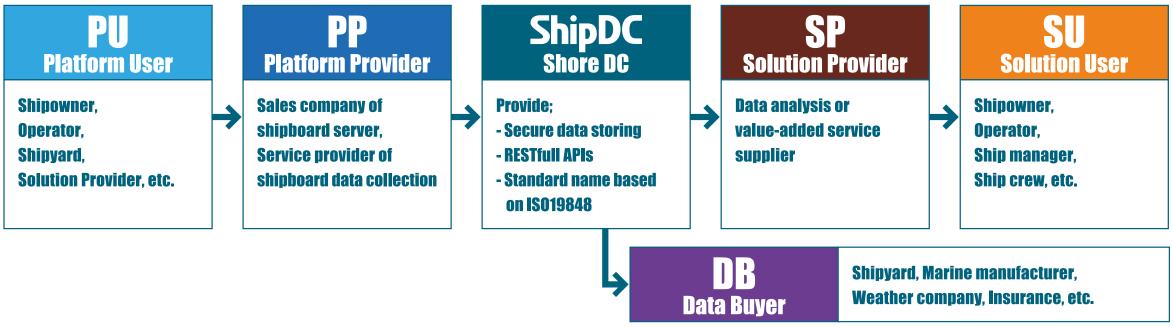
The IoS-OP Common Rules therefore clarify use of data applicable between stakeholders, formulating data transactions for each stakeholder, with a basic agreement applied uniformly and individual contracts applied according to their roles. The roles of stakeholders are clearly separated, and six roles are defined:

- Platform User (PU) - The data owner who pays the expense for data collection (shipboard equipment and communication costs) - Mainly shipowner, ship manager, operator, shipyard, etc.

- Platform Provider (PP) - The sales company of shipboard data server or service provider of shipboard data collection.

- ShipDC - The shore data center with the secure data storage on cloud, access control using secret keys, and data distribution via RESTfull APIs.





- Solution Provider (SP) - The supplier of data analysis or value-added service, such as remote maintenance support, performance analysis report, condition monitoring, etc.

- Solution User (SU) - The user of services of SP (Mainly shipowner, ship manager, operator, ship crew, etc.).

- Data Buyer (DB) - The data usage rights purchaser who utilizes data for their own product improvement (Mainly shipyard, marine manufacturer, etc.).

ShipDC can also convert the names of stored data readable by humans to machine readable standardized names from the Japan Ship Machinery and Equipment Association (JSMEA) Dictionary in accordance with ISO19848 “Standard data for shipboard machinery and equipment”, so that the shipowner or operator can obtain more benefit. The IoS-OP is the ecosystem where collection, distribution and utilization will lead to data driven innovation and where stakeholders can interact to build solutions in a collaborative manner.

The collaborative approach to data could also be extended to role sharing, because the IoS-OP can simplify the systems approach taken by stakeholders, which in itself can encourage more effective use of data, lower data transfer costs, more consistency in data governance and the streamlining of data transfer from ship to shore.

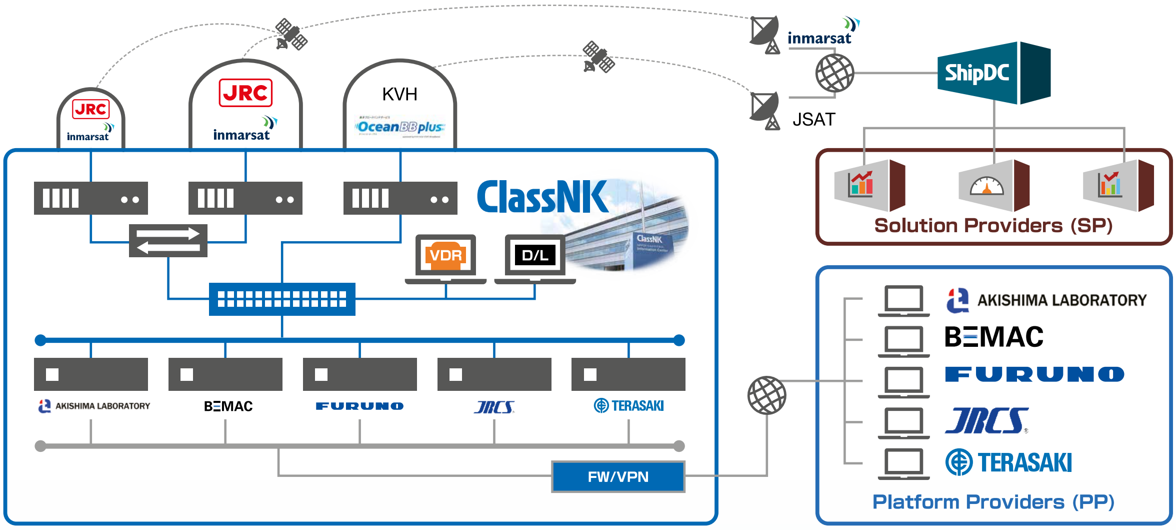
Given that transparency is one of the guiding principles of the IoS-OP, it is worth dwelling on the work to establish its collective direction of travel.

One small team of the Solution WG is focusing on measures specifically related to security concerns for PP, SP and DB in discussing risk assessment to ensure confidentiality with reference to the National Institute of Standards and Technology (NIST) SP800-171 and Information Security Management System (ISO27001).

This work aligns with the Smart Ship Application Platform (SSAP) project, through which JSMEA has contributed to International Standards Organization work to standardize capability of shipboard data server and data structure/naming.
Here, ISO19847 provides requirements for the way the shipboard data server collects data from other shipboard machinery and equipment, and shares it in a safe and efficient manner. These mainly functional requirements cover data input/output, storage, monitoring, backup and restoration, security and reporting. ISO19848, meanwhile, makes it easier to connect shipboard applications at manageable cost by bringing both standards to the software capturing and processing sensor data.

The IoS-OP Consortium provides the bridgehead for real-world adoption. Its focus is on the Testbed needed to enable technical verifications before shipboard installation of actual equipment and systems, drawing on a simulated shipboard data collection environment that is supported by satellite connectivity to enable data collection/storage tests at ShipDC. By using the IoS-OP testbed methodology, members can try out data transfer, new services, etc. without loss of time, effort and cost.

The shipboard data servers TERASAKI Marine Information Platform from Terasaki Electric Co., Ltd., and BEMAC IoT from BEMAC Corporation are ISO19847-compliant, making it possible to evaluate conformity to ISO standards for existing systems and services, examine new services, try the high-speed satellite communications service, and pre-test in advance of real



ship tests. Here, the 'shipboard' network equipment simulates the inboard LAN. Other shipboard servers such as the FURUNO Open Platform from Furuno Electric Co., Ltd., Fleet Monitor from Akishima Laboratories (Mitsui Zosen) Inc., and T330 from JRCS Co.Ltd, will be ISO19847-compliant in due course and can be evaluated with similar conformities. Satcoms comes via the Fleet Xpress (Inmarsat) and the OceanBB plus (SKY Perfect JSAT Corporation).

Pre-tests investigated engine preventive maintenance services via remote engine monitoring, considered new maintenance services remotely, and examined analysis services utilizing ShipDC's ship IoT data. They also trialed the satellite communications infrastructure used for ship-to-shore data communication and derived functional verifications of shipboard data servers and shipboard application.

Having launched the platform for IoS-OP, ShipDC has also gone on to strengthen the system infrastructure by expanding the API functions for data retrieval and expanding functions such as the management function for data usage rights. ShipDC, meanwhile, has developed the data management console system for visualization of data reception, storage, usage, usage right sales, etc. This means the PU itself can add ships and shipboard devices and revise meta information online, also issuing the data access key and setting access control etc.

ShipDC has also developed a standard data name conversion AI tool, so that the data name of each ship can be converted to standardized formats using natural language processing technology in AI (this feature is currently being trialed internally).

Furthermore, ShipDC is augmenting the nowcast meteorological and oceanographic data it offers through Japan Weather Association (JWA) with a newly-developed interface to provide IoS-OP users with global meteorological and oceanographic hindcast data (POLARIS Hindcast). This makes it possible for IoS-OP users to use more accurate hindcast data through the ShipDC API, and to expand the use of the ship's operational data.

At Sea Asia in April, ClassNK once more emphasized that ShipDC services facilitating data collection onboard and data transmission to shore to conduct tests such as data collection, sending and acquiring data using the IoS-OP were available free of charge for ShipDC members.

This is perhaps one reason ClassNK has been recognized in securing the Data Science Award 2018 for 'Practical Efforts to the Utilization of Ship IoT Data that Data Scientists Can Succeed'. Sponsored by The Japan DataScientist Society, the award honours projects and organizations that make significant contributions to the analysis and use of data. It was secured after judges considered the full range of efforts made by its subsidiary (ShipDC), in developing common rules, towards standardization, and in testbed methodology, but also through the training courses and internships that will make the next generation ready for the Data Science.

A systematic approach to cyber security

ClassNK's multi-layered cyber security strategy can ensure the safety of ships, crews and cargoes

From main engines and propulsion systems to cargo handling and navigation equipment, the common denominator for the systems that are critical to safe and efficient vessel operation is their reliance on computers. Left unguarded, ship systems are vulnerable to unauthorized interference, whether through error or by malicious design.

The International Maritime Organization's first comprehensive response to cyber security came in 2016, when the Maritime Safety Committee issued an interim circular to raise awareness which also offered owners high-level recommendations for safeguarding onboard processes and systems.

The following year IMO adopted further non-mandatory guidelines (MSC.428(98)) that brought cyber-risk under the purview of a vessel operator's safety management system, in line with the objectives and requirements of the ISM code. Crucially, evidence that cyber-risks have been appropriately addressed should be available for inspection no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

While being clear on what is required, MSC's resolution did not go into details on how companies should assess the risks and prepare for achieving the requirements. Recognising a need to help vessel operators close this gap, ClassNK set about investigating the threat landscape and the sort of workarounds and remedial actions that would be needed to protect vulnerabilities.

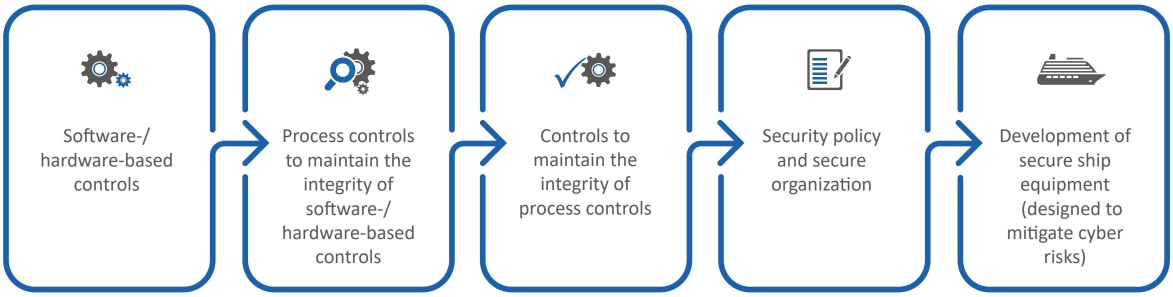
> *ClassNK has separated its recommendations across five layers, touching on different aspects of the cyber security threat*

The extensive research effort has now been distilled and compiled into the ClassNK Cyber Security Approach, a guidance document which provides stakeholders with a new and methodical approach for assessing their exposure to cyber risk and identifies measures to mitigate them.

In doing so, ClassNK has considered risk both from the perspective of operational technology (OT) used for controlling machinery and equipment and information technology (IT) used for manipulating data. As ships become more connected and automated, the distinct boundaries that traditionally separated OT and IT systems are becoming increasingly blurred and it is no longer possible to tackle one without tackling the other. This necessitates a response that balances physical, technical, and organizational mitigations.

Accordingly, ClassNK has separated its recommendations across five layers, touching on different aspects of the cyber security threat. The first layer covers controls on software and hardware, where defences are typically secured technologically. The second covers processes to maintain software and hardware integrity, which mostly focus on user procedures. The third layer addressed the maintenance of those procedures, for example, by training. The fourth layer concentrates on building resilience into the organization framework that underpins vessel operations. Importantly, this aligns with requirements set out by IACS, BIMCO, OCIMF and other industry bodies.

A multi-layered approach to cyber security onboard



Software-/hardware-based controls

Process controls to maintain the integrity of software-/hardware-based controls

Controls to maintain the integrity of process controls

Security policy and secure organization

Development of secure ship equipment (designed to mitigate cyber risks)

The fifth layer looks beyond equipment and systems already in service, and is instead directed at urging OEMs and software developers to prioritize security and adopt relevant ISO and IEC standards in the design and testing of new solutions. These layered Guidelines are augmented by six annexes that apply to universal aspects of the digital infrastructure used on ships: access control and authentication; software updates; managing portable devices; physical protection; external communication; and software integrity. The salient points from these annexes are summarized below.

Annex 1: Access control and authentication

Access control is a first principle of systems protection: interference with an electric power system can lead to failure/black-out, for example; again unauthorized changes to a propulsion system may result in it rejecting commands from the authorized operator, and loss of vessel control.

Access control policies and user authentication methods must be well-designed to ensure they achieve their objectives. A single username and password combination that is shared among multiple crew members for the sake of convenience and not frequently changed is a weak defense: information can be easily passed on to unknown parties by contractors visiting the ship or if a crew member leaves the company.

A shortcoming of shared-access policies is that, if a problem does occur, it makes it hard to track who made what changes to a system. Furthermore, most users should have no need to modify configuration files or alter thresholds for safe equipment operation but, if access is shared, an individual's role, function and intended usage may not be clear. The level of privilege granted should also take account of whether access is being granted locally, remotely or over a network connection. Multi-factor authentication techniques are recommended for highly privileged accounts.

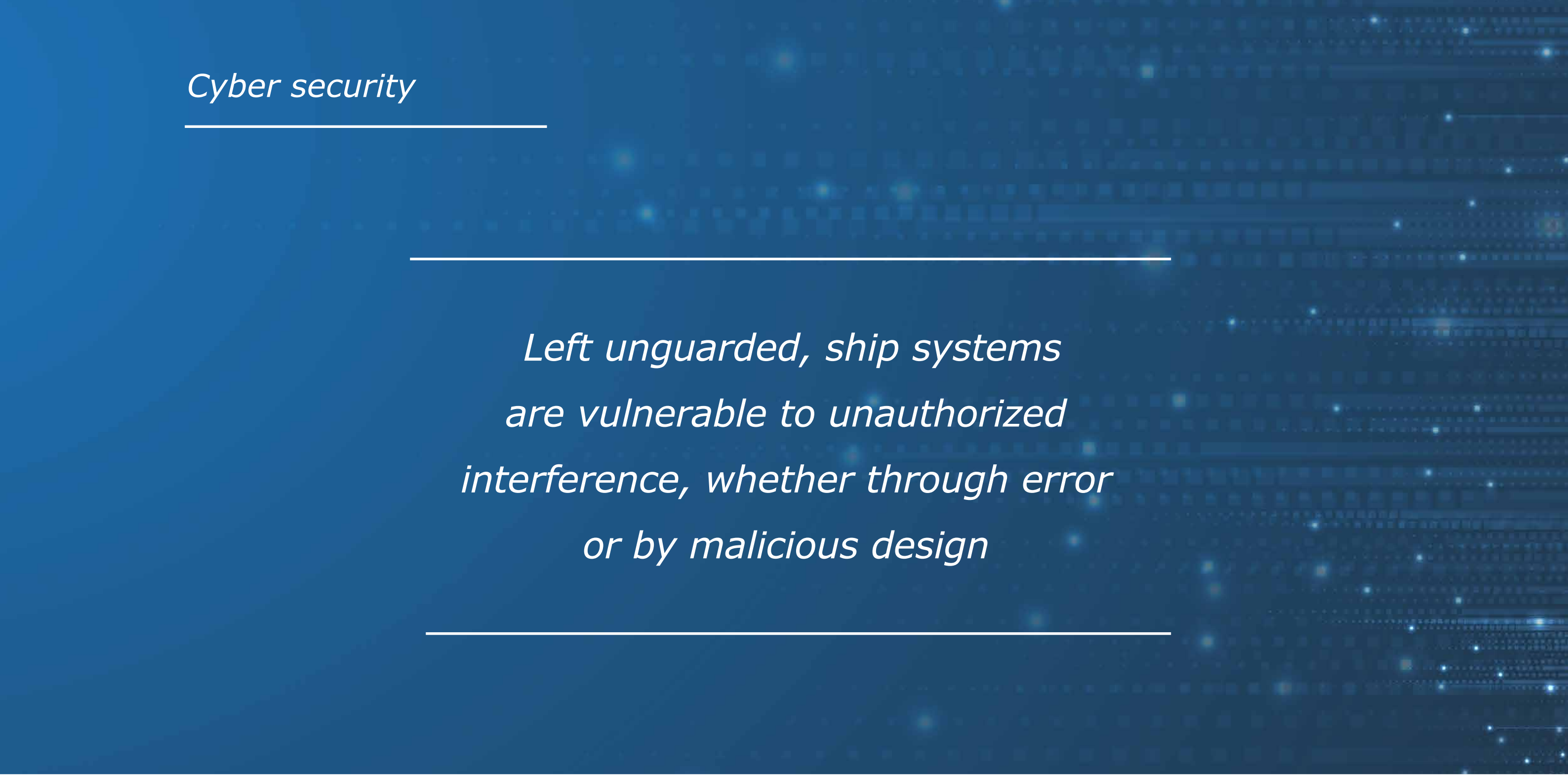
Annex 2: Software updates

It is a simple reality that software has a much shorter shelf-life than physical equipment. With appropriate maintenance and care, mechanical systems used on ships can – and are expected to – last for years, possibly decades. Electrical components and electronics too are reasonably long-lived. Once any teething problems have been solved, systems should give several years of problem-free service.

By comparison, as anyone who owns a smartphone will confirm, software has a much briefer life-cycle. Software updates are rolled out to provide additional functionality, to fix bugs in existing functionality, and to remove security vulnerabilities that have come to light since the code was originally written. Neglecting to implement these updates in a timely and methodical fashion may give rise to situations where unauthorized access to a system becomes possible by exploiting lingering vulnerabilities. In the case of unfixed bugs, meanwhile, malfunctions or unpredictable behaviour can occur in certain scenarios. In either case, operational safety is put at risk.

Fortunately for vessel owners, the updates for shipboard software are much less frequent than the apps on your phone. However, this does not mean that they are less important. In fact, with the safety of a multi-million dollar asset at stake, having the appropriate update policy and procedures in place is all the more imperative.

The first step is to perform an audit of onboard software systems and then develop, document and maintain a current baseline configuration of these systems. These should be treated as live documents and should be reviewed periodically, when circumstances require (for



Left unguarded, ship systems are vulnerable to unauthorized interference, whether through error or by malicious design

example, after a major system failure) and as an integral step of any new software installation.

Previous versions of baseline configurations should always be retained to support roll-back if an update causes unexpected results. Before rolling-out an update, it is essential to assess the potential knock-on impact on other supporting or dependent systems. For example, older software from OEMs for controlling certain equipment may not function correctly, or at all, on the latest PC operating systems. In parallel to the functionality and compatibility considerations, a security impact analysis should be carried out. In the case of more substantial updates, rigorous testing in a non-live environment is highly recommended.

Annex 3: Managing portable devices

Portable devices such as USB memory sticks, hard-drives and even smartphones, can all conceal malware that their owners know nothing about. When plugged into an onboard computer, these digital stowaways can slip onto and infect the machine they are connected to, and from there spread across the vessel's network.

These devices can be easily brought onboard by crew and other personnel, such as third-party contractors, and are convenient to use, which makes them particularly difficult risk to manage. In some cases, they have a legitimate function. For example, an officer may copy chart updates or voyage plans onto a memory stick to transfer them from the planning station to the front-of-bridge ECDIS, or a system integrator may use a portable hard-drive to install new software or transfer supporting documentation onboard.

For this reason, in addition to defining a policy coordinating the responsible use and management of portable devices, including memory sticks, procedures that encourage behavioural change among crew should be considered. In educating crew on safeguarding measures, it is important to emphasise the 'why' as much as the 'how'.

Simple steps such as physically marking media can make a big difference by providing a visual signal to crew, reminding them of distribution limitations and usage caveats. This can be further supported by setting up security perimeters defining areas where such media can or cannot be used.

It is also worth noting that portable devices are not only an entry point for malicious code, but a route for confidential/sensitive data to leak out of a vessel. One way to reduce this risk is for information to be encrypted before it is stored and transported on a portable device. If the device is no longer needed, any files must be securely deleted before disposal.

Annex 4: Physical protection

It is possible when considering cyber security to overly concentrate on electronic access to ship's systems and onboard networks, and not give enough attention to the risks that can arise from unauthorized physical access to hardware or the physical environment in which systems operate.

To this end, a vessel cyber-security policy should take account of facility access - who should be allowed where, and when. Onboard visitors should always be escorted by a trusted member of the crew, for example. Logs should be maintained for entry and exit points of critical infrastructure, such as server rooms and other control centres. Keys and lock combinations should be changed periodically.

Monitors and other displays should also switch to a neutral lock-screen after a specified duration of inactivity to ensure that sensitive information is not inadvertently revealed to passers-by. In addition to obvious hardware installations, such as PCs and user terminals, 'invisible' infrastructure, including cabling and

network access points should be properly secured.

As vessels become increasingly dependent on electronic and computerized systems for their safe operation, steps should be taken to ensure a constant power supply. In the event of a primary power loss, a short-term uninterruptible back-up should take over to facilitate an orderly shutdown of discretionary equipment so as not to compromise vessel safety. This should be supported by a longer-term alternate power supply capable of maintaining minimally required operational capability if primary power cannot be easily restored. Server rooms and other control system hubs should be protected from water ingress, extremes of temperature and humidity and be fitted with appropriate fire-suppression systems.

Annex 5: External communication

A fundamental requirement of a cyber security strategy at sea is to manage the interfaces responsible for connecting a ship's systems to the outside network in order to prevent unauthorized access by remote third-parties.

This is particularly relevant for maintaining the integrity of modern navigation systems that need to download nautical charts and associated data. While accurate, up-to-date chart data is vital for safe vessel operation, the outside connection – unless it is properly configured – provides a doorway for malicious codes and gives cyber-criminals an entry point to vessel systems.

For this reason, it is important that security-sensitive functions are properly isolated and that particular attention is paid to securing shared system resources. Mechanisms for shielding against or limiting the effect of known attack modes, such as denial of service attacks, should be employed.

Maintaining clear boundaries between different parts of onboard networks is essential. Subnetworks should be implemented to ensure that publicly accessible areas are physically or logically separated from zones concerned with vessel operation.

All traffic destined for outside the boundary of the ship's network should pass through designated and managed gateways. As a general rule the number of external connections to systems should be kept to a minimum, with any unused ports closed. Traffic should be monitored for unusual or suspicious activity at external and key internal boundaries. IT managers should also consider what happens if parts of the security system fail and take steps to lessen the impact.

Sensitive files and data should always be encrypted before transmission. Additional processes may be needed to handle the management – generation, distribution, storage, access and destruction – of cryptographic keys.

Annex 6: Software integrity

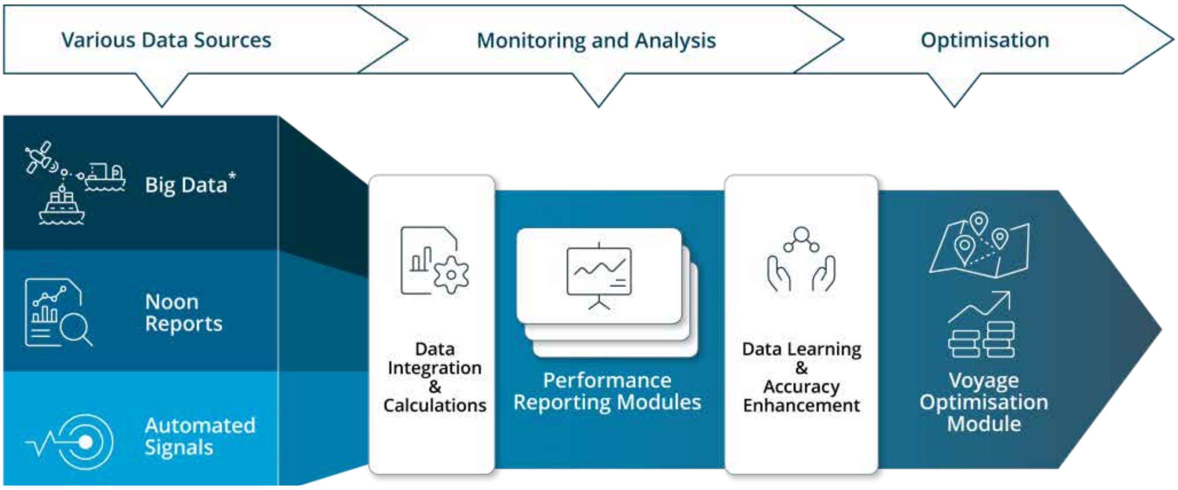
Intrusion detection and anti-virus utilities are prerequisites for protecting the integrity of software and any OS modules from executing malicious or erroneous operations. Mechanisms to localise the effects of any damage from rogue code are strongly recommended.

External threats such as viruses and malware arriving over the network are not the only culprits. Upgraded software can sometimes act erratically or in unexpected ways. There are cases of malware being introduced through an update. For this reason, all software and firmware updates should undergo thorough testing to detect unusual behaviours before it is allowed to be deployed in a live environment.

Again, the ship's network should be routinely monitored and raise an alarm if unauthorized local, network or remote connections are detected. Automated tools that maintain logs of such intrusions can be helpful to support near real-time and post event analysis for plugging previously unknown security holes.

NAPA adds catalyst to the ship data mix

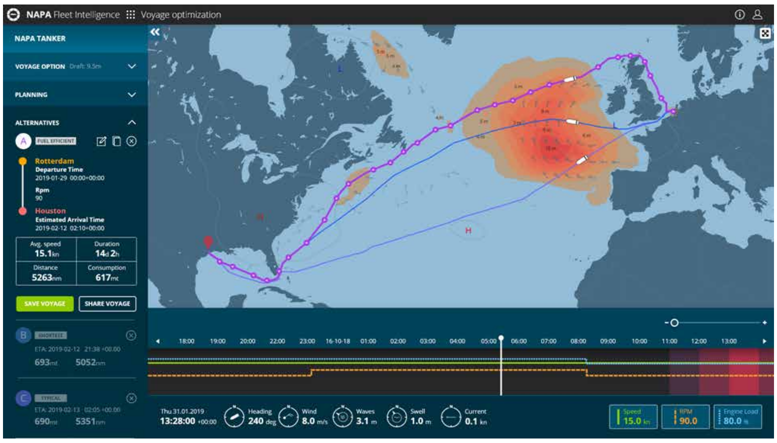
Fleet Intelligence platform unlocks next generation voyage optimization


Various Data Sources
Monitoring and Analysis
Optimisation
Big Data*
Noon Reports
Automated Signals
Data Integration & Calculations
Performance Reporting Modules
Data Learning & Accuracy Enhancement
Voyage Optimisation Module

For over thirty years, NAPA has been helping its customers make the decisions that matter to them. All of our solutions are driven by deep naval architecture expertise and understanding, combined with a legacy of pioneering the development of computer science applications in shipping, such as big data, machine learning and the internet of things. Thanks to this heritage, we have become the trusted leader across ship design and stability solutions for the maritime industry, with 95% of all ships designed by NAPA customers.

The application of this knowledge goes far beyond the design stage, where NAPA started out 30 years ago. For example, our loading and emergency computers for decision support are widely used throughout the industry. We have also pioneered the application of data science and naval architecture to create voyage and performance optimization solutions. This is why we are proud to be the first service provider for the Internet of Ships Open Platform (IoS-OP) initiative from ClassNK subsidiary Ship Data Center Co., LTD. (ShipDC), providing ship performance analytics and voyage optimization capabilities. IoS-OP is a universal platform developed in order to enable the sharing of vessel operational data between stakeholders, the sale of usage rights to shipyards and manufacturers, and many other services. By pursuing new business models and general business improvements, it aims to create opportunities for a new maritime cluster in the digital age that will continue into the next generation.

The need for these solutions could not be greater. Planning voyages to avoid hazards is a basic element of safe seafaring, but there is also a strong economic case – shipping's margins are tight and will only become tighter with increased fuel prices post 2020. Every tonne of fuel saved by avoiding bad weather, or optimising a maintenance schedule, is money in the bank. More importantly, the industry now has a clear deadline for reducing carbon emissions – reducing total emissions by 50% by 2050 vs 2008 levels. No one technology can be the magic bullet – but routing and speed optimization will


NAPA Fleet Intelligence · Voyage optimization

NAPA TANKER

VOYAGE OPTION Draft: 9.5m

PLANNING

ALTERNATIVES

A FUEL EFFICIENT

Rotterdam
Departure Time
2019-01-29 00:00+00:00
Rpm
90

Houston
Estimated Arrival Time
2019-02-12 02:10+00:00

Avg. speed	Duration
15.1kn	14d 2h
Distance	**Consumption**
5263nm	617mt

SAVE VOYAGE · SHARE VOYAGE

B SHORTEST
ETA: 2019-02-12 21:38 +00:00
693mt 5052nm

C TYPICAL
ETA: 2019-02-13 02:05 +00:00
690mt 5351nm

Thu 31.01.2019
13:28:00 +00:00
Heading 240 deg
Wind 8.0 m/s
Waves 3.1 m
Swell 1.0 m
Current 0.1 kn
Speed 15.0 kn
RPM 90.0
Engine Load 80.0 %

be instrumental in reaching these targets. Better routing and voyage planning will save time, money and enhance safety.

Because of this, NAPA is determined to offer powerful voyage and performance optimization tools to the widest possible segment of the industry. One of the key issues we have identified in this instance is the diversity of data sources available to the industry. In this regard, shipping bears out William Gibson's famous observation that the future is 'here, but not evenly distributed'.

On the one hand, many vessels and companies are using Internet of Things solutions, taking advantage of data from onboard sensors and automation systems to gain access to a rich dataset that gives a wealth of information on every aspect of vessel performance. The IoS-OP is one great example of this – where the challenge is to use big data solutions to turn masses of data into usable insights.

On the other, many ships are still relying solely on noon reports for data, which significantly limits the quality of information available. This is why, in our latest iteration of our Fleet Intelligence platform, we have created a solution that is scalable and flexible, delivering insights regardless of the available data sources.

This is where NAPA's unique expertize and understanding of hull monitoring and vessel performance makes such a difference. Combining data collected from sensors and automation systems with hydrodynamic models and algorithms, for example, gives a detailed picture of the different factors affecting vessel performance. However, this level of detail often requires significant capex on the part of the owner to install such a system.

Recognizing this, NAPA Fleet Intelligence enables accurate ship performance assessment with zero onboard installations by combining different data sources. NAPA Fleet intelligence includes hydrodynamics-based NAPA Performance Models of the entire global fleet of approximately 55,000 vessels, based on their publicly available main characteristics and dimensions.

These models unlock the next generation of voyage optimization solutions by functioning as digital twins of a vessel, based on the naval architectural principles of ship design, and through applying hydrodynamic models for resistance calculation. We simulate the ship resistance in the actual weather conditions such as wind, waves, water depth, and combine it with the actual location of the vessel and the actual speed and heading of the vessel. We can also merge this information with data such as noon reports. In this way, it is possible to more accurately monitor and optimise performance and to examine factors such as the effect of hull fouling. This enables improved estimates of required voyage time and sea margin, planning of hull maintenance and provides up-to-date information on the ship performance for fuel efficient voyage optimization.

This in turn unlocks a great opportunity for shipping. With the introduction of EU-MRV, and IMO DCS, we are seeing the beginning of an era in which more data than ever on ship performance is widely available. However, data on its own is often useless, or even burdensome. Experience and knowledge of the wider shipping context are vital in turning such data into useful insights that can drive forward a cleaner and more profitable industry. With thirty years of naval architecture expertise, NAPA is ideally placed to do just that.

In building our solutions, we prioritize ease of use and inter-operability with other tools and services. We want to ensure that the solutions we build are created together with industry, and can be used to bring together insights from as many stakeholders as possible to create the clearest possible view of performance, and in turn, the most impactful insights. In working with the IoS-OP, we look forward to collaborating with a range of partners to ensure that the data we collect can be turned into the most effective insights possible.

Warm waters and breathtaking scenery

Nagasaki is home to the '10 million dollar night view'

Located in southwest Japan on the island of Kyushu, Nagasaki is a prefecture brimming with extraordinary scenery and historical importance. The region offers a blend of traditional Japanese culture and non-Japanese culture from The Netherlands, Portugal, and China. Its multicultural background is greatly shaped by the fact that Nagasaki was one of Japan's only ports which remained open to the rest of the world during the nation's isolation period in the Edo era over 150 years ago.

Today, Dejima, the former Dutch trading post where merchants from Europe would come to conduct business with the local Japanese people, is open to the public as a prime sightseeing spot positioned in the heart of Nagasaki City. Appearing like an ancient medieval town on the horizon, an old-fashioned pedestrian bridge hangs over a small body of water and leads to the wooden array of buildings that closely replicates the original Dutch trading post. Visitors often come dressed in traditional Japanese clothing to take relaxing walks in the area.

Overlooking Nagasaki City from a height of 333 meters equivalent to the height of Tokyo Tower, Mount Inasa stands as a symbol of the city. A cable car provides access from the base to the top of the mountain where there is an observation platform perfect for viewing the city and ocean below. This touristic spot is particularly popular at night, as Nagasaki is home to one of the top three night views in all of Japan and known for its '10 Million Dollar Night View'.

Approximately an hour's drive from Nagasaki's capital city, steam can be found drifting from vents in the streets of Unzen. This seaside town features one of Japan's hottest and most active hot springs, Obama Onsen. Tourists and locals enjoy the various bathhouses and natural hot-spring powered steaming pots used for cooking vegetables, eggs, seafood and more. It is in this same location that the 'Hot Foot 105' foot bath is located. Its name refers to both the temperature of the water source (105 degrees Celsius) and the length of the foot bath (105 meters) which can accommodate a vast number of visitors at a time and is the longest foot bath in the country. One of the recommended ways of spending an afternoon at Obama Onsen is to watch the setting sun on the horizon beyond the ocean while soaking your feet in the foot bath and snacking on freshly steamed vegetables.

Standing out among the many fascinating regions of Japan, Nagasaki is a must-see destination ready to provide an unforgettably pleasant experience.

ClassNK events:

- **NOR-SHIPPING, OSLO, NORWAY, 4TH - 7TH JUNE**

  Please visit ClassNK at stand B02-10

- **GASTECH, HOUSTON, USA, 17TH-19TH SEPTEMBER**

  Please visit ClassNK at stand S50

- **MARINTEC CHINA, SHANGHAI, CHINA, 3RD-6TH DECEMBER**

CONTACT DETAILS FOR THIS ISSUE:

ClassNK Public Relations Team

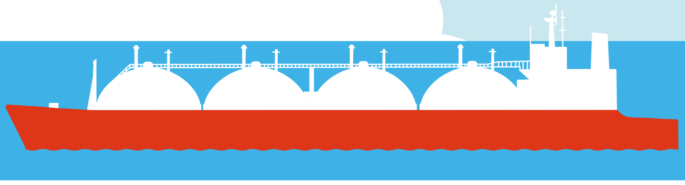
4-7 Kioi-cho
Chiyoda-ku
Tokyo 102-8567
Japan
Tel: +81-3-5226-2047
Fax: +81-3-5226-2039
E-mail: eod@classnk.or.jp

ClassNK Oslo Office

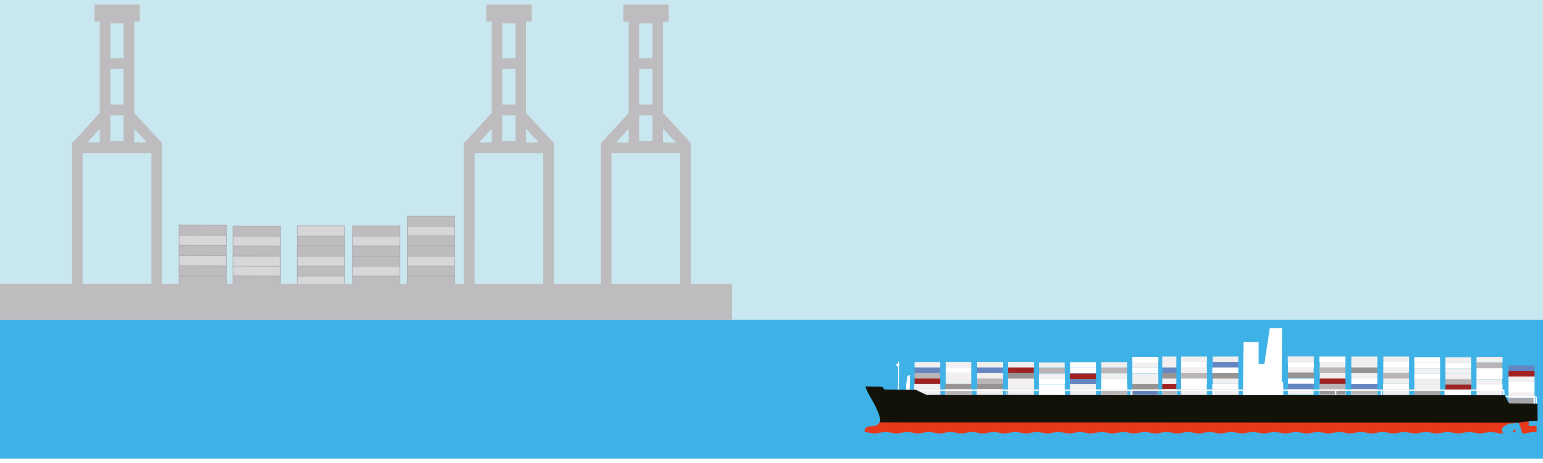
Fridtjof Nansens Plass 5
N-0160
Oslo
Norway
Tel: +47-22-33-1770
Fax: +47-22-33-3860
E-mail: ol@classnk.or.jp

www.classnk.com

World class support, anytime anywhere in the world



ClassNK is a global classification society, providing the highest quality survey and certification services through a network of over 130 exclusive surveyor offices across the world. Established over a century ago, our highly qualified surveyors are there to support your needs, when you need them. Learn more about our efforts to advance maritime safety and protect the marine environment at www.classnk.com



ClassNK www.classnk.com