



CASE STUDY

Naval Sector



Cybersecurity to meet present and future **challenges.**

Brief presentation of the company



Our client is an important national shipyard dedicated to the **construction of ships**.



It receives important **orders** for the construction of ships of all types: fishing, leisure, research, etc.



It has recently received an order where its client has requested that the ship under construction complies with the recent **cybersecurity requirements** required by international regulations.



The design and construction of the new ship must incorporate the necessary measures to successfully comply with the cybersecurity requirements of the International Maritime Organization (**IMO**), which will be certified by an accredited company once the ship is built.

02

Description of the problem/challenge

These requirements on **cyber** risk management are newly implemented and our client has no **experience** on the implications these requirements have in the shipbuilding process.



Resolution **MSC 428(98)** "Management of maritime cyber risks in security management systems" and Circular **MSC-FAL.1/Circ.3** "Guidelines on maritime cyber risk management" require decision makers to "take the necessary measures to safeguard shipping from current and emerging threats and vulnerabilities related to the digitization, integration and automation of shipping procedures and systems.

For this purpose, different methodologies have been developed by companies in the sector, **adopting the criteria of the international standard IEC 62443 for risk analysis and segmentation of ship communication networks.**

This is an area where the shipyard has no experience and requires our specialized assistance to incorporate measures to **meet these requirements and pass the final certification of the vessel.**

Description of the work performed

A **consultancy** service is provided with accompaniment during the whole construction process to check the **cybersecurity** characteristics of the different elements and facilities of the ship. In addition to an analysis of the areas and conduits of the different systems and their associated risks. Finally, technical evaluation tests are carried out.



1

The **technical cybersecurity characteristics** of the different components are compiled and checked with the list of contracted suppliers: propulsion systems, communications, navigation, ballasting, watertightness, power generation...

2

An analysis of the interconnection of the different systems and the associated risks is performed in accordance with the **international standard IEC 62443**. In order to guarantee an overall "**Essential +**" level of security, a series of recommendations are made to ensure an adequate level of protection.

3

During the **construction phase** of the ship, a team of experts is sent to the shipyard to carry out a series of **technical tests to check the security level of networks**.



DNV-GL

CLASS PROGRAMME

Type approval

DNVGL-CP-0231

Edition January 2018

Cyber security capabilities of control
system components

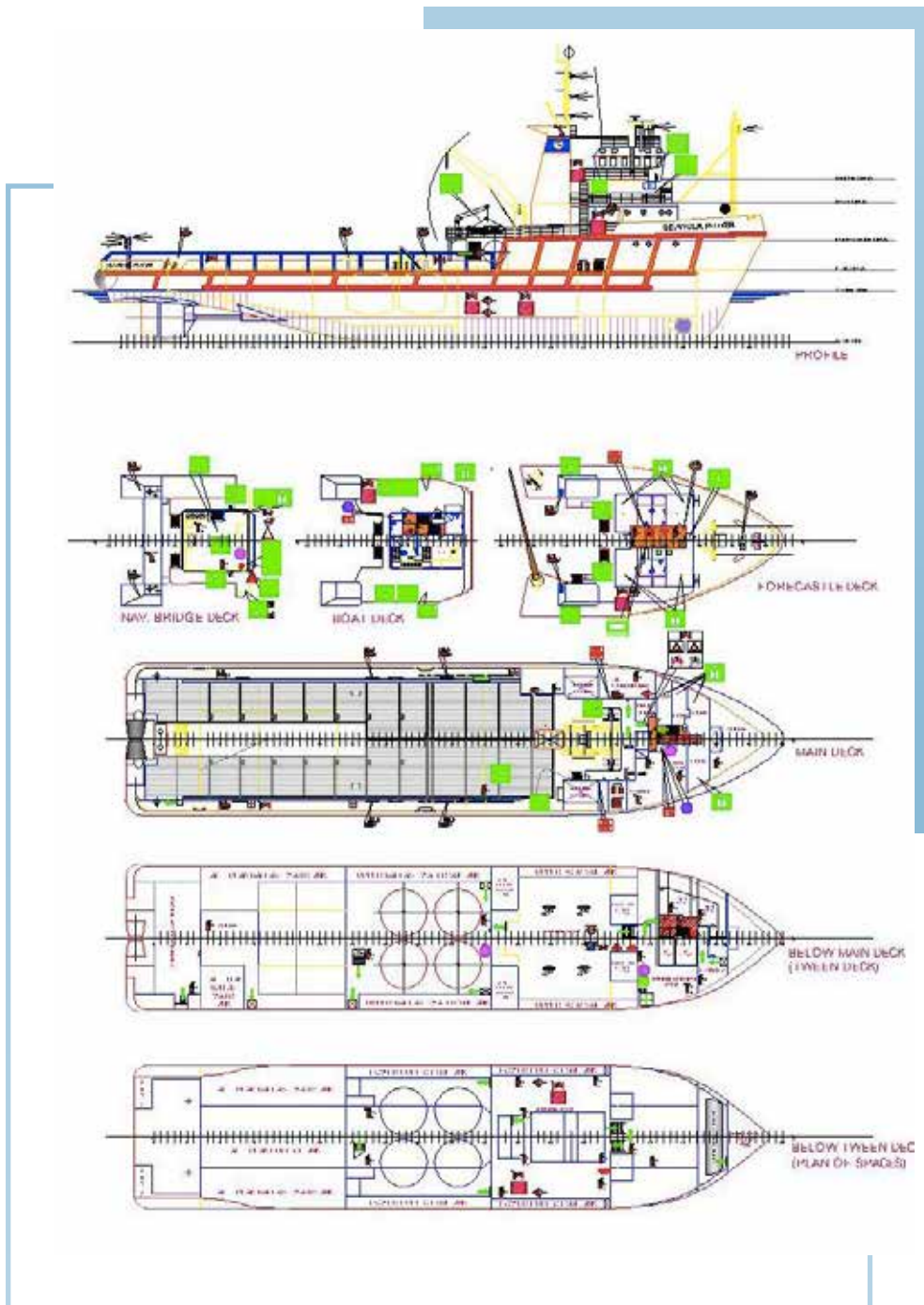
The content of this service document is the subject of intellectual property rights reserved by DNV GL AS (DNV GL). The user accepts that it is prohibited by anyone else but DNV GL and/or perform classification, certification and/or verification services, including the issuance of certificates and/or declarations of conformity, wholly or partly, on the basis of and/or pursuant to this document whether free of charge or chargeable, without DNV GL's prior written consent. DNV GL is not responsible for the consequences arising from any use of this document by others.


**This electronic pdf version of this document, available free of charge
from <http://www.dnvgl.com>, is the officially binding version.**

DNV GL AS


Benefits obtained

As a result of the actions carried out, the customer obtains a **series of benefits**:






The client is assured that each of the different project **components complies with the minimum cybersecurity specifications required**. In this way, **possible cost overruns** caused by the installation of systems with inadequate characteristics **are avoided**.



It will have a **PR according to the architecture of the different ship systems, their level of risk and their interconnections**. It will be able to adopt the necessary measures to guarantee the required general security level.



The finished ship's security level guarantees the required Security Level and facilitates obtaining the corresponding **certification by an accredited company**.



GRUPO
Anticipating a
cyber secure world

MADRID

Avda de Manóteras 46
BIS 6°C
28050 Madrid
T (34) 902 882 992

BARCELONA

Llull, 321
08019 Barcelona
T (34) 933 030 060

VALENCIA CERT

Ramiro de Maeztu, 7
46022 Valencia
T (34) 963 110 300
F (34) 963 106 086

VALENCIA HQ

Dr Joan Reglà, 6 bajo
46010 Valencia
T (34) 963 110 300
F (34) 963 106 086

SEVILLA

Calle Gonzalo Jiménez
de Quesada 2, Planta 18
Edificio Torre Sevilla
41092 Sevilla
T (34) 902 882 992

SAN SEBASTIÁN

C/ Juan Fermín Gilisagasti
nº 2 (Zuatzu)
Edificio Pi@ - Oficina 121
20018 Donostia
T (34) 902 882 992



SANTIAGO DE CHILE

Calle de Padre Mariano
Nº 82 of. 1102
Comuna de Providencia
T +56 9 9440 4365

C.D. MÉXICO

Monte Athos 420
CDMX 11000
T (+52) 55 5035 7868

BOGOTÁ

Carrera 14, nº 98-51,
Oficina 701
T (57) 601 745 74 3

BRUSELAS

Rue Beillard, 20
1040 Bruselas
T (32) (0) 474 532 974

LISBOA

Av. do Brasil, 1
1749-008 Lisboa
T (351) 21 7923729

ROTTERDAM

Stationsplein 45, 4th floor
3013 AK Rotterdam
T (34) 963 110 300

Síguenos en



@s2grupo



s2grupo.es