Technical Information Note
028

Date: 2022-08-22

WinGD cyber security roadmap

All WinGD engines with WiCE- and UNIC-based control systems

Contents

1 Introduction

Increased interconnection between traditional Operation Technology (OT) and Information Technology (IT) systems has led to elevated cyber security risk. Cyber security includes tools, policies and actions that can be used to protect the cyber environment, the organisation and users' assets against malicious cyber activity. WinGD is focused on protecting its customers by making its digital products resilient to malicious activities.

WinGD is increasing the cyber security of its digital products in line with IMO resolution MSC.428(98) for cyber risks addressing safety management systems, effective as of January 2021. WinGD's cyber security roadmap includes two key drivers:

- Hardening of existing systems and technologies according to best practices
- Compliance with relevant cyber security standards as trusted references

2 Cyber security requirements

WinGD's cyber security roadmap references DNV cyber security rules (DNV-RU-SHIP-Pt6Ch5, Sec.21) based on the following:

- DNV cyber security requirements are directly derived from the IEC 62443 international industrial security standard, but tailored to the marine industry
- DNV offers progressive security levels (see Table 2-1)

Table 2-1: DNV cyber security rules and definitions

SP3 *SP2*	*Cyber secure (“Advanced”)*	*Advanced cyber security level for the vessel's essential systems*
SP1	*Cyber secure (“Essential”)*	*Cyber security level for the vessel's essential systems*
SP0	*Cyber secure*	*Initial cyber security level (aligned with IMO resolution MSC.428(98) and MSC-FAL.1/Circ.3) for all systems under consideration*

- DNV supports a Type Approval program for certification of cyber security systems of level DNV SP1 and higher prior to ship integration (see DNV-CP-0231) and defines WinGD's scope of supply
- DNV's cyber security rules address the complete supply chain security and ship integration process (see DNV-CG-0325). From design to final testing on board, this defines interfaces and roles between system supplier, system integrator and ship owner.

3 Cyber security architecture

The cyber security architecture for WinGD products has been defined with the following system integration philosophy:

- Minimal impact on existing ship interfaces
- Limited dependency of WinGD cyber security features on additional ship infrastructure

Specific hardening measures may vary between WinGD products. The following points are considered for each product:

- Identification and authentication requirements for control system commissioning tools
- Removable device protection via hardware and/or software
- Antimalware protection via antivirus and/or signed software
- Whitelisting of network interfaces towards WinGD's products (zone and conduits definition)
- Denial of Service (DoS) protection for critical systems
- Log of relevant cyber security events by dedicated system logging infrastructure
- Backup and rollback with minimal ship crew interaction

4 Affected WinGD products

WinGD's cyber security roadmap addresses the following WinGD products:

- WinGD control systems (WiCE- and UNIC-based)
- WinGD Integrated Digital Expert (WiDE)

WinGD tightly monitors changes to cyber security requirements and adapts its roadmap to support ship owners in achieving the required security levels. The roadmap only reflects approximate lead times.

5 WinGD control systems

WinGD's control systems' cyber security roadmap is focused on the newly developed WiCE modular platform, which includes the following systems (see Figure 5-1):

- The Engine Control System (ECS)
- The Hybrid Control System (HCS)
- iBoxes for control of all add-on systems (iCER, iSCR, iGPR, etc.)

For the UNIC ECS, DNV Security Profile 0 (DNV SP0, see Table 2-1) will be standard delivery starting from the end of 2022-Q4. Further measures are not planned beyond DNV SP0 compliance.

For the WiCE ECS, DNV SP1 Type Approval is planned for end of 2022-Q3 and will be standard delivery starting from the beginning of 2023-Q1. If DNV SP1 is required for projects ordered prior to this date, please contact WinGD on a project-specific basis.

Levels beyond DNV SP1 compliance are not considered standard and may only be ordered as additional services.

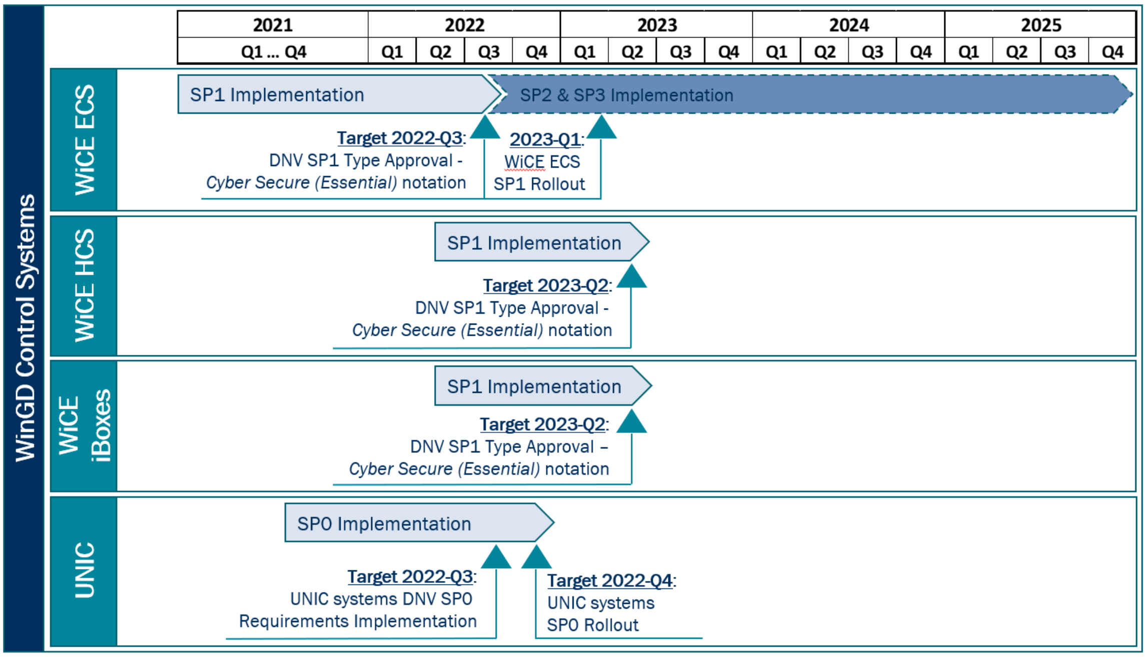
WinGD Control Systems
2021
Q1 ... Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
Q3
Q4
2024
Q1
Q2
Q3
Q4
2025
Q1
Q2
Q3
Q4
WiCE ECS
SP1 Implementation
SP2 & SP3 Implementation
Target 2022-Q3: DNV SP1 Type Approval - Cyber Secure (Essential) notation
2023-Q1: WiCE ECS SP1 Rollout
WiCE HCS
SP1 Implementation
Target 2023-Q2: DNV SP1 Type Approval - Cyber Secure (Essential) notation
WiCE iBoxes
SP1 Implementation
Target 2023-Q2: DNV SP1 Type Approval – Cyber Secure (Essential) notation
UNIC
SP0 Implementation
Target 2022-Q3: UNIC systems DNV SP0 Requirements Implementation
Target 2022-Q4: UNIC systems SP0 Rollout

Figure 5-1: WinGD's control systems' cyber security roadmap

6 WinGD Integrated Digital Expert (WiDE)

WinGD's WiDE cyber security roadmap ensures the system is compliant with the following DNV cyber security levels (see Figure 6-1):

1. **WiDE SP0** with DNV SP0
2. **WiDE SP1** with DNV SP1
3. **WiDE SP3** with DNV SP3, also incorporating DNV SP2

WiDE SP0 will be standard for all WiDE systems ordered starting from the end of 2022-Q2. If WiDE SP0 is required for projects ordered prior to this date, please contact WinGD on a project-specific basis. WiDE SP0 will be added without change to the 2022 Data Collection and Monitoring (DCM) system prices.

WiDE SP1 will be available starting from 2023-Q4 and therefore cannot yet be ordered. Further details for WiDE SP1 will be provided by the end of 2022-Q4.

WiDE SP3 is not currently standard and can only be ordered as an additional service.

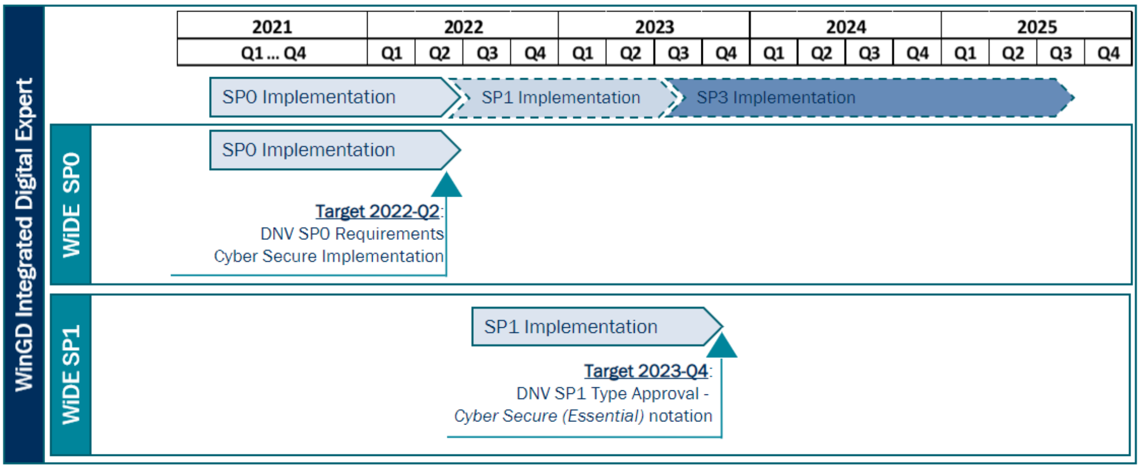

Figure 6-1: WinGD's WiDE system cyber security roadmap