



RWS INFORMATIE

VSP Bijlage 10 – GSH03.10GD-Softwareregister

Project	MPV-50
Zaaknummer	31199153
Datum	21 september 2026
Versie	1.0
Status	Definitief

1	Naam	Software kritische werktuigen en apparatuur
	Kader	Generieke Scheepshandboek Veiligheid Management Systeem (VMS, of ook wel, binnen terminologie International Safety Management (ISM), Safety Management Systeem (SMS). Tevens Scheeps-veiligheidsplan (SVP) conform Internationale code voor de beveiliging van schepen en havenfaciliteiten (ISPS code).
	Proceseigenaar	Afdelingshoofd Operations
	Document(hoofdstuk)nr.	GSH03.10GD0.2
	Gerelateerd Document nr.	<i>Deze procedure is een gerelateerd document!</i>
	Documenttype	Procedure
	Aantal pagina's	2
	Aantal bijlagen	Nvt.
	Status	Definitief
	Uitgegeven door	Richard Mik, SHE-Q adviseur.
	Datum uitgifte	02 juli 2021
	Datum van kracht	01 augustus 2021
	Laatste revisienummer	0.1
	Datum revisie	4 November 2024

1. Doel

Het traceren van softwarewijzigingen moet worden opgenomen in een proces voor wijzigingsbeheer.

2. Reikwijdte

Hoewel deze procedure initieel gestoeld is op basis van vereisten onder de ISM code en dus prioritair geldt voor ISM plichtige, gecertificeerde schepen van de Rijksrederij (>500GT dus), kan deze procedure ook gelden als "good practice" voor andere schepen binnen de Rijksrederij van <500GT (tot 100GT) in het kader van risico gestuurd onderhoud.

3. Verwachting

Juist managen van software (wijzigingen). Tabel 1 de aanbevolen velden voor het bijhouden van wijzigingen. Een dergelijk mechanisme dient gebruik te worden om te verwijzen naar de traceringsinformatie binnen het configuratiebeheerproces.

Software change request #	1	2	3	4	5	6	7	...
Major/Minor								
Vendor tracking number								
Date change made								
System SFI* or GMOD** code								
System name								
System tag number								
Description of change								
Previous software version								
New software version								
Vessel name								
Sister vessel name								
More sister vessel names [...]								
Date software change was tested								
Date software change was closed								
Impacts of other systems/Tests needing to be performed								
Reference to any other issue tracking system #								

Tabel 1

3.1 Patchbeheer voor software

Een van de meest voorkomende kwetsbaarheden is ongepatchte software en aanvallers zijn snel in staat de overhand te krijgen wanneer softwarepatches niet up-to-date worden gehouden. Softwarepatches voor Operationele Technologie (OT) en Informatie Technologie (IT) ondersteuning moeten daarom worden beheerd door een gedefinieerd proces dat het volgende omvat:

- regelmatig onderzoek naar nieuwe waarschuwingsberichten over kwetsbaarheden van de OT en softwaresystemen van derden, welke veelal door RWS CIV worden aangeleverd en leveranciers en CERT's zoals de kennisbank voor kwetsbaarheidsanalyse op www.cert.org.
- beoordeling van de criticiteit van patches het verkrijgen van de patches en updates
- het maken van een back-up van het systeem voor het geval er iets misgaat. Dit is vooral belangrijk wanneer het OT-systeem nodig is voor productie.
- het testen van de patches voordat ze worden geïnstalleerd (indien mogelijk eerst op een redundant systeem) en nagaan of een herstart nodig is. Het is met name van belang een plan te hebben voor het opnieuw opstarten van OT-systemen die nodig zijn voor productie
- goedkeuringsproces (de eigenaar van het schip en de productleverancier hebben contractuele afspraken gemaakt over perioden voor de
- goedkeuring en levering van patches en updates of alternatieve workarounds voor kwetsbaarheden)
- de afhandeling van de goedkeuring van patches door de productleverancier en
- afhandeling van het patchen van aanvullende software.

In het ideale geval kunnen de patches worden gepland tijdens onderhoudsvensters. Indien de OT-systemen echter redundante systemen hebben, kunnen de patchupdates eerder worden uitgevoerd (BSI-ICS Security Compendium Version 1.23, Par. 5.6.4 Patchbeheer).

3.2 Softwareregister

Naast het bijhouden van softwarewijzigingen wordt aanbevolen een softwareregister aan te leggen en bij te houden. Dit register moet worden gekoppeld aan en geraadpleegd in het proces voor het beheer van softwaremutaties en moet up-to-date worden gehouden na patches, updates en fixes. Tabel 2 bevat nuttige velden die moeten worden bijgehouden voor elk softwareafhankelijk afhankelijk systeem.

<i>Software register</i>	<i>SW #1</i>	<i>SW #2</i>	<i>SW #3</i>	<i>SW #4</i>	<i>SW #5</i>	<i>SW ...</i>
Vendor name						
CPU/RCU/SBC/device manufacturer						
The firmware						
Model no of CPU/RCU/SBC/device						
Hardware version of CPU/RCU/SBC/device						
System that software is backed up from						
TAG No of cabinet where software is installed						
Description of state of software (pre-FAT, FAT, pre-commissioning, commissioning, release)						
Software description (name of software application, could be the software developed by the vendor for the control of equipment such as PLC code, vessel management system application software, web client, HMIs, etc.)						
Patches applied to the software (could be contained within the version identifier)						
Configuration files*						
Software revision						
Date of software revision						
Type of software (source, executable, other)						
Final location of software backup						
I/O or signal lists, and its version						
Cause and effects information and it's version						
Operating systems and their versions/patches						

Tabel 2