IEC 61162-460

Edition 2.0 2020-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

Maritime navigation and radiocommunication equipmentand systems – Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité

IEC 61162-460:2018-05/AMD1:2020-01(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IEC 61162-460

Edition 2.0 2020-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

AMENDMENT 1
AMENDEMENT 1

Maritime navigation and radiocommunication equipmentand systems – Digital interfaces –
Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security

Matériels et systèmes de navigation et de radiocommunication maritimes – Interfaces numériques –
Partie 460: Émetteurs multiples et récepteurs multiples – Interconnexion Ethernet – Sûreté et sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 47.020.70

ISBN 978-2-8322-7764-5

FOREWORD

This amendment has been prepared by IEC technical committee 80: Maritime navigation and radiocommunication equipment and systems.

The text of this amendment is based on the following documents:

FDIS	Report on voting
80/943/FDIS	80/951/RVD

Full information on the voting for the approval of this amendment can be found in the report on voting indicated in the above table.

The committee has decided that the contents of this amendment and the base publication will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

Introduction to the Amendment

This amendment provides greater clarity to the external security requirements in 6.3, updates the alert management in 8.2.7 and associated tests in 10.11.6 to comply with bridge alert management and provides an improved test of firewalls in 10.8.4.

2 Normative references

Delete the following existing normative references:

IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results*

IEC 62288:2014, *Maritime navigation and radiocommunication equipment and systems – Presentation of navigation-related information on shipborne navigational displays – General requirements, methods of testing and required test results*

Add the following new normative references:

IEC 62923-1, *Maritime navigation and radiocommunication equipment and systems – Bridge alert management – Part 1: Operational and performance requirements, methods of testing and required test results*

IEC 62923-2, *Maritime navigation and radiocommunication equipment and systems – Bridge alert management – Part 2: Alert and cluster identifiers and other additional features*

6.3.1 Overview

Replace the existing first and second paragraphs with the following new text:

All traffic from uncontrolled networks is passed or processed through a 460-Gateway or 460-Wireless gateway. A 460-Gateway consists of firewall(s) (see 6.3.2) and may include support for one or any combination of the following functions:

- direct communication (see 6.3.3);
- DMZ with application servers (see 6.3.5.2);
- DMZ with interoperable access to file storage (see 6.3.5.3).

Firewall(s) provide network-access security for the uncontrolled network and the 460-Network. Firewalls for external and internal interfaces may be provided by the same application.

The 460-Gateway components may be implemented in one device or in different devices. Figure 2 shows an example of a 460-Network with a 460-Gateway.

6.3.2.1 External firewall

Replace the existing paragraph with the following new paragraph:

An external firewall blocks all traffic unless it is registered (i.e. whitelisted) and destined only to equipment in the DMZ. This means that, in principle, all direct communication to or from a 460-Network is not allowed.

6.3.2.2 Internal firewall

Replace the existing paragraph with the following new paragraph:

An internal firewall blocks all traffic unless it is either destined to equipment in a 460-Network and it originates from equipment in the DMZ or it is destined to equipment in the DMZ and it originates from equipment in a 460-Network. All traffic passing through the internal firewall is registered (i.e. whitelisted) in advance.

6.3.5.1 Firewall

Replace the existing title with the following new title:

6.3.5.1 General

Replace the existing second and third bullets with the following new bullets:

- firewall(s) shall be provided which are configured with the combination of source and destination IP address, protocol and destination port number (see 6.3.2);
- all connections between uncontrolled networks and a 460-Network shall be registered (i.e. all network traffic that does not match a set firewall rule shall be blocked by the firewall);

6.3.5.2 Application server

Replace the existing second paragraph with the following new paragraph:

If provided, the application server shall provide an application level authentication mechanism, such as password, smartcard, digital signature, dongle, etc., of clients from uncontrolled networks.

8.2.7.1 Alerts and indication

Replace, in the existing first paragraph, the existing reference "IEC 62288" *with* "IEC 62923-1".

Table 2 – Summary of alert of network monitoring

Replace the existing title of the second column "Cause" *with* "Purpose".

Replace, in the last column, the existing unique identifiers at alert source corresponding to the alerts listed below with the following new identifiers:

Direct connection to uncontrolled network as a caution (see 6.3.4)	3159
Direct connection to uncontrolled network as a warning (see 6.3.4)	3158
Connected to uncontrolled network (see 6.3.5.1)	3163
Network traffic capacity may be exceeded (see 8.2.2)	3166
Network traffic capacity exceeded (see 8.2.2)	3168
Network redundancy lost for xxxx (see 8.2.3)	3173

8.2.7.2 Alert management interface

Replace the existing second paragraph with the following new paragraph:

The alert management interface, if provided, shall be compliant with the sentences of Annex E and comply with the communication requirements of IEC 62923-1 and IEC 62923-2. In the BAM concept, the network components act as alert sources.

8.2.7.4 Remote acknowledgement and silencing of alerts

Replace the existing first paragraph with the following new paragraph:

Remote acknowledgement shall only be possible for category B alerts.

10.8.4 Firewall

Replace the existing second paragraph with the following new paragraph:

Set an EUT in accordance with the manufacturer's instructions between a 460-Network and an uncontrolled network. Using a network scanner with port scan function, set it to scan the entire address range for the 460-Network, DMZ and uncontrolled network. Use packet capture software running in promiscuous mode and confirm by analytical evaluation that packets do not pass through the EUT from the uncontrolled network to the 460-Network and vice-versa as follows:

- port scan UDP and TCP test for all ports 1-65535 to the internal address range of the 460-Network;
- if DMZ is provided, port scan UDP and TCP test for all ports 1-65535 to the address range of the DMZ;

- port scan UDP and TCP test for all ports 1-65535 to the address range of the uncontrolled network.

Example test:

Using the Nmap®[5] network scanning tool with an address range for a 460-Network of 192.168.22.0/24, for a DMZ of 172.31.16.0/24 and for an uncontrolled network of 10.100.100.0/24.

- Port scan UDP and TCP test to the internal address range of the 460-Network:

  complete a ping test with TCP port scan with the command "nmap -p 1-65535 -sV -sS -T4 192.168.22.0/24";

  complete a ping test with UDP port scan with the command "nmap -p 1-65535 -sV -sU -T4 192.168.22.0/24".

- Port scan UDP and TCP test to the address range of the DMZ:

  complete a ping test with TCP port scan with the command "nmap -p 1-65535 -sV -sS -T4 172.31.16.0/24";

  complete a ping test with UDP port scan with the command "nmap -p 1-65535 -sV -sU -T4 172.31.16.0/24".

- Port scan UDP and TCP test to the address range of the uncontrolled network;

  complete a ping test with TCP port scan with the command "nmap -p 1-65535 -sV -sS -T4 10.100.100.0/24";

  complete a ping test with UDP port scan with the command "nmap -p 1-65535 -sV -sU -T4 10.100.100.0/24".

5 Nmap® ("Network Mapper") is the trademark of a product supplied by the Nmap Project, a free and open source utility for network discovery and security auditing (https://nmap.org). This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the product named. Equivalent products may be used if they can be shown to lead to the same results.

10.11.6.2 Alert management interface

Replace, in the existing first paragraph, the reference "IEC 61924-2:2012, 8.3" *with* "IEC 62923-1".

Replace, in the first bullet point of the existing second paragraph, the words "the state diagram of IEC 61924-2:2012, Annex J" *with* "with the communication requirements of IEC 62923-1 and IEC 62923-2".

Bibliography

Add the following new references:

IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results*

IEC 62288:2014, *Maritime navigation and radiocommunication equipment and systems – Presentation of navigation-related information on shipborne navigational displays – General requirements, methods of testing and required test results*

AVANT-PROPOS

Le présent amendement a été établi par le comité d'études 80 de l'IEC: Matériels et systèmes de navigation et de radiocommunication maritimes.

Le texte de cet amendement est issu des documents suivants:

FDIS	Rapport de vote
80/943/FDIS	80/951/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cet amendement.

Le comité a décidé que le contenu de cet amendement et de la publication de base ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Introduction à l'Amendement

Le présent amendement apporte davantage de clarté aux exigences de sécurité externe en 6.3, il met à jour la gestion des alertes du 8.2.7 et les essais associés du 10.11.6 en vue d'être conformes à la gestion des alertes sur le pont et il fournit une amélioration de l'essai des pare-feu du 10.8.4.

2 Références normatives

Supprimer les références normatives existantes suivantes:

IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems – Integrated navigation systems – Part 2: Modular structure for INS – Operational and performance requirements, methods of testing and required test results* (disponible en anglais seulement)

IEC 62288:2014, *Matériels et systèmes de navigation et de radiocommunication maritimes – Présentation des informations relatives à la navigation sur des affichages de navigation de bord – Exigences générales, méthodes d'essai et résultats d'essai exigés*

Ajouter les nouvelles références normatives suivantes:

IEC 62923-1, *Matériels et systèmes de navigation et de radiocommunication maritimes – Gestion des alertes à la passerelle – Partie 1: Exigences d'exploitation et de fonctionnement, méthodes d'essai et résultats d'essai exigés*

IEC 62923-2, *Matériels et systèmes de navigation et de radiocommunication maritimes – Gestion des alertes à la passerelle – Partie 2: Identifiants d'alerte et de groupe et autres caractéristiques supplémentaires*

6.3.1 Vue d'ensemble

Remplacer les premier et second alinéas existants par le nouveau texte suivant:

Tout trafic provenant de réseaux non contrôlés est effectué ou traité par la passerelle-460 ou la passerelle sans fil-460. Une passerelle-460 est constituée de pare-feu (voir 6.3.2) et peut inclure la prise en charge d'une ou de toute combinaison des fonctions suivantes:

- communication directe (voir 6.3.3);
- DMZ avec serveurs d'applications (voir 6.3.5.2);
- DMZ avec accès interopérable au stockage de fichiers (voir 6.3.5.3).

Les pare-feu fournissent la sécurité de l'accès au réseau pour le réseau non contrôlé et le réseau-460. Les pare-feu pour les interfaces externe et interne peuvent être fournis par la même application.

Les composants de la passerelle-460 peuvent être mis en œuvre en un seul dispositif ou en différents dispositifs. La Figure 2 représente un exemple de réseau-460 avec une passerelle-460.

6.3.2.1 Pare-feu externe

Remplacer l'alinéa existant par le nouvel alinéa suivant:

Un pare-feu externe bloque tous les trafics, sauf les trafics enregistrés (c'est-à-dire figurant sur listes blanches) et destinés uniquement aux matériels dans la DMZ. Ceci signifie, en principe, que toute communication directe vers ou depuis un réseau-460 n'est pas admise.

6.3.2.2 Pare-feu interne

Remplacer l'alinéa existant par le nouvel alinéa suivant:

Un pare-feu interne bloque tous les trafics, sauf les trafics qui sont soit destinés aux matériels d'un réseau-460 et qui proviennent des matériels de la DMZ, soit destinés aux matériels de la DMZ et qui proviennent des matériels d'un réseau-460. Tous les trafics qui traversent le pare-feu interne sont enregistrés (sur listes blanches) à l'avance.

6.3.5.1 Pare-feu

Remplacer le titre existant par le nouveau titre suivant:

6.3.5.1 Généralités

Remplacer le deuxième et le troisième points existants par les nouveaux points suivants:

- des pare-feu doivent être fournis, en étant configurés avec la combinaison de l'adresse IP source et destination, du protocole et du numéro de port de destination (voir 6.3.2);

- toutes les connexions entre les réseaux non contrôlés et un réseau-460 doivent être enregistrées (c'est-à-dire que tout le trafic du réseau qui ne correspond pas à une règle de pare-feu définie doit être bloqué par le pare-feu);

6.3.5.2 Serveur d'applications

Remplacer le deuxième alinéa existant par le nouvel alinéa suivant:

Le cas échéant, le serveur d'applications doit fournir un mécanisme d'authentification du niveau d'application, tel que mot de passe, carte intelligente, signature numérique, clé électronique, etc., du client, à partir des réseaux non contrôlés.

8.2.7.1 Alertes et indication

Remplacer, dans le premier alinéa existant, la référence existante "IEC 62288" *par* "IEC 62923-1"*.*

Tableau 2 – Résumé des alertes de la surveillance du réseau

Remplacer le titre existant de la deuxième colonne "Cause" *par* "Objet".

Remplacer, dans la dernière colonne, les identificateurs uniques à la source de l'alerte existants correspondant aux alertes énumérées ci-dessous par les nouveaux identificateurs suivants:

Connexion directe à un réseau non contrôlé en tant que mise en garde (voir 6.3.4):	3159
Connexion directe à un réseau non contrôlé en tant qu'avertissement (voir 6.3.4):	3158
Connecté à un réseau non contrôlé (voir 6.3.5.1):	3163
La capacité du trafic du réseau peut être dépassée (voir 8.2.2):	3166
Capacité du trafic du réseau dépassée (voir 8.2.2):	3168
Redondance du réseau perdue pour xxxx (voir 8.2.3):	3173

8.2.7.2 Interface de gestion des alertes

Remplacer le deuxième alinéa existant par le nouvel alinéa suivant:

L'interface de gestion des alertes, le cas échéant, doit être conforme aux sentences de l'Annexe E et être conforme aux exigences portant sur les communications de l'IEC 62923-1 et de l'IEC 62923-2. Dans le concept BAM (bridge alert management), les composants du réseau servent de sources d'alerte.

8.2.7.4 Acquittements et mise en sourdine des alertes à distance

Remplacer le premier alinéa existant par le nouvel alinéa suivant:

L'acquittement à distance doit uniquement être possible pour les alertes de catégorie B.

10.8.4 Pare-feu

Remplacer le deuxième alinéa existant par le nouvel alinéa suivant:

Définir un EUT conformément aux instructions du fabricant entre un réseau-460 et un réseau non contrôlé. À l'aide d'un balayage de réseau avec une fonction de balayage de port, effectuer le réglage en vue de balayer l'ensemble de la plage d'adresses pour le réseau-460, la DMZ et le réseau non contrôlé. Utiliser un logiciel de capture de paquets fonctionnant en mode espion et confirmer par une évaluation analytique que les paquets ne passent pas par l'EUT entre le réseau non contrôlé et le réseau-460 et inversement comme suit:

- effectuer l'essai de balayage des ports UDP et TCP pour tous les ports 1-65535 pour la plage d'adresses internes du réseau-460;
- si la DMZ est fournie, procéder à l'essai de balayage des ports UDP et TCP pour tous les ports 1-65535 pour la plage d'adresses de la DMZ ;
- effectuer l'essai de balayage des ports UDP et TCP pour tous les ports 1-65535 pour la plage d'adresses du réseau non contrôlé.

Essai en exemple:

À l'aide de l'outil de balayage de réseau Nmap®[5] avec une plage d'adresses pour un réseau-460-de 192.168.22.0/24, pour une DMZ de 172.31.16.0/24 et pour un réseau non contrôlé de 10.100.100.0/24.

- Effectuer l'essai de balayage des ports UDP et TCP pour la plage d'adresses internes du réseau-460 :

  réaliser un essai de ping avec balayage de port TCP avec la commande "nmap -p 1-65535 -sV -sS -T4 192.168.22.0/24";

  réaliser un essai de ping avec balayage de port UDP avec la commande "nmap -p 1-65535 -sV -sU -T4 192.168.22.0/24".
- Effectuer l'essai de balayage des ports UDP et TCP pour la plage d'adresses de la DMZ:

  réaliser un essai de ping avec balayage de port TCP avec la commande "nmap -p 1-65535 -sV -sS -T4 172.31.16.0/24";

  réaliser un essai de ping avec balayage de port UDP avec la commande "nmap -p 1-65535 -sV -sU -T4 172.31.16.0/24".
- Effectuer l'essai de balayage des ports UDP et TCP pour la plage d'adresses du réseau non contrôlé ;

  réaliser un essai de ping avec balayage de port TCP avec la commande "nmap -p 1-65535 -sV -sS -T4 10.100.100.0/24";

  réaliser un essai de ping avec balayage de port UDP avec la commande "nmap -p 1-65535 -sV -sU -T4 10.100.100.0/24".

5 Nmap® ("Network Mapper") est l'appellation commerciale d'un produit distribué par le Projet Nmap, service public de source libre et ouverte pour la découverte réseau et l'audit de sécurité (https://nmap.org). Cette information est fournie à l'intention des utilisateurs du présent document et ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif du produit ainsi désigné. Des produits équivalents peuvent être utilisés s'il peut être démontré qu'ils conduisent aux mêmes résultats.

10.11.6.2 Interface de gestion des alertes

Remplacer, dans le premier alinéa existant, la référence "8.3 de l'IEC 61924-2:2012" *par* "IEC 62923-1".

Remplacer, dans le premier point du second alinéa existant, les mots "au diagramme d'état de l'Annexe J de l'IEC 61924-2:2012," *par* "aux exigences portant sur les communications de l'IEC 62923-1 et de l'IEC 62923-2".