Standard IEC 62443-4-2.
IACS UR E27
“Cyber resilience of on-board systems and equipment”.
Exor eX700 and eX700M Series.
Chromium documentation.

History

Rev	Date	Description	By
0.1	Jul 2024	Draft	Stefano Dell'Oro
1.0	Aug 2024	Final Review and update	Fausto Gastaldin – Giuseppe Marras

Reference

Cross Reference	Filename	Description
[1]		

General content

Description of security capability

The document shall describe compliance with required security capabilities for the system. A separate section shall be dedicated for each requirement, and the following information shall be described:

- description of how the required capability is implemented in the system and its hardware/software components.
- in case a security capability is deemed not applicable or not relevant, this shall be described and justified.
- if the system or any of its components cannot comply with a requirement, proposed compensating countermeasure(s) shall be described.

Configuration guidelines

The document shall specify recommended security settings in the system as per SR 7.6 in [4.8.7]. The document shall include guidelines on how to carry out the configuration as well as any necessary tools needed. Default settings shall be specified.

Test Procedure

The document shall include instructions for how the user can verify correct operation of the system's security functions as required by item no.19 in section 4.1. (n.19 ->The document shall specify how to verify during scheduled test and maintenance of the vessel that required security functions operate as intended, see SR 3.3).

Requirements

1 FR 1 – Identification and authentication control

1.1 Description of security capability

Chromium relies on the authentication and user identification mechanisms of the BSP.
For requirements CR 1.1 through CR 1.14 refer to the documentation produced for BSP.

2 FR 2 – Use control

2.1 Description of security capability

Chromium relies on BSP's access control.
For requirements CR 2.1 through CR 2.13 refer to the documentation produced for BSP.

3 CR 2.4 - EDR 2.4 – Mobile code

3.1 Description of security capability

Using Chromium there is a risk of being able to introduce malicious code if the toolbar is enabled and the user can then freely browse the web.
There is an option to disable the toolbar and thus prevent the user from accessing other websites.
It is the responsibility of the system integrator to ensure that the web address that is loaded into the browser is reliable and secure.

3.2 Configuration guidelines

The administrator can disable the toolbar and prevent the user from freely browsing the web in the Web Browser of the System Settings.
Go to https://IPaddress/machine_config link and enter username and password, then:

*Path: **System Settings**> click **Web Browser***

Click "EDIT" in the toolbar at the top right, disable Enable toolbar parameter if enabled and click "SAVE".

3.3 Test Procedure

Log in to https://IP_HMI_address via your PC's browser.
There must be no toolbar and you cannot edit or insert a custom web address.

4 CR 3.1 – Communication integrity

4.1 Description of security capability

Using protocol HTTP/HTTPS, it guarantee the integrity of communications.
Refer to CR 3.1 – Communication integrity requirement of the documentation produced for BSP.

5 CR 3.2 - EDR 3.2 – Protection from malicious code

5.1 Description of security capability

Malicious code can be introduced into the system if the toolbar is enabled, and the user can then freely browse the web. The control for malicious code must be implemented externally (e.g. IDS/IPS) to device. On the device, you can also disable USB /SD interfaces or check the software before its installation.

5.2 Configuration guidelines

To prevent malicious code from being introduced using the toolbar, refer to CR 2.4 - EDR 2.4 – Mobile code requirement Configuration guidelines.

5.3 Test Procedure

Refer to CR 2.4 - EDR 2.4 – Mobile code requirement to test protection from malicious mobile code.

6 CR 3.3 – Security functionality verification

6.1 Description of security capability

For verification of the intended operation of each security function, refer to the Test Procedure section of the documentation produced for each requirement.

7 CR 3.6 – Deterministic output

7.1 Description of security capability

The deterministic behavior of outputs in the bootup phase can be guaranteed by watchdog that restores the system in case of freezing or crashing.

Another way to guarantee the deterministic behavior of outputs is the fallback concept. In the System Settings it is possible to configure a fallback page that is displayed in case of malfunctions.

7.2 Configuration guidelines

To configure the fallback page, go to https://IPaddress/machine_config link and enter username and password of an admin account, then:

*Path: **System Settings**> click **Web Browser***

Click “EDIT” in the toolbar at the top right, enable Fallback page parameter and enter the web address of the page to be shown in case of malfunctions.
When finished, click “SAVE” in the toolbar.

7.3 Test Procedure

To verify the functioning of the watchdog it is necessary to subject the device to an attack and cause it to crash.
For example, open an application capable of connecting to the HMI using the SSH protocol (e.g. Putty).
Enter the IP address of the device and port 22 on which it is listening to, and press “connect”.
In the opened “login:” window, enter username and password.
To simulate a crash, launch the command “sudo killall HMI” that kills the Chromium process. The watchdog intervenes by restarting the panel.

8 CR 4.1 – Information confidentiality

8.1 Description of security capability

The information confidentiality of Chromium depends on the information confidentiality of the BSP.
For requirements CR 4.1 through CR 4.3 refer to the documentation produced for BSP.

9 CR 6.1 – Audit log accessibility

9.1 Description of security capability

The access to audit logs on a read-only basis for authorized humans and/or tools depends on the BSP.
Refer to CR 6.1 – Audit log accessibility requirement of the documentation produced for BSP.

10 FR 7 – Resource availability

10.1 Description of security capability

Chromium’s availability of components against the degradation or denial of essential services depends on the BSP.
For requirements CR 7.1 through CR 7.8 refer to the documentation produced for BSP.