**IACS UR E27**
**“Cyber resilience of on-board systems and equipment”.**

**Test Plan UN78 / UN65**
**Linux core eX7xxM / (UN78) Functional Test**
**Linux core eX7xx / (UN65) Functional Test**
**JMobile Functional Test**

| **History** | | | |
|---|---|---|---|
| Rev | Date | Description | By |
| 0.1 | Jul 2024 | Test procedure of security capabilities | Giuseppe Marras -<br>Kavin Manohanran |
| 1.0 | Sept 2024 | Final Review and update | Fausto Gastaldin –<br>Giuseppe Marras |
| 1.1 | Sept 2024 | Updated adding ref to BSP 2.1.421 UN78 eX700M & Chromium. Fixed bootloader eX700 to 1.0.25 (errata) | Fausto G<br>Giuseppe M. |
| | | | |
| | | | |

| Test performed by | Signature |
|---|---|
| Giuseppe Marras | GM |
| Kavin Manohanran | KM |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

Author: Marras G. - Kavin Manohanran

Date: Jul-2024

## 1 Test Setup Description.

The next test plan will check the compliance of the eX700 and eX700M series devices with the requirements described in section 4.1 of the IACS UR E27 standard.

**Table 1: System configuration**

| Model Family Name | CPU Model | Testplan Application |
|---|---|---|
| Series eX7xxM | UN78 iMX8 Quad core | ✓ |
| Series eX7xx | UN65 iMX6 DL and iMX6 QC | ✓ |

The next sections show for each module the hw and sw configurations under test.

### 1.1 Systems sw configuration

SW configuration is common to all tested systems.

**Table 2: SW configuration**

**eX700M Series**

| Type | Signature | Version | Notes |
|---|---|---|---|
| Bootloader | UN78-xxxx-bootloader | 1.3.15 | |
| MainOS(core) | UN78XXXX-mainos | 3.1.421<br>2.1.421 | JMobile/CODESYS<br>Chromium |
| ConfigOS(core) | UN78XXXX-configos | 3.1.421<br>2.1.421 | |
| JMobile | | 4.5.2.390 | |
| | | | |

**eX700 Series**

| Type | Signature | Version | Notes |
|---|---|---|---|
| Bootloader | b03d-hsxx-bootloader<br>b03q-hsxx-bootloader | 1.0.25 | |
| MainOS(core) | UN65XXXX-mainos | 3.1.421 | JMobile/CODESYS/Chromium |
| ConfigOS(core) | UN65XXXX-configos | 3.1.421 | |
| JMobile | | 4.5.2.390 | |
| | | | |

### 1.2 Test Instruction

The TESTPLAN is the FUNCTIONAL list test, project used during testing must be saved and available for Q.A.control.
The checklist test is not performable for all models check with the text “NOT APPLICABLE” test you can not perform in your unit.
Test already marked DO NOT PERFORM are not requested for the testing section
The operator has to perform testing in according with the document. Report in the follow table any error found during testing.

## 2 Tests

All tests must to be performed if not otherwise described using:

1. An eX700 or eX700M series HMI device,
2. JMobile studio installed on PC,
3. Chromium web browser on the HMI device,
4. PC
5. An application for SSH connection installed on the PC (e.g. Putty)
6. LAN connection to the device,

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 1 | Human user identification and authentication:<br><br>The CBS shall identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1) | **Expected result:**<br>Upon entering credentials relating to different users, the device provides the possibility to continue their operations based on their roles.<br>**Acceptance criteria:**<br>The test is accepted if the expected result is “Passed” for at least two users<br><br>**BSP**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address**<br>**3. Without centralized access control (not supported)**<br><br>**Test Steps:**<br>**Case – 1: Remote access with browser**<br>From your PC browser:<br>1. Type https://deviceIPaddress/machine_config<br>2. Enter your username<br>3. Enter your password<br>4. press enter on the keyboard or the “Proceed” button<br>5. The system will let the user continue.<br>6. Log off<br>7. Repeat the same operations described in points 2, 3 and 4 using a different user<br><br>**Case – 2: Direct access from the panel**<br>HMI turned on and appropriately connected to the network:<br>1. Tap on one of the items you see on the home screen<br>2. Enter username<br>3. Enter password<br>4. The system will let the user continue.<br>5. Log off<br>6. Repeat steps 2 and 3 with a different user<br><br>**Case – 3: Access the panel via SSH**<br>HMI with SSH protocol enabled:<br>1. Open an application capable of connecting to the HMI using the SSH protocol (e.g. Putty),<br>2. Enter the IP address of the device and the port 22 on which it is listening<br>3. Press “connect”,<br>4. In the opened “login:” window, enter username<br>5. Press enter<br>6. Enter your password<br>7. Log off<br>8. Repeat steps 2 to 6 using a different user.<br><br>**JMobile**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address** | Passed |

| | | | |
|---|---|---|---|
| | | **Test steps:**<br>**Case – 1: Access from PC**<br>1. Open JMobile studio<br>2. Projectview> Security> double-click Users<br>3. In the Users editor, click + to add a user: one row is added to the table. If you change the name of the new user by entering an existing name.<br>4. Configure the desired properties.<br>5. Open or to do a new project<br>6. Download the project to the HMI<br>7. Open Chromium<br>8. Connect the HMI with web browser with the ip https://IP/machine_config<br>9. Enter the username you created<br>10. Enter the password you created<br>11. Log-off<br>12. Repeat steps 9 and 10 with a different user<br><br>**Case – 2: Access on HMI**<br>1. Open JMobile studio<br>2. ProjectView> Security> double-click Users<br>3. In the Users editor, click + to add a user: one row is added to the table. If you change the name of the new user by entering an existing name.<br>4. Configure the desired properties.<br>5. Open or to do a new project<br>6. download the project to the HMI<br>7. On HMI Enter the username and password you created<br>8. Log-off<br>9. Repeat step 7 with a different user<br><br>**Case – 3: Access from FTPS**<br>1. Open JMobilestudio<br>2. Security>user groups>authorization settings>ftp<br>3. In FTP option we can configure specific ip in allow ip address or allow all ip by enabling the allow all option then select use ftps only<br>4. There is additional folders option where u can add path of a storage device where we should enable the option enable FTP authorization<br>5. Connect with Ftp clients like FileZilla for file transferring with ipaddress and port number<br>6. Access Ftp by action button with ftpget and ftpput functionality<br>7. Click ftpget or put to add to the action button<br>8. In action properties ftpconfig>press + >configure ftp servers > Ftp remote file name > ftp local file name<br>9. Press action button to verify file transfer | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 2 | Account management<br>The CBS shall provide the | **Expected result:**<br>the creation, modification, deletion and disabling/enabling of an account.<br>**Acceptance criteria:** | Passed |

| | | | |
|---|---|---|---|
| | capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3) | The test is "Passed" if an admin performs the tasks in "Expected result"<br>**BSP**<br>**The same steps described below can also be carried out directly on the device.**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address**<br>**3. Without centralized access control (not supported)**<br>**4. Users belonging to the ADMIN role**<br>**Test Steps:**<br>**Case – 1: Creating an account**<br>From your PC browser:<br>1. On the URL bar, type https://ipaddress/machine_config to reach and press enter<br>2. Enter the username<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System Settings", click on the "Authentication" item<br>5. Click on USERS<br>6. Click on "EDIT"<br>7. Click on the "+" sign and fill in the required fields<br>8. Click on the "ADD User" button<br>9. Type the password of the user who is operating under the role of "Admin" and click confirm<br>**Case – 2: Enabling/Disabling an account**<br>1. After creating an account, in the same "Authentication" and then "Users" sections you will see the name of the newly created user who is enabled by default. To disable it: click on "EDIT"<br>2. Move the cursor of the "Enabled" item to the left<br>3. Confirm when prompted.<br>**Case – 3: Account deletion**<br>1. To delete the account in the same "Authentication" and "Users" sections: click on "EDIT",<br>2. Next to the account to be deleted, click on the "-" symbol<br>Confirm by entering the password of the user with the Admin role who is operating..**Case – 4: Edit account**<br>To proceed with modifying the account by entering a new password, role or changing the validity of the password, in the "Authentication" and "Users" sections:<br>1. Click Edit<br>2. In correspondence with the account to be modified, click on the symbol ⌄ and modify the parameters,<br>3. Click the "Update" button<br>Confirm by entering the password of the user with the Admin role who is operating.<br>**JMobile**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address**<br>**3. Users belonging to the ADMIN role**<br>**Test Steps:**<br>**Case – 1: Creating an account:**<br>1. Open JMobile studio<br>2. ProjectView> Security> double-click Users<br>3. In the Users editor, click + to add a user: one row is added to the table. If you change the name of the new user by entering an existing name.<br>4. Configure the desired properties.<br>**Case – 2: Enabling/Disabling an account:** | |

| | | | |
|---|---|---|---|
| | | 1. Open JMobile studio<br>2. ProjectView> Security> double-click Users<br>3. Flag “inactive” to disable. Remove the flag from “inactive” to enable<br>**Case – 3: Account deletion**<br>1. Open JMobile studio<br>2. ProjectView> Security> double-click Users<br>3. Click on user to delete<br>4. click “-“ to delete user<br>5. Confirm<br>**Case – 4: Edit account**<br>1. Open JMobile studio<br>2. ProjectView> Security> double-click Users<br>3. Click on user’s property to modify | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 3 | Identifier management<br>The CBS shall provide the capability to support the management of identifiers by user, group and role.<br>(IEC 62443-3-3/SR 1.4) | **Expected result:**<br>The HMI can’t have two identical users and they must be identifiable.<br>**Acceptance criteria:**<br>If the requirement is not met directly on the device, it must support LDAP<br>**BSP**<br>**The same steps described below can also be carried out directly on the device.**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address**<br>**3. There is a user already created**<br>**4. Users belonging to the ADMIN role**<br>**5. Without centralized access control (not supported)**<br>1. System settings><br>2. Click authentication><br>3. Click “edit”<br>4. In the toolbar at the top right, click + in the users section<br>5. Enter a username that already exists and click on “add user”<br>6. The alert should appear<br>**JMobile**<br>**1. The HMI is already connected to a specific network**<br>**2. Has its own IP address**<br>**3. Users belonging to the ADMIN role**<br>On JMobile Studio from PC:<br>1. ProjectView><br>2. Security><br>3. double-click Users<br>4. In the Users editor, click + to add a user: one row is added to the table.<br>5. change the name of the new user by entering an existing name, the alert should appear. | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 4 | Authenticator management | | |

| | | | |
|---|---|---|---|
| | The CBS shall provide the capability to:<br>- Initialize authenticator content<br>- Change all default authenticators upon control system installation<br>- Change/refresh all authenticators<br>- Protect all authenticators from unauthorized disclosure and modification when stored and transmitted.<br>(IEC 62443-3-3/SR 1.5) | **Expected result:**<br>1. The account, at first login, can use a default or pre-configurated authenticators,<br>2. The device recognizes the default authenticator at first use and then it recognizes its change,<br>3. Device, periodically, enforce to change authenticators<br>4. Authenticators when stored, used and transmission, they must be encrypted.<br>**Acceptance criteria:**<br>The test is “Passed” if an admin performs the tasks in “Expected result”.<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device.**<br>**1. The HMI already connected to a specific network,**<br>**2. the HMI has its own IP address**<br>**3. There is a user already created or you are in the first installation phase**<br>**4. perform the steps with users belonging to the ADMIN role**<br>**5. Without centralized access control (not supported)**<br><br>**Initialize authenticator content**<br>**At first configuration:**<br><br>1. At initial stage of login after reboot will go to normal login page in which the credentials of USER:admin and Password:admin<br>2. click login which prompts to change the default password to desired password<br>3. After the password has been set, we get logged out enter the username and new password to login<br><br>**Change all default authenticators**<br>**After creation an account:**<br>1. Open Chromium<br>2. Digit https://IP address/machine_config<br>3. Enter the credentials provided<br>The device forces the user to change the password and warns that a reboot will be performed<br><br>**Change/refresh all authenticators:**<br><br>In System Settings<br>1. Click Authentication<br>2. Click “EDIT” in the toolbar at the top right<br>3. Click + in the Users section<br>4. Set a time limit after which the user must change his password, the desired number of days must be entered as the value of the Password validity (days) parameter.<br>5. Check when the period expires<br><br>**Protect all authenticators**<br>**In this case, for verification, specific cybersecurity techniques or software must be used such as the following:**<br><br>1. Token based authentication try to intercept the token with the intercepting tools like (Burp, Zap) and try manipulating the token .<br>2. Session management Web application security tools like OWASP ZAP or Burp Suite, Test for session fixation, session hijacking, and proper session expiration<br>3. Penetration Testing Comprehensive penetration testing frameworks like Metasploit. Conduct thorough penetration testing to identify and exploit weaknesses in authentication mechanisms.<br>4. Perform regular security audits to ensure compliance with best practices and identify any potential weaknesses in authentication systems.(Using Nessus scans)<br><br>**JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address** | Passed |

| | | | |
|---|---|---|---|
| | | **3. Perform the steps with users belonging to the ADMIN role**<br>**4. JMobile Studio installed on a PC**<br>**5. Availability of a new JMobile project on HMI**<br>**Initialize authenticator content**<br>On the project login page, if not appropriately modified by JMobile Studio, the username and password to use will be the default ones (username: admin; password: admin). However, when these are changed and the user is given the opportunity to customize the setting, the default user will be able to log in with the password provided and set it as desired<br>**Change all default authenticators**<br>After creation an account:<br>1. Set “Change initial password” on “True” value<br>2. Download the project<br>3. open browser on your PC<br>4. Type https://IPdeviceaddress<br>5. Enter the credentials provided<br>6. You will be enforced to change the password<br>**Change/refresh all authenticators:**<br>1. After creation an account:<br>2. Set “Password aging” and “Warning” to have a warning before its expiration date<br>3. Download the project<br>4. Check when the period expires:<br>5. Open browser on your PC<br>• Type https://IPdeviceaddress<br>• You have a warning for expiration date<br>**Protect all authenticators**<br>**In this case, for verification, specific cybersecurity techniques or software must be used such as the following:**<br>1. Token based authentication try to intercept the token with the intercepting tools like (Burp, Zap) and try manipulating the token .<br>2. Session management Web application security tools like OWASP ZAP or Burp Suite, Test for session fixation, session hijacking, and proper session expiration<br>3. Penetration Testing Comprehensive penetration testing frameworks like Metasploit. Conduct thorough penetration testing to identify and exploit weaknesses in authentication mechanisms.<br>4. Perform regular security audits to ensure compliance with best practices and identify any potential weaknesses in authentication systems.(Using Nessus scans) | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 5 | Wireless access management<br>The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6) | OUT of SCOPE because eX700 and eX700M don’t expose Wi-Fi interface | |

<table>
<tr><th>#</th><th>Objective and requirements</th><th>Conditions</th><th>Check</th></tr>
<tr><td>6</td><td>Strength of password-based authentication<br>The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.<br>(IEC 62443-3-3/SR 1.7)</td><td><b>Expected result:</b><br>You can use a password that is compliant to the principal’s standard<br><b>Acceptance criteria:</b><br>The test is “Passed” if a device accept a password that contains:<br>• At least 8 characters in total<br>• At least one lower case and one upper case letter<br>• At least one numeric character<br>• At least one special character [@$!%*_|/.:;()[]{}?&^=+<>#]<br><b>BSP</b><br><b>The same steps described below can also be performed directly on the device.</b><br><b>1. The HMI already connected to a specific network,</b><br><b>2. the HMI has its own IP address</b><br>In System Settings<br>1. Click Authentication<br>2. Click “EDIT” in the toolbar at the top right<br>3. Click + in the Users section<br>4. You have a description of minimum criterias for a secure password.<br>5. Check if is true trying to set a password without one of that criterias<br>6. Give the possibility to the user to know the policy and test it.<br><b>JMobile</b><br><b>1. The HMI already connected to a specific network,</b><br><b>2. The HMI has its own IP address</b><br><b>3. Perform the steps with users belonging to the ADMIN role</b><br>After creation an account set:<br>1. “Password minimum length”<br>2. “Must contain special characters”<br>3. “Must contain numbers”<br>4. “Must contain lower case and upper case”<br>5. Download the project<br>6. open browser on your PC<br>7. Type https://IPdeviceaddress<br>8. Enter new password with the right criterias<br>If you try to type a password that isn’t comply with criterias, you have a warning.</td><td>Passed</td></tr>
</table>

<table>
<tr><th>#</th><th>Objective and requirements</th><th>Conditions</th><th>Check</th></tr>
<tr><td>7</td><td>Authenticator feedback<br>The CBS shall obscure feedback during the authentication process.<br>(IEC 62443-3-3/SR 1.10)</td><td><b>Expected result:</b><br>1. When you write the password to authenticate, you read only asterisks,<br>2. If you write in wrong manner the password or username, you have feedback of wrong authentication, but you don’t know if you wrong username or password.<br><b>Acceptance criteria:</b><br>The test is “passed” if you achieve that is describe in “Expected result”.<br><b>BSP</b></td><td>Passed</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | **The same steps described below can also be performed directly on the device.**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Your account is already created**<br><br>**Case – 1:** On your PC:<br>1. Open your browser<br>2. Digit https://IP address/machine_config<br>3. Enter your username<br>4. Enter your password. You cannot read it.<br><br>**Case – 2:** On your PC:<br>1. Open your browser<br>2. Digit https://IP address/machine_config<br>Enter your usernameEnter your wrong password. You can read a message that said "Invalid credentials".<br>Repeat the steps wronging the username.<br><br>**JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Your account is already created**<br>**4. The project is downloaded on HMI**<br><br>**Case – 1:**<br>1. Open browser on your PC<br>2. Type https://ipdeviceaddress<br>3. Enter your username<br>4. Enter your password. You cannot read it. You can read it only if you click on "eye symbol".<br><br>**Case – 2:**<br>1. Open browser on your PC<br>2. Type https://ipdeviceaddress<br>3. Enter your username<br>4. Enter your wrong password. You have a warning reporting "The username or password is incorrect"<br>Repeat the steps wronging the username. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 8 | Authorization enforcement<br><br>On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.<br>(IEC 62443-3-3/SR 2.1) | **Expected result:**<br>After role assignation, an account must have different permissions to operate on the device or on its applications.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is describe in "Expected result".<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device.**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br><br>From your PC's browser: | Passed |

| | | | |
|---|---|---|---|
| | | 1. In the address bar, type https://ipaddress/machine_config to reach and press enter<br>2. Enter your username<br>3. Enter the password and press enter on the keyboard or the “Proceed” button,<br>4. On the left you will read the list of items relating to "System settings", clicking on the "Authentication" item<br>5. Click on USERS<br>6. Click on “EDIT”<br>7. Click on the “+” sign and fill in the required fields<br>8. Click on the “ADD User” button<br>9. Type the password of the user who is operating under the role of “Admin” and click confirm.<br>10. Repeat the steps to create an user under the role of “user”<br>11. Enter on HMI with account under admin role and note your permission<br>12. Press Log out<br>13. Enter on HMI with account under user role and note different admin permission with admin also in its visualization.<br>**JMobile**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. You must have a ready project**<br>On your PC:<br>1. Open JMobile studio<br>2. Projectview> Security> double-click Users<br>3. In the Users editor, click + to add an account: one row is added to the table. If you change the name of the new user by entering an existing name.<br>4. Configure the desired properties and assign it to admin group.<br>5. Repeat steps to create another account and assign it to guest group.<br>6. Follow this path: projectview> Security> double-click usergroups > Authorization Settings column<br>7. Click the bottom: a dialog appears with a list of widgets and actions. You can modify access permissions for each one in the list and for each one project page.<br>8. Click OK<br>9. Download the project,<br>10. Open your browser<br>11. Type https://IP_HMI_address<br>12. Enter the credentials for admin account<br>13. Press “enter” or “Login” button<br>14. You can do all action<br>15. Click “Logout” if it is implemented in the project or close your browser<br>16. Repeat the actions from point 10 to 13<br>17. Your visualization and your permissions are change and they follow the settings in point 7<br>18. Click “Logout” if it is implemented in the project or close your browser. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 9 | Wireless use control<br>The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted | OUT OF SCOPE<br>(Wireless not supported) | |

| | | | |
|---|---|---|---|
| | security industry practices (IEC 62443-3-3/SR 2.2) | | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 10 | Use control for portable and mobile devices<br>When the CBS supports use of portable and mobile devices, the system shall include the capability to<br>a) Limit the use of portable and mobile devices only to those permitted by design<br>b) Restrict code and data transfer to/from portable and mobile devices<br>Note: Port limits / blockers (and silicone) could be accepted for a specific system<br>(IEC 62443-3-3/SR 2.3) | OUT of SCOPE because there is no component level requirement associated with IEC 62443-3-3 SR 2.3. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 11 | Mobile code<br>The CBS shall control the use of mobile code such as java scripts, activex and PDF.<br>(IEC 62443-3-3/SR 2.4) | **Expected result:**<br>The device does not allow the execution of scripts and the reading of .pdf files<br>**Acceptance criteria:**<br>The introduction of unsafe mobile code into the system can occur using external USB devices or SD interfaces. The test is "passed" if you disable these and use the browser provided within BSP only just to access system settings in localhost or configure it only to navigate in a fixed page.<br>**BSP**<br>**The same steps described below can also be performed directly on the device.**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>From your PC's browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Clicking on the "Security" item<br>6. In "External devices" section, by default the item for USB and SD are enabled. Disabled it to avoid executing potential malicious code.<br>7. Exec a script or open a file .pdf | Passed |

| | | | |
|---|---|---|---|
| | | **JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. You must have a ready project**<br>**5. Using the browser widget (only if necessary)**<br>**6. Using the PDF viewer (only if necessary)**<br><br>**The address bar will be read only, and the user cannot enter a web address:**<br>1. Open JMobile studio<br>2. Select a browser widget in a page<br>3. Double click on the address bar of browser widget<br>4. On the left, click datalink<br>5. Click Access Type<br>6. Select R<br><br>**PDF viewer**:<br>If it is necessary to use a PDF viewer you must first verify that the PDF loaded into the PDF viewer is reliable and secure. Additionally, using JMobile Studio, you should add the -hide-open-button option when the PDF viewer launch event is triggered, using this option, the icon to open a different file will be removed from the PDF toolbar (to restrict navigation to PDF file already opened and passed via command line). | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 12 | Session lock<br><br>The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock.<br>(IEC 62443-3-3/SR 2.5) | **Expected result:**<br>When the session isn't in use, after a certain set time, it logs out<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device.**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br><br>From your PC's browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Clicking on the "Authentication" item<br>6. Click on the "Session" item<br>7. Click Edit<br>8. Set the "Inactivity timeout" and "Session timeout"<br>9. Click ☑<br>10. Wait the configured time, the account should log out and you will see the login page<br><br>**JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role** | Passed |

| | | | |
|---|---|---|---|
| | | **4. You must have a ready project**<br><br>On your PC:<br><br>1. Open JMobile studio<br>2. Projectview> Security> double-click Users<br>3. In the Users editor, for your account, set “Logoff time”<br>4. Download the project<br>5. Enter your credentials<br>6. Press “enter” or “Login” button<br>7. Wait the configured time, the account should log out and you will see the login page | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 13 | Auditable events<br><br>The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication.<br>(IEC 62443-3-3/SR 2.8) | **Expected result:**<br>There must be collection of logs as per requirement<br>**Acceptance criteria:**<br>The test is “passed” if you achieve that is described in “Expected result”.<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br><br>From your PC’s browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the “Proceed” button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click Logs<br>6. Click “Get” button to download the log files<br>7. Open the file tar.gz<br><br>**JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. You must have a ready project**<br><br>**On your PC:**<br><br>1. Open JMobile studio<br>2. Projectview> Configuration > Security > double-click audittrail<br>3. By default, Audit trail logging is disabled. To enable it flag on “Enable Audit Trail” check box<br>4. Set your logs from the main tabs (Tags, Alarms, Recipes and Miscellaneous)<br>5. Download the project which must include audit widget.<br>6. In the address bar of your pc’ browser, type https://ipaddress to reach the device and press enter,<br>7. Enter your credentials<br>8. Press “enter” or “Login” button<br>9. “Play” with your project<br>10. Check what is recorded for JMobile in your widget.<br><br>If you have configured log saving, you can also view the recordings on the device you indicated. | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 14 | Audit storage capacity<br><br>The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded.<br>(IEC 62443-3-3/SR 2.9) | **Expected result:**<br>The amount of memory allocated for log files must be configurable and there must be a mechanism to protect against a failure of the component when it reaches or exceeds the audit storage capacity.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. the HMI has its own IP address**<br>**3. perform the steps with users belonging to the ADMIN role**<br><br>From your PC's browser:<br>1. in the address bar, type https://IPaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. on the left you will read the list of items relating to "System settings",<br>5. click Logs<br>6. click "EDIT" in the toolbar at the top right<br>7. click edit to insert Audit Size (MB)<br>8. click Save in the toolbar.<br>9. "Play" with your BSP and with other users until registrations reach the limit you set. Once the limit is reached, another file of the same size will be created. This will happen four times. Then the oldest will be deleted<br><br>**JMobile**<br><br>1. **The HMI already connected to a specific network,**<br>**2. the HMI has its own IP address**<br>**3. perform the steps with users belonging to the ADMIN role**<br>**4. You must have a ready project**<br><br>On your PC:<br><br>1. Open JMobile studio<br>2. Click ProjectView<br>3. Click Configuration<br>4. Click Events Buffer<br>5. Click Size tab<br>6. Set your buffer.<br>7. Click on "Storage device" button<br>8. Click on your chois and click on "Save a copy when full"<br>9. Set how you want the other options<br>10. Click OK<br>11. Download the project<br>12. Enter your credentials<br>13. Press "enter" or "Login" button<br>14. "Play" with your project<br>15. When your buffer is full, logs will be saved where configured | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 15 | Response to audit processing failures<br><br>The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure.<br>(IEC 62443-3-3/SR 2.10) | **Expected result:**<br>When a machine malfunction occurs that causes its operating system to crash, the device has the capability to protect against the loss of essential services and functions in the event of an error in audit processing<br>**Acceptance criteria:**<br>The test is "passed" if the watchdog intervenes and the device resets, preserving the logs.<br><br>**BSP and JMobile**<br><br>Watchdog is a hardware timing system that allows the CPU to detect an infinite program loop or deadlock situation. This detection may allow you to take steps to correct the situation, generally by performing a system reset. This system is present in the device. To verify its functioning, you must trigger a serious event on the device to block it or modify the code that governs the timing.<br><br>**Testing**<br>1. The watchdog functionality is enabled by default when the crash occurs it can be stored and viewed for audit.<br>2. The log can be viewed in /mnt/data/hmi/qthmi/deploy/var/log viewing the log and check for watchdog trigger by JMobile<br>3. The watch dog functionality represents the crash time and the reason for the crash | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 16 | Timestamps<br><br>The CBS shall timestamp audit records.<br>(IEC 62443-3-3/SR 2.11) | **Expected result:**<br>The timestamp must be present in the log file<br>**Acceptance criteria:**<br>The test is “passed” if you achieve that is described in “Expected result”.<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. the HMI has its own IP address**<br>**3. perform the steps with users belonging to the ADMIN role**<br><br>From your PC’s browser:<br>1. in the address bar, type https://IPaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the “Proceed” button,<br>4. on the left you will read the list of items relating to "System settings",<br>5. click Logs<br>6. click “Get” button to download the log files<br>7. open the file tar.gz how you prefer.<br>8. Check for the presence of the timestamp.<br><br>**JMobile** | Passed |

| | | | |
|---|---|---|---|
| | | 1. **The HMI already connected to a specific network,**<br>2. **the HMI has its own IP address**<br>3. **perform the steps with users belonging to the ADMIN role**<br>4. **You must have a project ready with logs enabled and in it you must have audit widget.**<br>On the HMI:<br>1. View the audit widget<br>2. Check for the presence of the timestamp. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 17 | Communication integrity<br>The CBS shall protect the integrity of transmitted information.<br>Note: Cryptographic mechanisms shall be employed for wireless networks.<br>(IEC 62443-3-3/SR 3.1) | **Expected result:**<br>In communications involving devices, manipulation must be detected and then data retransmitted.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br>**BSP:**<br>For services included in the BSP, integrity is supported in the following protocols: SSH, HTTPS, FTPS, NTP, DHCP<br>802.1X standard is supported for ETH and Wi-Fi authentication (this is possible only with the use of the plug in).<br>**JMobile:**<br>The protocols that ensure the integrity of transmitted information are:<br>HTTPS<br>FTPS<br>OPC UA<br>Generally, TCP based protocols integrate by design integrity check. For the other protocols to use them, mitigation measures must be taken, such as keeping the firewall always up or using a secure network.<br>**Test case**<br>The integrity for protocols above is guaranteed by design | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 18 | Malicious code protection<br>The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection | **Expected result:**<br>Unauthorized, potentially malicious software cannot be installed on the device. There must be a mechanism that protects against malware<br>**Acceptance criteria:**<br>The test is "passed" if in a device there is an antivirus, or it supported by an external mechanism (e.g. IDS/IPS).<br>**BSP**<br>Malicious code can be introduced from an external USB device or SD interface. The system can be configured to avoid this disabling the USB and SD card ports and therefore perform the following steps: | Passed |

| | | | |
|---|---|---|---|
| | mechanisms<br>(IEC 62443-3-3/SR 3.2) | BSP<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br><br>From your PC's browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter,<br>2. Enter your username ,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click Security<br>6. Click External Devices<br>7. Disable external USB<br>8. Disable SD card<br><br>If you still want to use the aforementioned interfaces to run external software, we recommend scanning the software with an antivirus beforehand.<br><br>**JMobile**<br><br>- Project signature test:<br>Sign the project following the steps documented in the JMobile Studio user manual (Project Signature).<br>Download the project on the HMI device. You will be prompted for the certificate to use which must correspond to the certificate installed on the HMI device.<br>- Project files encryption test:<br>Encrypt the project following the steps documented in the JMobile Studio user manual (Project Files Encryption)<br>When the project is encrypted, every time you open the project on JMobile Studio you will be asked to enter the password.<br>When the HMI Runtime detects that a project is encrypted and does not know the password to decrypt the project, it will show a dialog where to enter the password. The password will be requested only once and then stored in a secure area of the HMI device. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 19 | Security functionality verification<br><br>The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance<br>(IEC 62443-3-3/SR 3.3) | **Expected result:**<br>Capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance<br>**Acceptance criteria:**<br>The test is "passed" if you provide the customer with guidelines for carrying out tests to verify the correct functioning of the safety functions.<br><br>For verification of the intended operation of each security function, refer to the Test Procedure section of the documentation produced for each requirement. | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 20 | Deterministic output<br><br>The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be:<br>- Unpowered state,<br>- Last-known value, or<br>- Fixed value<br>(IEC 62443-3-3/SR 3.6) | **Expected result:**<br>Following an attack that causes a machine crash, the device has the ability to enter the Last-known value state<br>**Acceptance criteria:**<br>The test is "passed" if the watchdog operation or the OOM Killer (Out of Memory Killer) intervene.<br><br>**BSP and JMobile**<br><br>To verify the functioning of the watchdog it is necessary to subject the device to an attack and cause it to crash.<br>Another component that allows the system to reach a predetermined state in case of malfunction is the OOM Killer (Out of Memory Killer). The OOM Killer is a component of the Linux kernel that kills the process if it consumes a large amount of memory: this anomaly must be caused by simulating an attack<br><br>**Test cases**<br>1. The watchdog functionality is enabled by default when the crash occurs it can be stored and viewed for audit.<br>2. The log can be viewed in /mnt/data/hmi/qthmi/deploy/var/log viewing the log and check for watchdog trigger by JMobile<br>3. The watch dog functionality represents the crash time and the reason for the crash | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 21 | Information confidentiality<br><br>The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.<br>Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit.<br>(IEC 62443-3-3/SR 4.1) | **Expected result:**<br>The device must provide the ability to protect the confidentiality of information both in transit and at rest<br>**Acceptance criteria:**<br>The test is “passed” if you achieve that is described in “Expected result”.<br><br>**BSP**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br><br>**At rest:**<br>The data partition, which contains the applications and their settings, is protected by authentication, only the administrator or authorized users can access it. It is not encrypted.<br>The settings partition, that contains the settings of your device (this means the configuration parameters entered using the System Settings interface), is not encrypted but only the administrator or authorized users can access it.<br>**In transit:**<br>The following protocols provide confidentiality of information:<br>• Https<br>• Ftps<br>• SSH<br>If possible, keep others disabled.<br><br>**jmobile**<br><br>**1. The HMI is already connected to a specific network**<br>**2. It has its own IP address**<br>**3. Users belonging to the ADMIN role**<br>**4. A project must already be downloaded to the HMI** | Passed |

| | | | |
|---|---|---|---|
| | | At the project level, a guarantee of information protection is provided by the project files encryption and the project signature.<br>Protocols such as https, ftps, OPC-UA, Codesys PLC Handler and Siemens protocols ensure confidentiality of information.<br>If possible, keep others disabled.<br><br>**Test cases**<br><br>**1.** Login to https://ipaddress/machine_config in the panel with user and password<br>**2.** Use tools like wireshark to capture packets and analyze the packets to check whether the transport packet is through TLS 1.2 or 1.3 layer<br>**3.** Tools like Etter cap helps in performing man-in-the middle attack to Test the network's resilience to MITM attacks.<br>**4.** Assess cryptographic measures perform under high traffic conditions to ensure they do not degrade performance. While running isic tool for creating high traffic in the network<br>**5.** (Only with plugin) Got to system system setting>network>wifi switch on the wi-Fi setting to connect the panel to the wi-Fi<br>**6.** Test the wi-Fi to connect with a latest wpa connection | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 22 | Use of cryptography<br><br>If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations.<br>(IEC 62443-3-3/SR 4.3) | **Expected result:**<br>Cryptographic algorithms, key sizes, and mechanisms must comply with commonly accepted practices and recommendations in the security industry.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br><br>**BSP**<br>Services in use that comply with internationally recognized and proven security practices and recommendations are:<br><br>- System shadow file<br>- protects passwords with SHA512 hashes<br><br>- Secure Boot<br>- dmsetup encrypts data partition with the following algorithm specifications: capi:tk(cbc(aes))-plain<br><br>- 802.1x:<br>- EAP-MD5 (Challenge)<br>- EAP-TLS<br>- accepted TLS versions: 1.2, 1.3, implementation based on OpenSSL<br>- EAP-TTLS (tunneled TLS)<br>- accepted TLS versions: 1.2, 1.3, implementation based on OpenSSL<br>- supported authentication modes:<br>- PAP (Password Authentication Protocol)<br>- MSCHAP (Microsoft Challenge Handshake Authentication Protocol)<br>- MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol V2)<br>- CHAP (Challenge Handshake Authentication Protocol)<br>- MD5 (Challenge)<br><br>- PEAP (protected EAP)<br>- accepted TLS versions: 1.2, 1.3, implementation based on OpenSSL and GNUTLS (MSCHAPV2 only)<br>- supported authentication modes:<br>- MD5 (Challenge)<br>- GTC (Generic token card)<br>- MSCHAPV2 (Microsoft Challenge Handshake Authentication Protocol V2)<br><br>- System Secrets | Passed |

  - Secrets are encrypted using AES 256

- OpenSSL library (used by curl, wget, and others)
  - TLS has been restricted to versions 1.2 and 1.3
  - supported ciphers:
    TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, DHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305, ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-CHACHA20-POLY1305, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, DHE-RSA-AES256-SHA256, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-SHA, RSA-PSK-AES256-GCM-SHA384, DHE-PSK-AES256-GCM-SHA384, RSA-PSK-CHACHA20-POLY1305, DHE-PSK-CHACHA20-POLY1305, ECDHE-PSK-CHACHA20-POLY1305, AES256-GCM-SHA384, PSK-AES256-GCM-SHA384, PSK-CHACHA20-POLY1305, RSA-PSK-AES128-GCM-SHA256, DHE-PSK-AES128-GCM-SHA256, AES128-GCM-SHA256, PSK-AES128-GCM-SHA256, AES256-SHA256, AES128-SHA256, ECDHE-PSK-AES256-CBC-SHA384, ECDHE-PSK-AES256-CBC-SHA, SRP-RSA-AES-256-CBC-SHA, SRP-AES-256-CBC-SHA, RSA-PSK-AES256-CBC-SHA384, DHE-PSK-AES256-CBC-SHA384, RSA-PSK-AES256-CBC-SHA, DHE-PSK-AES256-CBC-SHA, AES256-SHA, PSK-AES256-CBC-SHA384, PSK-AES256-CBC-SHA, ECDHE-PSK-AES128-CBC-SHA256, ECDHE-PSK-AES128-CBC-SHA, SRP-RSA-AES-128-CBC-SHA, SRP-AES-128-CBC-SHA, RSA-PSK-AES128-CBC-SHA256, DHE-PSK-AES128-CBC-SHA256, RSA-PSK-AES128-CBC-SHA, DHE-PSK-AES128-CBC-SHA, AES128-SHA, PSK-AES128-CBC-SHA256, PSK-AES128-CBC-SHA

- GnuTLS library (used by wpa-supplicant, x11vnc and others)
  - supported ciphers and algorithms (gnutls-cli compiled manually):
    - Certificate types: CTYPE-X.509, CTYPE-Raw Public Key
    - Protocols: VERS-TLS1.0, VERS-TLS1.1, VERS-TLS1.2, VERS-TLS1.3, VERS-DTLS0.9, VERS-DTLS1.0, VERS-DTLS1.2
    - Ciphers: AES-256-CBC, AES-192-CBC, AES-128-CBC, AES-128-GCM, AES-192-GCM, AES-256-GCM, AES-128-CCM, AES-256-CCM, AES-128-CCM-8, AES-256-CCM-8, ARCFOUR-128, ESTREAM-SALSA20-256, SALSA20-256, CHACHA20-32, CHACHA20-64, CAMELLIA-256-CBC, CAMELLIA-192-CBC, CAMELLIA-128-CBC, CHACHA20-POLY1305, CAMELLIA-128-GCM, CAMELLIA-256-GCM, GOST28147-TC26Z-CFB, GOST28147-CPA-CFB, GOST28147-CPB-CFB, GOST28147-CPC-CFB, GOST28147-CPD-CFB, AES-128-CFB8, AES-192-CFB8, AES-256-CFB8, AES-128-XTS, AES-256-XTS, AES-128-SIV, AES-256-SIV, GOST28147-TC26Z-CNT, MAGMA-CTR-ACPKM, KUZNYECHIK-CTR-ACPKM, 3DES-CBC, DES-CBC, RC2-40, NULL
    - MACs: SHA1, SHA256, SHA384, SHA512, SHA224, UMAC-96, UMAC-128, AEAD, MD5, GOSTR341194, STREEBOG-256, STREEBOG-512, AES-CMAC-128, AES-CMAC-256, AES-GMAC-128, AES-GMAC-192, AES-GMAC-256, GOST28147-TC26Z-IMIT, OMAC-MAGMA, OMAC-KUZNYECHIK
    - Digests: SHA1, SHA256, SHA384, SHA512, SHA224, MD5, GOSTR341194, STREEBOG-256, STREEBOG-512
    - Key exchange algorithms: ECDHE-RSA, ECDHE-ECDSA, RSA, DHE-RSA, DHE-DSS, PSK, RSA-PSK, DHE-PSK, ECDHE-PSK, SRP-DSS, SRP-RSA, SRP, ANON-DH, ANON-ECDH, VKO-GOST-12, RSA-EXPORT
    - Compression: COMP-NULL
    - Groups: GROUP-SECP192R1, GROUP-SECP224R1, GROUP-SECP256R1, GROUP-SECP384R1, GROUP-SECP521R1, GROUP-X25519, GROUP-GC256B, GROUP-GC512A, GROUP-X448, GROUP-FFDHE2048, GROUP-FFDHE3072, GROUP-FFDHE4096, GROUP-FFDHE6144, GROUP-FFDHE8192
    - Public Key Systems: RSA, RSA-PSS, RSA, DSA, GOST R 34.10-2012-512, GOST R 34.10-2012-256, GOST R 34.10-2001, EC/ECDSA, EdDSA (Ed25519), EdDSA (Ed448), DH, ECDH (X25519), ECDH (X448)
    - PK-signatures: SIGN-RSA-SHA256, SIGN-RSA-SHA384, SIGN-RSA-SHA512, SIGN-RSA-PSS-SHA256, SIGN-RSA-PSS-RSAE-SHA256, SIGN-

RSA-PSS-SHA384, SIGN-RSA-PSS-RSAE-SHA384, SIGN-RSA-PSS-SHA512, SIGN-RSA-PSS-RSAE-SHA512, SIGN-EdDSA-Ed25519, SIGN-EdDSA-Ed448, SIGN-ECDSA-SHA256, SIGN-ECDSA-SHA384, SIGN-ECDSA-SHA512, SIGN-ECDSA-SECP256R1-SHA256, SIGN-ECDSA-SECP384R1-SHA384, SIGN-ECDSA-SECP521R1-SHA512, SIGN-ECDSA-SHA3-224, SIGN-ECDSA-SHA3-256, SIGN-ECDSA-SHA3-384, SIGN-ECDSA-SHA3-512, SIGN-RSA-SHA3-224, SIGN-RSA-SHA3-256, SIGN-RSA-SHA3-384, SIGN-RSA-SHA3-512, SIGN-DSA-SHA3-224, SIGN-DSA-SHA3-256, SIGN-DSA-SHA3-384, SIGN-DSA-SHA3-512, SIGN-RSA-RAW, SIGN-RSA-SHA1, SIGN-RSA-SHA1, SIGN-RSA-SHA224, SIGN-RSA-RMD160, SIGN-DSA-SHA1, SIGN-DSA-SHA1, SIGN-DSA-SHA224, SIGN-DSA-SHA256, SIGN-RSA-MD5, SIGN-RSA-MD5, SIGN-RSA-MD2, SIGN-ECDSA-SHA1, SIGN-ECDSA-SHA224, SIGN-GOSTR341012-512, SIGN-GOSTR341012-256, SIGN-GOSTR341001, SIGN-DSA-SHA384, SIGN-DSA-SHA512

- System Services:
    - Avahi Daemon: no authentication/encryption support
    - SNMP Server: no authentication/encryption support
    - SSH Server:
        - minimum protocol version: 2
        - ciphers and algorithms
            - ciphers: chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
            - key exchange algorithms: sntrup761x25519-sha512@openssh.com, curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256ca
            - signature algorithms: ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, sk-ssh-ed25519@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, rsa-sha2-512, rsa-sha2-256
            - host based accepted algorithms: ssh-ed25519-cert-v01@openssh.com, ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp521-cert-v01@openssh.com, sk-ssh-ed25519-cert-v01@openssh.com, sk-ecdsa-sha2-nistp256-cert-v01@openssh.com, rsa-sha2-512-cert-v01@openssh.com, rsa-sha2-256-cert-v01@openssh.com, ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, sk-ssh-ed25519@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, rsa-sha2-512, rsa-sha2-256
            - host key algorithms: ssh-ed25519-cert-v01@openssh.com, ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp521-cert-v01@openssh.com, sk-ssh-ed25519-cert-v01@openssh.com, sk-ecdsa-sha2-nistp256-cert-v01@openssh.com, rsa-sha2-512-cert-v01@openssh.com, rsa-sha2-256-cert-v01@openssh.com, ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, sk-ssh-ed25519@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, rsa-sha2-512, rsa-sha2-256
            - pub key accepted algorithms: ssh-ed25519-cert-v01@openssh.com, ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp521-cert-v01@openssh.com, sk-ssh-ed25519-cert-v01@openssh.com, sk-ecdsa-sha2-nistp256-cert-v01@openssh.com, rsa-sha2-512-cert-v01@openssh.com, rsa-sha2-256-cert-v01@openssh.com, ssh-ed25519,ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, sk-ssh-ed25519@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, rsa-sha2-512, rsa-sha2-256

- Web Server (nginx 1.20.1):
    - accepted TLS versions: 1.2, 1.3
    - ciphers have been limited to
    - EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

- Cloud Service
  - negotiated with server - sample output: Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 256 bit EC, curve prime256v1, signature: ecdsa-with-SHA256

Services that do not comply with internationally recognized and proven security practices and recommendations are:

- System Services:
  - VNC Service
    - password-based authentication: insecure (RFB challenge-response)
    - encryption (X11 BSP only)
      - accepted TLS versions: 1.2, 1.3

These services use unsafe encryption algorithms. We currently have no safe alternatives, but these services are optional and can be disabled. The following describes the procedure for disabling VCN Service. The same procedure should be followed to disable Cloud service:

The same steps described below can also be performed directly on the device

1. The HMI already connected to a specific network,
2. the HMI has its own IP address
3. perform the steps with users belonging to the ADMIN role

From your PC’s browser:

1. in the address bar, type https://IPaddress/machine_config to reach the device and press enter,
2. Enter your username ,
3. Enter the password and press enter on the keyboard or the “Proceed” button,
4. on the left you will read the list of items relating to "System settings",
5. click Services
6. click VCN Service
7. click “EDIT”  if enable in the toolbar at the top right and uncheck Enabled parameter
8. click “SAVE” in the toolbar

The use of secure algorithms listed above are implemented by design. If you want to manually verify, you should use tools like Wireshark to capture the packets and analyze them.

**JMobile**

Cryptography is used:

- Project encryption
  - projects are encrypted using AES-128-cbc, AES-256-cbc

- Project signature
  - projects are signed using private key of certificate; verification is done at runtime using public key of certificate; so, it should take the signing algorithm specified in certificate.

    It is the responsibility of the system integrator to choose which encryption algorithm to use.

- HTTPs

  - accepted TLS versions: 1.2 or more
  - supported ciphers and algorithms: EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

- Send mail TLS version

  - accepted TLS versions: 1.2 or more
  - supported ciphers and algorithms:

| | | | |
|---|---|---|---|
| | | EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>- Zip encryption: no authentication/encryption support<br>- Protocols encryption/signature<br>- OPC-UA, Codesys PLC Handler and Siemens protocols support encryption<br>All other protocols provided by JMobile do not support encryption, so it is recommended not to use them.<br>- FTPs<br>- accepted TLS versions: 1.2 or more<br>- supported ciphers and algorithms:<br>EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>- User management module - user password encryption<br>- Password are encrypted using PBKDF2, PKCS5_PBKDF2_HMAC<br>- JM Studio - Inside Manage target dialog and Project download dialog<br>- Used in encrypt/decrypt panel BSP passwords and store in registry. OpenSSL EVP_aes_128_cbc() cypher is used<br>- Exor licencing (.xlic)<br>- Exor licensing uses this algorithm from OpenSSL with EVP_sha256() cypher to encrypt the license data verified with a public key<br>- QFTP client in HMIstudio and runtime<br>- accepted TLS versions: 1.2 or more<br>- supported ciphers and algorithms:<br>EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>- Curl lib in HMI client to HMI server<br>- accepted TLS versions: 1.2 or more<br>- supported ciphers and algorithms:<br>- EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>- Database<br>- accepted TLS versions: 1.2 or more<br>- supported ciphers and algorithms:<br>- EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>- LDAP<br>- accepted TLS versions: 1.2 or more<br>- supported ciphers and algorithms:<br>- EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH<br>The use of secure algorithms listed above are implemented by design. If you want to manually verify, you should use tools like Wireshark to capture the packets and analyze them. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 23 | Audit log accessibility | **Expected result:** | Passed |

| | | | |
|---|---|---|---|
| | The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools.<br>(IEC 62443-3-3/SR 6.1) | Access to audits log must be read-only.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br><br>**BSP**<br>**1. The HMI already connected to a specific network,**<br>**2. the HMI has its own IP address**<br>**3. perform the steps with users belonging to the ADMIN role**<br><br>Audit must be read/write only by administrators<br><br>**Test cases**<br><br>1. Login as admin in system settings page from the HMI<br>2. Locate log in the system settings<br>3. They are associated with two logs option<br>a) OS logs<br>b) security logs<br>5. Download the log files by pressing GET option<br>6. The logs get downloaded and available in the reading format<br>7. Repeat steps with a user.<br><br>**JMobile**<br><br>**1. the HMI is already connected to a specific network**<br>**2. has its own IP address**<br>**3. users belonging to the ADMIN role**<br>**5. A project must already be downloaded to the HMI**<br><br>Audit logs can be accessed on a read-only basis using the table audit widget.<br><br>Open your project with JMobile Studio and go to the page where to show audit logs:<br>Path: ProjectView> Pages> open the page where to show audit logs<br><br>Then add Audit view widget:<br>Path: View> Toolbars and Docking Windows> Widget Gallery> Audit Tables> Audit view<br><br>Drag and drop the widget inside the page. Select the widget to open the properties dialog and configure them.<br><br>**Test cases**<br>Log in to HMI and go to the page where the table audit widget is located. You should see audit records correctly. | |

| **#** | **Objective and requirements** | **Conditions** | **Check** |
|---|---|---|---|
| 24 | Denial of service protection<br><br>The CBS shall provide the minimum capability to | **Expected result:**<br>The device under DDOS attack must maintain essential functions<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result". | Passed |

| | | | |
|---|---|---|---|
| | maintain essential functions during dos events.<br>Note: It is acceptable that the CBS may operate in a degraded mode upon dos events, but it shall not fail in a manner which may cause hazardous situations.<br>Overload-based dos events should be considered, i.e. Where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed.<br>(IEC 62443-3-3/SR 7.1) | **BSP and jmobile**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**Test cases**<br>1. Connect the panel directly to simulate the DOS attack and DDOS attack by using some tools like HULK,ISIC and with help of some scripts to perform storm attack, dos attack and DDOS attack<br>2. Trying to simulate the real time attack for protection of HMI<br>3. Identifying the ports which can be attacked with nessus and nmap<br>4. During the attack the HMI is monitored for memory spike crash and unable for the user to use the interface<br>5. Once the attack has been complete the panel is restarted and available check for availability of the users and data<br>6. Check the logs for received packets and functions happening in the system | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 25 | Resource management<br>The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.<br>(IEC 62443-3-3/SR 7.2) | **Expected result:**<br>The execution of simultaneous software processes or multiple simultaneous accesses to different services must not cause the device's resources to be exhausted<br>**Acceptance criteria:**<br>The test is “passed” if some measures have been implemented.<br>**BSP and JMobile**<br>The devices have a max number of connections for services such as VNC, HTTP/HTTPS and SSH. The firewall can provide help in meeting this requirement by reducing unnecessary services. Mechanisms to protect against brute force attacks are implemented. | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 26 | System backup<br>The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations<br>(IEC 62443-3-3/SR 7.3) | **Expected result:**<br>The device has the ability to provide its own backup without interfering with normal operations.  Additionally, the device must provide the ability to validate the integrity of the information being backed up before starting to restore that information<br>**Acceptance criteria:**<br>The test is “passed” if you achieve that is described in “Expected result”.<br>**BSP:**<br>To back up to your device, perform the following steps:<br>The same steps described below can also be performed directly on the device<br>1. The HMI already connected to a specific network,<br>2. The HMI has its own IP address<br>3. Perform the steps with users belonging to the ADMIN role<br>From your PC’s browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter, | Passed |

| | | | |
|---|---|---|---|
| | | 2. Enter your username ,<br>3. Enter the password and press enter on the keyboard or the “Proceed” button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click Management<br>6. Use the "Get" button to backup inside an external memory (e.g. USB key) the contents of the Data and the Settings partitions.<br>7. The Config OS mode is required. You will be prompted to restart into Config OS.<br>8. Insert admin password and press confirm<br>9. Once restarted, repeat steps 5 and 6.<br><br>**JMobile**<br>JMobile allows backup.<br>To perform backup of Runtime and project, follow this steps:<br>• In JMobile HMI Runtime right click to open the context menu.<br>• Select Backup: the Backup dialog is displayed.<br>• Select the path for storing the backup file. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 27 | System recovery and reconstitution<br><br>The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.<br>(IEC 62443-3-3/SR 7.4) | **Expected result:**<br>The device has the ability to perform a restore starting from a backup<br>**Acceptance criteria:**<br>The test is “passed” if you achieve that is described in “Expected result”.<br><br>**BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. A backup is available**<br><br>From your PC’s browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the “Proceed” button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click Management<br>6. Use the "Update" button to restore the contents of the Data and the Settings partitions.<br>7. The Config OS mode is required. You will be prompted to restart into Config OS.<br>8. Insert admin password and press confirm<br>9. Once restarted, repeat the steps 5 and 6<br>10. You must provide even an MD5 checksum file. The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix (e.g.: data.tar.gz, data.tar.gz.md5)<br>11. Download the backup and the MD5 file.<br><br>**JMobile**<br><br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. A backup is available**<br><br>Restore the backup package can be perform on HMI device from the Context Menu or from the System Settings (see points 1 to 11 of BSP)<br><br>From the Context Menu on PC or device:<br>1. Click Update | Passed |

| | | | |
|---|---|---|---|
| | | 2. Click Browse…<br>3. Select your backup file<br>4. Click Next | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 28 | Alternative power source<br>The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5) | OUT of SCOPE because there is no component level requirement associated with IEC 62443-3-3 SR 7.5. | |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 29 | Network and security configuration settings<br>The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6) | **Expected result:**<br>The device must provide an interface that allows you to enter network configuration parameters<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result".<br>**BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>From your PC's browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click Network<br>6. Click "EDIT" in the toolbar at the top right. If you enable DHCP you have the configuration parameters directly from your network. And configure the IP address, Net Mask, Gateway. While, if you disable DHCP, you must enter the required parameters. You also have the option to configure the 802.1.x protocol if you have a radius server<br>7. Save your changes by clicking "SAVE" in the toolbar.<br>**JMobile**<br>JMobile takes the network settings that come from the BSP | Passed |

| # | Objective and requirements | Conditions | Check |
|---|---|---|---|
| 30 | Least Functionality<br>The installation, the availability and the access | **Expected result:**<br>The device must provide the ability for each supported role/user to keep features, ports, services, etc. Disabled. With whom you do not need to interact.<br>**Acceptance criteria:**<br>The test is "passed" if you achieve that is described in "Expected result". | Passed |

| | | | |
|---|---|---|---|
| | rights of the following shall be limited to the strict needs of the functions provided by the CBS:<br>- operating systems software components, processes and services<br>- network services, ports, protocols, routes and hosts accesses and any software (IEC 62443-3-3/SR 7.7) | **BSP**<br>**The same steps described below can also be performed directly on the device**<br>**1. The HMI already connected to a specific network,**<br>**2. The HMI has its own IP address**<br>**3. Perform the steps with users belonging to the ADMIN role**<br>**4. There is a role different to ADMIN**<br><br>From your PC's browser:<br>1. In the address bar, type https://ipaddress/machine_config to reach the device and press enter,<br>2. Enter your username,<br>3. Enter the password and press enter on the keyboard or the "Proceed" button,<br>4. On the left you will read the list of items relating to "System settings",<br>5. Click "Security". In this section you can keep disable the "External Device"<br>6. Click "Applications". In this section you can keep disable the applications<br>7. Click "Services". In this section you can keep disable the services<br>8. Click "Authentication"<br>9. Click "Roles"<br>10. Click on › for a certain role. In the section that opens, you can decide which sections to show to users of the role and enable them to read-only or edit the entries included in the sections. To do this you must click on "Edit".<br><br>**JMobile**<br><br>1. **The HMI already connected to a specific network,**<br>2. **The HMI has its own IP address**<br>3. **Perform the steps with users belonging to the ADMIN role**<br>4. **There is a usergroup**<br>5. **You must have a ready project**<br><br>On your PC:<br>1. Open JMobile studio<br>2. Open your project<br>3. Open projectview<br>4. Click "Security"<br>5. Click "usergroup"<br>6. In the column "Authorization Settings", click on xxx_Authx and then on □ botton. You will be able to see a new window where you can apply all the necessary permissions. When you're done, all users in that group will be able to do/see what you determined. | |

**End of Document**