Standard IEC 62443-4-2.
IACS UR E27
“Cyber resilience of on-board systems and equipment”.
Exor eX700 and eX700M Series.
JMobile 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 CR 1.1 – Human user identification and authentication

1.1 Description of security capability

Through security management, application developers can configure the application to be accessible on all interfaces capable of human user access (both local access and remote access) only after the user signs in with its own username and password.

1.2 Configuration guidelines

Open your project with JMobile Studio.
Security management is enabled by default. Make sure it really is:

*Path: **ProjectView**> right-click **Security**> if disabled, click **Enable***

To make the system comply with this requirement when using local access, no default user must be configured, and context menu must be disabled.
By default, context menu is disabled; the default user, on the other hand, is active and must be disabled.

- Make sure the context menu is disabled

  *Path: **ProjectView**> double-click **Project properties**> **Properties** pane> **Runtime**> **Context Menu**> must be set to **on action***

- Default user can be disabled from the “Default User” check box in the Users editor:

  *Path: **ProjectView**> **Security**> double-click **Users***

  Make sure that no user is configured as the default user.

The system, by default, is compliant with this requirement when using remote access via Remote Client or Remote HMI Client. Make sure that the Force Remote Login is enabled:

*Path: **ProjectView**> right-click **Security**> **Force Remote Login** must be flagged*

Finally, make sure that the JS Remote Debugger is disabled in the production environment:

*Path: **ProjectView**> double-click **Project properties**> **Properties** pane> click **Show Advanced Properties**> **Runtime**> set **JavaScript Debug** and **Allow JavaScript Remote Debugger** properties to **false***

By default, these two properties are already set to false.

1.3 Test Procedure

Download the project to the HMI.

- Access using any interface, local or remote. For example, on HMI you must be asked to authenticate with username and password before you can log in.
  Enter the username and password you created.
  Log-off and reauthenticate using another user.

- Access from your PC by connecting to the HMI with a web browser at the IP address https://IP_HMI_address.
  You must be asked to authenticate with username and password before you can log in.
  Enter username and password.
  Log-off and reauthenticate using another user.

CR 1.1 RE (1) – Unique identification and authentication

1.4 Description of security capability

Each human user is uniquely identified and authenticated by a username/password combination.
It is not possible to define two users with the same combination of username and password.

1.5 Test Procedure

Open your project with JMobile Studio and go to Users Editor:

Path: ***ProjectView****>* ***Security****> double-click* ***Users***

Click + to add a user: one row is added to the table.
Change the name of the new user by entering an existing name.
An alert should appear informing you that the user already exists, and another name should be used.

2 CR 1.3 – Account management

2.1 Description of security capability

Through security management, the system provides the capability to support the management of all accounts.
When security management is enabled, application developers can restrict access to various widgets and operations by configuring users, user groups and assigning specific authorizations and permissions to each group. They can perform actions on users such as add user, delete user, edit user, activate user and disable user.
LDAP/Active directory support for JMobile Studio and Runtime is also available.

2.2 Configuration guidelines

Open your project with JMobile Studio.
Security management is enabled by default. Make sure it really is:

Path: ***ProjectView****> right-click* ***Security****> if disabled, click* ***Enable***

Users and user groups can be managed in the Users editor and the UserGroups editor:

Path: ***ProjectView****>* ***Security****> double-click* ***Users***
Path: ***ProjectView****>* ***Security****> double-click* ***UserGroups***

The Users editor allows the configuration of users, such as add (by clicking the + button), delete (by clicking the - button) and edit users.
The UserGroups editor allows specific permissions and authorizations to be assigned to user groups and thus to users, such as widget permissions, action permissions, tag permissions, FTP authorizations and HTTP authorizations:

Path: ***ProjectView****>* ***Security****> double-click* ***UserGroups*** *>* ***Authorization Settings*** *column*

Click the button: a dialog appears with a list of widgets and actions. You can modify access permissions for each one in the list.

2.3 Test Procedure

Open your project with JMobile Studio and go to Users Editor:

Path: ***ProjectView****>* ***Security****> double-click* ***Users***

- Click + to add a user: one row is added to the table. Configure the desired properties. On the HMI, verify that the user is in use.
- Flag "inactive" to disable user. Remove the flag "inactive" to enable user. On the HMI, verify that the user is disable and then enable.
- To delete a user, select it and click - to delete. Confirm. On the HMI, verify that the user is deleted
- Click on user's property to edit it. On the HMI, verify that the properties set are in use.

3 CR 1.4 – Identifier management

3.1 Description of security capability

Each account is uniquely and unambiguously identified by the username.
It is not possible to define two accounts with the same username.

3.2 Test Procedure

Refer to CR 1.1 RE (1) – Unique identification and authentication requirement for test procedure.

4 CR 1.5 – Authenticator management

4.1 Description of security capability

Through security management configuration, the system:
- supports the use of initial authenticator content.
- supports the recognition of changes to default authenticators made at installation time.
- functions properly with periodic authenticator change/refresh operation.
- protects authenticators from unauthorized disclosure and modification when stored, used and transmitted.

The creation of a user account can only be done by the administrators or authorized users (users that can manage other users).
When the administrator or a user with permission creates an account, he can create and define a default or pre-configurated password, in order for the account owner to be able to authenticate.
It is also possible to force the newly created user to redefine the password at the first login and force the users to define a new and different password after a configurable number of days with the ability to show a warning before the password expires.
LDAP/Active directory support is also available.

Passwords are encrypted using PBKDF2, PKCS5_PBKDF2_HMAC.

4.2 Configuration guidelines

- Open your project with JMobile Studio and go to Users Editor:

  Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

  Click + to add a user: one row is added to the table.
  A new random password must be created and defined, which is different from previously created passwords.
  To set the user's password, you must edit the Password parameter.

  By default, when a new account is created, the user is not forced to change the password at the first login. To force password change, you must set the Change Initial Password parameter to true.

  Likewise, by default, a user is not forced to define a new password after a certain number of days. To configure a time limit after which the user must change his password, the desired number of weeks must be entered as the value of the Password aging (weeks) parameter. Make sure to enter a value other than 0, otherwise the password will never expire.

  It is also possible to show a warning before the password expires. The desired number of days must be entered as the value of the Warning (days) parameter. The value 0 means that the warning is not shown.
  By default, the warning is shown one day before the password expires.

  From the Settings command in the Users editor, there is the possibility to define parameters values that will be common to all users.

- New accounts can be also created at runtime via the AddUser action by users who can manage other users (Can manage other users property set).
  In this case, when the action is triggered (for example by clicking a button widget) the creator user must define a password for the newly created user and flag the "User must change his initial password" checkbox, so as to force the new user to redefine the password when he first log in. The "User must change his initial password" checkbox is not flagged by default.

4.3 Test Procedure

- Test default authenticator

  Open your project with JMobile Studio and go to Users Editor:

  Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

  The Change Initial Password parameter must be set to true for each user.
  Click + to add a user: one row is added to the table.
  Define a password and set the Change Initial Password parameter to true.
  Download the project and log in to HMI using the credentials of the new user. You will be forced to change the password.

- Change/refresh authenticator

  Open your project with JMobile Studio and go to Users Editor:

  Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

The Password aging (weeks) parameter must have a value other than 0 for each user.
Click + to add a user: one row is added to the table.
Define a password and set the Password aging parameter and the Warning (days) parameter to have a warning before password expiration date.
Check when the period expires.
Download the project and log in to HMI using the credentials of the new user. You have a warning for expiration date.

5 CR 1.6 – Wireless access management

5.1 Description of security capability

OUT of SCOPE because eX700 and eX700M don't expose wifi interface.

6 CR 1.7 – Strength of password-based authentication

6.1 Description of security capability

The system provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.
The application developer can define a minimum password length and whether the password must contain at least one special character and/or at least one number and/or lower case and upper case.
The application developer can also configure the time duration of the password (number of weeks).

6.2 Configuration guidelines

Open your project with JMobile Studio and go to Users Editor:

Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

At this point, the following parameters can be configured for each user:

- Password Minimum Length: the minimum length of the password.
- Must contain special characters: whether the password must contain at least one special character.
- Must contain numbers: whether the password must contain at least one numeric digit.
- Must contain lower case and upper case: whether the password must contain lower case and upper case.
- Password aging (weeks): the number of weeks before forcing a password change (1/52 weeks)

From the Settings command in the Users editor, there is the possibility to define parameters values that will be common to all users.

By default, minimum length of password is 4, password aging is 0 and password does not contain special characters, numbers, lower case and upper case.

6.3 Test Procedure

Open your project with JMobile Studio and go to Users Editor:

Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

Click + to add a user: one row is added to the table.
Define a password, set the Change Initial Password parameter to true and set the parameters:

- Password minimum length
- Must contain special characters
- Must contain numbers
- Must contain lower case and upper case

Download the project and log in to HMI using the credentials of the new user. You are asked to define a new password. Enter a new password with the right criteria. If you try to type a password that doesn't comply with criteria, you have a warning.

7 CR 1.10 – Authenticator feedback

7.1 Description of security capability

The system provides, for all services, the capability to obscure feedback of authenticator information during the authentication process.
Furthermore, no details are provided in case of authentication errors. The errors that are returned are always generic and do not allow a detailed understanding of what went wrong.

7.2 Test Procedure

- On the HMI, enter username and password. The password is obscured, you can read it only if you click the "eye" symbol.

- On the HMI, enter username and a wrong password. You have a message that says: "The user name or password is incorrect". You cannot figure out what you did wrong, whether the username or the password.

8 CR 2.1 – Authorization enforcement

8.1 Description of security capability

The system provides an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.
Is it possible to restrict access to various widgets and operations by configuring users, user groups and assigning specific authorizations and permissions to each group.
sy

8.2 Configuration guidelines

Open your project with JMobile Studio and go to UserGroups Editor:

Path: ***ProjectView*** *>* ***Security*** *> double-click* ***UserGroups*** *>* ***Authorization Settings*** *column*

Click the button: a dialog appears with a list of widgets and actions. Here you can configure all permissions and authorizations for the selected user group, such as widget permissions, action permissions, tag permissions, FTP authorizations and HTTP authorizations.

8.3 Test Procedure

Open your project with JMobile Studio and go to Users Editor:

Path: ***ProjectView*** *>* ***Security*** *> double-click* ***Users***

Click + to add an account, configure the desired properties and assign it to admin group.

Click + to add another account and assign it to guest group.
Go to UserGroups editor:

Path: ***ProjectView*** *>* ***Security*** *> double-click* ***UserGroups*** *>* ***Authorization Settings*** *column*

Click the button: a dialog appears with a list of widgets and actions. Configure guest group permissions and authorizations to your liking.
Download the project and log in to HMI using the credentials of the admin user. You have all permissions and authorizations.
Click "Logout" if it is implemented in the project or close your browser.
Log in to HMI using the credentials of the guest user. Your visualization and your permissions are changed, and they follow the previously configured settings for the guest group.

9 CR 2.2 – Wireless use control

9.1 Description of security capability

OUT of SCOPE because eX700 and eX700M don't expose wifi interface.

10 CR 2.3 – Use control for portable and mobile devices

10.1 Description of security capability

OUT of SCOPE because there is no component level requirement associated with IEC 62443-3-3 SR 2.3.
The requirement must be satisfied by external components.

11 CR 2.4 (EDR 2.4) – Mobile code

11.1 Description of security capability

The introduction of unsafe mobile code into the system can occur in two ways:

- Using browser widget
- Using PDF viewer

Certain steps can be taken to prevent the development, acquisition or introduction of unacceptable mobile code into the system. For example, do not use the widget mentioned above, or, if you must use them, make sure that the code introduced or that can be introduced is verified, safe and reliable.

11.2 Configuration guidelines

Do not use browser widgets.
If you need to use them, it is the responsibility of the system integrator to ensure that the web address that is loaded into the browser widget is reliable and secure. Furthermore, using JMobile Studio, you need to remove the address bar or remove the ability to edit the web address.
To remove the address bar:

Path: double click on the ***browser widget*** *> click on the* ***address bar*** *> right-click on the* ***address bar*** *> click* ***Delete***

To remove the ability to edit the web address (by default access type is R/W):

*Path: double click on the **browser widget**> click on the **address bar**> **Properties** pane> **Value**> **DataLink**> **Access Type**> select **R***

This means that the address bar is read only, and the user cannot enter a web address.

Do not use PDF viewers.
If you need to use them, it is the responsibility of the system integrator to ensure that the PDF that is loaded into the PDF viewer is reliable and secure. Furthermore, using JMobile Studio, application developer needs to add -hide-open-button option when event that launch PDF viewer is triggered, for example on press of a button:

*Path: click on the widget that triggers the event> **Properties** pane> **Events**> click **+** at the desired event> a dialog appears> click the **LaunchPDFViewer** action in the Action List under Page> under **Action Properties** enter the option -hide-open-button in the **arguments** parameter*

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).

11.3 Test Procedure

If a browser widget is implemented in the project, log in to HMI and go to the page where it is located. You cannot edit or insert a custom web address.

If a PDF viewer is implemented in the project, log in to HMI and start the PDF viewer. You cannot open a different PDF file.

12 CR 2.5 – Session lock

12.1 Description of security capability

The system provides the capability to protect against further access by initiating a session lock after a configurable time period of inactivity. The session lock remains in effect until the human user who owns the session re-establishes access by authenticating.

12.2 Configuration guidelines

- Open your project with JMobile Studio. The inactivity time limit after which the session is locked can be configured in the Users editor:

  *Path: **ProjectView**> **Security**> double-click **Users***

  The Logoff time (minutes) parameter defines the minutes of inactivity after which the user is logged off. Make sure it is not 0.

- At runtime, the logoff time can be configured when you are adding or editing a user (through the actions AddUser and EditUsers).
  In the dialog that appears to add or edit a user, you can find the Inactivity logoff time (min) field. Make sure you do not enter the value 0.

12.3 Test Procedure

Open your project with JMobile Studio and go to Users Editor:

*Path: **ProjectView**> **Security**> double-click **Users***

Set “Logoff time” for your account.
Download the project and log in to HMI using your credentials.
Wait the configured time, the account should log out and you will see the login page.

13 CR 2.8 – Auditable events

13.1 Description of security capability

Through Audit trail logging feature, the system provides the capability to generate audit records relevant to security. Each record contains information on the actions executed, the user that performed them and a sequential number to easily check the presence of all records.
The resources for which all events are logged in the audit buffer are:

- Tags: keep track of when tag value changes.
- Alarms: keep track of when user acknowledges or resets an alarm event.
- Recipes: keep track of when user downloads or uploads recipes.
- Miscellaneous Resources:
  - User login details: keep track of when user login, logout or change password.
  - User management actions: keep track of when a user is added, removed or when the user properties are modified.
  - System actions: keep track of system actions (HMI Device Restart, Power On, Backup, Update, Download, enter in System Setting, open Project Manager).
  - FTP actions: keep track of ftpGET, ftpPUT, OpenTextEditor, SaveTextEditor.
  - Buffer actions: keep track of dump and delete actions on alarms, audit or trends buffers.

All changes to the selected resources are logged to the audit buffer with the timestamp, username that performed the operation and some additional information concerning the modified resource (e.g. new value and previous value for tags).

Furthermore, the LogMessage macro gives the possibility to developer to decide to keep track of some events (e.g. when a button is pressed, when a page is activated, etc.) into the audit trail.

13.2 Configuration guidelines

Open your project with JMobile Studio.
Audit trail logging is disabled by default. To enable it:

*Path: **ProjectView**> **Security** > double-click **AuditTrail**> flag the **Enable Audit Trail** checkbox (disabled by default)*

From the main tabs (Tags, Alarms, Recipes and Miscellaneous) of the Audit trail Editor you can switch between the list views of the available resources.
In the Miscellaneous tab, by default, all resources that can be tracked have tracking disabled, except for User login details, which is already enabled instead.
All resources in the Miscellaneous tab must have the Audit checkbox flagged:

*Path: **ProjectView**> **Security** > double-click **AuditTrail**> click **Miscellaneous** tab> click **+ All** button*

If you want to keep track of some events using the LogMessage macro, you must execute the System LogMessage action when the event is triggered, for example on press and on release of a button.
The System LogMessage action is linked to widgets in the Event section of the Property pane (Page Editor):

*Path: click on the widget that triggers the event> **Properties** pane> **Events**> click **+** at the desired event> a dialog appears> click **+** near Action List> select **LogMessage** under **System** entry in the **Action** tab> under **Action Properties***

*enter the name of the audit buffer where add the message (**Event**) and the message to add inside the audit buffer (**Message**)> click **Ok***

13.3 Test Procedure

Open your project with JMobile Studio and go to the page where to show audit logs:

*Path: **ProjectView**> **Pages**> open the page where to show audit logs*

Then add Audit view widget:

*Path: **View**> **Toolbars and Docking Windows**> **Widget Gallery**> **Audit Tables**> **Audit view***

Drag and drop the widget inside the page. Select the widget to open the properties dialog and configure them.
Download the project on HMI.
Login on the HMI
Play with JMobile and verify on your widget that all execute operations are recorded.

14 CR 2.9 – Audit storage capacity

14.1 Description of security capability

Through the "Events Buffer" page the application developer can configure the size of the audit buffers and activate the backup of the audit events when the buffer is full.
Audit trail records are stored using a circular buffer. This is to ensure that the device will not run out of memory.

14.2 Configuration guidelines

Open your project with JMobile Studio.
To configure the size of the audit files:

*Path: **ProjectView**> **Configuration** > **Events Buffer**> **Size** tab*

To activate the backup of the audit events when the buffer is full:

*Path: **ProjectView**> **Config** > **Events Buffer**> **Storage Device** tab*

Click the button: a dialog appears. Here you can configure the backup of the audit events.
Enable Save a copy when full option (by default it is disabled), so the HMI device will save a copy when the events buffer is full before it is overwritten by newer data.

14.3 Test Procedure

Open your project with JMobile Studio.
Configure the size of the audit files:

*Path: **ProjectView**> **Configuration** > **Events Buffer**> **Size** tab*

Configure the path to save the backup of the audit events when the buffer is full:

*Path: **ProjectView**> **Config** > **Events Buffer**> **Storage Device** tab> click the button> **Backup Archive***

Download the project and log in to the HMI.
“Play” with your project and when your buffer is full, logs will be saved in the previously configured path. Verify that it complies to the size configured.

15 CR 2.10 – Response to audit processing failures

15.1 Description of security capability

Audit records are events protected by a watchdog. In case of a crash, the watchdog protects them by rebooting the machine.

The audit records are stored within a pre-allocated storage capability.
Audit trail records are stored using a circular buffer. If the buffer gets full, old logs are replaced by new ones, so the latest audit is always logged.
There is an option to take a copy of audit to an external disk, when allocated capacity is full. So that all the data can be preserved.

15.2 Configuration guidelines

Open your project with JMobile Studio.
Watchdog is enabled by default. Make sure it really is:

*Path: **ProjectView**> double-click **Project properties**> **Properties** pane> **Runtime**> **Enable Watchdog**> must be set to **true***

See also CR 2. 9 – Audit storage capacity requirement configuration guidelines.

15.3 Test Procedure

To verify the functioning of the watchdog, you must trigger a serious event on the device to block it or modify the code that governs the timing.
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 JMobile process. The watchdog intervenes by restarting the panel.

See also CR 2. 9 – Audit storage capacity requirement test procedure.

16 CR 2.11 – Timestamps

16.1 Description of security capability

All the information in the audit buffer is saved with the timestamp. Timestamp in audit is saved as UTC which can be converted to any format as user required.

16.2 Test Procedure

Open your project with JMobile Studio and go to the page where to show audit logs:

*Path: **ProjectView**> **Pages**> open the page where to show audit logs*

Then add Audit view widget:

Path: ***View*** *>* ***Toolbars and Docking Windows*** *>* ***Widget Gallery*** *>* ***Audit Tables*** *>* ***Audit view***

Drag and drop the widget inside the page. Select the widget to open the properties dialog and configure them.
Download the project on HMI.
Login on the HMI
Play with JMobile and verify on your widget the existence of timestamp

17 CR 3.1 – Communication integrity

17.1 Description of security capability

The protocols that ensure the integrity of transmitted information are:

- HTTPS
- FTPS
- OPC UA
- Siemens protocols

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.

18 CR 3.2 - EDR 3.2 – Protection from malicious code

18.1 Description of security capability

A project can be encrypted to secure intellectual property and not be readable or editable by unauthorized users.
The HMI device can be configured to accept only signed projects. The signature makes sure that only authorized users can update the JMobile HMI Runtime application. To configure the HMI device to accept only signed projects, an x.509 certificate is required to sign the projects.

Malicious code can still be introduced despite Secure Boot, project files encryption and project signature.
As documented for CR 2.4 - EDR 2.4 – Mobile code requirement, the code introduced or that can be introduced using the browser widget or PDF viewer must be verified, safe and reliable. This must be guaranteed by the system integrator.

18.2 Configuration guidelines

For project files encryption and project signature, here are the links to the JMobile Studio user manual:

- Project Signature
- Project Files Encryption

To prevent malicious code from being introduced using the browser widget or PDF viewer, refer to
CR 2.4 - EDR 2.4 – Mobile code requirement Configuration guidelines.

18.3 Test Procedure

- Project signature test:
  Sign the project following the steps documented in the JMobile Studio user manual (Project Signature).
  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.

- Project files encryption test:
  Encrypt the project following the steps documented in the JMobile Studio user manual (Project Files Encryption)

When the project is encrypted, every time you open the project on JMobile Studio you will be asked to enter the password.
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.

Refer to CR 2.4 - EDR 2.4 – Mobile code requirement for test procedure related to the mobile code.

19 CR 3.3 – Security functionality verification

19.1 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.

20 CR 3.6 – Deterministic output

20.1 Description of security capability

Generally this requirement is implemented by PLC controller. HMI side, watchdog reboots the system in case of freeze or crash of services taking back the device at initial status.

Other controls can be implemented at application level and in case of abnormal behavior, the application can be taken to a known state. For example, show a page that informs that the user is not authorized to access a particular resource he has requested.

20.2 Configuration guidelines

Open your project with JMobile Studio.
Watchdog is enabled by default. Make sure it really is:

Path: ***ProjectView****> double-click* ***Project properties****>* ***Properties*** *pane>* ***Runtime****>* ***Enable Watchdog****> must be set to* ***true***

20.3 Test Procedure

To verify the functioning of the watchdog, you must trigger a serious event on the device to block it or modify the code that governs the timing.
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 JMobile process. The watchdog intervenes by restarting the panel.

21 CR 4.1 – Information confidentiality

21.1 Description of security capability

At the project level, a guarantee of information protection is provided by the project files encryption and the project signature.

A project can be encrypted to secure intellectual property and not be readable or editable by unauthorized users.

The HMI device can be configured to accept only signed projects. The signature makes sure that only authorized users can update the JMobile HMI Runtime application. To configure the HMI device to accept only signed projects, an x.509 certificate is required to sign the projects.

Protocols such as HTTPs, FTPs, OPC-UA, Codesys PLC Handler and Siemens protocols ensure confidentiality of information.
All other protocols provided by JMobile do not support encryption, so if used they could compromise the confidentiality of information.

Finally, the system allows to restrict access to various widgets and operations by configuring users, user groups and assigning specific authorizations and permissions to each group.
This allows information to be protected from unauthorized access.

21.2 Configuration guidelines

Refer to CR 3.2 - EDR 3.2 – Protection from malicious code requirement for project signature and project files encryption.

Refer to CR 2.1 – Authorization enforcement requirement for configuring user group authorization and permissions.

21.3 Test Procedure

Refer to CR 3.2 - EDR 3.2 – Protection from malicious code requirement and CR 2.1 – Authorization enforcement requirement for test procedure.

22 CR 4.3 – Use of cryptography

22.1 Description of security capability

Encryption is required to protect confidentiality and integrity of the information. For each protocol indicated, devices use the following encryption algorithms. Their use is indicated by common standards.

Cryptography is used in these cases:

- 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
- Zip encryption: no authentication/encryption support
- Protocols encryption/signature
  - OPC-UA and Codesys protocols support encryption
  - All other protocols provided by JMobile do not support encryption, so it is recommended not to use them.
- FTPs

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

- User management module - user password encryption
  - Password are encrypted using *PBKDF2*, *PKCS5_PBKDF2_HMAC*
- JM Studio - Inside Manage target dialog and Project download dialog
  - Used in encrypt/decrypt panel BSP passwords and store in registry. OpenSSL EVP_aes_128_cbc() cypher is used
- Exor licencing (.xlic)
  - Exor licensing uses this algorithm from OpenSSL with EVP_sha256() cypher to encrypt the license data verified with a public key
- QFTP client in HMIstudio and runtime
  - accepted TLS versions: *1.2 or more*
  - supported ciphers and algorithms:
    EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
- Curl lib in HMI client to HMI server
  - accepted TLS versions: *1.2 or more*
  - supported ciphers and algorithms:
    EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
- Database
  - accepted TLS versions: *1.2 or more*
  - supported ciphers and algorithms:
    EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
- LDAP
  - accepted TLS versions: *1.2 or more*
  - supported ciphers and algorithms:
    EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH

22.2 Test Procedure

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.
Filter captured packets using the IP address of the panel.

To check the encryption algorithms supported by OPC-UA:

- Using the panel as an OPC-UA server, look for the packet that is called "Server Hello, Change Cipher Spec" and:
  - Check that the Transport Security Layer field contains a TLS version greater than 1.2
  - Check that the Transport Security Layer> TLSV1.x> Handshake Protocol> Cipher Suite field contains a valid encryption algorithm (e.g. TLS_AES_256_GCM_SHA384)

- Using the panel as an OPC-UA server client, look for the packet that is called "OpenSecureChannel" and:
  - Check that the OpcUa Binary Protocol section contains the SecurityPolicyUri (with a value different from http://opcfoundation.org(UA/SecurityPolicy#None)), SenderCertificate and ReceiverCertificateThumbprint fields.

23 CR 6.1 – Audit log accessibility

23.1 Description of security capability

Audit logs can be accessed on a read-only basis using the table audit widget.

23.2 Configuration guidelines

Open your project with JMobile Studio and go to the page where to show audit logs:

Path: ***ProjectView****>* ***Pages****> open the page where to show audit logs*

Then add Audit view widget:

Path: ***View****>* ***Toolbars and Docking Windows****>* ***Widget Gallery****>* ***Audit Tables****>* ***Audit view***

Drag and drop the widget inside the page. Select the widget to open the properties dialog and configure them.

23.3 Test Procedure

Log in to HMI and go to the page where the table audit widget is located. You should see audit records correctly.

24 CR 7.1 – Denial of service protection

24.1 Description of security capability

The system provides a mechanism to protect against brute force attacks. There is a limit to the number of consecutive invalid access attempts during a certain time period. After the number of bad passwords allowed has been exceeded, the system introduces a delay between access attempts.

24.2 Configuration guidelines

Open your project with JMobile Studio.
Login lock is disabled by default. To enable it, you must act by changing the user group settings:

Path: ***ProjectView****>* ***Security****> double-click* ***UserGroups*** *>* ***Authorization Settings*** *column*

Click the button: a dialog appears with a list of widgets and actions. Go to Miscellaneous tab and check Enable login lock on wrong passwords.
It is possible to define:

- Tries without lock: the number of incorrect passwords accepted before inserting a delay between passwords.
- Minimum/Maximum timeout: the initial delay and the maximum delay will not be further increased.

In this way the login lock feature is implemented for all users belonging to the group.
This operation must be done for all user groups.

24.3 Test Procedure

On HMI, enter username and a wrong password several times.
After reaching the limit of possible attempts, you have a message that says: “Error : Username or password is wrong. Login locked for a while”.
You can no longer attempt to access the system for a certain period of time.

25 CR 7.2 – Resource management

25.1 Description of security capability

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.

26 CR 7.3 – Control system backup

26.1 Description of security capability

The system allows you to backup to an external memory all the content of the HMI device, including:

- JMobile HMI Runtime
- HMI Application Project
- CODESYS Project

The backup copy can be used to restore the content of the HMI device at a later time or copy it to a new HMI device.

26.2 Configuration guidelines

The backup function automatically performs the following procedure:

27 Unloads the current project to unlock files in use.

28 Unload CODESYS service

29 Archives the content of the \QTHMI folder (containing JMobile HMI Runtime, projects, dynamic files such as recipes, alarms, trends and so on) to a .zip file (standard or encrypted).

30 Reset the HMI device (reloads the project).

To start the backup procedure:

31 In JMobile HMI Runtime right click to open the context menu.

32 Select **Backup:** the **Backup** dialog is displayed.

33 Select the path for storing the backup file.

Note: The backup process does not include files stored in USB and SD cards. Dynamic data such as recipes, trends, events stored in these devices will not be included in the backup.

33.1 Test Procedure

After configuring the backup settings as previously indicated, run it and check where it was done and whether it was created correctly in the indicated path.

34 CR 7.4 – Control system recovery and reconstitution

34.1 Description of security capability

Thanks to the ability to make backups, the system can be recovered and reconstituted to a known secure state after a disruption or failure.

34.2 Test Procedure

For the restore function, following these steps:
From the Context Menu on PC or device:

1. Click Update
2. Click Browse…
3. Select your backup file
4. Click Next

From system setting:

- make a backup as indicated above
- in the address bar, type https://IPaddress/machine/config to reach the device and press enter,
- Enter your username ,
- Enter the password and press enter on the keyboard or the “Proceed” button,
- on the left you will read the list of items relating to "System settings",
- click Management
- use the "Update" button to restore the contents of the Data and the Settings partitions.
- The Config OS mode is required. You will be prompted to restart into Config OS.
- Insert admin password and press confirm
- Once restarted, repeat the steps 5 and 6
- 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)
- Upload the backup and the MD5 file.

35 CR 7.5 – Emergency power

35.1 Description of security capability

OUT of SCOPE because there is no component level requirement associated with IEC 62443-3-3 SR 7.5.

36 CR 7.6 – Network and security configuration settings

36.1 Description of security capability

Network and security configurations are inherited from the BSP.
To configure network and security settings, refer to the documentation produced for BSP.

37 CR 7.7 – Least functionality

37.1 Description of security capability

It is possible to restrict access to various widgets and operations by configuring users, user groups and assigning specific authorizations and permissions to each group.

37.2 Configuration guidelines

Refer to CR 2.1 – Authorization enforcement requirement for configuring user group authorization and permissions.

37.3 Test Procedure

Refer to CR 2.1 – Unsuccessful login attempts requirement for test procedure.