IACS UR E27
"Cyber resilience of on-board systems and equipment".
Exor eX700 and eX700M Series.

INFORMATION SUPPORTING THE OWNER'S INCIDENT RESPONSE AND RECOVERY PLAN

History			
Rev	Date	Description	By
0.1	Jul 2024	Draft	Giuseppe Marras
1.0	Aug 2024	Final Review and update	Fausto Gastaldin – Giuseppe Marras

Reference		
Cross Reference	Filename	Description
[1]		

General Contents

The document shall also include necessary user manuals and guidance enabling the owner to establish incident response/recovery plans and verify intended operation of security functions (SR 3.3).
It shall include procedures or instructions allowing the user to accomplish the following:

1. Local independent control (see UR E26 sec. 4.4.2)
2. Network isolation (see UR E26 sec. 4.4.3)
3. Forensics by use of audit records (see UR E27 sec. 4.1 item no.13)
4. Deterministic output (see UR E26 sec. 4.4.4 and UR E27 sec. 4.1 item no. 20)
5. Backup (see UR E27 sec. 4.1 item no. 26)
6. Restore (see UR E27 sec. 4.1 item no. 27)
7. Controlled shutdown, reset, roll-back and restart (see UR E26 sec. 4.5.3)

Note:

This document refers only to the points 3, 4, 5 e 6 of the general content because they are typical of a device supplier.

1. Forensics by use of audit records:

When, for any reason, it is necessary to perform a log analysis, proceed as follows

BSP

From your PC's browser or directly on the device:

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 Logs
6. click "Get" button to download the log files
7. open the file tar.gz.

JMobile

The Audit trail is a chronological sequence of audit records. Each record contains information on the actions executed and the user that performed them.

This function provides process tracking and user identification with timestamp for events.

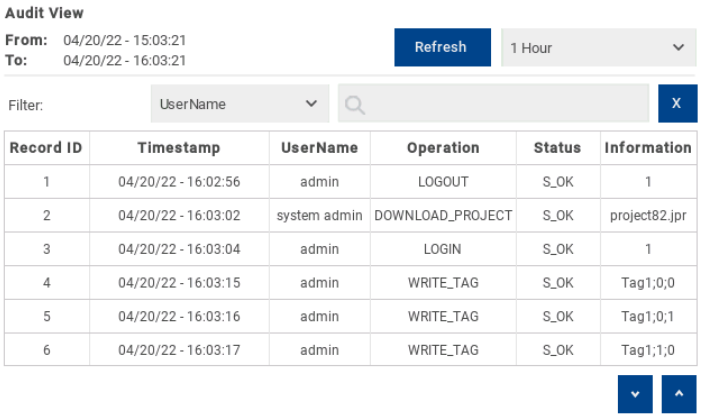
Backup Archive
If Save a copy when full option is enabled, the HMI device will save a copy when the events buffer is full before it is overwritten by newer data.

Parameter	Description
Path	Where events buffer data will be copied. The below wild cards are supported • %n = Events buffer name • %y = Year • %M = Month • %d = Day • %h = Hour • %m = Minutes • %s = Seconds
Time Spec	Timestamp of events • Local Use the time of the HMI device where the project is running • Global Use global time (GMT)
Date Format	Time and Date format. Placeholders can be used (see "Time and Date placeholders")
Separate Date and Time	When "true", the date and the time are placed into two different fields
Cleanup after backup	When "true", the event buffer is clean up after completing the backup. When "false", the older events are removed when new events are incoming (circular buffer)
Language	Language to use
Signed	When "true", the additional file with the signature is added (see "Signed CSV files")

Table audit widget

Path: Widget Gallery> Basic> Audit Tables

Display contents of the audit trail inside a widget



Record ID	Timestamp	UserName	Operation	Status	Information
1	04/20/22 - 16:02:56	admin	LOGOUT	S_OK	1
2	04/20/22 - 16:03:02	system admin	DOWNLOAD_PROJECT	S_OK	project82.jpr
3	04/20/22 - 16:03:04	admin	LOGIN	S_OK	1
4	04/20/22 - 16:03:15	admin	WRITE_TAG	S_OK	Tag1;0;0
5	04/20/22 - 16:03:16	admin	WRITE_TAG	S_OK	Tag1;0;1
6	04/20/22 - 16:03:17	admin	WRITE_TAG	S_OK	Tag1;1;0

Buttons:

- REFRESH
  Retrieve trend data from internal buffer and refresh table view

- BACKWARD/FORWARD
  Move the display window forward or backward as specified in the duration parameter

Filter:
Use the combo box to select the column where search for and the text filed on the right to enter the string to search to.

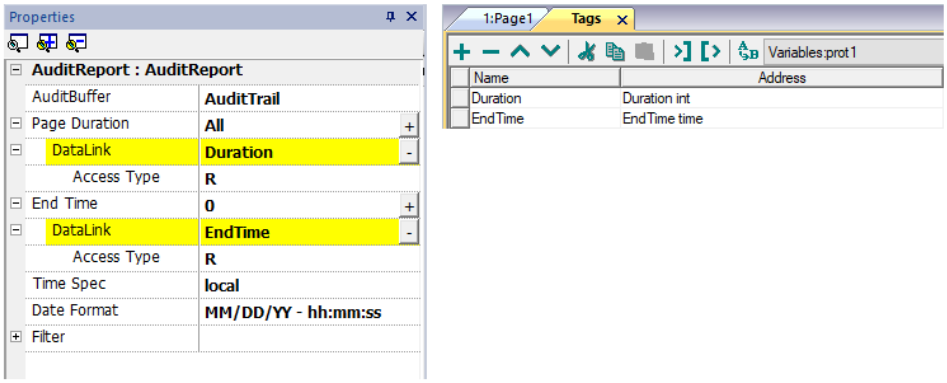
Parameter	Description
AuditBuffer	Event Buffer from which the event list is retrieved (see "Events Buffer")
Heading	Heading label
Default Duration	Initial value of time window to show
End Time	Upper limit of the time displayed in the table in units of 1 second
Time Spec	Time format: • **Local** = show the time values of the HMI device. • **Global** = show the time values using UTC format.
Date Format	Select the Date and Time format
Filter List	Labels to show in filter column selection
Timestamp Sorting	Set how to sort the time stamp data • Ascending • Descending
Table Layout	Defines the characteristics of the scroll bar and allows to remove the header of the table

Printing audit table
An audit table widget without buttons can be found and used from the print report gallery. The table can be drawn and enlarged to fill the entire page. If the number of lines to printed is greater of one page, the audit table will be printed using additional pages.

Using the "attach to tag" feature is possible to use tags to define some properties of the historical trend to print at runtime:

- Page Duration
- End Time

"Page Duration" with "End Time" define the piece of the audit buffer to print.



Exporting audit trail as .csv files

Data recorded inside the audit trail can be exported inside a csv file using the SaveEventArchive action. See "SaveEventArchive" for details.

File structure

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2	**Record ID**	**Date**	**Time**	**User ID**	**Interface**	**Action**	**Status**	**Data**				
3	1	27/03/2018	14:22:06	SYSTEM_IDAL	SYSTEM_IDAL	SYSTEM_POWERON	S_OK					
4	2	27/03/2018	14:22:06	admin	LOCAL	LOGIN	S_OK	1				
5	3	27/03/2018	14:22:08	admin	LOCAL	WRITE_TAG	S_OK	Tag1	0	1		
6	4	27/03/2018	14:22:09	admin	LOCAL	WRITE_TAG	S_OK	Tag2	0	1		
7	5	27/03/2018	14:22:26	admin	LOCAL	WRITE_TAG	S_OK	Tag2	1	5	This is a test	
8	6	27/03/2018	14:22:50	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag1	1	1		
9	7	27/03/2018	14:22:50	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag2	5	3		
10	8	27/03/2018	14:22:50	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag3	0	5		
11	9	27/03/2018	14:22:50	admin	LOCAL	DOWNLOAD_RECIPE	S_OK	Recipe0	set-00			
12	10	27/03/2018	14:22:54	admin	LOCAL	ACK_ALARM	S_OK	Alarm2				
13	11	27/03/2018	14:22:58	admin	LOCAL	RESET_ALARM	E_FAIL	Alarm2				
14	12	27/03/2018	14:23:02	admin	LOCAL	DUMP_AUDIT_BUFFER	S_NEEDNOT_NOTIFY	AuditTrail				
15												
16												
17	**Record ID**	**Date**	**Time**	**User ID**	**Interface**	**Action**	**Status**	**Data**				
18	13	27/03/2018	14:23:24	admin	LOCAL	DELETE_AUDIT_BUFFER	S_OK	AuditTrail				
19	14	27/03/2018	14:23:26	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag1	1	2		
20	15	27/03/2018	14:23:26	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag2	3	4		
21	16	27/03/2018	14:23:26	SYSTEM_IDAL	SYSTEM_IDAL	RECIPE_WRITE_TAG	S_OK	Tag3	5	6		
22	17	27/03/2018	14:23:26	admin	LOCAL	DOWNLOAD_RECIPE	S_OK	Recipe0	set-01			
23	18	27/03/2018	14:23:27	user1	CGI	LOGIN	S_OK	192.168.49.242				
24	19	27/03/2018	14:23:37	user1	CGI	WRITE_TAG	S_OK	Tag1	6	55		
25	20	27/03/2018	14:24:28	admin	LOCAL	DUMP_AUDIT_BUFFER	S_NEEDNOT_NOTIFY	AuditTrail				
26												

Exported data file has the following content	
RecordID	Each record is stored with a progressive number which will give the possibility to easily identify missing records or confirm that they are not lost. Note that the progressive number is not reset to zero when the buffer is deleted.
Date, Time	Event time stamp. Time can be configured as local or global from the dump action.
User ID	User that perform the operation
Interface	LOCAL: when the action is performed in the HMI device CGI: when the action is performed by a remote client. SYSTEM_IDAL: when the action is performed from the JMobile HMI Runtime application
Action	Action executed.
Status	Result of the executed action • S_OK Action executed correctly • E_FAIL Action non executed • S_NEEDNOT_NOTIFY Action triggered (will be executed asynchronously)
Information	Additional info related with the executed action.

2. Deterministic output.

This requirement specifies that the device 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:
- Unpowered state,
- Last-known value, or
- Fixed value

For Exor's device the component that allows you to bring the device back to a "known" operating state is the watchdog. A watchdog timer is an electronic or software timer that is used to detect and recover from device malfunctions. Watchdog timers are widely used in devices to facilitate automatic correction of temporary hardware faults, and to prevent errant or malevolent software from disrupting system operation.
During normal operation, the device regularly restarts the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the device fails to restart the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective actions. The corrective actions typically include placing the device and associated hardware in a safe state and invoking a device reboot.

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. OOM Killer also intervenes automatically.

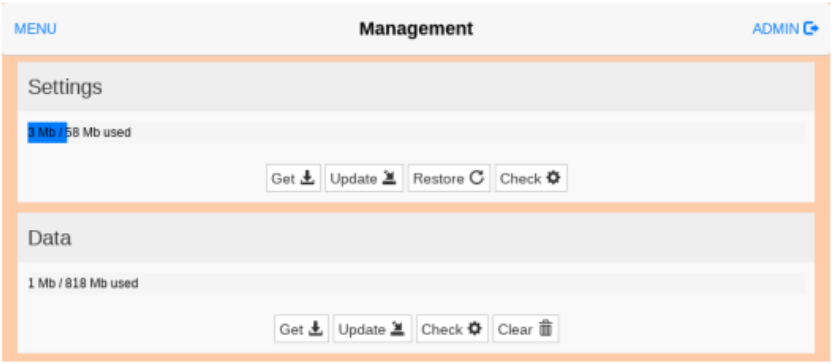
3. Backup and Restore

Exor devices provide the ability to perform backup and restore in the following way:

BSP and JMobile

To backup or restore all the installed applications with their settings, you must open the System Settings interface in Config OS mode using the tap-tap procedure or on your PC.
Then log as admin and select the "Management" option. From this page, you can use the "Get" button to backup inside an external memory (e.g. USB key) the contents of the Data and the Settings partitions. Use instead the "Update" button to restore the contents from a previous backup.

Management command is available only when logged as admin.



Data Partition
The data partition contains the applications and they settings
Settings Partition
The settings partition contains the settings of your device (this means the configuration parameters entered using the System Settings interface)

When you update the System Settings from a backup you must be sure that the backup was executed from a device with the same BSP version (Main OS).

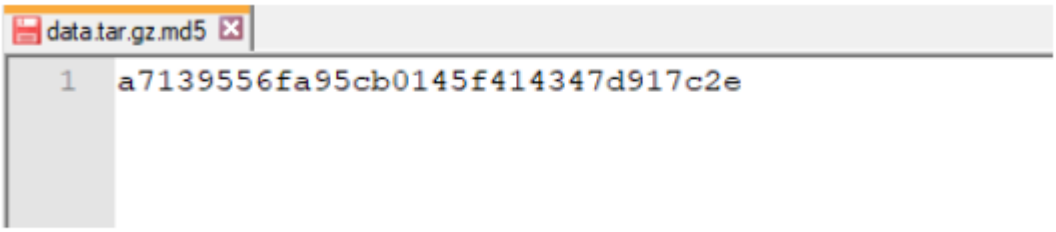
The MD5 file
The "Get" command will provide only a file with the contents of the partition (e.g. data.tar.gz), but if you want to restore the same file, using the "Update" command, you must provide even an MD5 checksum file.
The MD5 checksum file must have the same name as the files that you want to load with the .md5 suffix as e.g.:

- data.tar.gz
- data.tar.gz.md5

On the Internet, it is easy to find various tools that calculate the MD5 checksum of a file. On Windows 10 it is also possible to use the "CertUtil" utility on the command line, e.g.

```
CertUtil -hashfile data.tar.gz MD5 > data.tar.gz.md5
```

The MD5 checksum file must have only one line. If the utility that calculates the checkum generates a file with multiple lines, the additional lines must be deleted.



Only JMobile

Backup/restore of Runtime and project

You can backup all the content of the HMI device, including

- JMobile HMI Runtime
- HMI Application Project
- CODESYS Project

to an external memory. This 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.

The backup function is available only if enabled for the logged user.

Backup function
The backup function automatically performs the following procedure:

- Unloads the current project to unlock files in use.
- Unload CODESYS service
- Archives the folder (containing JMobile HMI Runtime, projects, dynamic files such as recipes, alarms, trends and so on) to a .zip file (standard or encrypted).
- Reset the HMI device (reloads the project).

To start the backup procedure:
1. In JMobile HMI Runtime right click to open the context menu.
2. Select Backup: the Backup dialog is displayed.
3. Select the path for storing the backup file.

Restore function
Restore the backup package can be perform on HMI device
- from the Context Menu (see "Update package" for details of the user manual)
- or from the System Settings (see previous paragraph).