“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Version #	Date of Publication	Internal reference	Description
SV1.7 IR25	**02/2024**	PEP1087587R	Fixed the issue that some non-extended chars not compatibles with web password
		PEP1060887R	**Security Updates** The following third-party components have been updated to address cybersecurity vulnerabilities: - VxWorks DHCP client and CVE-2021-29998 - VxWorks DHCP sever and CVE-2021-29999

Cybersecurity Remediation & Mitigation

Schneider Electric is aware of multiple ethernet services vulnerabilities, including **RTU protocols (DNP3/IEC60870), SNMP, FTP, HTTP and Modbus**. The impact of a successful exploitation of this vulnerability may result in a **denial of service, privilege escalation, access control bypass, or other unauthorized access.**

Customers should immediately apply the following mitigations to reduce the risk of exploitation.

- Enable IP ACL. For information, refer to the User Manual section "The Messaging Configuration Tab"
- Disable FTP/HTTP if not necessary to use. For information, refer to the User Manual section "Configuration Screen", "Module Configuration Screen"
- Changing default password of FTP from embedded web page, refer to the User Manual section "FTP Security Page"
- Changing default username/password of HTTP access from embedded web page, refer to User Manual section "Security" "Security Page"
- Reduce the “Offline Poll Period” of RTU protocols to avoid ARP grammar issues. Refer to the User Manual section “Channel Parameters”
- Use controllers and all associated modules only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.
- Use firewalls/VPNs to protect and separate the control system network from other networks to avoid communication robustness issues.

“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric’s security notification service here:

https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

"BMX NOR 0200H" FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Version #	Date of Publication	Internal reference	Description
SV1.7 IR24	**08/2022**	PEP1007881R	**New Features:** 1. Read-only mode added as IEC104 Server 2. Quality variable mapped to M_IT DDT as IEC104 Server
		PEP1017882R	Fixed the issue of wrong responding with ActCon & ActTerm by C_SC_Command when module is configured as IEC60870-5-101/IEC60870-5-104 Slave
		PEP0635793R	**Cybersecurity:** Fixed a DoS attack vulnerability *Reference CVE-2021-22788 for further detail*
		PEP0638539R	**Cybersecurity:** Fixed an insufficient input validation vulnerability *Reference CVE-2021-22787 for further detail*
		PEP0655042R	**Cybersecurity:** Fixed a weak hashing algorithm vulnerability *Reference CVE-2018-7242, CVE-2010-2967, CVE-2011-4859 for further detail*
		PEP0675259R	**Cybersecurity:** Fixed a BadAlloc multiple RTOS vulnerabilities *Reference CVE-2020-35198, CVE-2020-28895 for further detail*
		PEP0675675R	**Cybersecurity:** Fixed HTTP Server Buffer overflow & Out of Bounds read *Reference CVE-2022-0222 for further detail*
		PEP0678281R	**Cybersecurity:** Fixed an improper privilege management vulnerability *Reference CVE-2020-7562, CVE-2020-7564 for further detail*

"BMX NOR 0200H" FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

Version #	Date of Publication	Internal reference	Description
SV1.7 IR23	**07/2021**	PEP0536472R	**Enhancement:** Support redundant channel functionality of IEC60870-5-104 when module is configured as IEC60870-5-104 server. Maximum 2 redundant groups can be configured from 4 channels. Active channel can be controlled by either module itself or external client.
		PEP0621793R	Fixed the issue of responding immediately with ActCon and Act Term without considering the duration of the pulse when module is configured as IEC60870-5-101 Slave
		PEP0624883R	**Enhancement:** Support to exclude value "0" as BO Pulse_Trip commands in DNP3 Client/Master channel parameters. This enhancement facilitated some applications to avoid mis-operation when control value is initialed to "0".
		PEP0656329R	Fixed the issue for wrong C_SE_NC command data type is transferred to CPU when configured CMD Queue Size is bigger than 1.
		PEP0626292R	Cybersecurity improvement *Reference CVE-2020-7540 for further detail*
		PEP0634012R	Cybersecurity improvement *Reference CVE-2020-7540 for further detail*
		PEP0635012R	Cybersecurity improvement *Reference CVE-2020-7541 for further detail*

“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

		PEP0635013R	Cybersecurity improvement *Reference CVE-2020-7539 for further detail*
		PEP0636120R	Cybersecurity improvement *Reference CVE-2015-6461 for further detail*
		PEP0636150R	Cybersecurity improvement *Reference CVE-2020-7562 for further detail*
		PEP0639932R	Cybersecurity improvement *Reference CVE-2021-22749 for further detail*
		PEP0635773R	Cybersecurity improvement *Reference CVE-2021-22785 for further detail*
		PEP0659902R	Cybersecurity improvement *Reference CVE-2020-7564 for further detail*
		PEP0643713R	*Cybersecurity improvement* *Reference CVE-2020-7534 for further detail*
		PEP0558190R	Cybersecurity improvement
		PEP0558191R	Cybersecurity improvement
		NA	Fixed the defect that cross check for CPU register between I-frame counter and data point is not worked

"BMX NOR 0200H" FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

<table>
<tr><td></td><td></td><td>NA</td><td>Fixed the defect on I-Frame configuration is set to default when modifying channel's ip address</td></tr>
<tr><td></td><td></td><td>PEP0658953R</td><td><b>Enhancement:</b> New feature to prevent downgrading firmware to SV1.7 IR<23 with PV >=18 (see below notice)

<b><i>NOTICE</i></b>

<b>FIRMWARE UPGRADE FAILURE</b>
Previous firmware version (SV<"1.7 IR23") is disallowed to download to BMXNOR0200H with PV version >= 18 because of new hardware components. If a firmware downgrade was performed in this case, Unity Loader will show "Flash upgrade error" during firmware reload. BMXNOR0200H is not able to complete firmware downgrade at last and need to reload SV>="1.7 IR23" for recovery from application failure (due to the Web page in SD card already been overwritten by old version, inconsistent firmware and web page version will lead module unexpected behaviors).

In brief, "SV1.7 IR23" is the minimum firmware requirement for BMXNOR0200H PV18 (and later) modules which delivered from Schneider Electric manufacture.

Compatibility of BMXNOR0200H is shown as below:
<table>
<tr><th>Firmware version (SV)/Web Page version
Hardware Version (PV)</th><th>&lt;="1.7 IR22"</th><th>&gt;="1.7 IR23"</th></tr>
<tr><td>&lt;= PV17</td><td>✓</td><td>✓</td></tr>
<tr><td>&gt;= PV18</td><td>✗</td><td>✓</td></tr>
</table>
<b>Failure to follow these instructions can result in equipment damage.</b></td></tr>
</table>

“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

SV1.7 IR22	**01/2021**	PEP0568517R	**Issue Description:** Fixed BMXNOR SNMP – Trust Boundary Violation Cybersecurity issue. *Reference CVE-2020-7536 for further detail*
		PEP0602666R	**Enhancement:** Add I-frame counter value for each IEC60870 channel diagnostic.
SV1.7 IR21	**04/2020**	PEP0567554R	**Issue Description:** When BMXNOR is configured as RTU protocol server/slave, Client/Master (e.g. SCADA) consecutively triggered multiple pulse mode commands (e.g. C_DC) with high frequency to BMXNOR, then module may loss ip/mac during running. Address information (IP address and Mac address) in on-line diagnostic tab will show "zero" and module communication hasn't response. **Recovery:** Power cycle the failed module **Workaround:** None
SV1.7 IR20	**10/2019**	PEP0539866R	**Issue Description:** For a Read Class 0/1/2/3 request from SCADA, at communication reconnection or periodic integrity check, NOR is sending the DNP3 points mapped in the M580. If the current value of PLC register type INT is linked to an Analog point Input 16 bits, with a value < 0, NOR respond with an Over-range flag and provide the default value 32767. **Recovery:** None **Workaround:** None
		PEP0531288R	**Issue Description:** When the same XML file is imported multiple times, the message "File Import Fail" or "Import not success" gets returned. This results in the FTP session freezing.

			Recovery: Power cycle this NOR module **Workaround:** None
		PEP0546313R	**Issue Description:** This issue is DNP3 AO value inconsistency upon Integrity Data Poll in virtual clients (multiple clients). To change the analog output value by unity application, read back data throught Integrity data poll from virtual clients is not updated (no issue on master clients). **Recovery:** None **Workaround:** None
SV1.7 IR19	**03/2019**	PEP0464548R	**Issue Description:** Issue is on DNP3 Analog Output when flag is changed and configured as "synch on demand" mode, the value via Integrate Poll is different with the value via event. For example, AO value is changed from 10 to 20 by DNP3 master, and flag is 1. Then user changed flag bit to 0. User will observe point event value is 10 and flag is 0, while integrate Poll value is 20 and flag is 0. **Recovery:** None **Workaround:** Not using flag bit controled by programming in CPU
		PEP0433881R	**Issue Description:** Cyber security issue with the default FTP account. The default FTP user account cannot be deleted, and the password cannot be changed in the FTP Security web page. **Recovery:** None **Workaround:** None
		UNITY00089977	**Issue Description:** Analog out flag bit (configured by ARRAY format) is not correct in case of synch on demand mode and NOR works as DNP3 server/slave. Only first flag bit associated with first value in ARRAY structure (check by event or intergrate Poll) is correct, all other points flag bits in ARRAY are not correct.

"BMX NOR 0200H" FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

			Recovery: None **Workaround:** Not use ARRAY format for Analog Out point in this case
		PEP0488266R	**Enhancement:** customer's identifiers "230"(without a timestamp) and "231"(with a timestamp) of standard IEC 60870-5-104. Custom ID 230/231 are both for 64-bit points for double floating type. RTU shall repeat 64-bit points 4 bytes data from remote slave side to SCADA side.
SV1.7 IR18	**11/2018**	PEP0474774R	**Issue Description:** Fixed a defect that occurs when a BMXNOR0200H that is connected to a PSTN modem using the serial connection. The 'Dial In' operation could fail after the first try. When this occurs, the Modem is unable to get a response from the BMXNOR0200H. If the user resets the module, the operation will work for one time and fail again. **Recovery:** Click "Reset Communication" on Web page or power cycle the BMXNOR0200H **Workaround:** None
SV1.7 IR17	**08/2018**	PEP0434896R	**Issue Description:** Fixed a defect about DNP3 Server channel swaps when Ethernet cable is disconnected and reconnected. When customers configure multiple DNP3 Server channels (with IP address configured for each channel), sometimes the channel will be swapped when the cable for one of servers is disconnected and reconnected. Example - Assuming IP address A is configured on Channel 0 for SCADA A, IP Address B is configured on Channel 1. When ethernet cable of A is disconnected and reconnected, customer will observe SCADA A will connect to Channel 1. There is no impact on communication even channel swapped after cable reconnected. **Recovery:** Cold restart BMXNOR0200H module **Workaround:** None
		NA	Add C_SE_NB and C_SE_NC multi-request function to optimize communications

“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

SV1.7 IR15B	**04/2017**	PEP0347378R	Add Unsol Class disable/enable to web page.
		PEP0344247R	Add option to enable the sending of time setting on BusX
		PEP0336968R	Update timestamp for all objects no matter the value changes or not
		PEP0336082R	Fixed a defect about synchronize time to M340 CPU
		PEP0331224R	synchronize M580 CPU RTC with NOR module
		PEP0326657R	Improve DHCP behavior
		PEP0275075R	Add Quality bit for all routing points in DNP
		PEP0252543R	Fixed the defect on GPRS reconnection
SV1.7 IR10	**03/2016**	NA	Fixed an issue for manufacturing test of RTU V1.7
		PEP0127382R	Updated user manual on transition mode description
		PEP0127402R	Event configurable point by point on IEC protocol
		PEP0130226R PEP0213084R	Support reading the binary and analog outputs status on DNP3
		PEP0190283R	Modify website description on event backup
		PEP0213024R	Fix a defect of time display on webpage
		PEP0213044R	Support 16-bit mapping for %SW

“BMX NOR 0200H” FIRMWARE HISTORY

See "Unity Loader - A SoCollaborative Software User Manual" for firmware upgrading procedure

Note: Our firmware is continuously reviewed and updated in order to maintain the highest level of quality of our products. Schneider Electric recommends all customers to have their installation up to date with the newest firmware version to protect their infrastructures against cybersecurity threats and experience the best quality. For further information please visit the Schneider Electric Cybersecurity Support Portal:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

		PEP0216350R	Limit DNP client channels to 32
		PEP0220248R	Enhancement on managing the Modem retry times
		PEP0242596R	Fix defect on sending Email via GPRS if Eth cable not connect
		PEP0246582R PEP0310459R	Cyber security improvement
		PEP0251699R	Allow 16bit DNP3 analog mapping
		PEP0266093R	fix defect on SNMP
		PEP0272754R	Add Quality bit for all routing points for IEC
		PEP0272815R PEP0276331R PEP0293568R	Fix defect on time zone
		PEP0273545R	Add NOR module quality bit according to PLC status
		PEP0278973R	Enhancement on outputs control, only the health outputs can be controlled
		PEP0280504R	Improve local Freeze time precision
		PEP0281933R	Update rack viewer with new modules
		PEP0285781R	Improve GSM initialization command
		PEP0287964R	Improvement on IP address acquisition

		PEP0288871R	enhance the importing of .xml file with long address
		PEP0289651R	Fix defect of time stamp display in data log file
		PEP0297480R PEP0311088R	Improve the data exchange between CPU and NOR module
		PEP0307177R	Fix a webpage defect on Unloc Array size limitation
		PEP0308646R	TCP reconnection enhancement at DNP3 client
		PEP0319301R	Remove the Debug agent port
		PEP0321336R	Optimize the configuration for multiple channels
SV1.6 IR4	**7/2013**	Original Release	