



From
BT-VS/MKP

Product Management

Nuremberg
12.01.2023

Release Letter

Products:	<i>H.264/H.265 Firmware for CPP14.1 HD/UHD/MP cameras</i>
Version:	<i>8.71.0066</i>

— This letter contains latest information about the above-mentioned firmware version.

1 General

This firmware release is a feature release based on FW 8.30.0082.
It is an upgrade for CPP14.1 based cameras only.

Changes since last release are marked in [blue](#).

From
BT-VS/MKP

Product Management

Nuremberg

12.01.2023

2 Applicable products:

- FLEXIDOME multi 7000i
- FLEXIDOME multi 7000i IR



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

3 Important notes:

3.1 *Two-factor authenticated firmware signature*

The security of the signature of the firmware file has been strengthened by using a two-factor authentication process for signing the final released firmware file.

The new signature protects from non-released versions being installed in production systems. As a result, pre-release (beta) versions, required sometimes in projects, need to have a special license installed prior to the firmware update. Requests for pre-release versions need to be handled via tech support tickets in order to allow tracking and require a concession signed by the customer.

3.2 *“Originally manufactured” certificate*

All cameras are prepared to receive a unique Bosch certificate during production, assigned and enrolled by Escript LRA. These certificates prove that every device is an original Bosch-manufactured and untampered unit.

Escript is a Bosch-owned company, providing the Bosch certificate authority (CA).

Enrollment of the certificates in production is asynchronous to this firmware release.

3.3 *Secure Element (TPM)*

All CPP14 devices incorporate a new secure crypto-microcontroller, which we call our Secure Element.

“A Secure Element is a tamper-resistant platform capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities.”¹ In this specific case the requirements are defined in the Trusted Platform Module library specification defined by the Trusted Computing Group (TCG). As the Secure Element supports the main functionalities specified by TCG, the ones needed for an IoT device, it is often referred to as a “TPM”.

Due to security reasons, the firmware or functionality of the secure crypto-microcontroller cannot be altered in the field.

Thus, not all new security features become available on devices with older secure crypto-microcontroller hardware or firmware revisions.

3.4 *Secure Boot Protection*

All CPP14 devices are shipped with secure boot enabled, protecting the device from execution of unauthorized code.

Even in the case that an attacker could circumvent all other security barriers, any malicious code would never become active due to secure boot hindering the camera to start with unauthorized code.

¹ <https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf>, page 1

From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

3.5 Open-Source Software

Bosch Security Systems is an advocate of integrating open-source software into its products. The use of open-source software is noted in the *Service* menu on the *System Overview* page of every camera's web interface. For general information regarding open-source software in Bosch Security Systems products, please visit <http://www.boschsecurity.com/oss>.

- This software is based in part on the work of the Independent JPEG Group.
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

4 New Features

- Highly reliable SD card recording with life cycle monitoring
Industrial SD cards which provide wear level data can be monitored for their health and expected lifetime, providing much more reliable SD card recording.
Three vendors have been tested and qualified:
 - Micron
 - Sony
 - Western Digital (SanDisk)Due to the high dynamic in the Industrial SD card market, no direct reference to the models can be given.
Therefore, Bosch has selected specific WD models and provides them as accessory:
 - MSD-064G, MSD-128G, MSD-256G, SD-064G, SD-128G, SD-256G
- Genetec Stratocast support has been re-enabled with the same feature set as known from former platforms.
- Dynamically colored privacy masks, depending on surrounding video added. This can be used to not distract the operator due to intense color, e. g. white privacy mask in night scene.
- A stronger hashing algorithm, SHA384, is supported for HTTPS and network authentication 802.1x usages with RSA key certificates.
- The network parameter 'hostname' now remains in the configuration during factory default sequence due to application variant switching.
- Support of up to 4096 bit RSA key length in the Secure Element. This allows the creation of Certificate Signing Requests with up to 4096 bit RSA keys, and securing private data with hardware-protected 4096 bit RSA encryption and signature keys.
- Certificates with key length of 3072 bit and 4096 bit, using hashing algorithm of up to SHA256, can be used for HTTPS, EAP-TLS and user authentication usages.
- Network authentication 802.1x with EAP-MD5 and EAP-TLS is now supported.
- More streaming resolutions were added on streams 2 and 3.
- Support of ONVIF Profile M, including MQTT event forwarding.
- New Western Digital industrial SD cards with lifespan monitoring are supported.
- SNMP has been added, supporting v1 and v3, both including traps.
RCP+ integration is widely done to create similar support as of earlier platforms.
New MIB file is available and distributed with the firmware package.
- IR intensity level can be independently configured for each of the center and the four surrounding regions.
- Privacy masks can be enabled and disabled via a single switch command.
- For backward compatibility with legacy clients, applicable where alternative measures are put in place, the check on the HTTP referrer, an improvement to reduce the vulnerability for Cross Site Request Forgery (CSRF) attacks, can be disabled via the user interface.



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

- TLS 1.3 is supported, including the possibility to set the minimum TLS version.

5 Changes

- An issue is fixed where necessary network settings were set to default on application variant switching. This includes the hostname setting as well as the Remote Portal credentials.
- An issue is fixed where a profile name change did not appear immediately after pushing 'Set' button in the non-recording profile dropdown list, only after profile toggle.
- An issue is fixed where audio format could not be changed in browser after recording stopped, only after refreshing or re-opening the browser, or rebooting the camera.
- An issue is fixed with an ONVIF profile not responding with metadata for a specific line if configured for metadata only.
- An issue is fixed where JPEGs were corrupt when posted to FTP using TLS.
- An issue is fixed where an alarm output did not follow the day/night switch.
- An issue is fixed where the SNMP trap community name could not be changed.
- An issue with certain VCA events erroneously reporting 'signal loss' via ONVIF is fixed.
- An issue is fixed where the hostname was not transferred to DHCP/DNS on Windows 2019 Server.
- Description and explanation were improved in web browser interface on using country code instead of country name in Certificate Signing Requests.
- An issue is fixed where the EAP authorization was locked on PEAP, if included in the negotiation chain, but did not continue to EAP-TLS.
- The name of the menu 'IR Illumination' has changed to 'Illumination' only to prepare for white light illumination in future.
- ICMP redirects are now disabled by default.
- Security improvements require the minimum firmware to be set to 8.71 with this firmware to avoid firmware downgrade which would circumvent the security improvements.
- Due to higher security requirements, global licenses now need new license keys.
Note: These licenses can only be cleared via our repair services.
- Internal storage can be disabled and hidden for certain LATAM countries.
 - 12-01.65.01-4E2A8B15-3FE4DA2E-94234DB9-09F2F9F8-2E53B935
- The microphone can be permanently blocked to allow use of the cameras in countries where audio input is legally not permitted.
 - 12-01.63.01-380AAC7E-B71E0D3D-6ADCC50C-6F296E08-F3AFBB71
- Since increased security restrictions in browsers do not allow to use external company and device logo images, these non-functional controls were removed.
- An issue with changing image settings in menus 'Color', 'ALC' and 'Enhance' not breaking software sealing is fixed.



From
BT-VS/MKP

Product Management

Nuremberg

12.01.2023

6 System Requirements

For configuration purposes:

- Bosch Project Assistant 2.0.1 or higher
- [Bosch Configuration Manager 7.61 or higher](#)
- Web Browsers:
 - Google Chrome
 - Microsoft Edge (chromium based)
 - Mozilla Firefox

For operation purposes:

- Bosch Video Security app 3.2.1 or higher
- Bosch Video Security Client 3.2.2 or higher
- Bosch Video Management System 11.0 or higher
- Bosch Video Management System Viewer 11.0 or higher



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

7 Restrictions; Known Issues

User Interface

- If UAC is set to default in Windows 7, no snapshot or recording via LIVEPAGE is possible.
- Video and audio may be asynchronous during replay via Web page.
- In Firefox, no audio is audible on the Audio Settings page.
- Opera mini for mobile devices cannot work in Intranets because it gets all pages through an opera proxy on the Internet. If there is no Internet connection no content is provided.
- When changing GUI language, the browser cache may have to be deleted and the web browser be reloaded before the language will be selected correctly.
- Google Chrome requires a plug-in for displaying TIFF images to properly show the reference image.
- Fluent decoding of buffered .mp4 video from camera is strongly dependent on the browser. Jerky video may occur, e. g. with Mozilla Firefox 52.0, which is not a camera malfunction.
- Shutter time values in preview window might slightly deviate from rounded values selectable from dropdown menu.
- Privacy masks and other orientation-related parameters must be checked and eventually re-assigned after rotating a camera.
- On-screen display stamping
 - Font size minimum is ensured for lower resolutions if per mill value would be too small.
 - Font size is automatically limited when maximum display stamping capabilities are reached though values may indicate differently. Limitation is evenly distributed over all defined stamping sections.
- A defective SD card may show 'device ok' status while being unusable. Check recording status for high level error description.
- Microsoft Edge may request re-entering the login credentials multiple times after reactivating a sleeping tab.
- Stream limit settings change is directly executed without requiring the Set button.
- TLS 1.3 is not yet supported by Configuration Manager, though it allows this setting. Once minimum TLS version is set to 1.3, Configuration Manager will be locked out.
- When sensor modes are switched, e. g. from 5MP to 3.8 MP, resolutions in automatically generated scripts are not automatically updated, resulting in unsupported resolutions displayed for alarm e-mails. The images will be created with the resolution closest to the one in the script to keep alarm e-mails functional. As soon as a proper resolution is selected, the unsupported resolution disappears from the drop-down box.
- [Video may appear stuttering with Firefox 108.02, use different browser version or brand.](#)
- [With using 25 fps and 30 fps simultaneously on the four imagers, e. g. with some in corridor mode, some software decoders in browsers may show issues with asynchronous timestamps, appearing as grey video. To avoid this, use only either 25 or 30 fps for all four imagers.](#)



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

Encoding

- For H.264, only Main Profile using CABAC is supported. CAVLC is not supported.
- Frame rates in low light mode might vary and cause bit rate control to produce higher bit rates than set as maximum.
- With GOP structure set to IBP and IBBP the I-frame distance may not exactly correspond with the set value.
- For stream setting "Dual ROI" the maximum resolution of stream 2 might be limited regardless of a higher resolution selected in the encoder profile.
- Encoder quality regions are not implemented.
- In case of a high load, the least prioritized stream may drop to a very low frame rate, e. g. 1 or 2 fps, making it difficult for a decoder to synchronize due to a large GOP size. This may result in temporarily showing black video.
- On FLEXIDOME 7100i with stream limit of 5MP on each line, the maximum frame rate of 30 fps cannot be guaranteed, even with stream prioritization. A stream limit of 4MP with copy stream for streams 2 to 4 must be set to get full 30 fps.

Security

- When using certificates for mutual authentication, it must be ensured that the camera uses a solid and trusted time base. In case the time differs too much from the actual time, a client might be locked out. Then, only a factory default will recover access to the camera.
- Excessive signing, e. g. due to very short video authentication signing interval, may have an impact on TLS connection setup.
- If software sealing is active and SNMP is disabled in Network -> Network Services, no SNMP trap will be sent out on seal break due to the disabled service. The seal break itself is logged.
- Configuration changes in imaging settings do not break the software sealing.
- SHA384 is not supported for Elliptic Curve certificates as the hash would be truncated to the EC key length of 256 bit.

Network

- QoS values are set according to group Video/Audio/Control for UDP packets, but for TCP packets, only the QoS value for Video is inserted.

Note: Values are allowed to be entered as ToS values in increments of 4.

To set a valid DSCP enter a (ToS) value between 32 and 224 as increments of 8.

- Changes to IPv6 settings, e. g. prefix, are not taking effect until device is restarted.



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

VCA

- Slow moving objects may not be detected. There is a minimum speed for objects to be detected as moving.
- IVA and flow need at least 7.5 frames per second video input frame rate. If IVA or Flow are configured, minimum frame rate of 7.5 must be set in ALC mode.
- There is only one configuration for IVA. When analysis type is changed, e. g. from IVA to IVA Flow, the former configuration is lost. Due to this, it is not possible to change the analysis type in a VCA profile switch.
- If a VCA configuration using a rule engine is switched to a VCA configuration without using a rule engine, e. g. MOTION+ or IVA default configuration, the saved configuration is invalid. Forensic search with this configuration may lead to undesired search results.
- Due to a limitation of the script language that is used in the background, the delay timer for event triggered VCA starts immediately when the configuration is set. A trigger event during this period does not restart the timer. Once the timer has elapsed, operation is as desired.
- "Too dark" alarm is not triggered under normal conditions due to the cameras low-light capabilities.
- VCA shapes are not synchronized with video when using the open-source JavaScript library for decoding.
- In ceiling mount, when the gyro sensor is perpendicular to earth plane, the roll angle cannot be determined and appears unstable, thus must be ignored.
- Reference image becomes invalid with changing the base frame rate, or rotating or mirroring the image, and needs to be re-created.

MOTION+

- An alarm recording configured to be triggered by MOTION+ with masks may not be operational after reboot. Saving MOTION+ configuration without any changes recovers from that. Alternatively, masks may not be used with MOTION+.



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

Recording

- LUN size for local recording via “Direct iSCSI” is limited to 2 TB.
- VRM version 2.12 or higher is required.
- In some cases, formatting errors on external iSCSI drives may occur, which might need multiple tries to overcome.
- In rare cases it may happen that the owner of an iSCSI LUN is not displayed correctly. Recording is not affected, just previous owner remains displayed.
- If a device had primary and secondary recording running on SD card and is then added to a VRM system, the blocks used for primary recording will not be re-used, reducing the available recording space for the ANR recording. This can be solved by re-formatting the SD card.
- SD card recording performance is highly dependent on the speed (class) and performance of the SD card.
- With I-frame-only recording and audio also enabled for recording, audio will be fragmented or not audible during replay. Please disable audio recording in case of I-frame-only recording.
- Numbering of the recorded files on the replay page is not always contiguous. If snippets across block borders belong together, like pre-alarm and alarm recording, the snippets become logically united and only the lower file number is presented in the list.
- SDXC cards are formatted to FAT32 file system and not using the exFAT file system as being mandatory for SDXC standard compliance but fully recognized and accessible. The maximum size of 2TB is also supported with FAT32, once SD cards of that size might become available. FAT32 also increases portability to other than Windows platforms.
- If a local media is exchanged, existing former recordings are only discovered after rebooting the device.
- Physically removing the local storage media while recording causes the device to reboot. Recording must be stopped before removal.
- Changing audio format while audio is being recorded may cause unknown behaviour of the device and must be avoided.
- The storage system indicator status must be ignored during formatting of an SD card.
- Forcing the camera into an overload situation may cause undesired behaviour and in worst cases even recording gaps. It should always be ensured that the CPU load is not consistently around or at its maximum. This can be achieved by adapting encoder settings or avoiding too many tasks, e. g. client sessions, in parallel.
- Selection of streams for recording is limited to stream1 and 2 only.
- Encoder profile selection per stream is only possible for all four imagers simultaneously.
- Recording profile names are defined for defaults. Changes to the profile may mismatch with the pre-defined name, thus adaption may be advised.
- **Recording will continue even if local storage is deselected until already allocated storage spans are utilized, then stop.**



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

Export

- FTP exported files which include audio in a format other than AAC must be renamed from .mp4 to .m4a to allow correct playback in QuickTime.
- With JPEG Posting active when device is booting, the first posted JPEG image may be a no-cam logo.
- FTP posting with resolution 1080p delivers JPEG with size of 1920x1072 pixels due to 16 pixels macroblock boundary of the JPEG encoder.
- If FTP export files contain only a few frames some players might not correctly replay such a file, or the replay is too quick to recognize something. The exported file is not corrupt though it might seem so.
- Files exported using continuous FTP backup for Rec. 2 where stream 2 is set to I-frames only mode contain wrong timing information and play back too fast.
- FTP export file size is always 100 MB if resolution change occurred in exported time span.
- After modifying account settings, e. g. FTP server address, to get the changes applied either switching posting off and on or restarting the device is required.
- Using "export from memory" with pre-alarm recording exceeding the available memory will cause continuous recording on the account storage. Checking the memory requirement of the pre-alarm ring is advised to avoid unexpected memory consumption.
- Dropbox is not supported anymore.
- SD-card export of an entire file does not work. Manually configuring the export time will lead to a successful export though.

Miscellaneous

- Before upgrading FW, it is best practice to back-up all configurations first, incl. IVA and calibration.
- After reboot, the system time re-synchronisation may be delayed up to 9 seconds for SNTP respectively up to 14 seconds for time server protocol.
- AAC audio timestamps for UDP live video streams as well as for recording streams are based on 90 kHz instead of 16 kHz to ensure compatibility with Video SDK. AAC audio timestamps for TCP live video streams are based on the standard 16 kHz timestamps. Standard players should connect to live video with AAC audio using TCP.
- After changing the selectable camera mode via alarm input the switch back to a previous mode doesn't work anymore.
- Firmware upload stops recording when it fails or is terminated.
- Uploading a configuration file from a different camera platform may result in unpredictable behaviour.
- When combining CPU-intensive functions like e. g. encryption, watermarking, or dual recording, with high quality and high frame rate encoder settings, tuning of encoder profile settings might be required to avoid overload situations.
- No time change is allowed during the time when the "hour is repeated".



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

- Maintenance log file creation and download requires some time, though there is no progress indication, and needs to be waited for completion.
- Millisecond stamping is not supported.
- JPEGs with VCA overlay are not fully synchronized. Shapes might be slightly off.
- Audio back-channel in Chrome browser may be delayed when using an unsecure or unaccepted HTTPS certificate.
- In scenes with mixed lighting, the image appearance might be greenish. To solve this, switch the white balance mode to Sodium lamp Auto.
- If the configured bitrate for a JPEG is too low, the JPEG encoder will nevertheless create its minimally required bitrate, exceeding the expected bitrate.
- 5MP and larger JPEG streaming via RTSP is only possible with decoders supporting the ONVIF extensions.

JPEG streaming via RTSP is based on RFC 2435. This RFC only allows for a maximum JPEG size of 2048 by 2048.

With ONVIF, the original, larger JPEG headers can also be transmitted via RTP header extensions. Unfortunately, this only works with decoders using these extensions, i. e. it does not work with a standard VLC.

- JPEGs for JPEG posting and in alarm e-mails are taken from the JPEG stream, thus 'burn-in' metadata overlays are not possible.
- With using stream prioritization, non-prioritized streams will drop frame rate when camera is not able to fulfil all requested streams equally.

Please check the respective release letter of a camera for further device-specific restrictions.



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

8 Previous Revisions

8.1 *New Features with 8.30.0082*

- The sensor image can now also be rotated 90° to create an upright video mode. This mode efficiently captures details in long hallways without loss of resolution, mount the camera at right angles. For 20MP variant, the frame rate in this mode will be limited to 25fps.
- More streaming resolutions were added on streams 2 and 3.
- Support of ONVIF Profile M, including MQTT event forwarding.
- New Western Digital industrial SD cards with lifespan monitoring are supported.
- SNMP has been added, supporting v1 and v3, both including traps. RCP+ integration is widely done to create similar support as of earlier platforms. New MIB file is available and distributed with the firmware package.
- IR intensity level can be independently configured for each of the center and the four surrounding regions.
- Privacy masks can be enabled and disabled via a single switch command.
- For backward compatibility with legacy clients, applicable where alternative measures are put in place, the check on the HTTP referrer, an improvement to reduce the vulnerability for Cross Site Request Forgery (CSRF) attacks, can be disabled via the user interface.
- TLS 1.3 is supported, including the possibility to set the minimum TLS version.



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

8.2 Changes with 8.30.0082

- Camera Trainer license is not needed anymore, and Camera Trainer function is allowed by default.
- An issue is fixed where in certain HDR scenes a flicker in the video could be noticed in high exposure areas.
- Noise reduction is improved for specific HDR scene or halogen light.
- Color reproduction (white balance) is improved for particular scenes with mixed lighting (e.g. sun and halogen) where the image turned greenish.
- A few issues with display of name and time stamping in the video are fixed
- An issue with display of date format in MM/DD/YYYY is fixed.
- Custom color for privacy masks improved match.
- The IVA overlay lines in full screen mode in the web browser now show up correctly.
- Defog is now set and activated by default.
- An issue is fixed where, in scenes with mixed lighting, the image appearance might have been greenish.
- An issue is fixed where reboot of a FLEXIDOME multi 7000i in non-optimal light conditions may end in unfocused video.

During a penetration test, Kaspersky Lab, who was contracted by Bosch for IP camera security maturity certification, detected a vulnerability which required immediate action to ensure the security of installations using our cameras.

For more details refer to our Security Advisory BOSCH-SA-033305-BT, published at our Security Advisory web page

<https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

or visit our PSIRT website at <https://psirt.bosch.com>.

- An issue which provided a possibility to conduct a CSRF (Cross Site Request Forgery) attack is fixed (CVE-2021-23848).



From

BT-VS/MKP

Product Management

Nuremberg

12.01.2023

8.3 Changes with 8.00.0155

- VCA frame rate has been set to quarter sensor frame rate, now processing every fourth image. This reduces system load in order to allow the required streaming performance. As a side-effect VCA objects may be detected later, overlays might slightly lag behind, and too fast moving objects might not be detected.
- VCA can be switched off per imager and does not impose any CPU load in this case.
- Tooltip is activated on CPU load indicator in top bar of web interface to provide more details.

8.4 New Features with 8.00.0153

- Support of the new multi-sensor camera FLEXIDOME multi 7000i.
- Quad-streaming capability providing three independently configurable H.264/H.265 streams plus M-JPEG stream per video imager.
- Stream prioritization for one of the H.264/H.265 streams per video imager.
- Support for next generation Secure Element microcontroller (TPM), supporting up to 4096 bit RSA keys
- Flexible on-screen display stamping
 - Font size can be defined per stamping section, resolution-independent by per mill of screen size.
Font size will automatically be limited to the possible maximum size, evenly distributed over all stamping sections.
 - Text and background colours can be defined per stamping section.

Please note that the firmware running this platform inherits the functionality and features from firmware version 7.80 for platforms CPP6, CPP7 and CPP7.3. For a complete overview of the comprehensive feature set and the history of introduction refer to release notes of one of these platform firmware releases.