

From BT-SC/MKP8.1	Product Management	Nuremberg 13.12.2018
----------------------	--------------------	-------------------------

## Release Letter

Products:	<b><i>H.264/H.265 Firmware for CPP7.3 HD/MP cameras</i></b>
Version:	<b><i>6.60.0065</i></b>

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

### 1 General

This firmware release is a feature release based on FW 6.51.0028. It is an upgrade for CPP7.3 based cameras only.

Changes since last release FW 6.51.0028 are marked in [blue](#).



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## 2 Applicable products:

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 5000i (IR)
- AUTODOME IP starlight 7000i
- DINION IP bullet 4000i
- DINION IP bullet 5000i
- DINION IP bullet 6000i
- FLEXIDOME IP 4000i
- FLEXIDOME IP 5000i
- MIC IP starlight 7000i
- MIC IP fusion 9000i

From BT-SC/MKP8.1	Product Management	Nuremberg 13.12.2018
----------------------	--------------------	-------------------------

### 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 firmware file. This new process has been prepared for with firmware 6.50 and comes into effect with succeeding versions.

The new signature protects from non-released versions being installed in productive 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.

In case a firmware must be downgraded from a device with firmware 6.51 or higher installed, the downgrade is only possible via firmware 6.50 with an updated signature. Please contact our customer service or technical support to get a link to this firmware.

#### 3.2 *Firmware file encryption*

In order to upload version 6.51 to a device running a firmware version below 6.50, you need to upgrade first to version 6.50, since older firmware versions do not support firmware file decryption.

#### 3.3 *“Originally manufactured” certificate*

Since firmware version 6.30 all cameras are prepared to receive a unique Bosch certificate during production, assigned and enrolled by Escrypt LRA. These certificates prove that every device is an original Bosch-manufactured and untampered unit.

Escrypt is a Bosch-owned company, providing a public certificate authority (CA).

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

#### 3.4 *TPM*

All CPP7.3 devices incorporate a Trusted Platform Module (TPM) with own firmware.

This TPM hardware and firmware have been enhanced over time to allow for additional security features.

Due to security reasons, the firmware or functionality of the TPM cannot be altered in the field.

Thus, not all new security features become available on devices with older TPM hardware or firmware revisions.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## 4 New Features

### Security

- Software sealing is extended to cover more static parameters of image pre-processing and moving camera control.
- Manual and automatic logout functionality added to the web browser interface:
  - A “Logout” button is available in the blue navigation bar between “Links” and help icon.
  - A timeout in minutes for the browser session can be defined via the Web Interface -> ‘Live’ functions menu.
- Enhancements for Alarm Task Scripting:
  - A seal break event can be used to trigger alarm task scripts.
  - An SD card lifespan alarm can be used to trigger alarm task scripts.
- Enhancements for SNMP:
  - A seal break event can trigger an SNMP trap.
  - An SD card lifespan alarm can trigger an SNMP trap.
  - An event from the Embedded Login Firewall can trigger an SNMP trap.

### Moving cameras

- A “snap to area” function is added to allow selection of a new image area that the camera zooms to. The rectangle to define the area can be drawn over the video by holding “CTRL”.
- Inactivity period selection for moving cameras is extended up to 24 hours.
- Number of privacy masks on MIC 7000 and MIC 9000 increased from 24 to 32.

### ONVIF

- Signalling of ‘idle object’ is added to the ONVIF metadata stream.

### Miscellaneous

- Genetec Stratocast cloud is supported.
- 5MP cameras received a 3 MP downscale resolution option.
- Enhanced prediction can be disabled in Encoder Profile Expert settings for compatibility with non-compliant software decoders that do not support long-term references.
- IGMPv3 enhancements to support source-specific multicast (SSM) scenarios.

### VCA

- An object that triggered an alarm is marked accordingly and displayed in orange color for a short period to allow easier visual detection.

For details on enhancements and changes in Intelligent Video Analytics and Essential Video Analytics, please refer to the separate release notes.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## 5 Changes

- An issue in a multipathing scenario, where during start-up 802.1x EAP/TLS caused iSCSI recording to use the alternative path, is fixed.
- An issue where the ONVIF metadata stream occasionally stopped is fixed.
- Remote recording on CPP-ENC devices is fixed but requires CPP-ENC devices to run FW 5.97.10 or higher because of the recently added security features, which impact RCP+ communication and password handling.
- The default use of 1024 bit RSA keys for self-signed certificate generation is limited to cameras with older hardware that would require time-extensive 2048 bit key generation in software. On all cameras with hardware acceleration a minimum length of 2048 bit is used for RSA keys by default. Certificates with 2048 bit keys can be used on all cameras.

## 6 System Requirements

- Web Browsers:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox
- DirectX 11
- [MPEG-ActiveX 6.32 or newer](#)
- Configuration Manager 6.01 or newer



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## 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.
- 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.
- 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 in 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.

### 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.



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

### 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.
- Underscore character (“\_”) and blank space are not allowed in common name in certificates.
- Excessive signing, e.g. due to very short video authentication signing interval, may have an impact on TLS connection setup.
- Client authentication is not working using Microsoft Edge as the browser does not send any certificate for client authentication, so the camera has nothing to authenticate.
- Video authentication using SHA hashing mechanisms are not functional if no self-signed certificate has been created yet. Opening an HTTPS connection once is prerequisite.
- **Creating 2048 bit keys for self-signed certificates may take more than 20 seconds, extending the initial boot cycle, which may occasionally cause a timeout on the very first HTTPS connection to a camera. The next connection attempt typically is successful.**
- **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.**

### 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.
- IP addresses 172.20.1.0/30 which include 172.20.1.0 to 172.20.1.3 are reserved for internal communication and must not be used as device addresses. Products without internal communication ignore this restriction and allow the use of this range.

### IVA

- IVA and flow need at least 12.5 frames per second video input frame rate. If IVA or Flow are configured, minimum frame rate of 12.5 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.
- 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.
- On devices with VCA FPGA an outgoing IPv6 connection fails when device is initiator, e.g. trying to resolve a time server domain name,
- “Too dark” alarm is not triggered under normal conditions due to the cameras low-light capabilities.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

### **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+.

### **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.
- 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.





From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

- 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.
- 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.

### 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 pixel 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.
- Getting the file list from Dropbox may fail if there are too many objects (files and folders). Limit is approximately higher than 500 objects but also dependent on file name length etc.

### ONVIF conformance

- When using GetPresets command preposition names are not set for scene1 to scene6.

### DIVAR hybrid / network

- Cameras running FW 6.4 are only compatible with DIVAR network / hybrid FW 1.2.1 and higher. With earlier DIVAR network / hybrid firmware versions, the I-frame distance needs to be adapted to 30 or less.



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

**Dome cameras**

- Autopan starts outside of defined range if orientation is set to “Inverted”.
- Tilt up limit is treated as lower tilt limit if orientation is set to “Inverted”.
- In AUTODOMEs, blanked sector may trigger a “too dark” alarm.
- On AUTODOMEs, privacy masking does not cover the complete configured area if privacy mask is placed too close to the edge of a scene. Move the target position to the center of the scene before creating a privacy mask.
- If LIVEPAGE is refreshed during recording of Tour A/B on AUTODOMEs the button “Stop display” will falsely display “Start recording” but still continue tour recording.
- After a firmware upload it may happen that the Privacy Masks and settings from Installer Menu are set to default. Make sure to check if Privacy Masks and Installer Menu settings are still valid after uploading new firmware.
- For optimal image performance the user is advised not to turn off contrast enhancement during normal camera operation.
- To improve Recorded (Guard) tour playback accuracy, Bosch recommends users record tours using the User Interface (UI) instead of using a keyboard. In the event that the Recorded (Guard) tour loses position accuracy during playback, users should re-home the camera using the “Find home” button on the Live page.
- MIC 7000 orientation can be switched between normal and canted.
- When the user changes orientation from normal/canted to inverted (or vice versa), MIC 7000 will tilt itself up and over so that the visor and wiper are on top. If there is an attached illuminator this would result in the illuminator hitting the MIC's body. To avoid this, MIC 7000 will not allow an orientation change while the illuminator is attached. A warning message with “Yes/No” selection will be displayed when the user clicks the orientation radio button and the MIC has an illuminator.
- On AUTODOME 7000 and MIC 7000 “HDR” can be selected in the preposition mapping but has no effect as it is not supported in these models.
- NTCIP requires to have the SNMP port enabled to become functional. As the SNMP port, amongst others, has been closed by default if not needed due to security improvements, it must be re-enabled to allow NTCIP to work.
- Scene/VCA profile may not be correctly restored, causing the Sketch button to be disabled.



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

**Miscellaneous**

- After firmware upload while daylight saving time checkbox is activated the time zone must be adjusted.
- 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.
- After downgrade configuration integrity cannot be ensured and settings need to be checked or re-configured. Sometimes even a factory default might be required, which is anyway recommended after a firmware downgrade.
- When a configuration file is loaded to an incompatible camera, e.g. a configuration file from a HD camera loaded onto a VGA camera, encoder settings might become invalid and need to be re-configured.
- Uploading a configuration file from a different camera platform may result in unpredictable behaviour.
- If it shall be checked if the image is not frozen, use milliseconds timestamp to verify.
- Intelligent Defog default is OFF under "Low bitrate" scene mode.
- 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".
- Maintenance log file creation and download requires some time, though there is no progress indication, and needs to be waited for completion.
- Millisecond stamping on 60 fps cameras is refreshed with 30 Hz only, updating only every second frame.
- JPEGs with VCA overlay are not fully synchronized. Shapes might be slightly off.

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



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

## 8 Previous Revisions

### 8.1 Changes with 6.51.0028

- This version includes a fix for a recently discovered security vulnerability. The vulnerability potentially allows the unauthorized execution of code on the device via the network interface. Bosch rates this vulnerability at 9.4 (Critical) and recommends customers to upgrade devices with updated firmware versions. For detailed information please refer to the published Security Advisory.

### 8.2 New Features with 6.51.0026

- **Support of AUTODOME IP starlight 5000i (IR) family**, incl.
  - up to 32 privacy masks
  - 8 instead of 5 corner points per privacy mask
  - High Dynamic Range (HDR)
- Third-party serial protocol over IP is now supported for Pelco and Cohu protocols. Please note that a special license is required as this functionality lowers the overall security of the camera. Extra measures might be needed to be put in place to protect the system.

### 8.3 Changes with 6.51.0026

- Password reset mechanism changed
  - Clearing passwords of all three legacy users was changed to only reset/change the password for the user 'service' to 'service', while passwords of all other users including 'live' and 'user' as well as other 'service' users stay unchanged.
  - The user can then logon to the camera using user 'service' with password 'service'. He should then change the password for the service user again.
- General privacy mask improvements
- Long-term reference enhancements to improve support for 3<sup>rd</sup> party decoders



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

#### 8.4 ***New Features with 6.50.0128***

- **Improved image performance for the following cameras:**
  - DINION IP 4000i IR
  - DINION IP 5000i IR
  - DINION IP starlight 6000i IR
  - FLEXIDOME IP 4000i
  - FLEXIDOME IP 5000i
  - AUTODOME IP 4000i
  - AUTODOME IP 5000i
- **Image pre-processing enhancements on DINION IP starlight 6000i IR:**
  - A user slider to tune the maximum gain allowance is added
  - A user slider to tune the day to night switch-point is added
  - A new scene mode is now available for optimized License Plate Recognition (LPR)
- **Intelligent Streaming enhancements**
  - Statistics pages have been added for live and recording streams. These provide guidance for optimally adjust bitrate and quality settings, and make judgement on averaging easier in order to optimize storage consumption.
  - Intelligent Streaming configuration parameters in encoder profiles are now grouped.
  - Encoder quality regions are now also supported on CPP7.3 platform.
- **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:

  - Sony
  - SanDisk
  - Micron

Due to the high dynamic in the SD card market, no direct reference to the models is given. Latest Industrial SD cards from all three vendors support this feature.
- **ONVIF Profile T is now supported**
- H.265 B frames support can be selected in Installer menu to allow for lower bitrates at certain resolutions.
- Digital zoom is now support on thermal image of MIC IP fusion 9000i
- Thermal module flat-field correction (FFC) on MIC IP fusion 9000i can be set to 'auto modus'.
- Intelligent Tracking can be triggered by point-and-click feature in web interface.
- Manual iris control for AUTODOME 4000i/5000i has been added.
- Current gain value is visualized in video preview window.



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

- The ID out of the best face detection is attached to the JPEG filename when posted via FTP and also added to the metadata stream to allow searching.
- SNI support has been added to improve load-balancing for cloud-based solutions.

### Security features

- **Software Sealing**

The camera configuration can be 'sealed' once it should not be changed anymore. Any change of the sealing status and any change to static configuration, accidentally or intentional, will break the seal, creating an alarm message that can be used by the video management system to launch an appropriate alarm scenario.

All modifications affecting the sealing status are logged separately.

- Firmware files are now encrypted.
- Files received via HTTP upload are checked for correct size.
- "Secure renegotiation" is signalled in TLS.
- In case of certificate user authentication, the clock base is re-adjusted, e.g. after battery loss.

## 8.5 Changes with 6.50.0128

- After updating to firmware version 6.50, users will be able to take advantage from boosted performance and enhanced image quality on all CPP7.3 (4000i, 5000i, 6000i) based cameras:
  - Overall improved contrast and sharpness (reduced haziness)
  - Improved visibility in scenes with highlights and dark areas
  - Improved facial detail visibility in scenes with strong backlight
  - Maintain more color in dark scenes
  - Stronger sharpening when it is getting darker by directional sharpening
  - The default shutter function in the ALC menu is now also available in HDR mode
- Specifically for the AUTODOME IP 5000i two additional improvements are available:
  - Better preserved highlights in dark scenes
  - Improved depth of field by introducing zoom-dependent iris control
- Missing SD resolutions have been added to stream 1 options.

## 8.6 Changes with 6.44.0020

- Cipher suites were enhanced by TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256.
- An issue with simultaneous multicast streams, introduced with FW 6.43, has been fixed.
- An issue with ONVIF SetImageSettings, where incorrect settings could be applied when an unsupported namespace was used, has been fixed.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

- An issue with ONVIF IVA messages suspended, when more than one IVA rule was configured, has been fixed.
- An issue with VCA calibration lost after image rotation has been fixed.
- An issue with EAP-TLS certificates with CRL extension, intermittently prohibiting authentication, has been fixed.
- An issue with panoramic cameras, where pre-positions could not be set in the web interface when in on-board dewarping mode, has been fixed.
- Various smaller issues have been fixed.

From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

### **8.7 New Features with FW 6.43.0027**

- ITS versions of AUTODOME and MIC cameras can be enabled to allow NTCIP protocol over serial interface.
- A possibility to increase the Power-over-Ethernet (PoE) demand signalled via LLDP has been added. This may help to optimize the power management on switches and e.g. also eases to use the cameras in outdoor housings with PoE-powered heating systems.
- IGMP version can now be set to a specific version. Automatic detection is still default.

### **8.8 Changes with FW 6.43.0027**

- After updating to firmware version 6.43, users will be able to take advantage from boosted performance and enhanced image quality of AUTODOME IP 5000i and AUTODOME IP 5000i IR:
  - Improvement on depth of field
  - Overall improved contrast
  - Improved visibility for foggy scenes
- After updating to firmware version 6.43, users will be able to take advantage from boosted performance and enhanced image quality of AUTODOME IP 4000i:
  - Overall improved contrast
  - Improved visibility for foggy scenes
- Improvements on Multipathing support for storage devices.
- Various smaller issues have been fixed.

**Note:**

Due to improved image tuning in this firmware version, the behavior of various image enhancement sliders can be different than in older FW releases. Therefore it is recommended to perform a "Restore Mode Defaults" after the firmware update is finished in order to get the best performance. This button can be found under: Configuration -> Camera -> Scene Mode





From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

## 8.9 Changes with FW 6.42.0021

- Stronger user name and password policy is enforced. The following rules apply:
  - User names must be at least five (5) characters long.
  - User name and password must not be identical.
  - A password must consist of minimum eight (8) characters.
  - A password must contain both upper-case and lower-case letters.
  - A password must include one or more numerical digits.
  - A password must include at least one of these special characters:  
! ? " # \$ % ( ) { } [ ] \* + - = . , ; ^ \_ | ~ \Other special characters (like space @ : < > ' & etc.) are not supported.
- Multicast discovery port is now configurable via browser interface.
- The base frame rate default for DINION IP bullet 6000i has been changed to 60 fps.
- An issue where sporadically no video was shown after power cycle has been fixed.
- An issue where Automatic Network Replenishment ANR failed when SD card is broken has been fixed.
- Improved behavioural response on denial of service attacks.
- Various ONVIF communication issues have been fixed.
- Various smaller issues have been fixed.

## 8.10 Changes with FW 6.41.0037

- Various smaller issues have been fixed.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## **8.11 Features with FW 6.40.0240**

### **Encoding**

- Support of H.265 compression  
A camera can be configured to use either H.265 or H.264. As H.265 requires more CPU performance, there might be limitations to maximum frame rate under certain conditions.

#### Note:

H.265 requires approx. 4 times the performance for decoding compared to H.264. Installed workstations, decoders and software might lack the performance to fluently decode H.265 streams.

### **Intelligent Streaming**

- Intelligent Streaming is a combination of features and functions to optimize bitrate consumption of recorded video. It benefits from improved noise reduction in still areas of the image, an average noise level communicated to the encoder, larger GOP size, strong use of prediction in case of B slices, and dynamic tuning of quantization parameters (QP) in the encoder.
- The strength of the bitrate optimization can be set via 5 levels. Savings can be up to 90% using H.265 compression but are strongly scene-dependent.
- Intelligent Streaming is enabled by default in medium setting.

### **Imaging**

- Support of 120 dB high dynamic range for 5000 camera series has been added.
- Improved noise filtering in still scenes.

### **VCA**

For details on VCA 6.40 please refer to the separate release notes of Essential Video Analytics or Intelligent Video Analytics.

### **ONVIF**

- ONVIF manual iris and focus controls added.
- Feature coverage of the ONVIF metadata stream has been extended to include e.g. object classes, object shape polygons, faces, flame and smoke detection info.
- Profile G support
  - Recording start and control has been added.
  - Recording search and replay functionality has been added.
  - Tested with ONVIF Device Test Tool 16.07 SR2 rev. 617.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

## Security

- Password enforcement
  - New cameras with this firmware installed will only become operable after the password for the administration level (user "service") has been assigned.
  - Other users "user" and "live" will only become accessible after the administrator assigned passwords to them.
  - Cameras which are updated to this firmware from a version lower than 6.40 will not change their behaviour and remain at their former protection level unless reset to factory defaults.
- Signed firmware file enforcement  
Only Bosch-signed firmware will be accepted by the camera without compromises.
- Data encryption on iSCSI storages
  - The payload on an iSCSI drive is encrypted using a symmetric XTS encryption scheme (block encryption).
  - The camera uses a number of public keys to asymmetrically encrypt the XTS key for multiple receivers. These public keys are maintained in the certificate store via certificates. Usage can be defined as for „recording1“ and/or „recording2“.
  - Payload encryption is possible on SD cards as well as on external iSCSI storage.
  - A client that shall be allowed to replay this footage must have its cert/key registered and activated.
  - The Video Recording Manager (VRM) may also be a receiver to decrypt the payload data for replay.
- SRTP payload encryption for live and replay  
SRTP provides payload encryption of UDP streams via TLS, similar to what HTTPS does by using TLS for TCP streams. Also encrypted multicast connections are possible.
- SNMPv3 support
  - New alternative SNMP support provides encryption and authentication. This new service will provide pure MIB-II access.
  - Legacy functions, like NTCIP support or mapping of dedicated RCP commands to SNMP Enterprise MIB nodes, are only provided with existing SNMPv1 implementation.
- Certificate revocation list (CRL) support
- To improve usability and provide a more compact overview, the web user interface for the certificate store has been updated. It now allows direct tagging of certificates for usages. The former split into two areas (Files and Usage) is removed.



From

BT-SC/MKP8.1

Product Management

Nuremberg

13.12.2018

- Stronger encryption and password protection for configuration file
  - The configuration file is encrypted and password-protected before download.
  - The user as the owner of this configuration file is prompted for the password.
  - The password is required when the configuration file is uploaded to a camera.
  - The configuration file is encrypted using standard mechanisms but not intended to be opened or modified by the user, thus the encryption key itself is kept internal and not exposed.
- Stronger encryption for maintenance log file  
The maintenance log file as being used in tech support cases is encrypted with a Bosch public key. Only tech support staff is authorized to decrypt and open the file.
- The minimum TLS version can be defined, e.g. to avoid vulnerabilities from TLS 1.0 and 1.1.
- The Telnet console has been completely removed and is substituted by a new logging facility providing:
  - A more structured output including timestamp, severity and module sources
  - Search and filtering for specific events via web user interface
  - Direct output to a syslog server
  - Configuration to produce similar “debug” printouts for tech support as previously
- Consolidation of running services, visualized on new page “Network Services”.  
Only those services (HTTP, HTTPS, RTSP, RCP, iSCSI, NTP, discovery, ONVIF discovery) are running which are required for activated functionality. All other services (FTP, SNMP, UPnP, GB/T 28181) and their respective ports are deactivated.
- The password unlock functionality (support recovery option) can be disabled.
- CHAVE cameras
  - Multiple trusted issuers are now allowed for client certificate authentication.
  - An option to not wipe the SXI certificate when a factory default is issued has been added.
- Installation Code has been enhanced with a block for crypto-coprocessor version indicators.  
The Installation Code thus has a length of 48 digits instead of only 44 digits.



From  
BT-SC/MKP8.1

Product Management

Nuremberg  
13.12.2018

### Miscellaneous

- SMTP port is configurable via web interface.
- Multipathing support for storage devices.
- User name from certificate for EAP-TLS is used as EAP identity, if provided.
- 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.
- Cameras can connect to the CBS Remote Portal installer service.
- New illuminators for MIC 7000 are supported.
- Large OSD font can be selected, roughly doubling the size of the fonts used for stamping.
- Intelligent Auto Exposure (IAE) has been extended to cameras without FPGA.
- An event playback button has been added to the Live page to allow a quick playback of the last event in case there was an incident and the camera was connected remotely to check what happened instead of checking live and then go to the playback page.
- Default device date is set to firmware build time in case of invalid RTC time to avoid lock-out in case of certificate-based authentication.
- Dropbox API has been updated. The API used before was going obsolete on June 28th, 2017.
- Improved certificate parser to support more attributes used e.g. by various mail providers.
- A banner mode for stampings has been introduced, allowing large scale stamping on top or bottom of image.

The firmware basis is equivalent to the platforms CPP4, CPP6 and CPP7 and inherits all the features that exist upon them.

The "Previous Revisions" section thus mainly lists the features that are commonly introduced with the FW 6.40 for all four platforms in addition to the unique features introduced with the platform CPP7.3. For earlier features please refer to release notes from the other platforms.