



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

Release Letter

Products:	<i>H.264 Firmware for AVIOTEC cameras</i>
Version:	<i>7.50.0079</i>

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

1 General

This firmware release is a feature release based on FW 6.61.0074.
It is an upgrade for CPP6 based AVIOTEC cameras only.

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

2 Applicable products:

- AVIOTEC IP starlight 8000



From		Nuremberg
BT-SC/ETP-MKP1	Product Management	28.08.2019

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. 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 CPP6 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.

3.5 *AVIOTEC IP starlight 8000*

The firmware for AVIOTEC IP starlight 8000 is created separately since FW 7.10, and thus releases may not follow the exact release builds as with other CPP6 cameras.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

4 New Features

- Latency of live video, when no MPEG-Active-X is used, has been reduced by using an open source JavaScript library.
- Alarm Task Scripting Language (ATSL) has been enhanced to allow a free username that can be used with sending an HTTP POST command to e.g. control an I/O device.
- The IVA Task Script Language has been enhanced by a temporal "within" element, allowing to add debounce and aggregation times on states.
- Connection establishment over RTSP with parameter "vcd=3" provides an XML stream with extension tag where the original RTP VCD data packet is encapsulated with base64 encoding. This allows for the possibility to send ONVIF and VCD data in one stream.
- An alarm message can be created if time synchronization fails, and an SNMP trap can be sent.
- A dashboard, available under service permissions, provides a compact but extensive view on parameters that might be especially helpful for troubleshooting. An export function provides even more details than displayed on the dashboard page.
- Scene mode names in fixed cameras have been adapted to reflect their intended use cases better and synchronized between fixed and moving cameras. Scene modes settings have been tuned accordingly to better match their intended applications.
- IP address can now be changed dynamically during runtime, not requiring a reboot cycle anymore. This allows for quarantine network transition on 802.1x network configurations as well as for dynamic IP address assignment from DHCP.
- Support of China GB/T 28181 has been updated to comply with 2016 standard.
- AES encryption on RTP connections is now possible, allowing encrypted UDP multicast connections in a BVMS setup.
- Default value for TLS has been set to version 1.2 to increase security by default. This may cause incompatibility with older client applications.
- Session cookie has been secured by default, disallowing authentication forwarding to MPEG ActiveX and other applications, like replay via Video Security Client. Re-authentication is required for these applications when called out of the web browser despite an already authenticated browser session.
- An option to export from RAM recording buffer allows recording exports on the fly without requiring an SD card or external iSCSI storage.
- A separate hostname setting is introduced. For backward compatibility, the hostname setting is still pre-filled from entries in the camera and unit name fields but can then be configured independently.
- Multicast connections for audio streams are now supported.
- An auto back-focus command is introduced to initiate an auto back-focus adjustment cycle without the need for entering the Lens Wizard.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

5 Changes

- The menu item "Image posting" has been moved within the sidebar menu into the "Recording" section. A link to configure accounts has been added.
- The special character '+' is not allowed in passwords anymore as it conflicts with some authentication methods.
- ONVIF AbsoluteMove command now allows the optional parameter "speed" for pan and tilt movements.
- ATSL commands now use HTTP digest authentication. Basic authentication is disabled.
- Face Detector has been improved.
- The sensitivity slider standard position for flame and smoke detection is changed.
- The size sliders for flame and smoke are fixed set to minimum size and hidden.
- Stream 1 resolution on FLEXIDOME IP panoramic 6000/7000 can now also be set to 1440x1440 pixels.
- An issue is fixed where too small pre-alarm recording buffers caused sporadic error messages.
- An issue is fixed where sporadically a wrong Ethernet link mode was detected.
- An issue is fixed where empty connections could be established using an obsolete URL.
- An issue is fixed where sequence numbers in metadata RTP streams were wrong after VCA was reconfigured.
- An issue is fixed where no folder could be added to a Dropbox account.
- An issue is fixed where device could not be registered in Remote Portal anymore.
- HTTP digest authentication is set as default.
- iSCSI MSS setting has been removed.

6 System Requirements

- Web Browsers:
 - Microsoft Internet Explorer 11 or higher
 - Mozilla Firefox
- DirectX 11
- MPEG-ActiveX 6.33 or newer
- Configuration Manager 6.20 or newer



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

7 Restrictions; Known Issues

User Interface

- If UAC is set to default in Windows 7, no snapshot or recording via LIVE page is possible.
- Video and audio may be asynchronous during replay via Web page.
- In rare cases it may happen that no recordings can be found on PC with Windows XP SP2 and IE6. Internet Explorer may stay in status 'connecting on replay page'. An update of Internet Explorer is recommended.
- 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.
- If an intranet site is opened, IE10 automatically runs in compatibility mode. This leads to a misbehaviour that no timeline is shown on the PLAYBACK page. Therefore the function "Display intranet sites in Compatibility View" must be disabled.
- Upgrading the firmware to version 6.10 may require clearing the Web browser cache to have the new user interface style appear.
- In dewarped multi cameo views (like quad and double panoramic), selection of cameo can be done in the scene and ROI menu only, not by clicking in the video
- 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.
- Exchanging the company and device logo might not be possible anymore due to strengthened web browser security features, although the settings are still possible in the web user interface.
- **Firmware upload in recovery mode (app0) is very slow on products produced with FW 6.32 up to FW 6.5x. Be patient and don't interrupt the upload.**



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

Encoding

- Only H.264 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.
- Aspect ratios 16:9 and 4:3 are not combinable. Aspect ratio from stream 1 will lead.
- 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 is 432p regardless of a higher resolution selected in the encoder profile.
- If bit rate is already reaching maximum level due to image content to be encoded, encoder quality regions with setting "object" cannot be improved for quality anymore and differences will gradually be reduced.
- With DINION IP ultra 8000 MP, rotation to upright (90° or 270°) in combination with analog video out does not allow 25 fps, despite the setting being available in the dropdown menu. Frame rate of 15 fps must be selected.

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.
- Cameras with security coprocessor version 3 with an externally applied certificate will fail HTTPS connections requesting SHA256. The restriction applies to all functions using the private key from the certificate, including
 - EAP-TLS with client authentication
 - TLS-Time with client authentication
 - TLS-Syslog with client authentication

With self-signed certificate, HTTPS is fully functional.

- 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.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

Image Processing

- For optimal image performance the user is advised not to turn off contrast enhancement during normal camera operation.
- In cases where the camera is configured to do very little noise filtering (far lower than default settings of the camera), in a low-light scene the bit rate needed for encoding the unfiltered, low-noise image is high. If the target and maximum encoding bit rate values do not match this bit rate requirement, blockiness or stuttering images may result. On these occasions please apply stronger temporal or spatial filtering and/or reduce sharpness.
- When resolution 3840x2160 or 3584x2016 is selected, no B frames are supported and the GOP structure is always IP despite B frames can be configured in the encoder profile.
- ROI PTZ combined with IDNR enabled may blur image when no motion is present in the scene.
- When the camera runs in HDR mode, the analog output menu cannot be used by pressing the local menu button. In this mode, pressing the menu button on the camera will switch on the analog output, pressing it once again will switch the analog output off. Aspect ratio and zoom and focus changes can only be done via IP in the FW configuration.

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.
- 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.
- On devices with VCA FPGA an outgoing IPv6 connection fails when device is initiator, e.g. trying to resolve a time server domain name,
- [VCA shapes are not synchronized with video when using the open source JavaScript library for decoding.](#)



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

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+.

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.
- Link-local addresses from the Auto-IP range (169.254.1.0/16) must not be entered manually.
- Reboot will not be performed automatically after uploading a SSL certificate or SSL key; must be done manually.

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.
- Throughput limit for simultaneous recording and local replay at 100% playback speed is:
 - maximum total recording bit rate of 7 Mbps for external iSCSI recording
 - maximum total recording bit rate of 10 Mbps for SD card recording, depending on SD card performance
- 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



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

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.
- 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.
- Triggered recording (backup) tasks in buffered recording configuration are not persistent over a power cycle. Pending backups to central recording will be lost when a device reboots.
- When local SD-card recording is active, both live Stream1 and the recorded stream will use Encoder Profile parameters of Profile 3. The default profile 3 parameters may in certain conditions lead to encoding artefacts in the recorded stream and live Stream1. In this case, consider the following changes: Lower the resolution, lower the frame rate, lower the sharpness and/or raise temporal/spatial filtering.
- Physically removing the local storage media while recording causes the device to reboot. Recording must be stopped before removal.
- Sporadically occurring incorrect time zone info in recording packets may lead to gaps displayed in the playback timeline. The video footage within the gap cannot be replayed but becomes accessible via exporting the affected period. This may happen with firmware 6.32 below built 111.
- Remote recording is not working with actual firmware on devices running FW 5.5x or older because of the recently added security features, which impact RCP+ communication and password handling.



From		Nuremberg
BT-SC/ETP-MKP1	Product Management	28.08.2019

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.
- 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.
- 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.
- 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.

DIVAR IP 2000 / 5000

- Due to its improved security features, firmware 6.4 is not fully backward compatible with DIVAR IP 2000 and DIVAR IP 5000. Upgrading cameras to FW 6.4 without to-be-released firmware upgrades for DIVAR IP 2000 and DIVAR IP 5000 may cause configuration problems and possibly stop recording.

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.
- Cameras running FW 7.50 are only compatible with DIVAR network / hybrid FW 3.0.0 and higher. Compatibility with earlier DIVAR network / hybrid firmware can be obtained by re-enabling basic authentication or by using HTTPS.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

Miscellaneous

- 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 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.
- 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.
- Please take note that, whenever you change the application variant, the camera resets to factory defaults.
- Analogue output does not support 90° and 270° rotation.
- AVIOTEC cameras only support 180° rotation.
- 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.
- RCP and HTTP commands from ATSL script use HTTP digest authentication. Receivers only supporting basic authentication are no more supported.
- Audio back-channel in Chrome browser may be delayed when using an unsecure or unaccepted HTTPS certificate.

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



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

8 Previous Revisions

8.1 Changes with 6.61.0025

- AVIOTEC IP starlight 8000 is covered again with this release.
- An issue is fixed where VCA counters were reset when VCA editing was started.
- An issue with a broken certificate chain in the “originally Bosch manufactured” certificate used for HTTPS by default has been fixed. Corrupt certificates will be repaired.

8.2 New Features with 6.60.0065

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.

ONVIF

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

Miscellaneous

- Genetec Stratocast cloud is supported.
- 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			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.3 Changes with 6.60.0065

- 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.

8.4 Changes with 6.51.0028

- This version includes a fix for a recently discovered security vulnerability CVE-2018-19036. 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 BOSCH-2018-1202-BT.

8.5 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.
- Lens Wizard issue fixed for DINION IP starlight 8000 MP in combination with a LVF-5005N-S1250 lens



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

8.6 New Features with 6.50.0128

- **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.

- **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**

- Current gain value is visualized in video preview window.
- 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.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.7 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.
- 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.

8.8 New Features with FW 6.43.0027

- 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.

8.9 Changes with FW 6.43.0027

- Improvements on Multipathing support for storage devices.
- Various smaller issues have been fixed.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.10 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.
- 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.

8.11 Changes with FW 6.41.0037

- Various smaller issues have been fixed.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

8.12 New Features with FW 6.40.0240

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 80% but are strongly scene-dependent.
- Intelligent Streaming is enabled by default in medium setting.

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.
A downgrade to a non-signed firmware is not possible anymore.
- 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.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

- 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.
- 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.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

Imaging

- 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.

Miscellaneous

- SMTP port is now configurable via web interface.
- Multipathing support for storage devices.
- User name from certificate for EAP-TLS is used as EAP identity, if provided.
- Cameras can connect to the CBS Remote Portal installer service.
- 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.

8.13 Changes with FW 6.40.0240

- Installation Code has been enhanced with a block for crypto-coprocessor version indicators. The length of the Installation Code has been extended to 48 digits instead of only 44 digits.
- Improved certificate parser to support more attributes used e.g. by various mail providers.



From		Nuremberg
BT-SC/ETP-MKP1	Product Management	28.08.2019

8.14 New Features with FW 6.32.0111

Security

- Strengthened password policy:
 - New passwords must now be a minimum of 8 characters including special characters.
 - Passwords are continuously demanded; message cannot be hidden anymore.
- For full support of HSTS, an option “HSTS plus HTTP redirection” has been added.
- Fallback to TLS 1.0 can be disabled.

VCA

- JPEG with VCA overlay is now also available in full screen view.

For details on VCA 6.30 please refer to the release notes of Intelligent Video Analytics.

Miscellaneous

- Improved user interface for 802.1x settings. Interface shows an EAP-MD5 password field and lists the EAP-TLS certificates with a link to the certificate store.
- Security coprocessor (TPM) version is listed in system overview.
- Preposition widget on Live page can be completely disabled in Web appearance settings.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.15 Changes with FW 6.32.0111

- Limited frame rate stream capability names are presenting the frame rate as “skip” value, which is used as divisor in relation to the base frame rate.
A value “skip 5” results e.g. in 12 fps if base frame rate is set to 60 fps, or in 5 fps if base frame rate is set to 25 fps.
- In preparation for ONVIF Profile Q support, planned for next major firmware release, the default setting for Automatic IPv4 address assignment has changed from “On” to “On plus Link-Local”, a setting that had already been in the option list before.
Though this might seem a small change, it may have an impact:
The former default IP address 192.168.0.1 will virtually become obsolete.
Instead, the camera will assign itself an auto-IP address out of the range 169.254.1.0 to 169.254.254.255 as long as there is no other IP address assigned by a DHCP server.
(https://en.wikipedia.org/wiki/Link-local_address)
The advantage is that there are no more duplicate IP addresses, which is considered prohibited in a network.
- VCA overlays are drawn after scaling to improve visibility.
- An issue has been fixed where the maintenance log could not be downloaded.
- An issue has been fixed where the wrong SD card recording status was displayed.
- A security leak, which allowed to extract critical data from the device, has been fixed.
- A problem with incorrect time zone info in recording packets causing gaps in timeline has been fixed.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.16 New Features with FW 6.30.0140

Security

- The user management has been extended to allow free assignment of usernames. Each user can be assigned a user group representing live, user, or service level.
- New user management system allows to dynamically create a user for whom the password can be treated as token. Also timeout before user account expires is possible.
- Token-based authentication implemented to allow user management based on communication with Microsoft Active Directory Federation Services.
- Secure FTP connection (FTP over TLS) is implemented.
- ICMP redirect messages are not accepted anymore by default. Acceptance can be re-enabled via RCP+ command, if needed.
- Video authentication is now also possible on RTSP streaming. It can be enabled with CGI parameter 'auth=1' which requests picture info packets (payload type 97).

Recording

- Recording to iSCSI now supports LUN size up to 64 TB.
- A PTZ preposition can be stored in a recording profile, allowing to record only a 'region of interest' (ROI) of the full image.

ONVIF

- ONVIF encoder profile settings can be verified via http://<ipaddress>/onvif_encoder_profiles.
- Manual focus and iris control is now supported via ONVIF command.
- Tamper detection alarms are now forwarded to and included in ONVIF event services.

Video Fire Detection

- Automatic mask detection has been added to AVIOTEC IP starlight 8000 camera.
- Relay 1 automatically follows video fire detection alarm on AVIOTEC IP starlight 8000 camera.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

VCA

- Web page layout has been improved for better usability and larger video for configuration.
- Video analytics now fully support 16 tasks in RCP+ and IVA Task Script Language.
- JPEGs can now include VCA overlays in Live page, alarm e-mails and JPEG Posting.
For JPEG snapshot a new query parameter 'VCAOverlay' can be added to the URL, e.g.
`http://<ipaddress>/snap.jpg?VCAOverlay=1`.
- Video can now be paused during VCA configuration.
- Reference image is now stored as JPEG instead of TIFF for broader compatibility.
- Tamper detection "too bright / too dark" was no more functional due to too high dynamic on our cameras.

To solve this issue, sliders for the brightness level have been added for manual adjustment.

For details on VCA 6.30 please refer to the release notes of Essential Video Analytics or Intelligent Video Analytics.

Miscellaneous

- HTML5 video tag is used to display a continuous MP4 video file from the camera on browsers not supporting NPAPI plug-ins (MPEG-ActiveX) like Firefox, Chrome and MS Edge.
- A "Links" section in the main navigation (blue top bar) has been added, leading to a DownloadStore page providing latest tools, apps and supportive software.
- Unicode characters are now also possible on all configuration strings.
- Time server IP address can be accepted to be overwritten by DHCP.
- Display of preposition widget on Live page can be configured.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.17 Changes with FW 6.30.0140

- “Image too noisy” is removed as it never occurs due to the high dynamic of image processing.
- Downscaled images 4CIF/CIF are now encoded as PAL resolution (704x576 resp. 352x288) when camera is set to 25/50 fps base frame rate.
- Fixed a potential recording issue which could cause recording to stop due to insufficient storage error handling under rare error conditions, like e.g. massive irregular network connection interrupts to storage system.

8.18 New Features with FW 6.22.0008

- A high-resolution/limited-frame-rate capability has been introduced for stream 2 on various cameras.

8.19 Changes with FW 6.22.0008

- Writing to ONVIF MaxFrameRate is now possible to improve compatibility with clients not using encoding interval. Written values are presented in same format when read.
- The microphone can be permanently blocked, irreversibly for users, via a global license key to allow use of the cameras in countries where audio input is legally not permitted.
License type 2:
 - 12-01.63.01-380AAC7E-B71E0D3D-6ADCC50C-6F296E08-F3AFBB71

The permanent block can only be lifted by releasing this license via our service organization. If not legally required to completely disable the audio function, audio can simply be switched off, or the microphone sensitivity set to zero, always reversible through configuration.

The global license type 1 as being presented with release notes of FW 6.00.0079 is not functional on CPP6 platform devices.



From			Nuremberg
BT-SC/ETP-MKP1	Product Management		28.08.2019

8.20 New Features with FW 6.21.0008

- DINION IP panoramic 7000 has been enhanced with a high-resolution/low-frame-rate mode for stream 2, providing 2640x2640 pixels at 5 frames per second while the first stream provides the same resolution at full frame rate.

8.21 Changes with FW 6.21.0008

- An issue with fragmented EAP-TLS transfer has been fixed, allowing support for Microsoft Windows NPS and RADIUS.
- An issue with ONVIF Analytics Service has been fixed.
- GUI translations and some embedded help files have been updated.
- Wrong wording on time protocol settings has been fixed.

Note:

To avoid a potential timing issue with older bootloader firmware that, in combination with the actual FW 6.21 load pattern, may very rarely lead to a camera reboot, this firmware release includes an updated bootloader that is applied if an outdated bootloader is being detected during firmware upgrade, opening a short window of approximately one second of vulnerability against power loss.

Be especially careful that the camera does not lose power during firmware upgrade.



From

BT-SC/ETP-MKP1

Product Management

Nuremberg

28.08.2019

8.22 New Features with 6.20.0089

Cameras

- P-iris control for DINION IP 8000 cameras supported.
- Support for Video Fire Detection camera AVIOTEC.

Security

- Support of TLS 1.2 with updated cypher suites including AES 256 encryption.
- Device access security has been improved by:
 - Implementation of signed time synchronization
 - Signature-protected password unlock procedure
 - Telnet over HTML5 web sockets in browser, using secure TLS connection
 - Throttling of wrong password entries
 - Urging user towards setting a device password, strength meter provided
- Firmware, which is signed with a private certificate, is authenticated before transfer to Flash to ensure a secure firmware upload.
- Certificate handling has been enhanced by:
 - Auto-generation of self-signed certificates for SSL
 - User-defined creation of self-signed certificates
 - Possible upload of certificates with encrypted private keys
 - Improved recorded video authentication without PKI required
 - Storage and retrieval of certificate in recording for verifying signed video
- Web GUI security has been improved to prevent Cross-Site-Scripting in Browser.
- Use of secure connections can be advertised via support of HSTS.

8.23 Changes with 6.20.0089

- 56-bit encryption disabled for secure connections to increase minimum security level.
- Telnet service (system console) is now disabled by default.