Security Systems

BOSCH

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Release Letter

Products:	*H.264 Firmware for* *CPP6 UHD/MP cameras*
Version:	*7.89.0045*

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

1 General

This firmware release is a maintenance release based on FW 7.89.0045.
It is an upgrade for CPP6 based cameras only.

Firmware release 7.84 is the last feature release for CPP6 cameras.
Firmware will be maintained for field and security issues.

Changes since last release are marked in blue.

BOSCH and the symbol are registered trademarks of Robert Bosch GmbH, Germany

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

2   Applicable products:

- DINION IP starlight 8000 12MP
- DINION IP ultra 8000 12MP
- DINION IP ultra 8000 12MP with C/CS mount telephoto lens
- FLEXIDOME IP panoramic 7000 12MP 180
- FLEXIDOME IP panoramic 7000 12MP 360
- FLEXIDOME IP panoramic 7000 12MP 180 IVA
- FLEXIDOME IP panoramic 7000 12MP 360 IVA
- FLEXIDOME IP panoramic 6000 12MP 180
- FLEXIDOME IP panoramic 6000 12MP 360
- FLEXIDOME IP panoramic 6000 12MP 180 IVA
- FLEXIDOME IP panoramic 6000 12MP 360 IVA

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

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 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 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 or higher 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. This can be achieved by uploading the combined firmware file multiple times until the required firmware version is installed.

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 the Bosch certificate authority (CA).
Enrollment of the certificates in production is asynchronous to this firmware release.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

3.4   Secure Element ("TPM")

All CPP7 devices incorporate a secure 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.

3.5   Open-Source Software

Bosch Security Systems is 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, please visit http://www.boschsecurity.com/oss .

3.6   NTCIP

Cameras prepared for Intelligent Traffic System (ITS) applications support NTCIP protocol, which was updated to meet NTCIP 1205 v01 AMENDMENT 1 in November 2020 as from firmware 7.72.0008 onwards. This update may break compatibility with outdated ITS software.

3.7   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.
AVIOTEC firmware is not content of this combined firmware file.

---

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

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

4 New Features

- Traditional Chinese language and characters have been added to the UI of the camera web page; however, this implementation does not include the language as an option for On-Screen Display (OSD).

5   Changes

- We've made some updates to the firmware infrastructure for object geolocation on moving cameras. Now, it delivers data even while the camera is panning or moving. It is not required anymore to be in a 3D tracking mode on a pre-position. Unlike before, the system now considers global calibration when the camera is not in its pre-positions, such as during intelligent tracking. The position accuracy decreases with object distance and PTZ movement, 3D tracking at a calibrated pre-position should be used for maximum accuracy. Due to an issue in Configuration Manager 7.71, a global calibration has to be repeated if a pre-position was calibrated.

- Default settings have been changed for the RCP+, HTTP, RTSP, RCP, SNMP, ISCSI, UNPN, and NTP ports. These will become effective with new cameras and by factory-defaulting a camera but will not be affected by upgrading firmware to avoid functional interrupts of existing installations. For detailed information on "Security by Default" please refer to our tech note at https://www.boschsecurity.com/xc/en/solutions/video-systems/data-security/#downloads .

- The issue with incorrectly displayed parameters of the bandwidth throttle settings on the web GUI has been resolved.

- Improved recorder initialization during device boot-up to ensure proper signalization and normal operation.

- Fixed issue where recording configuration based on VCA Event Trigger was not set after a camera reboot, resulting in recordings not starting.

- Fixed medium and high-level vulnerabilities in a third-party library.

- Changes were made to the architecture of recording communication to provide a more robust solution to our customers and reduce the likelihood of recording gaps in atypical circumstances.

- Fixed an issue that prevented some devices from displaying the dashboard while connected to the Remote Portal UI.

- Fixed issue where uploading a config file failed when the service password contained the character "%".

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

6   System Requirements

- Web Browsers:
    - o   Google Chrome
    - o   Microsoft Internet Explorer 11 or higher
    - o   Microsoft Edge (Chromium based)
    - o   Mozilla Firefox
- DirectX 11
- MPEG-ActiveX 6.34 or newer (for IE only)
- Configuration Manager 7.50 or newer

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

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 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.

- 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.

- 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.

- RTSP live stream via media stream library is not possible with Safari browser on iOS/iPad.

- Password length for 'service', 'user' and 'live' is limited to 19 characters. Password length for all other users defined in one of the user groups is limited to 31 characters.

- Due to the recently introduced security feature 'HTTP referrer check' the browser connection will not be automatically redirected after an IP address change.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Automatic Network Replenishment (ANR)

- Due to its nature of internal and external recording and an internal replay in addition, ANR puts a high load to a camera. Measures must be taken to ensure the camera is not running into an overload situation, e. g. by reducing bitrates. Especially with FLEXIDOME IP panoramic cameras, running in onboard dewarping mode and recording more than a single line, such an overload situation might be reached easily without careful settings.

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.

- 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

    o EAP-TLS with client authentication

    o TLS-Time with client authentication

    o 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.

- More complex ciphers require more processing time during connection handshake, slowing down the connection setup.

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.

- 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.

- Multicast streaming must not be used in combination with bandwidth throttling or treated very carefully. The same is valid for any other bitrate-creating source or function inside the camera, e. g. recording or exports. It must be ensured that the average total bitrate created by the camera does not exceed the available and configured bandwidth, otherwise data may be lost, or the camera may behave unresponsive.

- When multicast streaming is used with encryption via RTSPS/SRTP, accessing the multicast stream unencrypted is no more possible as the same multicast group is used.

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.

From			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

- 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

- With FW upgraded from 6.32.xxx to version 6.41 or higher, the IVA calibration data get lost.

- "VCA configuration" user group and its assignment need to be configured and used in Configuration Manager 7.20 only

- 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,

- After firmware upgrade to version 6.10 the minimum object size seems being reset when editing 'motion in field' task. As a proposed workaround check minimum object size and correct value as applicable.

- IVA configuration is lost during upgrade from FW 5.9x to FW 6.1x.

- VCA shapes are not synchronized with video when using the open-source JavaScript library for decoding.

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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.

- 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 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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.

- FLEXIDOME IP panoramic 7000 cameras may run into packet loss with on-board dewarping and ANR activated. Encoder profiles may have to be adapted to avoid memory excess.

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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- When recording to RAM and 'Export from memory' the recording status page may not show the correct recording status.

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 7.10 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.

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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- After changing the application variant in the Installer menu, the camera reboots and starts counting down time until it tries to reconnect to the rebooted camera, IE doesn't always reconnect so it keeps showing only the waiting circle (named hourglass in earlier times) In this case resetting the browser with ctrl+F5 will re-establish connection with the camera.

- 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.

- FLEXIDOME IP panoramic 7000 and 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.

- Audio back-channel in Chrome browser may be delayed when using an unsecure or unaccepted HTTPS certificate.

- RCP commands CONF_DATE_MONTH, CONF_DATE_DAY and CONF_DATE_YEAR can be read as P_STRING or as T_OCTET (year as T_WORD) but can only be written as T_OCTET (T_WORD for year), not as P_STRING.

- Currently only convex polygons privacy masks are supported.

- When using the GetVideoEncoderConfiguration command to fetch encoder configurations with known tokens, the system response will uniformly indicate either H.264 or H.265 encoding. This occurs independent of potential variations in configurations among streams.

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

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

8   Previous Revisions

8.1   New Feature with 7.89.0030

- The date format for display stamping is enhanced to allow also French date format.

- The enhanced settings for bandwidth throttling now allow better adaptation to the network's transmission and buffering capabilities.

- The certificates web page now also shows the hash algorithm used on certificates.

- A 'video loss' error is introduced for internal fault situations that disrupt valid video throughout the processing chain.

- We've introduced an enhanced feature for camera naming. For CPP7 cameras, the firmware is ready to receive up to 6 different lines, each containing 31 characters. However, many clients, like VMSs or Cloud services, only have one field for configuring camera names in their UI, limiting our customers to utilize only one of the lines available on the firmware of our cameras when configuring via their clients.

  With the recent change, clients that only offer one field for camera names in their UI are now allowed to input up to 64 characters in their single-line camera name fields, instead of 31 as previously.

  The firmware enhancements will distribute the longer names across multiple lines, optimizing display within the constraints of a one-line user interface. The camera names displayed by our cameras will continue to contain 31 characters. This change should not affect integration with existing UIs; no additional configuration is required.

8.2   Changes with 7.89.0030

- An issue in which the camera stopped recording during a security scan was identified and fixed with this release.

- As best practice to reduce potential attack surfaces and limit the exposure of sensitive services we are changing the default behavior of the cameras by disabling the initial configuration of NTP server port.

- As best practice to increase the default security, alarm task scripts using HTTP commands will now default to use HTTPS. Connections to unsecure devices need to explicitly address '*Port(HTTP)*' and set '*SSL(false)*'. Scripts are not automatically converted and may need to be enhanced.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- We have successfully addressed multiple vulnerabilities identified in the libraries used within our firmware. While additional protective measures are in place, we strongly encourage users to upgrade to the latest firmware.

- An issue with occasionally empty ONVIF tags is fixed.

- An issue with ONVIF command GetAudioEncoderConfigurationOptions is fixed.

- SNMP trap list has been cleaned up from unused traps and enhanced by a power supply trap on applicable cameras.

- This release resolves a multicast streaming issue causing camera disconnections and live video interruptions, notably during sequential or rotational presentation of multiple cameras by VMS or other systems.

- An issue with web pages sporadically loading slowly is fixed.

- Addressed an issue related to the EAP-TLS authentication process. Previously, the camera transmitted an inaccurate "Cipher Suite" list via the client message, leading to potential confusion regarding supported cypher suites for specific firmware versions.

8.1 New Features with 7.87.0029

- A banner has been introduced which allows to provide a system use notification to a user before authenticating.
- A switch has been added to directly activate or deactivate VCA without requiring the configuration plug-in.

8.2 Changes with 7.87.0029

- An issue is fixed where the audio recording format was disabled and could not be changed after recording was stopped.
- An issue is fixed where the web interface was lacking responsiveness when HTTP was deactivated.
- An issue, apparent in FW 7.81 and higher, is fixed where video via RTSP over TCP sporadically appears black after recovering from a network interruption.
- An issue is fixed where a camera could be driven into constant overload due to non-closed connections, requiring a restart to recover.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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 CONF_ALARM_OVERVIEW did not return proper state flags for VCA external simple states.
- Improved overall security by updating 3rd party components due to regular security maintenance.
- Some legacy RCP+ commands received a higher authentication level to further reduce the attack surface and improve security by default.

8.3 New Features with 7.86.0019

- The video.mp4 URL now accepts parameters to stream using RTSP, and also to access stream 2.
- The RCP command CONF_ALARM_OVERVIEW now includes recording errors and SD card mounting states.

8.4 Changes with 7.86.0019

- An issue with manual iris or focus control via ONVIF is fixed.
- An issue with certain VCA events erroneously reporting 'signal loss' via ONVIF is fixed.
- IVA detection results improved by pre-determined lens distortion models for DINION IP thermal 8000.
- An issue, introduced with firmware 7.85, where putting the camera in corridor mode caused continuous reboots, is fixed.
- Multiple vulnerabilities in 3rd party libraries that were identified during UL 2900-3-2 certification are fixed.
- An issue is fixed where 802.1x authentication failed when EAP-PEAP is requested prior to EAP-TLS.
- An issue is fixed where necessary network settings were set to default on application variant switching, now including hostname and unit name.

8.5 New Features with 7.85.0016

- Cipher suites have been extended to provide higher security by adding the following ciphers:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

BOSCH and the symbol are registered trademarks of Robert Bosch GmbH, Germany

      o   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- DNS resolution has been extended to also cover URLs in FTP accounts.

- On cameras with value level 7000 and higher, Camera Trainer is now enabled without requiring a license.

8.6 Changes with 7.85.0016

- An issue is fixed where the video stream is interrupted when an encoder profile is changed, e. g. due to adaptation for event recording by a DIVAR hybrid or network.

- An issue, introduced with firmware 7.81, is fixed where the OSD font size is too small (half height) when resolution is set to 1080p or higher.

- An issue is fixed by a better description in the web user interface that a certificate signing request requires the country code instead of the country name.

- An issue is fixed in the ONVIF metadata translation where latitude and longitude values were swapped.

8.7 New Features with 7.84.0023

- Bandwidth throttling has been added to allow the camera being installed on networks with limited throughput capacity. This allows a single video stream to adapt to a limited network, avoiding temporary overload of the transmission equipment due to transmission bursts. The available bandwidth can be configured as kbps values in the Ethernet section of the Network Access menu. The camera will then limit its data generation on the network to this maximum Ethernet transmission value to avoid bursts in the network traffic. The Ethernet input on the camera is not limited.

- The Network Access menu has been separated for IPv4 and IPv6 addresses. IPv4 and IPv6 can now separately be configured and activated.

- IP filter entries have been extended to allow up to 20 IP addresses or ranges.

- For certificate-based network authentication, and in case of an unsubstantiated time base, the camera may assume its time from the overlapping validity periods in the EAP-TLS certificates, if this feature is enabled via the camera's settings.
  With valid certificates, this will allow the camera to connect to the network even in case of an invalid system time due to e. g. a longer power loss.

8.8 Changes with 7.84.0023

- An issue is fixed where insufficient memory allocation caused sporadic unresponsiveness of a camera's web user interface.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- An issue is fixed where a wrong color was applied to alarm-triggered bounding boxes when using Camera Trainer.

8.9   Changes with 7.83.0027

- DNS resolution is now also supported for the ONVIF Profile M Event Broker URL.

- An issue is fixed where Camera Trainer showed a wrong class number.

- An issue is fixed where a certificate-based user could not be created via the web interface.

8.10 New Features with 7.82.0025

- Firmware version 7.81 introduced an additional check on the HTTP referrer, an improvement to reduce the vulnerability for Cross Site Request Forgery (CSRF) attacks. For backward compatibility with legacy clients, applicable where alternative measures are put in place, this check can be disabled via the user interface.

- For TLS usage and 802.1x certificate verification, SHA384 hashing is now supported.

- For 802.1x, server certificate verification can be disabled, when a specific global license is installed. A server certificate is then no more required or will not be considered if installed. The license key to disable the server certificate verification is:
  - 12-01.48.01-3C683BD3-54B029FA-7E5ADCC5-6F29CD7F-55B0528E

  The license key to enable the server certificate verification is:
  - 12-01.48.00-EE2A44C1-EE5CC9E0-0BB6FBBD-2B582636-2CBBB1FC

8.11 Changes with 7.82.0025

- An issue, introduced with FW 7.81, where the ONVIF command GetEventProperties did not show the old IVA events nor the new RuleEngine events anymore, is fixed.
  With FW 7.82 it will show the configured RuleEngine events.
  A proper implementation should use the ONVIF commands GetRules and GetSupportedRules for a comprehensive rule presentation.

- An issue with internal adaptation of the iSCSI MSS when the MTU value is changed is fixed.

- An issue where the camera did not receive an IP address via DHCP after 802.1x authentication is completed is fixed.

- An issue with increased response time for ONVIF Profile M event handling via MQTT is fixed.

- Due to a change in the Dropbox API, the support for Dropbox will be deprecated.
  We are working on providing an alternative, which will be announced with a future firmware version.

From			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

8.12 New Features with 7.81.0060

- Support of ONVIF Profile M, including MQTT event forwarding.
- China standard GB/T 28181 has been put under a global license. When GB/T 28181 shall not be available it can be disabled with a global license key. This is irreversible for customers and can only be reversed via service and repair. The license also prohibits downgrading to earlier versions which provided GB/T 28181 as standard feature.
  License key to disable GB/T 28181 is:
  - o 22-01.47.01-BF365391-21ABCB3D-28699CE4-3BD3AB09-FE25CD61
- New Western Digital industrial SD cards with lifespan monitoring are supported.
- Privacy masks can be enabled and disabled via a single switch command.
- Audio alarm menu has been enhanced to allow shaping for certain audio occurrences.
  - o Alarm thresholds are separated per frequency band.
  - o Sensitivity can also be set separately per frequency band, if required.
- Dashboard and dashboard export have been enhanced by iSCSI information and various other settings.
- Flexible person shape can be selected in 3D tracking.

8.13 Changes with 7.81.0060

- Selection of audio encoding (G.711, L16, AAC) and AAC modes (48 kbps, 80 kbps) are now separated. Indication is given that AAC 80 kbps is not functional with the livepage via RTSP.
- SNMP MIB has been extended by manufacturer name and serial number.
- An issue where alarm message text was not written to the correct metadata layer is fixed.
- An issue with IVA events not being forwarded via ONVIF is fixed.
- An issue with privacy mask "Auto" always being grey is fixed.
- Basemode names are auto-generated from the configured resolutions.
- An issue with wrong name stamping on lines 2 and 3 is fixed.

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			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

8.14 Changes with 7.80.0129

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

For more details refer to our Security Advisory BOSCH-SA-478243-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 with unauthenticated information extraction is fixed (CVE-2021-23847) (already fixed in 7.80.0128).
- An issue with reflected XSS in URL handler is fixed (CVE-2021-23848).
- An issue with denial of service due to invalid web parameter is fixed (CVE-2021-23852).
- An issue with improper input validation of HTTP header is fixed (CVE-2021-23853).
- An issue with reflected XSS in page parameter is fixed (CVE-2021-23854).

8.15 Changes with 7.80.0128

- An important fix was made to improve the overall security of the firmware.

8.16 Changes with 7.80.0127

- Usability improvements
  - Reboot request info is displayed when a license has been installed.
  - In case a Remote Portal user's login credentials are associated with multiple company accounts in Bosch Remote Portal, a message will be displayed in order to make sure that a "default commissioning company" will be defined. Otherwise a successful registration will be prevented.
- An issue is fixed where MSS and MTU settings may have come out of sync. During a write to the MTU size, the MSS is now checked and, if fragmentation would occur, would implicitly be adjusted to a value of MTU-40, before the MTU is reduced.
- An issue is fixed on panoramic cameras where GB/T 28181 alarm event notification was missing.

8.17 New features with 7.70.0126

Remote Portal

- Remote Portal registration has moved from advanced network settings to the new Cloud services section within the new Connectivity top menu

BOSCH and the symbol are registered trademarks of Robert Bosch GmbH, Germany

- Faster access to Remote Portal after device registration via "Visit Remote Portal" link
- Polished Remote Portal registration menu
- DNS/gateway check introduced to static IP addresses

VCA

- New (fourth) user group for "VCA configuration" introduced
    - this user group has the privilege to just configure VCA
    - it is possible to assign a user (created by the system integrator) to the new user group "VCA configuration"
    - Configuration Manager 7.20 is to be used only

ONVIF

- Increased resolution of absolute position coordinates

Network

- IPv6 Multicast support for RTSP and SRTP
- Accounts, DynDNS, and Cloud services were moved to the new Connectivity top menu

Miscellaneous

- Updated icon design in web interface
- Interfaces menu was integrated into Alarm menu
- Possibility to integrate milliseconds into JPEG filenames
- RCP+ documentation extended by Common Product Platform (CPP) support on command level
- Gain control can be de- (activated)
- P-Iris support for DINION 6000 / 7000
- HTML5 based PTZ control in browser

8.18 Changes with 7.70.0126

Fixes issues regarding

- PTZ functionality in 7.61
- Display of IVA rules in BVMS Configuration Client
- Access to reference image stream in BVMS
- IP Camera not able to write to iSCSI when SD card failed
- inaccessible recording when special character "%" was part of password
- periodic brightness alternation (fixed since 7.61)

8.19 Changes with 7.61.0023

- An issue with UDP multicast no longer working after upgrade to FW 7.60 is fixed.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- An issue is fixed where high-frequent motion recording with 10 seconds pre-alarm in RAM may stop sporadically.
- An issue, introduced with FW 7.60, is fixed where ANR was only doing alarm recording though being configured for continuous recording.

8.20 New Features with 7.60.0118

VCA

- In web browsers that do not support MPEG-ActiveX, VCA configuration is only possible via Configuration Manager. An info message to use Configuration Manager is presented, with a hint where to get Configuration Manager if it is not installed.
- Object filters 'height' and 'width', which are more intuitive than 'area' and 'aspect ratio', have been added.
- Metadata can be filtered to exclude certain not required content. This may help especially on low-bandwidth links, or to reduce load on successive algorithms and services.
- A new, more flexible aggregation time mechanism has been added to the rule engine script. This mechanism supersedes the old aggregation time setting (RCP command), which is applied after the rule engine globally. For backward compatibility, existing use of old aggregation time is kept on firmware update, otherwise removed from user interface.
- Gyro sensor, if available, has been added as option for camera tamper detection.

Miscellaneous

- The RTSPS service has been added to the Network Services page.
- Firmware upload is now possible via ONVIF.
- For Stratocast cloud access, the global motion/VCA alarm is forwarded via Stratocast protocol when VCA is activated, automatically creating a 'detect any object' rule.
- For Stratocast cloud access, Intelligent Streaming is now automatically activated.

8.21 Changes with 7.60.0118

- Due to switching from basic authentication to digest authentication only with the previous firmware release FW 7.50, backward compatibility was lost with devices in the field that only accept basic authentication, putting installed systems out of function.
  To solve this, the authentication method can be specified via a parameter for outgoing connections in Alarm Task Scripting. Refer to the updated ATSL manual.
- Audio alarm has been assigned with a default name.
- An issue is fixed where recording span events were reported as errors while being normal operational events.
- An issue of the revoked build 116, which could have caused recording to not restart after reboot, is fixed.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Note:
   Due to the changes in the recording engine, recording encryption is no more compatible with released VRM versions, and thus recording encryption must not be enabled. Otherwise, encrypted recordings will not be retrievable anymore until upgrading to a new VRM version.

8.22 New Features with 7.50.0079

- 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.
- 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.

8.23 Changes with 7.50.0079

- 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.
- Stream 1 resolution on FLEXIDOME IP panoramic 6000/7000 can now also be set to 1440x1440 pixels.

8.24 New Features with 7.10.0074

- 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.

8.25 Changes with 7.10.0074

- 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.

8.26 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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.

8.27 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.

8.28 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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.

8.29 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.

8.30 Changes with 6.51.0026

- Password reset mechanism changed
  o 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.
  o 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

8.31 New Features with 6.50.0128

- **Intelligent Streaming enhancements**
  o 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.
  o 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:
  o Sony
  o SanDisk
  o 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.

From			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

- **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.

8.32 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.

8.33 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.

8.34 Changes with FW 6.43.0027

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

8.35 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.

8.36 Changes with FW 6.41.0037

- Various smaller issues have been fixed.

8.37 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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Security

- Password enforcement

  o New cameras with this firmware installed will only become operable after the password for the administration level (user "service") has been assigned.

  o Other users "user" and "live" will only become accessible after the administrator assigned passwords to them.

  o 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

  o The payload on an iSCSI drive is encrypted using a symmetric XTS encryption scheme (block encryption).

  o 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".

  o Payload encryption is possible on SD cards as well as on external iSCSI storage.

  o A client that shall be allowed to replay this footage must have its cert/key registered and activated.

  o 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

  o New alternative SNMP support provides encryption and authentication. This new service will provide pure MIB-II access.

  o 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

  o The configuration file is encrypted and password-protected before download.

  o The user as the owner of this configuration file is prompted for the password.

  o The password is required when the configuration file is uploaded to a camera.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- o 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:
  - o A more structured output including timestamp, severity and module sources
  - o Search and filtering for specific events via web user interface
  - o Direct output to a syslog server
  - o 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
  - o Multiple trusted issuers are now allowed for client certificate authentication.
  - o An option to not wipe the SXI certificate when a factory default is issued has been added.

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
  - o Recording start and control has been added.
  - o Recording search and replay functionality has been added.
  - o Tested with ONVIF Device Test Tool 16.07 SR2 rev. 617.

Miscellaneous
- SMTP port is now configurable via web interface.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.
- 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.

8.38 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.

8.39 New Features with FW 6.32.0111

Security

- Strengthened password policy:
  - o New passwords must now be a minimum of 8 characters including special characters.
  - o 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

- 6000 series cameras support Essential Video Analytics.
- 7000 series cameras support Intelligent Video Analytics.
- 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 Essential Video Analytics or 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.

8.40 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.

8.41 New Features with FW 6.30.0140

Imaging

- Flexible video input orientation handling has been added, including mirror and rotate (90°, 180° and 270°). This allows corridor view applications using full resolution.

- [CPP4] Flexible video input orientation handling has been added, including mirroring and 180° rotation. This allows to correct the view of e.g. panoramic cameras if wall-mounted headfirst.

- FLEXIDOME IP panoramic 7000 cameras now allow reduced base frame rate of 12.5 fps to increase streaming capabilities for the second stream.

- [CPP4] A 1.3 MP application variant is now selectable for DINION IP bullet 4000 cameras.

From			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

- [CPP7] Built-in gyro sensor is supported for automatic orientation detection.

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.

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.
- Intelligent Tracking is now also available on cameras 2 and 3 of FLEXIDOME IP panoramic 7000 cameras in dewarping mode.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

- 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.

8.42 Changes with FW 6.30.0140

- Due to the introduction of image rotation, the high-resolution/low-framerate capability for
  stream 2 is conflicting and thus no more available on FLEXIDOME IP panoramic 7000
  cameras.

- "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.

- Removed non-supported mirroring option from FLEXIDOME IP panoramic 7000 MP cameras
  in dewarping mode.

8.43 New Features with FW 6.22.0008

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

From			Nuremberg	
BT-VS/MKP-XPT	Product Management		07.05.2024	

8.44 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:
  - o 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.

8.45 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.

8.46 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.

8.47 New Features with 6.20.0089

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Cameras

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

Security

- Support of TLS 1.2 with updated cypher suites including AES 256 encryption.
- Device access security has been improved by:
  - o Implementation of signed time synchronization
  - o Signature-protected password unlock procedure
  - o Telnet over HTML5 web sockets in browser, using secure TLS connection
  - o Throttling of wrong password entries
  - o 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:
  - o Auto-generation of self-signed certificates for SSL
  - o User-defined creation of self-signed certificates
  - o Possible upload of certificates with encrypted private keys
  - o Improved recorded video authentication without PKI required
  - o 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.

8.48 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.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

8.49 New Features with 6.11.0019

Imaging Enhancements

- On FLEXIDOME IP panoramic 7000 cameras user can choose via application variant in installer menu between edge dewarping inside the camera or client-side dewarping on an external platform.
- On-board dewarping on FLEXIDOME IP panoramic 7000 cameras with realization of virtual cameras, providing different types of dewarped scene representations: ePTZ, Panoramic, Double Panoramic, Quad, and Corridor

ONVIF

- Conformance was tested using recent ONVIF test tool 14.12.

8.50 Changes with 6.11.0019

- Adding small improvements and error corrections.
- Replay not working in BVC and BVMS clients for negative time zones has been fixed.

8.51 New Features with 6.10.0129

Graphical User Interface

- Tours re-arranged onto single page and scheduler for preset tour and alarm rules added for moving cameras.
- Encoder quality regions can be configured on moving cameras' preset positions with up to 8 regions.
- Video export format can be preselected from Bosch format including metadata and generic MP4 format on LIVE page.

Imaging Enhancements

- Digital Zoom mode added to lens settings page.
- Setting migration keeps all the previous imaging settings after camera upgraded to new firmware. Please note: This is only applicable after firmware 6.10.

Security Enhancements

- Certificate Store for management and assignment of client and server side certificates.
- Preparation for Public Key Infrastructure (PKI), enabled via special license, has been added.
- 56-Bit DES cipher suite is disabled for TLS connection.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

IVA Enhancements

- Object classification of object types "upright person"," bike", "car", "truck" replaces head detection.

- Improved robustness to moving background (water, branches), shaking, bad weather, fast illumination changes, low-light conditions, mutual object occlusions and to detection of idle / removed objects. Scene conditions are automatically determined.

- Geolocation allows setting a camera's global coordinates. The position of the tracked objects in the respective coordinate system is added to metadata. Camera viewers can show the tracked objects on a map.

- Usability improvements allow for easier calibration and easier drawing of elements and masks, including support of polygons.

- MOTION+ configuration has been reworked. Eight MOTION+ alarm fields with up to 16 nodes can now be set. Areas can be removed from processing via VCA masks, which will then suppress metadata generation in these areas.

Note: For details and complete overview refer to release notes of IVA 6.10.

ONVIF Enhancements

- IVA events can be received via ONVIF messages.

- Overlay metadata can be received in ONVIF XML format.

- AUX commands can be sent via ONVIF messages.

- Conformance was tested using recent ONVIF test tool 14.12.

Miscellaneous

- Missing time zones added for Caracas, Newfoundland, Kathmandu, Yangon, Samoa and Kiritimati Island.

- Internal storage can be disabled and hidden via special license for certain LATAM countries. This license can only be cleared via technical service and support.

- An additional area in the flash memory, holding a file system to store specific files or data, has been implemented. This area can hold such like the enhanced Chinese character table or the FPGA image for IVA cameras running in 5:4 setup, certificates or configuration data.
  With FW 6.10 necessary files can be installed by uploading a supplementary firmware file. For successive firmware versions the sections will be recombined.

- A customer logo up to 128x128 pixels with a depth of 256 colors can be uploaded as BMP file to be displayed in the camera name block. Options for placement are left, right or logo only.

8.52 Changes with 6.10.0129

- IPv6 operational improvements, e.g. netmask extended to 64 bit.
- Reference image is deleted when device is set to factory default.
- Larger font used for display stamping creates better visibility on large resolution.
- Fix for recording status while pre-alarm recording in RAM

8.53 Changes with 6.01.0008

- Various small bug fixes and improvements.
- ONVIF conformance was tested using recent ONVIF test tool 14.12SR1.

8.54 Features with 6.00.0079

Image Processing

- Support of FLEXIDOME IP panoramic 7000 12MP 360° and 180° cameras.

New Web browser user interface

- A new style and new colors are being introduced, according to the latest Bosch User Interface Style Guide for Software User Interfaces. Together with usability improvements this provides a completely new and improved user experience.
- Easier navigation is possible due to the main topics in the blue bar in the header of the Web pages as well as icon-supported navigation through the configuration pages.
- Live and replay pages have been enhanced with more intuitive controls and a new timeline which is easier to handle and better recognizable.
- Live video preview is shown on most configuration pages whenever sufficient space available.
- Privacy masks, encoder quality regions and IVA fields can be drawn as polygons instead of rectangles, all with the same controls.
- No Java applets are used on the Web pages anymore.

IVA

- Object classification added with the classes "upright person", "bike", "car", "truck".
- Mounting position and angle of panoramic cameras can be added to aid calibration for dewarping in the client software.
- Geolocation parameters can be added which are passed into metadata. This allows management systems to directly position the camera, or objects tracked by this camera into a map.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Recording

- Automated Network Replenishment (ANR) 2.0 has been enhanced to provide more robustness against SD card failures, including the possibility to add alternative storages.
- ANR can be configured through the Web interface with a single click.
- In ANR mode, SD card fill level is shown on recording status page.
- SD cards are automatically detected, prepared for use, and recording started without configuration required. SD card is added to managed storage media even if not inserted.
- A storage system indicator icon has been added to the Web page's title, providing a quick indication about the health status of SD card recording by green, yellow, or red color.
- An alarm is created if recording stops, usable in Alarm Task Scripting.

Network

- Auto-IP assignment for IPv4 (aka Link local, APIPA) has been added as an alternative setting to pure DHCP. In this mode, if no DHCP server is responding after 10 seconds, a link-local address will be chosen.
- IPv6 stateless auto-configuration has been enabled to allow IPv6 routability. The Auto-IPv6 address is displayed in Web browser menu below the manual IPv6 address, but is not configurable.
- 802.1x has been enhanced by EAP/TLS using specific certificate. Certificates for client and server side can be uploaded to be used for authentication.
- After a network link is re-established EAPOL communication is initiated to restart 802.1x authentication even if the switch does not initiate this.
- Secure SMTP over Transport Layer Security (TLS/SSL) is supported according to RFC-3207. Connection is established using plain text on port 25; then TLS is negotiated with "StartTLS" command.

ONVIF conformance

- A timeout range for continuous move has been added.
- ONVIF GetDigitalInputs is now implemented.
- CONF_ONVIF_STREAM_URI_EX allows storing a stream URI extension that is appended to the ONVIF stream URI.
- ONVIF can be switched off, advantageous in installations that have native RCP integration to avoid accidental access through ONVIF clients. ONVIF remains enabled by default, of course.

From			Nuremberg
BT-VS/MKP-XPT	Product Management		07.05.2024

Miscellaneous

- Platform type (CPP) is now displayed in System Overview page.
- ~~The microphone can be permanently blocked via a global license key to allow use of the cameras in countries where audio input is legally not permitted.~~
  - ~~02-01.63.01-1E034A4F-B9A37665-B468CBAD-D8945403-6891D511~~
  ~~The permanent block can be lifted by releasing this license via our support organization.~~
- Filename definition in ATSL has been enhanced. Date elements can now be maintained separately.