From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

Release Letter

Products:	***H.264/H.265 Firmware for CPP7.3 HD/MP cameras***
Version:	***6.42**.0021*

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

1 General

This firmware release is a maintenance release based on FW 6.41.0037.
It is an upgrade for CPP7.3 based cameras only.

Changes since last release FW 6.41.0037 are marked in blue.

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

2 Applicable products:

- AUTODOME IP 4000i
- AUTODOME IP 5000i
- AUTODOME IP starlight 7000i
- DINION IP bullet 4000i
- DINION IP bullet 5000i
- DINION IP bullet 6000i
- FLEXIDOME IP 4000i
- FLEXIDOME IP 5000i
- FLEXIDOME IP starlight 8000i HD
- FLEXIDOME IP starlight 8000i 6MP
- FLEXIDOME IP ultra 8000i MP UHD
- MIC IP starlight 7000i
- MIC IP fusion 9000i

Note:

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.

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

3 Changes

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

4 System Requirements

- Web Browsers:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox
- DirectX 11
- MPEG-ActiveX 6.11 or newer
- Configuration Manager 5.51 or newer

5 Restrictions; Known Issues

User Interface

- If UAC is set to default in Windows 7, no snapshot or recording via LIVEPAGE is possible.
- Video and audio may be asynchronous during replay via Web page.
- If a VCA configuration using a rule engine is switched to a VCA configuration without using a rule engine, e.g. MOTION+ or IVA default configuration, the saved configuration is invalid. Forensic search with this configuration may lead to undesired search results.
- In Firefox, no audio is audible on the Audio Settings page.
- Opera mini for mobile devices cannot work in Intranets because it gets all pages through an opera proxy in the Internet. If there is no Internet connection no content is provided.
- When changing GUI language, the browser cache may have to be deleted and the web browser be reloaded before the language will be selected correctly.
- Google Chrome requires a plug-in for displaying TIFF images to properly show the reference image.
- Fluent decoding of buffered .mp4 video from camera is strongly dependent on the browser, Jerky video may occur, e.g. with Mozilla Firefox 52.0, which is not a camera malfunction.

Encoding

- For H.264, only Main Profile using CABAC is supported. CAVLC is not supported.
- Frame rates in low light mode might vary and cause bit rate control to produce higher bit rates than set as maximum.
- With GOP structure set to IBP and IBBP the I-frame distance may not exactly correspond with the set value.
- For stream setting “Dual ROI” the maximum resolution of stream 2 might be limited regardless of a higher resolution selected in the encoder profile.
- Encoder quality regions are not implemented.

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.

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

Network

- QoS values are set according to group Video/Audio/Control for UDP packets, but for TCP packets, only the QoS value for Video is inserted.
- IP addresses 172.20.1.0/30 which include 172.20.1.0 to 172.20.1.3 are reserved for internal communication and must not be used as device addresses. Products without internal communication ignore this restriction and allow the use of this range.

IVA

- IVA and flow need at least 12.5 frames per second video input frame rate. If IVA or Flow are configured, minimum frame rate of 12.5 must be set in ALC mode.
- There is only one configuration for IVA. When analysis type is changed, e.g. from IVA to IVA Flow, the former configuration is lost. Due to this, it is not possible to change the analysis type in a VCA profile switch.
- Due to a limitation of the script language that is used in the background, the delay timer for event-triggered VCA starts immediately when the configuration is set. A trigger event during this period does not restart the timer. Once the timer has elapsed, operation is as desired.
- On devices with VCA FPGA an outgoing IPv6 connection fails when device is initiator, e.g. trying to resolve a time server domain name,
- “Too dark” alarm is not triggered under normal conditions due to the cameras low-light capabilities.
-

MOTION+

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

Recording

- LUN size for local recording via “Direct iSCSI” is limited to 2 TB.
- VRM version 2.12 or higher is required.
- In some cases formatting errors on external iSCSI drives may occur, which might need multiple tries to overcome.
- In rare cases it may happen that the owner of an iSCSI LUN is not displayed correctly. Recording is not affected, just previous owner remains displayed.
- If a device had primary and secondary recording running on SD card and is then added to a VRM system, the blocks used for primary recording will not be re-used, reducing the available recording space for the ANR recording. This can be solved by re-formatting the SD card.
- SD card recording performance is highly dependent on the speed (class) and performance of the SD card.
- With I-frame-only recording and audio also enabled for recording, audio will be fragmented or not audible during replay. Please disable audio recording in case of I-frame-only recording.
- Numbering of the recorded files on the replay page is not always contiguous.
  If snippets across block borders belong together, like pre-alarm and alarm recording, the snippets become logically united and only the lower file number is presented in the list.
- SDXC cards are formatted to FAT32 file system and not using the exFAT file system as being mandatory for SDXC standard compliance but fully recognized and accessible.
  The maximum size of 2TB is also supported with FAT32, once SD cards of that size might become available.
  FAT32 also increases portability to other than Windows platforms.
- If a local media is exchanged, existing former recordings are only discovered after rebooting the device.
- Physically removing the local storage media while recording causes the device to reboot. Recording must be stopped before removal.
- Changing audio format while audio is being recorded may cause unknown behaviour of the device and must be avoided.
- 5MP and larger JPEG streaming via RTSP is only possible with decoders supporting the ONVIF extensions.

  JPEG streaming via RTSP is based on RFC 2435. This RFC only allows for a maximum JPEG size of 2048 by 2048.
  With ONVIF, the original, larger JPEG headers can also be transmitted via RTP header extensions. Unfortunately, this only works with decoders using these extensions, i.e. it does not work with a standard VLC.
- After modifying account settings, e.g. FTP server address, to get the changes applied either switching posting off and on or restarting the device is required.
- The storage system indicator status must be ignored during formatting of an SD card.
- Forcing the camera into an overload situation may cause undesired behaviour and in worst cases even recording gaps. It should always be ensured that the CPU load is not consistently

around or at its maximum. This can be achieved by adapting encoder settings or avoiding too many tasks, e.g. client sessions, in parallel.

Export

- FTP exported files which include audio in a format other than AAC must be renamed from .mp4 to .m4a to allow correct playback in QuickTime.
- With JPEG Posting active when device is booting, the first posted JPEG image may be a no-cam logo.
- FTP posting with resolution 1080p delivers JPEG with size of 1920x1072 pixels due to 16 pixel macroblock boundary of the JPEG encoder.
- If FTP export files contain only a few frames some players might not correctly replay such a file, or the replay is too quick to recognize something. The exported file is not corrupt though it might seem so.
- Files exported using continuous FTP backup for Rec. 2 where stream 2 is set to I-frames only mode contain wrong timing information and play back too fast.
- FTP export file size is always 100 MB if resolution change occurred in exported time span.
- Getting the file list from Dropbox may fail if there are too many objects (files and folders). Limit is approximately higher than 500 objects but also dependent on file name length etc.

ONVIF conformance

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

Dome cameras

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

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

Miscellaneous

- After firmware upload while daylight saving time checkbox is activated the time zone must be adjusted.
- After reboot, the system time re-synchronisation may be delayed up to 9 seconds for SNTP respectively up to 14 seconds for time server protocol.
- AAC audio timestamps for UDP live video streams as well as for recording streams are based on 90 kHz instead of 16 kHz to ensure compatibility with Video SDK.
  AAC audio timestamps for TCP live video streams are based on the standard 16 kHz timestamps. Standard players should connect to live video with AAC audio using TCP.
- After changing the selectable camera mode via alarm input the switch back to a previous mode doesn't work anymore.
- Firmware upload stops recording when it fails or is terminated.
- After downgrade configuration integrity cannot be ensured and settings need to be checked or re-configured.
- When a configuration file is loaded to an incompatible camera, e.g. a configuration file from a HD camera loaded onto a VGA camera, encoder settings might become invalid and need to be re-configured.
- Uploading a configuration file from a different camera platform may result in unpredictable behaviour.
- If it shall be checked if the image is not frozen, use milliseconds timestamp to verify.
- Intelligent Defog default is OFF under “Low bitrate” scene mode.
- When combining CPU-intensive functions like e.g. encryption, watermarking, or dual recording, with high quality and high frame rate encoder settings, tuning of encoder profile settings might be required to avoid overload situations.
- No time change is allowed during the time when the "hour is repeated".
- Maintenance log file creation and download requires some time, though there is no progress indication, and needs to be waited for completion.
- Millisecond stamping on 60 fps cameras is refreshed with 30 Hz only, updating only every second frame.
- JPEGs with VCA overlay are not fully synchronized. Shapes might be slightly off.

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

6 Previous Revisions

6.1 Changes with FW 6.41.0037

- Various smaller issues have been fixed.

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

6.2 Features with FW 6.40.0240

Encoding

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

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

Intelligent Streaming

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

Imaging

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

VCA

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

ONVIF

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

From			Nuremberg
ST-VS/MKP1	Product Management		10.11.2017

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

Miscellaneous

- SMTP port is configurable via web interface.
- Multipathing support for storage devices.
- User name from certificate for EAP-TLS is used as EAP identity, if provided.
- Dynamically colored privacy masks, depending on surrounding video added. This can be used to not distract the operator due to intense color, e.g. white privacy mask in night scene.
- Cameras can connect to the CBS Remote Portal installer service.
- New illuminators for MIC 7000 are supported.
- Large OSD font can be selected, roughly doubling the size of the fonts used for stamping.
- Intelligent Auto Exposure (IAE) has been extended to cameras without FPGA.
- An event playback button has been added to the Live page to allow a quick playback of the last event in case there was an incident and the camera was connected remotely to check what happened instead of checking live and then go to the playback page.
- Default device date is set to firmware build time in case of invalid RTC time to avoid lock-out in case of certificate-based authentication.
- Dropbox API has been updated. The API used before was going obsolete on June 28th, 2017.
- Improved certificate parser to support more attributes used e.g. by various mail providers.
- A banner mode for stampings has been introduced, allowing large scale stamping on top or bottom of image.

The firmware basis is equivalent to the platforms CPP4, CPP6 and CPP7 and inherits all the features that exist upon them.
The “Previous Revisions” section thus mainly lists the features that are commonly introduced with the FW 6.40 for all four platforms in addition to the unique features introduced with the platform CPP7.3.
For earlier features please refer to release notes from the other platforms.