From			Nuremberg
ST-VS/MKP1	Product Management		19.01.2018

Release Letter

Products:	***H.264 Firmware for CPP7 HD/MP cameras***
Version:	***6.43**.0027*

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

1 General

This firmware release is a maintenance release based on FW 6.42.0021.
It is an upgrade for CPP7 based cameras only.

Changes since last release FW 6.42.0021 are marked in blue.

From			Nuremberg
ST-VS/MKP1	Product Management		19.01.2018

2 Applicable products:

- DINION IP starlight 6000
- DINION IP starlight 7000
- FLEXIDOME IP starlight 6000
- FLEXIDOME IP starlight 7000
- DINION IP thermal 8000

Note:

All CPP7 devices incorporate a Trusted Platform Module (TPM) with own firmware.
This TPM hardware and firmware have been enhanced over time to allow for additional security features.
Due to security reasons, the firmware or functionality of the TPM cannot be altered in the field.
Thus, not all new security features become available on devices with older TPM hardware or firmware revisions.

Note:

Since firmware version 6.30 all cameras are prepared to receive a unique Bosch certificate during production, assigned and enrolled by Escrypt LRA.
These certificates prove that every device is an original Bosch-manufactured and untampered unit.
Escrypt is a Bosch-owned company, providing a public certificate authority (CA).
Enrollment of the certificates in production is asynchronous to this firmware release.

From			Nuremberg
ST-VS/MKP1	Product Management		19.01.2018

3 New Features

- 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.

4 Changes

- After updating to firmware version 6.43, users will be able to take advantage from boosted performance and enhanced image quality of DINION IP starlight 6000 / 7000 and FLEXIDOME IP starlight 6000 / 7000:
  - Overall improved contrast and sharpness
  - Stronger sharpening in the detailed zones of the image
  - Retuned the balance between motion blur and image noise in both base modes (Starlight and HDR – Extended Dynamic mode). This generally reduces visible motion blur for moving objects, especially in dark scenes.
  - Improved blending of multiple exposures in HDR mode, especially in scenes with moving objects
- In addition to the starlight mode, the default shutter function in the ALC menu is now also available in HDR – Extended Dynamic mode
- Improvements on Multipathing support for storage devices.
- Various smaller issues have been fixed.

Note:

Due to improved image tuning in this firmware version, the behavior of various image enhancement sliders can be different than in older FW releases. Therefore it is recommended to perform a “Restore Mode Defaults” after the firmware update is finished in order to get the best performance. This button can be found under: Configuration -> Camera -> Scene Mode. This can be done for each scene mode individually. If you want to reset all scene modes, then it is recommended to perform a factory default.

5 System Requirements

- Web Browsers:
  - Microsoft Internet Explorer 11 or higher
  - Mozilla Firefox
- DirectX 11
- MPEG-ActiveX 6.13 or newer
- Configuration Manager 5.52 or newer

6 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 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.
- IE10 by default does not allow snapshots or recording from the LIVE page on local hard disk until one of the following actions is performed:
  - o - uncheck the box "Enable Protected Mode" in internet options/security
  - o - add the device's IP range to "Local intranet" zone
  - o - add the device's IP address to the trusted sites
  - o - start IE as administrator
- If an intranet site is opened, IE10 automatically runs in compatibility mode.
  This leads to a misbehaviour that no timeline is shown on the PLAYBACK page.
  Therefore the function "Display intranet sites in Compatibility View" must be disabled.
- 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

- 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.

From			Nuremberg
ST-VS/MKP1	Product Management		19.01.2018

Security

- When using certificates for mutual authentication, it must be ensured that the camera uses a solid and trusted time base. In case the time differs too much from the actual time, a client might be locked out. Then, only a factory default will recover access to the camera.
- Underscore character ("_") and blank space are not allowed in common name in certificates.
- Excessive signing, e.g. due to very short video authentication signing interval, may have an impact on TLS connection setup.
- Client authentication is not working using Microsoft Edge as the browser does not send any certificate for client authentication, so the camera has nothing to authenticate.

Network

- QoS values are set according to group Video/Audio/Control for UDP packets, but for TCP packets, only the QoS value for Video is inserted.
- IP addresses 172.20.1.0/30 which include 172.20.1.0 to 172.20.1.3 are reserved for internal communication and must not be used as device addresses. Products without internal communication ignore this restriction and allow the use of this range.
- Link-local addresses from the Auto-IP range (169.254.1.0/16) must not be entered manually.
- Reboot will not be performed automatically after uploading a SSL certificate or SSL key; must be done manually.

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.
- ROI PTZ combined with IDNR enabled may blur image when no motion is present in the scene.
- When the camera runs in HDR mode, the analog output menu cannot be used by pressing the local menu button. In this mode, pressing the menu button on the camera will switch on the analog output, pressing it once again will switch the analog output off. Aspect ratio and zoom and focus changes can only be done via IP in the FW configuration.
- 4:3 analog output mode is not possible in combination with HDR.

IVA

- IVA and flow need at least 12.5 frames per second video input frame rate. If IVA or Flow are configured, minimum frame rate of 12.5 must be set in ALC mode.
- There is only one configuration for IVA. When analysis type is changed, e.g. from IVA to IVA Flow, the former configuration is lost. Due to this, it is not possible to change the analysis type in a VCA profile switch.
- If a VCA configuration using a rule engine is switched to a VCA configuration without using a rule engine, e.g. MOTION+ or IVA default configuration, the saved configuration is invalid. Forensic search with this configuration may lead to undesired search results.
- Due to a limitation of the script language that is used in the background, the delay timer for event-triggered VCA starts immediately when the configuration is set. A trigger event during this period does not restart the timer. Once the timer has elapsed, operation is as desired.
- On devices with VCA FPGA an outgoing IPv6 connection fails when device is initiator, e.g. trying to resolve a time server domain name,
- 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.

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

- VRM version 2.12 or higher is required.
- In some cases formatting errors on external iSCSI drives may occur, which might need multiple tries to overcome.
- In rare cases it may happen that the owner of an iSCSI LUN is not displayed correctly. Recording is not affected, just previous owner remains displayed.
- If a device had primary and secondary recording running on SD card and is then added to a VRM system, the blocks used for primary recording will not be re-used, reducing the available recording space for the ANR recording. This can be solved by re-formatting the SD card.
- Throughput limit for simultaneous recording and local replay at 100% playback speed is:
  - maximum total recording bit rate of 7 Mbps for external iSCSI recording
  - maximum total recording bit rate of 10 Mbps for SD card recording, depending on SD card performance
- SD card recording performance is highly dependent on the speed (class) and performance of the SD card.
- With I-frame-only recording and audio also enabled for recording, audio will be fragmented or not audible during replay. Please disable audio recording in case of I-frame-only recording.
- Numbering of the recorded files on the replay page is not always contiguous.
  If snippets across block borders belong together, like pre-alarm and alarm recording, the snippets become logically united and only the lower file number is presented in the list.
- SDXC cards are formatted to FAT32 file system and not using the exFAT file system as being mandatory for SDXC standard compliance but fully recognized and accessible.
  The maximum size of 2TB is also supported with FAT32, once SD cards of that size might become available.
  FAT32 also increases portability to other than Windows platforms.
- If a local media is exchanged, existing former recordings are only discovered after rebooting the device.
- Physically removing the local storage media while recording causes the device to reboot. Recording must be stopped before removal.
- Changing audio format while audio is being recorded may cause unknown behaviour of the device and must be avoided.
- 5MP and larger JPEG streaming via RTSP is only possible with decoders supporting the ONVIF extensions.
  JPEG streaming via RTSP is based on RFC 2435. This RFC only allows for a maximum JPEG size of 2048 by 2048.
  With ONVIF, the original, larger JPEG headers can also be transmitted via RTP header extensions. Unfortunately, this only works with decoders using these extensions, i.e. it does not work with a standard VLC.
- The storage system indicator status must be ignored during formatting of an SD card.
- Forcing the camera into an overload situation may cause undesired behaviour and in worst cases even recording gaps. It should always be ensured that the CPU load is not consistently

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

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

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.

Miscellaneous

- The camera date/time will be set to default (Year 2000) after power loss exceeding the buffer period. It is important to ensure that the date/time is correct for recording. An incorrect date/time setting could prevent from correct recording.
- 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.
- A printout was added to telnet when sending an e-mail failed.
  A more detailed printout was added for the three error cases 'could not connect to server', 'authentication failed' and 'recipient not accepted'.
- 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.
- 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.
- 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.
- 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.

From			Nuremberg
ST-VS/MKP1	Product Management		19.01.2018

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.

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

7 Previous Revisions

7.1 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.

7.2 Changes with FW 6.41.0037

- Various smaller issues have been fixed.

7.3 Features with FW 6.40.0240

Intelligent Streaming

- Intelligent Streaming is a combination of features and functions to optimize bitrate consumption of recorded video. It benefits from improved noise reduction in still areas of the image, an average noise level communicated to the encoder, larger GOP size, strong use of prediction in case of B slices, and dynamic tuning of quantization parameters (QP) in the encoder.
- The strength of the bitrate optimization can be set via 5 levels. Savings can be up to 80% but are strongly scene-dependent.
- Intelligent Streaming is enabled by default in medium setting.

Security

- Password enforcement
  - 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
  - New alternative SNMP support provides encryption and authentication. This new service will provide pure MIB-II access.
  - Legacy functions, like NTCIP support or mapping of dedicated RCP commands to SNMP Enterprise MIB nodes, are only provided with existing SNMPv1 implementation.
- Certificate revocation list (CRL) support
- To improve usability and provide a more compact overview, the web user interface for the certificate store has been updated. It now allows direct tagging of certificates for usages. The former split into two areas (Files and Usage) is removed.
- Stronger encryption and password protection for configuration file
  - The configuration file is encrypted and password-protected before download.
  - The user as the owner of this configuration file is prompted for the password.
  - The password is required when the configuration file is uploaded to a camera.
  - The configuration file is encrypted using standard mechanisms but not intended to be opened or modified by the user, thus the encryption key itself is kept internal and not exposed.
- Stronger encryption for maintenance log file
  The maintenance log file as being used in tech support cases is encrypted with a Bosch public key. Only tech support staff is authorized to decrypt and open the file.
- The minimum TLS version can be defined, e.g. to avoid vulnerabilities from TLS 1.0 and 1.1.
- The Telnet console has been completely removed and is substituted by a new logging facility providing:
  - A more structured output including timestamp, severity and module sources
  - Search and filtering for specific events via web user interface
  - Direct output to a syslog server
  - Configuration to produce similar “debug” printouts for tech support as previously
- Consolidation of running services, visualized on new page “Network Services”.
  Only those services (HTTP, HTTPS, RTSP, RCP, iSCSI, NTP, discovery, ONVIF discovery) are running which are required for activated functionality. All other services (FTP, SNMP, UPnP, GB/T 28181) and their respective ports are deactivated.
- The password unlock functionality (support recovery option) can be disabled.
- 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.

Imaging
- Improved noise filtering in still scenes.

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

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

Miscellaneous
- SMTP port is now configurable via web interface.
- Multipathing support for storage devices.
- User name from certificate for EAP-TLS is used as EAP identity, if provided.
- 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.

7.4 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.

7.5 Features with FW 6.32.0111

Imaging

- Settings for maximum gain control have been added.

Thermal Imaging

- Support of up to 640x480 pixels (VGA) thermal image.
- False Color Mapping selectable from a range of templates.
- Flat Field Correction (FFC) is synchronized with video analytics.

Refer to the release letter of DINION IP thermal 8000 for a comprehensive feature overview.

Security

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

VCA

- JPEG with VCA overlay is now also available in full screen view.
- Analytics algorithms have been optimized to support thermal images.

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.

7.6 Changes

- 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.
- New tuning of image pre-processing has been applied to improve motion sharpness and to reduce artifacts.
- VCA overlays are drawn after scaling to improve visibility.
- For DINION IP thermal 8000, non-functional rotate, flip and mirror were removed from web user interface. In addition, some smaller user interface clean-ups were applied.
- 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.

7.7 New Features with FW 6.30.0140

The feature set of this CPP7 platform firmware is aligned with the feature set of CPP4 and CPP6 platforms. See below the latest feature additions in relation to former firmware 6.2x and new features specific to CPP7.
For earlier feature additions please refer to CPP4 or CPP6 release notes.

Imaging

- Flexible video input orientation handling, including mirror and rotate (90°, 180° and 270°) allows corridor view applications using full resolution.
- A 1.3 MP crop is available on stream 2 on 1080p variants.
- Built-in gyro sensor is supported for automatic orientation detection.

Security

- The user management allows 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 by default. Acceptance can be re-enabled via RCP+ command, if needed.
- Video authentication is 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 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 supported via ONVIF command.
- Tamper detection alarms are forwarded to and included in ONVIF event services.

VCA

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

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) leads to a DownloadStore page providing latest tools, apps and supportive software.
- Unicode characters are 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.

7.8 Changes with FW 6.30.0140

- 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.
- Fixed an issue with placed/taken objects generating no alarms within fields.
- Improved handling of FPGA boot-up.