Architecture and Engineering Specification

NLSS Gateway
GW-500, GW-3000, GW-4000, GW-5000

Date created: 12/20/2011
Revision #: 1.5
Revision Date: 06/06/2013

Table of Contents

Part 1. General

1.1 Summary

A. The Next Level Security Systems (NLSS) Gateway is a fully Integrated Physical Security Video Management System (VMS), Video Analytics (VA), Access Control (ACS) System, and NLSS Cloud Services (NCS) (formerly Remote Management Systems or RMS). It is a network-based platform that interoperates with third party IP Cameras, Encoders, and Access Control devices. A web browser-based interface provides access to the system for local and remote management.

1.2 References

The publications, regulations and standards listed below form a part of this specification to the extent referenced.

A. **FCC Part 15 Class B** – Specifies radio wave emission limits devices for which the purpose is not to produce radio waves, but which do anyway, such as computers, intended for use in (or adjacent to) residential and small business environments. *U.S. Federal Communications Commission.*

B. **EN 55022:2006+A1:2007** – Specifies radio disturbance characteristics, their limits and methods of measurement, for information technology equipment such as computers. *Cenelec (the European Committee for Electrotechnical Standardization).*

C. **EN 61000-3-2:2006+A1:2009+A2:2009** – Electromagnetic compatibility (EMC) limits for harmonic current emissions. *Cenelec*.

D. **EN 61000-3-3:2008** – Electromagnetic compatibility (EMC) limits for voltage changes, voltage fluctuations and flicker in public low-voltage supply systems. *Cenelec*.

E. **EN 55024:1998+A1:2001+A2:2003** – Immunity characteristics for information technology equipment, limits and methods of measurement. *Cenelec*.

F. **ICES-003 Issue 4 February, 2004** – Spectrum Management and Telecommunications Policy, Interference-Causing Equipment Standard (ICES). *Industry Canada.*

G. **IEEE 1100-2005** – Best practices for the powering and grounding of electronic equipment used in commercial and industrial applications. *Institute of Electrical and Electronic Engineers (IEEE)*.

H. **NFPA 70E** – Standard for electrical safety in the workplace. National Fire Protection Association (NFPA)

I. **NFPA 730-2011** – Guide for Premises Security.*NFPA*

J. **NFPA 731-2008** – Standard for the Installation of Electronic Premises Security Systems. *NFPA*

K. RoHS Compliant – Restriction of Hazardous Substances (RoHS) in Electrical and Electronic Equipment. Also known as Directive 2002/95/EC, it originated in the European Union and restricts the use of specific hazardous materials found in electrical and electronic products.

L. UL 796 – Requirements that apply to rigid printed-wiring boards and flexible printed-wiring board for use as components in devices or appliances. *Underwriters Laboratories Inc. (UL).*

1.3 Definitions

A. Door lock modes:

1. **Fail-safe:** Upon power loss, the door lock shall fail in an unlocked mode.
2. **Fail-secure:** Upon power loss, door lock shall fail in the locked mode.

B. Area access management:

1. **Card-In/Free Exit:** Refers to a method of area access management for a single point whereby the entry is controlled, requiring the use of an access card, and exit is not controlled, i.e., there is free exit door hardware, such as a panic bar or mechanical means of egress out of the area.
2. **Card-In/Card-Out:** Refers to a method of area access management for a single point whereby both the entry and exit are controlled, requiring the use of an access card on both sides of the door. There usually will be free exit door hardware, such as a panic bar or mechanical means of egress out of the area.

C. Video terminology:

1. **Frame rate:** The rate at which an imaging device, such as a video camera, produces consecutive images is known as the frame rate, which is expressed in frames per second (fps).
2. **Resolution:** Digital video image resolution, often referred to by the single word resolution, refers to the pixel elements, which are the tiny squares from which the image is built. Resolution is usually expressed as the number of horizontal and vertical counts of the image pixels, such as 640 (horizontal) x 480 (vertical) pixels.
3. **Bit rate:** The rate at which video data is transmitted, measured in Bits per Second (bps) or thousands of bits per second (Kbps), or millions of bits per second (Mbps). The amount of video data to be transmitted in any given time period can vary depending upon the complexity of the video image and the video encoding method used.
4. **Constant Bit Rate model (CBR)**: CBR is a video data-encoding model that maintains a fixed rate of video data for transmission, used where consistent network bandwidth utilization is desired.

5. **Variable Bit Rate model (VBR)**: VBR is a video data-encoding model that produces a variable rate of video data for transmission, used to optimize network utilization and storage space.

D. Video displays and resolutions:

1. **CIF**: *Common Intermediate Format* is a format originally used to standardize the horizontal and vertical resolutions in pixels of video signals commonly used in video teleconferencing systems. The CIF resolution is 352 × 288 pixels, although the term CIF is also used to refer to the common 350 x 240 recording resolution setting of some security video DVRs.
2. **4CIF**: Video resolution of 704 × 576 pixels, four times that of the CIF format.
3. **D-1**: A digital video standard from the Society of Motion Picture and Television Engineers (SMPTE), and is a 720 × 480 resolution in the U.S.
4. **HD**: High Definition video, referring to the two high definition video resolutions of 720p (1280 x 720 pixels) or 1080p (1920 x 1080 pixels). 720p is roughly 5 times the amount of video data than Standard Definition video (analog video) cameras provide.
5. **SD**: *Standard Definition* video is a digital video format that is 640 x 480 pixels, similar to the VGA analog video resolution.
6. **VGA**: *Video Graphics Array* refers to the computer display analog video standard of 640 x 480 pixels.
7. **Video Wall**: A video wall consists of multiple display monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large screen.

E. Video compression standards:

1. **H.264:** A standard for video compression. It is currently one of the most commonly used formats for the recording, compression, and distribution of high definition video. It is a required standard for Blu-ray Disc players, and is widely used by streaming Internet sources, including YouTube, the iTunes Store, and web software such as the Adobe Flash Player. H.264 standard defines 18 sets of capabilities called profiles, designed for specific types of video applications. Three commonly used profiles are the Baseline, Main and High profiles.
2. **H.264 Baseline Profile:** The Baseline Profile was designed to minimize complexity, perform well under a variety of conditions, and maintain flexibility for use over a broad range of network environments and conditions with low bandwidth requirements.
3. **H.264 Main Profile:** The Main Profile was designed with an emphasis on compression coding efficiency capability suitable for Mainstream consumer broadcast and storage applications. It is commonly used for Standard Definition (SD) digital video using the MPEG-4 format, with medium bandwidth requirements.

4. **H.264 High Profile:** The High Profile (HP) addresses high-end consumer use and other applications using high-resolution video, with medium bandwidth requirements. It is utilized for megapixel video broadcast and disc storage applications, including HD DVD and Blu-ray Disc.
5. **Sorenson Spark:** Also known as Sorenson H.263, it is the required video compression format for Flash Player 6 and 7.
6. **M-JPEG:** *Motion JPEG* (M-JPEG) is an informal name for a class of video formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image.
7. **MPEG:** The *Moving Picture Experts Group* is a working group of experts that was formed to set standards for coding and transmitting audio and video information in a digital compressed format. MPEG is also the name of the family of standards developed by the group.
8. **MPEG-4:** A group of encoding techniques that includes MPEG-4 AVC, also known as MPEG-4 Part 10 or H.264.

F. Audio compression standards:

1. **G.711:** A standard for audio data compression and expansion from the ITU Telecommunication Standardization Sector (ITU-T). The standard defines two formats:
   a. **a-law:** the G.711 format used in Europe.
   b. **µ-law:** also called *mu-law* and *m-law*, is the G.711 format used in the U.S. and Japan.
2. **G.726:** a speech encoding standard covering the transmission of voice data from the ITU-T.
3. **AAC:** *Advanced Audio Coding* is a compression and encoding scheme for digital audio, standardized by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Designed to be the successor of the MP3 format, AAC is also the default or standard audio format for iPhone, iPod, iPad, Nintendo DSi, iTunes, DivX Plus Web Player and PlayStation 3.

G. Network video devices:

1. **IP Camera:** Security video cameras that transmit video over IP networks are referred to as IP cameras, as well as *Network Cameras*.
2. **Network video encoder:** A network video encoder receives an analog video camera signal and converts it to any of several network video data formats identical to those used by IP cameras. A network video encoder usually contains other features found in IP cameras, such as web-based configuration of the video resolution and frame rates, and video analytics such as video motion detection.

3. **NLSS DC-400-2:** A network-based NLSS HD Decoder that can display up to four simultaneous streams of HD video from IP cameras, stored media content or available online content to one or two monitors. It supports multiple video pane layouts and is easily managed over an intuitive browser-based interface.

H. Network Protocols:

1. **ARP**: The *Address Resolution Protocol* is a telecommunications protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to hardware addresses.
2. **Bonjour**: Apple Inc.'s trade name for its implementation of Zeroconf (for *zero configuration*), a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.
3. **DHCP**: The *Dynamic Host Configuration Protocol* is a network configuration protocol for devices on IP networks, used to provide IP addresses automatically to requesting devices.
4. **DNS**: The *Domain Name System* is a naming system for networks that translates human-friendly domain names (such as www.google.com) into IP addresses.
5. **FTP**: The *File Transfer Protocol* is a standard network protocol used to transfer files from one computer to another host over a TCP-based network, such as the Internet.
6. **HTTP**: The *Hypertext Transfer Protocol* is the primary protocol of the World Wide Web, used by web browsers to request web pages and web servers to send web page data.
7. **HTTPS**: The *Hypertext Transfer Protocol Secure* is a combination of Hypertext Transfer Protocol (HTTP) with the SSL (Secure Sockets Layer protocol) or the TLS (Transport Layer Security protocol) to provide encrypted Internet connections.
8. **ICMP:** The *Internet Control Message Protocol* is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a computer or router could not be reached.
9. **IGMP:** The *Internet Group Management Protocol* (IGMP) is a communications protocol used by computers and routers on IPv4 networks to establish multicast connections. For example, a single data stream (such as a video stream) can be sent to multiple computers and devices.
10. **IPv4**: *Internet Protocol version 4* is the fourth revision in the development of the Internet Protocol (IP)—the principal communications protocol of the Internet. IPv4 is the first version of the protocol to be widely deployed.
11. **NTP**: The *Network Time Protocol* is a protocol for synchronizing the clocks of networked computer systems.

12. **RTMP**: The *Real Time Messaging Protocol* is a network protocol for streaming audio, video and data over the Internet, between a Flash player and a server.
13. **RTMFP**: *Real Time Media Flow Protocol* is a proprietary protocol developed by Adobe Systems for streaming data between Adobe Flash Players and applications built using the Adobe AIR framework.
14. **RTP**: The *Real-time Transport Protocol* defines a standardized data packet format for delivering audio and video over IP networks.
15. **RTSP**: The *Real Time Streaming Protocol* is a network control protocol designed for use in entertainment and communications systems to control streaming media servers, allowing the server to be controlled using VCR-like commands, such as play and pause, to facilitate real-time control of playback of media files from the server.
16. **TCP**: *Transmission Control Protocol*, one of the core protocols of the Internet protocol suite, often used together with IP as TCP/IP, to refer to the full set of Internet communication protocols.
17. **UDP**: The *User Datagram Protocol* (UDP) one of the core protocols of the Internet protocol suite and is used, for example, for streaming H.264 video data.
18. **UPnP**: *Universal Plug and Play* is a set of networking protocols originally developed for residential networks not having enterprise class network devices. It allows devices such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing and communications.

I. Access card and credential terminology:

> **Note**: These terms refer to various aspects of a card that is being used for visual identification, electronic identification and electronic access authorization purposes.

1. **Badge:** See ID Badge.
2. **Card**: A credit-card sized card (usually 3.370 × 2.125 inches), also called a security card or access card, used for security identification and access control purposes, and which contains a standards-based means of storing and transferring data electronically.
3. **Card Format and Credential Format:** Terms that refers to the way that the numeric information electronically encoded in the card is to be interpreted by the card reader and the access control system. There are formats considered to be *industry standard* and formats that are unique and proprietary, intended for the exclusive use of a single customer of an access card manufacturer. Card formats use

binary numbers (0's and 1's), and are often named for how many zeros and ones (bits – short for binary digits) are used for the format's data, such as a *37-bit format*.

4. **Credential**: A security card that has been issued to an individual after being personalized with visual and electronic identifying information.
5. **ID Badge**: A card used to identify the cardholder, which usually contains a photograph and other identifying information, such as the cardholder's name and organizational membership.
6. **Facility Code:** a unique number assigned to the customer by the card manufacturer, used in some card encoding formats to identify the facility to which the cardholder is being assigned access privileges.

J. Security industry standards organizations:

1. **ONVIF**: The *Open Network Video Interface Forum* (ONVIF) is a global and open industry forum with the goal to facilitate the development and use of a global open standard for the interface of physical IP-based security products.
2. **PSIA**: The *Physical Security Interoperability Alliance* (PSIA) is an industrial standardization initiative promoting interoperability of IP-enabled security devices.

K. Data encryption:

1. **AES:** *Advanced Encryption Standard* is a specification for the encryption of electronic data, developed by the National Institute for Standards and Technology (NIST) and adopted by the U.S. government and is now used worldwide. The strength of the encryption is directly related to the length of the encryption key (the number of data bits in the key). It is the first publicly accessible and open encryption method approved by the National Security Agency (NSA) for top secret information, which approved key lengths of 128, 192 and 256 bits. The strength of the encryption is indicated by citing the number of bits for the key length, such as *AES-128*.
2. **PGP:** *Pretty Good Privacy*, now commonly referred to as PGP, is an open data encryption standard that provides cryptographic privacy and authentication during data communications. PGP is often used for signing, encrypting and decrypting texts, E-mails, files, directories and whole disk partitions to increase the security of e-mail communications.

L. Remote management of multiple systems:

3. **NLSS Cloud Services:** NCS allows a customer to view and administer multiple sites (facility locations with one or more NLSS Gateways) by logging into a single portal, instead of separately logging in to each Gateway device. The devices managed by a Gateway can be monitored from the Cloud Services portal. This feature is formerly known as Remote Management Services or RMS.

1.4 System Description

A. The Gateway shall be a standards-based, networked platform that integrates Video Surveillance, Video Analytics, Access Control, and Intrusion Detection systems in a single appliance.

B. The Gateway shall operate in a standalone mode, with other Gateways, and/or in conjunction with a Next Level Cloud Services System.

C. The Gateway shall support live video, recorded video, and simultaneous display of both live and played-back recorded video.

D. The Gateway shall support live audio and recorded audio that is synchronized with recorded video.

E. The Gateway shall support multiple desktop video displays through the use of multiple NLSS DC-400-2 or later decoders.

F. The Gateway shall support video wall configurations through the use of NLSS DC-400-2 or later decoders.

G. The Gateway shall support approved third party Access Control devices integrated into the system from Assa Abloy, HID, and Mercury Security.

H. The Gateway shall support Event Management and Alarm Handling features integrated across the access, video and analytic feature sets.

I. The Gateway shall support a Web server for multiple Web browsers as the interface to the system.

J. The Gateway shall not require any specific client application software to be loaded on PCs used to access the Gateway application, with the exception of Adobe Flash Player, which is a free download.

K. The Gateway shall not require any licensing for individual cameras, the included 11 video analytic behaviors (including the glass break audio analytic), or individual AC doors.

L. The Gateway shall support multiple Gateways in the same network without imposing a fixed limit on the number of Gateways.

1.5 Submittals

A. General: Submittals shall be made pursuant to applicable contracts.

B. Product Data – the following Product Data shall be provided:

1. Data Sheets

2. Quick Start Guide

3. User Manual

1.6 Quality Assurance

A. Qualifications:

1. Installer shall be certified by NLSS to be experienced in performing electronic security systems installation and conditioning work similar to that required for this project.

2. Manufacturer shall be capable of providing field service representation during installation and of approving application method.

B. Standards and Guidelines: As appropriate for the country location of the facility or facilities, provide an installed electronic security system that complies with the following standards and guidelines:

1. FCC Part 15 Class B

2. EN 55022:2006+A1:2007

3. EN 61000-3-2:2006+A1:2009+A2:2009

4. EN 61000-3-3:2008

5. EN 55024:1998+A1:2001+A2:2003

6. ICES-003 Issue 4 February, 2004

7. IEEE 1100-2005

8. NFPA 70E

9. NFPA 730-2011

10. NFPA 731-2008

11. RoHS

12. UL 796

1.7 Delivery, Storage and Handling

A. Comply with manufacturer's requirements.

B. Deliver materials in manufacturer's original, unopened, undamaged containers with original identification labels.

C. Protect stored materials from environmental and temperature conditions following the manufacturer's instructions.

D. Handle and operate products and systems according to the manufacturer's instructions.

1.8 Project Site Conditions

A. The Gateway shall be capable of continuous operation under the following environmental conditions:

13. Temperature: 0-30°C (32-86°F)

14. Relative Humidity: 20% to 80%, non-condensing

1.9 Manufacturer's Warranty

A. Project Warranty: Refer to Conditions of the Contract for project warranty provisions.

B. Project Warranty Period: [specify term in number of years] commencing on Date of Substantial Completion.

Specifier Note: Coordinate paragraph below with manufacturer's warranty requirements.

C. Manufacturer's Warranty: Submit, for Owner's acceptance, manufacturer's standard warranty document.

1.10 System Startup/Owner's Instructions/Commissioning

A. Follow the instructions provided in the manufacturer's Quick Start Guide and User Manual.

1.11 Maintenance

A. The Gateway itself requires no maintenance other maintaining the appropriate environmental conditions specified in section *1.8 Project Site Conditions*.

Part 2. Products

2.1 Acceptable Manufacturer

A. The NLSS Gateway shall be supplied by:

Next Level Security Systems
6353 Corte Del Abeto, Ste. 102
Carlsbad, CA 92011,
(760) 444 – 1410
www.nlss.com

B. Substitutions: no substitutions will be considered or accepted.

2.2 NLSS Gateway

A. The NLSS Gateway shall be a standards-based, networked platform based on Linux Ubuntu, MySQL, Apache, PHP and Flash.

B. The Gateway shall support an easy-to-use, intuitive, Web-browser interface (NLSS Web Interface) to the system.

C. The Gateway shall natively support the security levels of Operator and Superuser, and shall provide independently configurable permissions for each Operator assignment. Additional Users may be added.

D. The Gateway shall support multiple simultaneous users on the system via multiple browser windows.

1. Users shall be defined with specific roles and require password verification to access the Gateway application.
2. Roles provide a means to define and assign user privileges to perform view, edit, add or delete actions under the Operation and Configuration menus within the Gateway application.

E. The main Gateway Modules that can be restricted are:

1. Operations
2. Cameras
3. Decoders
4. Doors
5. Cardholders/Users
6. Reporting
7. Views
8. Sequences
9. Media
10. Input Devices
11. Output Devices
12. Groups

13. Point of Sale

14. Areas

15. Zones

16. Configuration

17. Global

18. Identity

19. Access Control

20. Video

21. Permissions

22. Point of Sale

23. Intrusion

24. Face Recognition

25. License Plate Recognition

26. Events

F. The Gateway shall support the selection of one of the following user languages at system login: Dutch, English, French, Spanish, German, Italian, Romanian, and Portuguese.

G. The Gateway's Web Interface shall support the following web browsers and Adobe Flash Player:

1. Internet Explorer version 9.0 or above

2. Mozilla Firefox version 20 and above

3. Google Chrome version 26.0 and above

4. Apple Safari 5.1.9 for OS X v10.6, Safari 6.0.4 for OS X 10.7-10.8

5. Adobe Flash Player 11.5 and above

2.3 NLSS Gateway Hardware

A. The Gateway shall have one (1) or more 1 GB Ethernet ports.

B. The Gateway shall have six (6) or more USB 2.0 or above ports.

C. The GW-500 and GW-3000 shall have one (1) or more eSATA ports for connecting external data storage.

D. The Gateway shall have an internal Hard Disk Drive Raw Capacity (HDD) of the following capacity:

1. GW-500 – not less than 500GB

2. GW-3000 – not less than 2TB

3. GW-4000 – not less than 8TB (2- 4TB drives)

4. GW-5000 – not less than 2TB

E. The Gateway power consumption shall be:

1. GW-500 – 25 to 40 watts

2. GW-3000 – 50 to 95 watts

3. GW-4000 – 200 to 300 watts

4. GW-5000 – 250 to 420 watts

F. The Gateway mechanical dimensions shall be:

1. GW-500 – approx. 8”x 8”x2”

2. GW-3000 – approx. 12”x 13.25”x1.75”

3. GW-4000 – approx. 17.75”x15”x1.75”

4. GW-5000 – approx. 17.75”x15”x1.75”

2.4 NLSS System Features

A. The Gateway shall support

1. Local and remote firmware upgrades

2. Export of system logs

3. Backup and restoration of configuration

c. Manual backup and restoration of configuration

d. GW-3000 shall also support auto-backup to a Compact Flash (CF) card.

e. GW-4000 and GW-5000 shall also support auto backup to a SATA SSD card.

4. Manually setting the time of the system by selecting the time zone and setting the current hour and minute

5. Automatic setting of the system time through the use of a Network Time Protocol (NTP) Server

6. Manual static IP address provisioning

7. Automatic IP address provisioning via DHCP.

B. The Gateway shall display the following System Health information:

1. System memory utilization %

2. CPU usage %

3. Coprocessor usage %

4. # of active streaming video cameras

5. # of active recording video cameras

6. # of active Video Analytic rules

7. System uptime

8. Network bandwidth input/output Kbits per Second (Kbps)

9. # of doors online and total # of doors

C. The Gateway shall support local and remote IP networks through use of switches, routers and Virtual LANs (VLANs).

D. The Gateway shall support the following network protocols: TCP, UDP, IPv4, HTTP, HTTPS, RTP, RTSP, DHCP, DNS, ARP, ICMP, IGMP, NTP, FTP, Bonjour, UPnP, RTMP

2.5 NLSS Video Features

A. The Gateway shall automatically discover IP cameras that support:

1. ONVIF compliant discovery

2. Bonjour

3. UPnP

4. The following proprietary discovery protocols:

a. Arecont Vision

b. Panasonic

c. Sony

d. Verint

B. The Gateway shall support reading the video configuration parameters of IP cameras in the network.

C. The Gateway shall support multiple video streams on one IP camera with independent per-stream video parameter settings.

D. The Gateway shall support video analytics on a camera's primary video stream.

E. The Gateway shall support H.264 Main Profile, MPEG-4, and M-JPEG video compression formats.

F. The Gateway shall support video resolutions of HD 1080p, HD 720p, D1, 4CIF, VGA, CIF and multi-megapixel camera resolutions of any size; the use of video analytics shall restrict a camera's primary video stream resolution to a maximum of 1920x1080.[a]

G. The Gateway shall support aspect ratios of 16:9, 4:3, 9:16 (*corridor view*), and non-standard aspect ratios.

H. The Gateway shall support frame rates up to 60 frames per second (fps) for video streams including 1080p streams.

I. The Gateway shall support Constant Bit Rate (CBR) Model and Variable Bit Rate (VBR) Model.

J. The Gateway shall support multiple bit rates for video for both CBR and VBR.

K. The Gateway shall support multiple video compression formats, resolutions, aspect ratios, frame rates, bit rate models, and bit rates simultaneously.

[a] Note that full-image display at full resolution of some high-resolutions video images may be dependent upon the capabilities of the display monitor.

L. The Gateway shall support configuration of RTSP or HTTP server push for M-JPEG video streams from IP cameras that are not automatically discovered.

M. The Gateway shall support multiple third party IP cameras and video encoders from major manufacturers including those from the following vendors:

1. Arecont Vision

2. Avigilon

3. Axis

4. American Dynamic

5. Brickcom

6. Bosch

7. Canon

8. Channel Vision

9. D-Link

10. Grundig

11. HikVision

12. Hunt Electronic

13. IQInvision

14. Linear

15. Messoa

16. Panasonic

17. Pelco

18. Samsung

19. Sony

20. Speco Technologies

21. Verint DVTel

22. Vivotek

2.6 NLSS Video Analytic Features

A. The Gateway shall support the following video analytics behaviors:

1. Activity Detection

2. Direction

3. Dwell Time (Loitering)

4. Face Capture

5. Face Recognition

6. License Plate Capture

7. License Plate Recognition

8. Line Crossing

9. Object Moved

10. Object Taken Away

11. People Count

12. People Count Directional

13. Perimeter Crossing

B. The video analytics behaviors shall generate events that can be automatically displayed and logged by the system, and associated with the recorded triggered video.

C. The Gateway shall support analytics for video streams from any camera on the network as follows:

1. One (1) video analytic behavior assignment per camera

2. The number of cameras to which video analytic assignments can be made per Gateway will be dependent upon the total processing requirements of all video streams, and subject to a maximum total video data rate of 2 Mbps, for example.

3. The streams are defined as H.264, 720p, 15 fps, with bit rate of 2 Mb/s for VA. Non-VA (non-video analytic) streams can be H.264, 1080p, 30 fps with bitrate of 3 Mb/s.

4. The actual performance will vary based on video codec, resolution, frame, rate, bit rate, IP camera, and network, but the following has been tested successfully.

Platform	# Streams	# Analytic Behaviors	Video Encoding	Video Resolution	Frame Rate	Bit Rate
GW-500	16	0	H.264	1080p	30fps	3Mbps
GW-500	16	2	H.264	720p	15fps	2Mbps
GW-500	8	4[a]	H.264	720p	15fps	2Mbps
GW-3000	32	0	H.264	1080p	30fps	3Mbps
GW-3000	32	2	H.264	720p	15fps	2Mbps
GW-3000	16	4	H.264	720p	15fps	2Mbps
GW-4000	64	1	H.264	1080p	30fps	3Mbps
GW-4000	64	2	H.264	720p	15fps	2Mbps
GW-4000	32	6	H.264	720p	15fps	2Mbps
GW-5000	128	1	H.264	1080p	30fps	3Mbps
GW-5000	128	4	H.264	720p	15fps	2Mbps
GW-5000	64	10	H.264	720p	15fps	2Mbps

[a] Only one Face Recognition instance can be supported on the GW-500.

5. The Gateway shall support post processing of recorded video using video analytic behaviors (Forensic Analytics). The Gateway shall support running an analytic on a stored video segment to aid investigations on past events and collect data such as people counting.

2.7 Face Recognition Video Analytic

A. When the Face Recognition Video Analytic is activated for a camera, it grabs a still image of a face, and generates a Face Captured event.

B. For most applications, 720p resolution, at 15 fps, shall be sufficient for good Face Recognition accuracy.

C. Identified facial images shall be stored in a database, and used for comparison with the captured image to determine face recognition.

D. The Gateway shall allow users to manually add, edit and delete records of people in the Face Recognition database.

E. The Gateway shall automatically add Cardholders and their images to the Face Recognition database.

F. The Gateway shall allow users to add up to ten (10) facial images, in .jpeg format, for comparison.

G. The Gateway shall allow users to manually add, configure, edit, and delete Face Recognition groups.

H. The Gateway shall allow the importing of a *facialrecognition_configuration_template.csv* file, which lists the people to be associated with facial images.

1. An imported facialrecognition_configuration_template.csv file shall create a group, according to the *groupName* defined in the file.
2. Only one group name can be assigned to a facialrecognition_configuration_template.csv file.
3. Multiple facialrecognition_configuration_template.csv files can be imported to the database on the Gateway.
4. If multiple facialrecognition_configuration_template.csv files are imported with the same groupName, the total number of people in one group should not exceed 5000 entries.

I. Face Recognition shall generate the following events:

1. Face Recognized
2. Face Match Group
3. Face Mismatch Cardholder

J. Face Recognition shall support the following actions:

1. FaceRecognitionValidateCardholder
2. FaceRecognitionValidateGroup

2.8 License Plate Recognition

A. When the License Plate Recognition Video Analytic is activated for a camera, it grabs a picture of a license, and generates a License Plate Captured event.

B. For most applications, 720p resolution, at 15 fps, shall be sufficient for good License Plate Recognition accuracy.

C. License plate numbers are read from the image.

D. The license plate numbers shall be stored in a database, and used for comparison to determine License Plate recognition.

E. People and their associated with license plate numbers shall be stored in two tables in the Personal Vehicle Pool database.

1. The Gateway shall allow users to add, edit, and delete records for individual people in the database.

2. The Gateway shall allow users to assign one or multiple license plate numbers to a person.

3. The Gateway shall allow people to be assigned to a group.

4. The Gateway shall allow users to add, edit, and delete groups.

F. The Gateway shall allow the importing of an lpr.csv file, which lists the people to be associated with license plates.

1. An imported *lpr.*csv file shall create a group, according to the *groupName* defined in the file.

2. Only one group name can be assigned to an lpr.csv file.

3. Multiple lpr.csv files can be imported into the database on the Gateway.

4. If multiple lpr.csv files are imported with the same groupName, the total number of people in one group should not exceed 5000 entries.

G. The Gateway shall allow the importing of a list of license plate numbers using a *vehicles.csv* file.

1. This file shall associate people with license plate numbers and their vehicles, and include general information about the vehicle.

2. A license plate shall be associated to a person by the *userSuppliedID* field, as defined in the lpr.csv.

3. One person can be associated to multiple vehicles.

4. An individual vehicle.csv file shall be limited to 5000 entries.

H. License Plate Recognition shall generate the following events:

1. License Plate Recognized

2. License Plate Match Group

I. License Plate Recognition shall support the following action:

1. LicensePlateRecognitionValidateGroup

2.9 NLSS Audio Analytic Features

A. The Gateway shall support the following audio analytics behaviors:

1. Glass Break

2. Aggression

3. Car Alarm

4. Gunshot

B. By default, the Gateway shall support application of the glass break analytic to four video streams.

C. Audio analytics for aggression, car alarm, and gunshot analytics, and additional glass break streams are also available.

D. The glass break analytic shall detect breakage of laminate, plate, wired, and tempered glass, as are commonly found in commercial and residential buildings.

1. Breakage of different thicknesses and sizes shall be detected.

a. Plate: 2.4 mm - 6.4 mm

b. Tempered: 3.2 mm - 6.4 mm

c. Wired: 6.4 mm (the only thickness wired glass comes in)

d. Laminated: 6.4 mm

e. Minimum glass size, all types of glass: 300 mm x 300 mm

2. The analytic detects glass break up to 10 meters from the microphone, based on a representative environment for intrusion detection applications.

3. The analytic reliably detects glass break in typical intrusion detection scenarios up to at least 50 dB SNR (Signal to Noise Ratio).

4. A glass break simulator can be used to test that the analytic and camera are properly configured. An example is the Risco RG65 industry standard glass break simulator.

E. The car alarm analytic shall detect the seven standard types of car alarms used by major car manufacturers in Europe and North America. These car alarms are characterized by looping patterns

1. The analytic shall detect alarms up to 50 meters from the microphone.

2. The analytic shall reliably detect car alarms up to at least 10 dB SNR (Signal to Noise Ratio).

F. The aggression analytic shall characterize and detect the specific pitch, tone and intonation changes that occur in the voice patterns in response to a person becoming aggressive.

1. The analytic shall detect aggression up to 10 meters from the microphone.

2. The analytic shall reliably detect aggression up to at least 40 dB SNR (Signal to Noise Ratio).

G. The gunshot analytic shall detect various types of firearms being discharged, including the types of guns most commonly used in civilian gun crimes in the Americas, Europe, Middle East and Australasia.

1. Gunshots are characterized by the unique, un-silenced muzzle blast associated with a range of weapons typically used in crimes.

a. Hand guns, including: 9mm semi-automatics and revolvers with and without muzzle diffusers.

b. Shotguns, including: 20-gauge, and 12-gauge

c. Rifles including: .22 and 7.62 mm bolt action

d. Automatic rifles, including AK-47, AR-15

e. Semi-automatic rifles, including AR-15

f. Uzi submachine gun

2. The analytic shall detect a gun shot up to 100 - 200 meters from the point of discharge.

3. The analytic shall reliably detect gunshots up to at least 50 dB SNR (Signal to Noise Ratio).

H. The audio analytics shall meet the following environmental specifications:

I. Audio analytics shall be capable of application in both indoor and outdoor installations.

J. The analytics shall compensate for ambient sounds, including:

1. Traffic noise

2. Street noise.

3. Office and building noise

K. System performance of audio analytics will vary, based on:

L. Background noise levels

M. Microphone sensitivity settings (clipping/distorting/low-level)

N. Any audio signal process that is applied to the audio by the capture device, such as AGC (auto gain control).

O. Implementing audio analytics shall include the following configuration requirements:

1. Audio analytics shall require an IP camera with a built-in or external microphone, or an encoder.

2. The device shall support an audio sampling rate of 16 KHz, 16 bits, using the AAC codec.

3. The analytic's sensitivity shall be adjustable for each channel.

4. The audio analytic shall require a microphone with a frequency response equal to at least 100 Hz - 8 kHz +/- 6dB.

5. To prevent clipping or distortion:

a. The microphone shall be installed at least two meters from potential sound sources.

b. The microphone's sensitivity settings shall be adjustable on the camera or encoder.

6. The microphone sensitivity settings shall provide a reasonable level of audio to the NLSS Gateway and the analytic.

7. The effective range for microphones quoted in this document are typical detection ranges in representative environments, in which the analytic is likely to be used. The effective range varies, according to the physical and acoustic environment.

P. The audio analytics shall support the following cameras:

Axis	
Axis M1031	Axis P3343/-V
Axis M1054	Axis P3344/-V
Axis P1343	Axis P3346/-V
Axis P1344	Axis P3367-V
Axis P1346	Axis M501
Axis P1347	Axis M5014
	Axis Light Finder P3364
Sony[a]	
SNC-VB630	SNC-VM601
SNC-VM600	SNC-VM601B
SNC-VM600B	SNC-VM630

2.10 NLSS Video PTZ Features

A. The Gateway shall support Pan, Tilt, and Zoom (PTZ) IP Cameras via the browser interface.

B. The Gateway shall support PTZ presets.

C. The Gateway shall support PTZ patrols.

[a] Sony cameras require firmware version 1.3 or later.

2.11 NLSS Video Control Features

A. The Gateway shall support graphical video controls in the Web-browser. By default the graphical controls shall be permanently displayed in the browser, but may be or hidden and retrieved when desired by the user.

B. The Gateway's graphical video controls shall provide simple switching (toggling) between the display of live and recorded video for any selected camera.

C. The Gateway's graphical video interface shall include:

1. PTZ control.

2. Analytic setup control.

3. Bookmarking (manually defining events) for the camera timelines.

4. Fast Forward (FF), Rewind (RW), Pause, Play, and Live video controls.

5. Search by date and time of day.

6. Searches filtered by camera event type and/or event source.

7. Video export control.

8. Display of time, date, and stream information of the video currently playing or paused.

9. Full Screen video display option.

10. Filmstrip feature displaying thumbnail images of recorded video events in a timeline.

11. JPEG snapshot export control both on live and recorded video.

12. Digital Zoom feature.

13. Camera Output feature.

14. Per-Camera Event Report.

15. Per-Camera Event Log.

D. The video functionality shall support the association of doors with cameras, to provide easy access to door control from points of video viewing within the Gateway application.

2.12 NLSS Video Display Features

A. The Gateway shall support 1x1, 1x2, 2x1, 2x2 Layouts and Views in the Web-browser.

B. The Gateway shall support Views with synchronized playback between multiple streams.

C. The Gateway shall automatically discover NLSS DC-400-2 and later video decoders on the network.

2.13 NLSS Video Display Features (Decoder Required)

A. DC-400 refers to DC-400-2

B. The Gateway shall automatically discover NLSS DC-400 video decoders on the network.

C. The Gateway shall support 1x1, 1x2, 2x2, and 3x3, 1x4 and 2x4 Views in the Web-browser.

D. The Gateway shall support all views supplied by the decoder.

E. The Gateway shall support user-selectable Views containing multiple video streams, with View Layouts of up to nine (9) video streams, pushed to an HD video display via a DC-400 decoder.

F. The Gateway shall support View configuration by drag and drop assignment of Views into the Sequence Layout.

G. The Gateway shall support video walls by pushing multiple views to multiple HD displays via multiple DC-400 decoders (one decoder per HD display).

H. The Gateway shall support video display Sequences, in which two or more Views are displayed in user-configurable order, with individual sequence durations.

2.14 NLSS Audio Features

A. The Gateway shall support G.711 (both a-law and μ-law encoding), G.726, and Advanced Audio Codec (AAC) audio coding.

B. The Gateway shall support:

1. Live audio from IP cameras

2. Recorded audio from IP cameras

3. Audio in sync with recorded video

4. Audio volume and mute controls via the browser

5. Two-way audio

6. Audio Notification of Events

2.15 Media Library

A. The Gateway shall contain a Media Library to store audio and video files.

B. The library shall also hold the video exported from a camera.

C. The Gateway shall be able to manually play back an audio clip from the Media Library.

D. The Gateway shall be able to play an audio clip when triggered by an event or from the Web interface video player.

E. The Gateway shall be capable of holding video clips up to four hours in length.

F. The Gateway shall be capable of exporting a video clip to a local computer.

G. The Gateway shall allow a video export to be stopped.

H. The Gateway shall allow a media file to be locked to prevent deletion.

I. The Gateway shall include a series of default audio files that cannot be deleted.

J. The Gateway shall allow the default audio files to be replaced via the Media Library.

2.16 NLSS Storage Features

A. The Gateway shall support:

1. Internal storage of video, audio, events, and configuration data

2. Manual or automatic selection of storage target on a per camera basis

3. Direct Attached Storage (DAS)

4. External USB storage

5. Automatic availability of USB storage added to the system

6. External eSATA hard disk drive storage (GW-500 and GW-3000 only)

7. Network Attached Storage (NAS)

8. External iSCSI storage

9. External NFS storage

10. NLSS Cloud Storage

a. Requires a subscription for NLSS Cloud Storage.

b. Also requires a subscription NLSS Cloud Services (NCS).

c. Sufficient bandwidth for both NLSS Cloud Services and the exported clips exported to NLSS Cloud Storage: *at least* 1Mb or more. Preferred: 3Mb to 5Mb, or higher.

11. Automatic failover, with notification, from one storage volume to another if a storage volume becomes unavailable for continued data writing

12. Minimum and maximum video retention targets in units of days

13. Automatic grooming (deleting) of video data when system storage limits and/or video retention targets are met

14. Per-camera configuration of grooming settings.

2.17 Schedules

A. The Gateway shall support pre-configured and customizable schedules that can be used for multiple items such as event qualification, access control door unlock schedules, access levels, intrusion disarm schedules, and video recording.

B. The Gateway shall support custom Holidays. Up to 90 consecutive days may be included in the Holiday period per schedule.

2.18 Events

A. The Gateway shall support eight (8) user definable Event Severities (priorities).

B. The Gateway shall support the following user-configurable automatic actions for specific events:

Type	Action
Access Control	Door Momentary Unlock
Access Control	Door Relock
Access Control	Door Unlock
Access Control	Output Off
Access Control	Output On
Audio	Play Audio
Channel	Channel Set Active
Email	Email Send
PTZ Camera	PTZ Go to Home
PTZ Camera	PTZ Go to Preset
PTZ Camera	PTZ Start Patrol
Video Analytics	VA Start
Video Analytics	VA Stop
Video Analytics	Face Recognition Validate Cardholder
Video Analytics	Face Recognition Validate Group
Video Stream	Stream Record Start
Video Stream	Stream Record Stop
View	View Set Active

C. The Gateway shall support multiple automatic actions for specific events.

D. The Gateway shall support the following events:

1. Emergency events assigned the Emergency Severity level: these high-risk events are added automatically to emergency queue
2. Shunted events: these events are filtered out from the event log (example: faulty door events)
3. Locked events: these are events excluded from grooming (automatic deletion)

E. The Gateway shall support Incident Management:

1. Assignment of event status
2. Entry of log notes with date/time/user stamp

F. The Gateway shall support the following 105 Event Types:

Category	Event Type
Access Control	
	Access Denied
	Access Denied Trace
	Access Grant
	Access Grant Trace
	Cabinet Tamper
	Card Activated
	Card Deactivated
	Controller Offline
	Controller Online
	Door Auto Relock
	Door Auto Unlock
	Door Battery Low
	Door Contact Tamper
	Door Forced Open
	Door Held Open
	Door Not Unlocked
	Door Rex Tamper
	Door Secured
	Door Unlocked
	Input Active
	Input Inactive
	Input Tamper
	Output Active
	Output Inactive
	Reader Comm Loss (ReaderIOInterfaceCommLoss)
	Reader Comm Restored (ReaderIOInterfaceCommRestored)
Camera	
	Channel Loss
	Clip Exported
	Direction
	Discovered
	Dwell
	Export Failed
	Face Capture
	IO Event
	Line Crossing
	Motion Event
	Object Moved

Category	Event Type
	Object Taken
	Offline
	Online
	People Count
	Perimeter
	Snapshot Exported
	Tamper Event
	Video Bookmark
	Video Loss
	Video Resume
Decoder	
	Offline
	Online
Intrusion	
	Area Armed
	Area Cannot Arm
	Area Cannot Disarm
	Area Disarmed
	Panel Offline
	Panel Online
	Zone Alarm
	Zone Bypass
	Zone Fail
	Zone Fault
	Zone Force
	Zone Low Battery
	Zone Missing
	Zone Reset
	Zone Restore
	Zone Trip Count
	Zone Trouble
	Zone Verify
System	
	External (Ext) Storage Offline
	External (Ext) Storage Online
	Message
	Recording Failover
	Recording Failure
Transaction	
	POS Status Update
	POS Transaction Complete
	POS Transaction Data

Category	Event Type
	POS Transaction Start
	Terminal Interface Discovered
	Terminal Interface Offline
	Terminal Interface Online
User	
	Card Activated
	Card Deactivated
	Door Opened
	Emergency
	Login
	Logoff
	Mobile Stream Begin
	Mobile Stream End
Video Analytics	
	Activity
	Aggression Detected
	Car Alarm Detected
	Direction
	Dwell
	Face Capture
	Face Match Group
	Face Mismatch Cardholder
	Face Recognized
	Glass Break Detected
	Gun Shot Detected
	License Plate Captured
	License Plate Recognized
	Line Crossing
	Object Moved
	Object Taken
	People Count
	Perimeter

G. The Gateway shall support a flexible event and action system with configurable logic.

H. A User can create custom Actions by selecting any of 15 Action Types from the table below and the specific sub-function.

Action Type	Definition
ACDoorMomentaryUnlock	Temporarily unlocks the selected door.
ACDoorRelock	Locks the selected door.
ACDoorUnlock	Unlocks the selected door.

Action Type	**Definition**
ACOutputOff	Disables the selected I/O output.
ACOutputOn	Enables the selected I/O output.
ChannelSetActive	Activates a channel for the selected decoder.
EmailSend	Creates an email to send when an event occurs
FaceRecognitionValidateCardholder	A face capture is compared to pictures in the cardholders database. If no match is found after one minute, the action is triggered.
FaceRecognitionValidateGroup	A face capture is compared to pictures in the face recognition group database for a. If a match is found, the action is triggered.
Play Audio	Triggers an audio file to play through the speaker connected to a selected camera and stream.
PTZGoToHomePos	Returns a PTZ enabled camera to its home position.
PTZGoToPreset	Moves a PTZ enabled camera to a preset position.
PTZStartPatrol	Starts a Patrol sequence on a PTZ enabled camera.
StreamRecordStart	Starts recording of a camera or video stream when triggered by an event.
StreamRecordStop	Stops recording of a camera or video stream when triggered by an event.
VAStart	Starts a Video Analytic for the selected camera, when triggered by an event. *Note that only one analytic may be active for a camera*.
VAStop	Stops a Video Analytic for the selected camera, when triggered by an event.
ViewSetActive	Activates a view for the selected decoder.

I. The Gateway shall support the filtering of events being displayed by Event Category and Event Subtype.

J. The Gateway shall support an Event Log view of the system events from the web browser, filterable by Event Category and Severity.

K. The Gateway shall support acknowledgement of events including the ability to enter multiple time-stamped notes for specific events.

L. The Gateway shall support the ability to select an event and automatically pull up recorded video associated with that event.

M. The Gateway shall support a historical database of events that can be filtered, sorted, and searched by Event Category, Type, Severity, Device, Date, and Time.

N. The Gateway shall support a Grid View for viewing events, including face capture JPEGs, license plate capture JPEGs, and videos.

O. The Gateway shall support the ability to *lock* an event and associated information including recorded video, so that the related information cannot be groomed or deleted until the event is unlocked.

P. The Gateway shall support the ability to shunt and unshunt any event type by specific event source.

Q. The Gateway shall support events that have event status of *needs acknowledgement*, *open*, and *closed*.

R. The Gateway shall support an Event Pane display window containing the following elements as applicable to the specific event:

1. Loop of the event video in a repeating playback.

2. Clicking on the full screen icon shall take the user to the video player.

3. JPEG image of the camera view at the moment of the event.

4. User identification photo.

5. Event acknowledgement with an ability to enter User notes.

6. Time- and date- stamped Event history.

7. Control for exporting event data to CSV file and/or printing the event.

2.19 Event-Action Linkage

A. The Gateway shall support linking incoming events such as *motion* or *access denied* with a specific action such as *PTZ motion* or *email sending*.

B. The Gateway shall support Event-Action Linkages from 105 events and 18 action types (multiple actions per event).

C. Event-Action Linkage capabilities shall include:

8. Trigger actions based on defined schedule.

D. Changing event severity or setting *needs acknowledgement*.

E. Creating a custom Event Linkage, which would associate an Event Category with a *like* Event Type, an Event Schedule, Event Source, and custom Available Actions (see above). The Event Linkage can be assigned a Severity and an ability to require Acknowledgement.

2.20 Access Control System Description

A. The NLSS Gateway shall constitute a complete Access Control system with Video Management, Video Analytics, and Event Management.

B. The Gateway shall scale from small standalone deployments to large-scale deployments with hundreds of doors and multiple sites.

C. The Gateway shall support field-tested third party AC hardware (Assa Abloy, HID or Mercury) communicating with the Gateway over the network.

D. The Gateway shall support the capability to grant or deny access to controlled entry/exit portals.

E. The Gateway shall detect events and alarms, send them to a real time display for live operator processing and simultaneously store them for future investigations.

F. The Gateway shall support the following minimum capacities per-Gateway:

1. Users/Active Users: 100/10

2. Cardholders: 50,000

3. Reader capacities per third-party hardware in use:

Gateway	Assa Abloy/Sargent	HID	Mercury
GW-500	16	16	64
GW-3000	64	64	256
GW-4000	128	128	512
GW-5000	256	256	1024

4. Cameras capacities: (see section 2.6E)

5. Decoder capacities: 30

6. The Gateway shall not impose artificial limits on the number of cameras, encoders or doors supported.

2.21 Cardholders

A. The Gateway shall support a flexible system that can create, edit, and delete cardholder records.

B. The Gateway shall support the following information per person:

1. General Information

a. First Name

b. Middle Name

c. Last Name

d. Prefix

e. Suffix

f. Preferred Name (Nickname)

g. Personnel/Employee ID#

h. Cardholder Status (Active, Inactive, Terminated, Leave of Absence, PTO, Pending Hire, Returned, Lost, and Damaged)

i. Cardholder Type (Human Resources category selected from the drop-down list, such as employee, contractor, intern, temporary, student, etc.)

j. Vehicle Information

2. Credential Information

a. Activation Date and Deactivation Date

b. Badge Profile

c. Cards with Card # and Embossed #

d. Card Status

e. Photo

f. Access Levels

g. Contact information

h. Email

i. Phone #

j. SMS #

3. Organizational information

a. Department

b. Location

c. Supervisor

d. Title

4. User Defined fields = 20 (5 text, 5 numeric, 5 date, and 5 Boolean)

C. The Gateway shall allow enabling and disabling credentials via Cardholder Status, Card Status, or Access Levels.

D. The Gateway shall allow entry with extended unlock times for specific individuals, for compliance with the Americans with Disabilities Act (ADA).

E. The Gateway shall be able to trace the use of credentials throughout the system, even if the Access Control category is masked in the Event Pane.

F. The Gateway shall allow manual and/or scheduled enable/disable of credentials.

2.22 Access Levels

A. The Gateway shall support a flexible access level system that can apply to doors/readers and cardholders/credentials.

B. The Gateway shall have no fixed limit to the number of access levels it can support, however, the number of access levels available per cardholder record are defined by the manufacturer's hardware specifications, such as:

1. Assa Abloy/Sargent supports 15 schedules, 1 per cardholder record.

2. HID Edge supports 8 access groups per cardholder record.

3. Mercury Security supports 32 access levels per cardholder record.

C. Access levels shall be applied to cardholders/credentials.

2.23 Access Card Technology

A. The Gateway shall support the following access card bit formats:

1. 26-bit H10301

2. 37-bit H10302 (no Facility Code)

3. 37-bit H10304

4. Corporate 1000 (via user-definable custom card bit formats)

5. The Gateway shall support user-definable custom card bit formats.

6. Gateway shall support unformatted card format.

> **Note:** There can only be 1 active-37 bit access card format per system.

B. The Gateway shall support 125 kHz Proximity credentials and readers.

C. The Gateway shall support HID iCLASS 13.56 MHz credentials and readers.

D. The Gateway shall support the following reader modes:

1. Card Only

2. Card + PIN

3. PIN Only

4. Card or PIN

5. Locked

6. Unlocked

E. The Gateway shall support up to eight (8) card formats per intelligent controller. (*see Note under section 2.20A*)

F. The Gateway shall support facility codes based on the specifications of the intelligent controller.

2.24 ID Badge Creation

A. The Gateway shall support the creation of ID badges in either portrait or landscape orientation.

B. The Gateway shall support the importation of JPEG images, up to 320 x 240 pixels in size, for badge personnel photos and organization logos.

C. The Gateway shall support printing of badges directly from the web browser interface.

D. For Event reporting, the ID photo associated with cardholder is displayed with event related data.

2.25 Doors, Keypads, Readers, Strikes, Timeouts

A. The Gateway shall support default timeouts and individual overrides for:

1. Strike Time

2. Extended Strike Time

3. Door Held Open

4. Extended Door Held Open

B. The Gateway shall support REX (request-to-exit device) Timeout.

C. The Gateway shall support a primary and secondary REX, to allow the configuration of a standard REX to shunt the door contact, precluding a DFO alarm and an additional REX function for push button unlocks.

D. The Gateway shall support the use of keypad readers on Assa Abloy, Mercury and HID Edge E400 controllers.

E. The Gateway shall support the configuration of single door card-in/card-out readers on Mercury EP1501 controllers.

2.26 Access Control (AC) Hardware

A. The Gateway shall support the following third party access controllers and readers:

1. Mercury Security EP1501
2. Mercury Security EP1502
3. HID Edge ERP40 Reader/Controllers
4. HID Edge+ E400 Controllers
5. HID bioCLASS Biometric Keypad Smart Card Reader
6. Assa Abloy/Sargent vS1 PoE locks
7. Assa Abloy/Sargent vS2 Wireless locks

B. The Gateway shall support the following capacities:

Access Specifics										
Mfg	**Cardholders**	**Access Levels**	**Readers**	**Inputs**	**Outputs**	**Tamper Detection**	**Battery/UPS**	**Auto-Discovery**	**Event Buffer**	**Pin Codes**
Sargent v.S1/v.S2	2,000	15 schedules (1 per cardholder)	1	0	0	0	• Low Battery	no	10,000 transactions	4 digit pin code
HID Edge ERP40 int only	44,000	8 ACS groups per cardholder per controller	1	2 (DC=#1 & REX=#2)	2 (1=strike, 1=spare)	1	• AC Fail Monitor • Battery Fail Monitor	no	5,000 transactions	
HID Edge+ E400 int/ext	44,000	8 ACS groups per cardholder per controller	1	2 (DC=#1 & REX=#2)	2 (1=strike, 1=spare)	1	• AC Fail Monitor • Battery Fail Monitor	no	5,000 transactions	**You need to add an RK40 or RPK40 reader** 4-5 digit pin code
EP1501 (PoE)	240,000	32 per cardholder	1 in 1 out	2 (DC&REX)	2 (1=strike, 1=spare)	1	n/a	yes	50,000 transactions	8 card formats (1-37 bit) 5 digit pin code
EP1502	240,000	32 per cardholder	2	8 (DC=1+5, REX=2+6, 3/4/7/8=spare)	4 (2 strikes, 2 spare)	1	n/a	yes	50,000 transactions	8 card formats (1-37 bit) 5 digit pin code
MR50	n/a	n/a	1	2 (DC=#1 & REX=#2)	2 (1=strike, 1=spare)	1	n/a	no		
MR51e (PoE)	n/a	n/a	1	4 (DC=#1, REX=#2, 3/4 = spare)	2 (1=strike, 1=spare)	0	n/a	no		
MR52	n/a	n/a	2	8 (DC=1+5, REX=2+6, 3/4/7/8=spare)	6 (2 strikes, 4 spare)	1	n/a	no		
MR16-In	n/a	n/a	n/a	16	2	n/a	n/a	no		
MR16-Out	n/a	n/a	n/a	0	16	n/a	n/a	no		

C. The Gateway shall support the following third party AC Reader Interfaces:

1. Mercury Security MR52
2. Mercury Security MR50
3. Mercury Security MR51e

D. The Gateway shall support the following third party access hardware I/O modules:

1. Mercury Security MR16in
2. Mercury Security MR16out

E. The Gateway shall support the following third party Power over Ethernet (PoE) devices mentioned below:

1. Mercury Security EP1501

2. Mercury Security MR51e

3. HID Edge ERP40 Readers

4. HIDEdge+ E400 controllers

5. Assa Abloy/Sargent v.S1 locks

F. The Gateway shall support the following third party RS-485 data line multiplexer:

1. Mercury Security MUX8

G. The Gateway shall support the following third party card readers:

1. HID Prox

2. HID multiCLASS

3. HID iCLASS

2.27 Access Control (AC) Operations

A. The AC operations shall be seamlessly integrated into the NLSS Gateway functionality.

B. The access control functionality shall support the association of doors with cameras:

1. Providing an easy method for doors to be viewed by their associated camera for the purpose of supervised momentary unlock commands.

2. So that access control events can trigger video actions

C. The use of camera audio capabilities shall be available via the Operations menu.

D. The following access control operations shall be available (both locally and remotely) via the browser without going to a separate application:

1. Momentarily Unlock Door

2. Disable Credential

3. Enable Credential

4. Acknowledge access control Events

5. Select Event then display associated video.

2.28 Input Devices

A. The Gateway shall support dry contact input sensors used for general purpose I/O.

B. These input sensors are located on reader interface or an I/O interface, and can be connected to input devices.

C. These devices shall include motion detectors, power or battery failure detectors, electronic switches, etc.,

D. The interface shall provide icons with LEDs to indicate the device status.

1. Controller Connection Status

- Green = In Service/Online
- Yellow = Not in Service/Online
- Red = Offline
- Gray = Preprovisioned

2. Device Enabled Status

- Green = Enabled
- Red = Disabled

3. Device Active Status

- Red = Active (signal sent)
- Green = Not active

E. The Gateway shall provide the capability to associate a camera with an input device.

F. The Gateway shall provide a Push to Talk toggle to allow a user with the capability to communicate via the camera speaker and a local microphone, if a camera supports audio.

G. The Gateway shall record events related to the device in the Events Log.

2.29 Output Devices

A. The Gateway shall support output relays for general purpose I/O

B. These relays are located on a reader interface or an I/O interface, and can be connected to output devices.

C. These devices shall include alarms, warning lights, door unlock or lock electronic switches, etc.

D. The interface shall provide icons with LEDs to indicate the device status.

1. Controller Connection Status

- Green = In Service/Online
- Yellow = Not in Service/Online
- Red = Offline
- Gray = Preprovisioned

2. Device Enabled Status

- Green = Enabled
- Red = Disabled

3. Device Active Status

- Red = Active (signal sent)
- Green = Not active

E. The Gateway shall provide the capability to activate or deactivate a device from the web interface. This feature shall open or close the associated relay on the reader interface and I/O interface board.

F. The Gateway shall provide the capability to associate a camera with an output device.

G. The Gateway shall provide a Push to Talk toggle to allow a user with the capability to communicate via the camera speaker and a local microphone, if a camera supports audio.

H. The Gateway shall record events related to the device in the Events Log.

2.30 Maps and Floor Plans

A. The Gateway shall support seamlessly integrated maps and floor plans.

B. A Group's Show Map setting must be enabled to allow an image to be imported.

1. The recommended size of the .jpeg is 1300x800 @ 72dpi.

C. The Gateway shall allow the user to change the image by uploading a new map or floor plan.

D. Icons for devices included in the group shall be automatically placed on the map or floor plan.

E. The Gateway shall support the following map and floor plan functionality for the icons, without going to a separate application:

1. Arranging icons Doors, Cameras, Cardholders, Decoder, Users, Inputs, Outputs, Zones, Areas, Views, and Sequences from the floor plan.

2. Launching a separate dialog for the device managed by the icon.

3. Display cardholder or user information.

4. Display video associated with the selected device.

5. Performing momentary door unlock.

6. Open audio communication, if the camera supports audio I/O.

7. Displaying event information adjacent to the door control and camera control icons, with the ability to manage the event by clicking the event icon to go to event monitoring window with a single click to return.

8. Generating and printing reports via an icon to launch report from the map or floor plan (event type specific report content).

2.31 Reports

A. The Gateway shall support Reports that include, but are not limited to, the following reports, which shall be available both locally and remotely via the browser without going to a separate application:

1. Access Control:

- ACCESS GRANT - TRACE
- ACCESS DENIED
- ACCESS DENIED - TRACE
- CONTROLLER ONLINE
- CONTROLLER OFFLINE
- DOOR BATTERY LOW
- DOOR FORCED OPEN
- DOOR HELD OPEN
- DOOR UNLOCKED
- DOOR NOT UNLOCKED
- DOOR SECURED
- INPUT ACTIVE
- INPUT INACTIVE
- OUTPUT ACTIVE
- OUTPUT INACTIVE
- TAMPER
- ACTIVE CARDHOLDERS
- ACCESS LEVELS
- ACCESS LEVELS & CARDHOLDERS
- ACCESS LEVELS/CARDHOLDERS/DOORS

2. User:

- CARD ACTIVATED
- CARD DEACTIVATED
- DOOR OPENED
- LOG-IN
- LOG-OFF

3. Camera:

- CHANNEL LOSS
- CLIP EXPORTED
- DISCOVERED
- EXPORT FAILED
- IO EVENT
- MOTION EVENT
- ONNLINE
- OFFLINE
- SNAPSHOT EXPORTED
- VIDEO BOOKMARK
- VIDEO LOSS
- VIDEO RESUME
- EXT STORAGE ONLINE
- EXT STORAGE OFFLINE

4. Video Analytics

- ACTIVITY
- DIRECTION
- DWELL
- FACE CAPTURE
- LINE CROSSING
- OBJECT MOVED
- OBJECT TAKEN AWAY
- PEOPLE COUNT
- DIRECTIONAL PEOPLE COUNT
- PERIMETER

B. The Gateway shall support Report formats that include Column, Line, Pie Chart, and CSV data exports.

C. The Gateway shall support Report printing from the browser.

2.32 Cloud Services (Remote Management Services) Features

A. The NLSS Cloud Services system shall allow viewing multiple cameras from different sites in a single View.

B. The NLSS Cloud Services system shall allow the display and management of multiple sites from a single log-in screen.

C. The NLSS Cloud Services system shall provide a means for users to interface with their systems to:

1. Configure settings

2. Monitor live and recorded video

3. Search event data

4. Back up database

5. Create custom reports or set up automatic reports across multiple sites

6. Update software

7. Monitor system health

D. The NLSS Cloud Services system shall also include:

1. SMS/Email Notification based on event/alarm/system health

2. Access on most mobile devices including Android, iPhone, iPad, Netbooks

2.33 NextConnect®

A. The NLSS Cloud Services system shall enable users to establish a direct connection from the remote computer to the local NLSS Gateway or with other users on the system. This capability shall be accomplished using NextConnect—Next Level's patented peer-to-peer technology.

B. The NLSS Cloud Services system shall utilize decentralized system architecture to eliminate a single central point of failure.

C. The following system requirements shall be supported by the NextConnect technology:

1. Gateway-to-Gateway direct connections to assure remote video speed and quality, in contrast to central server-based video data streaming

2. Sharing of a single video stream by multiple users

3. Real-time video transcoding

4. Peer-to-peer video streaming

5. Unlimited simultaneous users

6. Peer to peer method of video streaming that ensures each stream's video quality and bandwidth minimization remain intact regardless of the number of users logged in to view a particular video stream.

2.34 Cloud Network Security Features

A. The NLSS Cloud Services shall use the following means to keep data private.

1. **Separate Database.** Each organization subscribing to the NLSS Cloud Services shall have an independent database.
2. **Multi-Tenant Model.** Within an organization's database, access to data shall be limited to authorized Users.
3. **Secure Connection.** The system shall force Client sessions to the Cloud Services web portals to utilize HTTPS, using the strongest encryption method the browser can negotiate (typically AES-256) and using standard gpg encryption that comes with GNU Linux.
4. **Secure Password Handling**. Passwords shall not be emailed or stored in the database. Instead, a secure one-way hash function shall be used that utilizes random data bits (i.e. a salt value) to create irreversible hash data, which shall be stored with the salt value so that passwords provided at logon can be similarly processed and validated against the stored values.
5. **Device Authentication.** Connections between Gateways and the NLSS Cloud Services servers shall be authenticated using X.509 digital certificates generated for each Gateway manufactured. Authenticated Gateways shall be securely connected to the NLSS Cloud Services system using AES-192 encryption.
6. **Certificate Authority.** The NLSS Cloud Services service shall maintain its own Certificate Authority used to manage & publish X.509 certificates and related Certificate Revocation Lists.
7. **Gateway-to-User Encryption.** Once a Gateway and a requesting web-browser *client* can successfully establish a peer-to-peer connection via the NextConnect method, all data exchanged between the two shall be protected using AES-128 encryption or stronger.
8. System data that is backed up from the Gateways by NLSS Cloud Services, such as Gateway configuration data, shall be encrypted using Open PGP standard as defined in RFC 4880. The data shall be encrypted prior to being stored in the NLSS Cloud Services system.

2.35 Point of Sale

A. Shall record each transaction as an event.

B. Recorded video shall be synchronized with each transaction.

C. Transactions shall be accessible from the Operations menu.

2.36 Intrusion Detection

A. The Gateway shall work with intrusion detection systems to associate cameras with a monitored location.

B. The Gateway shall allow intrusion panels to be added.

C. The Gateway shall gather information about areas, zones, keypads and zone expanders.

D. The Gateway shall accept alerts from the intrusion systems, and generate events from those alerts.

E. Intrusion panels shall be manually added to the Gateway.

F. From this connection, the Gateway shall gather information about areas, zones, keypads and zone expanders.

G. The Gateway shall allow Actions to be linked to these events.

H. The Gateway shall provide the capability to arm an area

I. The Gateway shall provide the capability to bypass zones.

Part 3. Execution

3.1 Examination

A. Examine substrates, areas and environmental conditions for compliance with requirements for proper installation and operation.

B. Remedy any unacceptable conditions before proceeding.

3.2 Installation

A. Install equipment in accordance with manufacturers' written instructions.

B. Install equipment in accordance with the National Electrical Code or applicable local codes

C. Ensure installation is secure and protected from accidental or weather damage.

3.3 Demonstration

A. Demonstrate proper functioning at final inspection

3.4 Technical Support and Training

A. Verify that technical support is available from the manufacturer and web-based training is available

3.5 Product Warranty

A. The Gateway shall be provided with a 12-month (from shipment date) product warranty for replacement and/or repair of defective equipment.