HARMAN
A SAMSUNG COMPANY

WHITE PAPER

AMX BY HARMAN
DEFINING SECURE AV

AKG AMX BSS CROWN dbx JBL PROFESSIONAL lexicon Martin Soundcraft

EXECUTIVE SUMMARY

Historically the biggest challenge to securing AV equipment has been the lack of standardized security profiles and policies for AV equipment. AV systems were often isolated from the enterprise network. Now, trends like "AV everywhere" and centralized AV device management demand that the AV system maintain a security posture in alignment with customer security goals. Starting with a select list of AMX branded centralized control and video distribution products, HARMAN is leading the AV industry to provide secure AV.

CONTENTS

INTRODUCTION

In firmware versions 1.4.x through 1.9.x the AMX NX Series Central Controllers have received a complete update of system security features designed to meet the strictest accreditation requirements. This includes all products with integrated NX Series Central Controllers.

- NetLinx NX Integrated Controllers NX-1200, NX-2200, NX-3200, NX-4200 and Massio ControlPads MCP-106, MCP-108
- Enova DVX All-In-One Presentation Switchers DVX-2255HD, DVX-2250-HD, DVX-3256HD, DVX-3255HD, DVX-3250HD, DVX-2265-4K, DVX-3266-4K
- Enova DGX 100 Series Digital Media Switchers, DGX800-ENC, DGX-1600-ENC, DGX3200-ENC, DGX6400-ENC, along with compatible boards and DXLink Transmitters and Receivers
- Incite Digital Video Presentation Switcher with Integrated Control, NCITE-813AC

In addition to the Central Controllers, AMX Modero X G5 Series Touch Panels v1.8.x have received security enhancements to allow them to securely provide the User Interface in a network environment.

SECURITY DESIGN METHODOLOGY

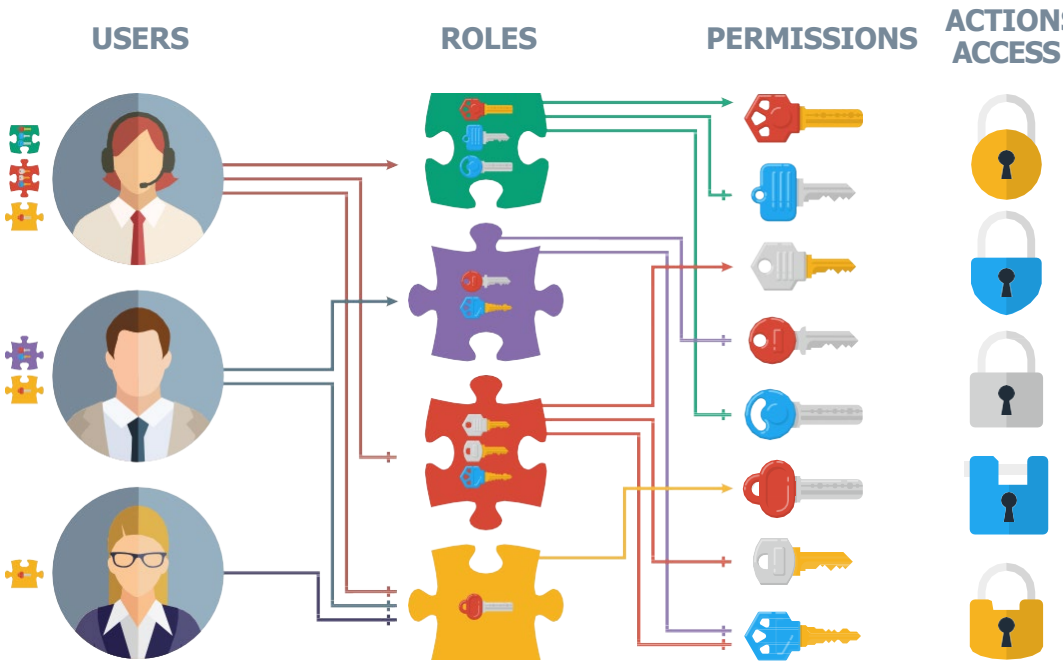
In order to create a target for security development, AMX took a risk management framework approach and analyzed security controls under frameworks such as ISO 27001 standards and the US National Institute of Standards and Technologies (NIST) SP800-53 to create an appropriate set of security controls for AV applications on the Network.

Once a control set was established, AMX surveyed security policies around the world, including (from the US) the Federal Information Processing Standard (FIPS) Publication 200, Committee on National Security Systems (CNSS) Instruction No. 1253 (CNSSI 1253), and Department of Defence Instruction (DoDI) 8510.01. AMX then applied the strictest control values for each control as the security target.

Security Design Philosophy

This does not dictate security controls, it provides the tools for the organization to enforce their security policy.

AMX realizes that different organizations have different risk profiles and security is “not one size fits all”. We make every effort to not dictate what controls or control values must be used on the systems but allow the organization to implement appropriate controls. For example, the Central Controller role based access control does not have fixed roles or role names allowing the organization which privileged actions should be assigned to each role and allowing roles to map by name to their existing LDAP schema.



Security should not impact functionality.

With the exception of restrictions on protocols, securing a system should not impact functionality to authorized users. This is extended to third party and legacy devices which do not have security features which meet organizational policy. These devices can be isolated from the enterprise network via the ICSLAN while still providing the advantages of IP control and management, proxied through the Central Controller.

AV systems should use the same security tools and techniques used for other IT assets and leverage existing IT assets.

AMX leverages standard IT security tools and techniques such as Lightweight Directory Access Protocol (LDAP) for authentication and authorization, syslog for consolidating and viewing security logs, and X.509 certificates to authenticate and secure devices.

Standalone devices must have the same security capabilities as devices which leverage enterprise assets. While in a large enterprise, operational efficiencies can be achieved by leveraging centralized infrastructure such as Active Directory for user management, the NX Series Central Controllers have internal features allowing the same controls and features provided by the centralized assets, including role based access control, password policy controls and full security logging.

Protect the workflow as well as the device.

Most AV systems limit security features to protecting the platform using features such as password protection and encryption. Because content is not accessible in a traditional AV system, the content routed through a HDMI switcher can't be accessed via the network, the potential impacts are limited to impacts to availability, or network intrusion vectors. There are however actions which can be taken as part of the user workflow accessed from the Touch Panel which may impact confidentiality and there may be other actions available at the user interface which should be considered privileged. AMX has extended role based access control, using the same authentication and authorization assets and configuration used for administrative access to the Touch Panel interface. These privileged actions are defined by the organization and implemented as part of the Touch Panel programming. Any control can be protected at a firmware level by setting a required privilege (added to one or more role) which will allow access or prompt for credentials of a user with elevated privileges. Any user actions can be sent to the security log fixing the paperwork trail problem.

Methodologically Defined and Implemented Security

The result of these efforts is the first AV system which includes the security features to meet any organizational risk assessment, applying controls which meet the policies of the organization, without the lost functionality of external mitigation.

The AMX Central Controller and G5 Touch Panels meet the statutory requirements for information systems used by the US Federal Government as defined under the Federal Information Security Management Act of 2002 (FISMA) and the Federal Information Security Modernization Act of 2014 (FISMA 2014). These include compliance with controls defined under NIST SP800-53R4, to the values set in Federal Information Processing Standard (FIPS) Publication 200 and FIPS Publication 140-2 compliant encryption.

The AMX Central Controller and G5 Touch Panels meet the statutory requirements for information systems used by the US Federal Government as defined under the Federal Information Security Management Act of 2002 (FISMA) and the Federal Information Security Modernization Act of 2014 (FISMA 2014).

ACCESS CONTROL

The Authentication, Authorization and Accounting (AAA) portion of the AMX Integrated Audio Visual System (IAVS) has a single **Security Policy Manager** which maintains the Authentication and Authorization requirements and configuration for the IAVS. The Security Policy Manager is a component of the Central Controller and maintains:

- Authentication and Directory Services policy
- Group membership (Directory Service) and Roles mapping
- Roles and permissions
- Permissions and credential requirements
- Password Policy

The Security Policy Manager can authenticate and authorize administrators and users either through the integrated directory service or to the organization's directory services, such as Active Directory via LDAP(S). The Security Policy Manager enforces login policy, including lockouts on failed login attempts and inactivity timers.

Password policy is enforced at the directory services level. If internal directory services are used password policy options include complexity, reuse, and lifetime. Users must change their password at first login and can change their own password.

Authentication

IAVS client devices and services do not directly authenticate users, but securely pass authentication and authorization requests to the Security Policy Manager through a Querier Application Programming Interface (QAPI) within system firmware. The Security Policy Manager then returns a Boolean Allow/ Deny to the IAVS client. This ensures that the security policy is maintained across all devices in the IAVS and facilitates management of the security policy.

For the purposes of a complete IAVS, Identity management is split into three categories:

- Administration
  - Authentication is a firmware level function, validating identity via internal LDAP directory services, or through external directory services such as Active Directory.
  - There may be more than one Administration Role for organizations which require segregated administrative privileges.
  - The web administrative interface supports two factor authentication through PKCS#11 smart cards attached to the administrative computer.
- User
  - This optional Identity Category is for the system User to authenticate and receive permission to perform programmed workflow functions on the IAVS.
  - User credentials are requested and transmitted to the Central Controller at a firmware level in G5 Series Touch Panels. Legacy Touch Panels can support entry of credentials through Touch Panel programming.
  - The G5 Touch Panels support two factor authentication through a USB CCID card reader and PKCS#11. This will support FIPS 201-compliant smart cards.
- Peripherals
  - Peripherals are client devices to the Central Controller. They authenticate with the Central Controller and allow administration based on the Central Controller granting permission.
  - Peripheral are locally, mutually authenticated within an individual Central Controller, either via configured User Name and Password or through 802.1x certificate Authentication.
  - The Security Policy Manager enforces login policy, including lockouts on failed login attempts and inactivity timers.
  - Password policy is enforced at the directory services level. If internal directory services are used password policy options include complexity, reuse, and lifetime. Users must change their password at first login and can change their own password.

Authorization

The Central Controller implements Role Based Access Control allowing for operationally defined and named roles.

Administrative interface

In addition to functionally defined permissions with these roles, data abstraction in the form of limiting allowed services to roles is implemented.

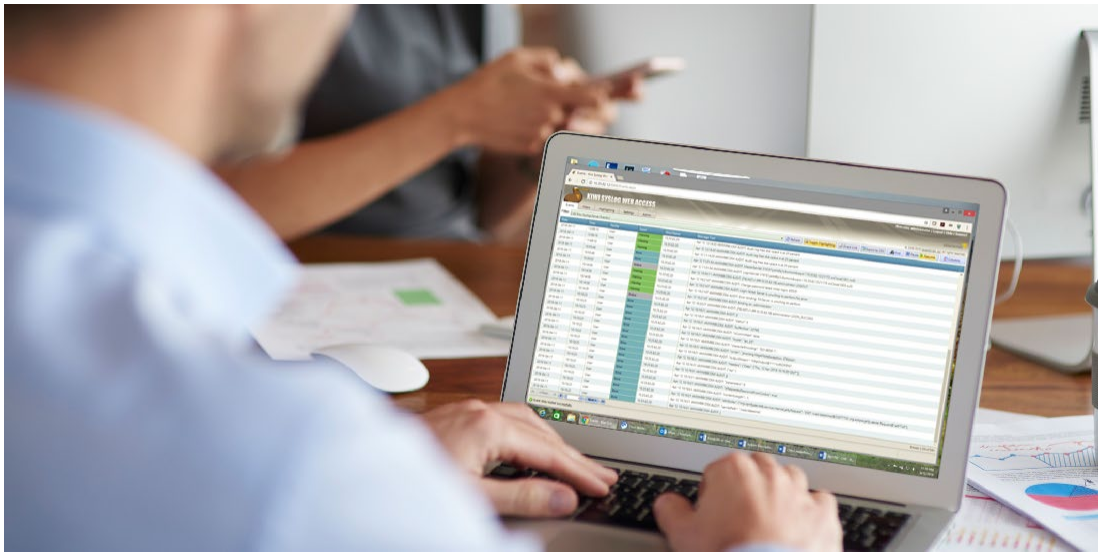
Access to administrative functions will require authentication and authorization through the Security Policy manager which verifies the credentials and authorization via the Active Directory servers and Group Membership.

User Interface

Four (4) workflow programmed permissions allow for role based access control to be extended to the room user interface. The requirements for access to various workflow actions, such as system access, security level changes, or administrative setup will be determined by the using organization.

Access to protected user functions will require authentication and authorization through the Security Policy manager which verify the credentials and authorization via the Active Directory servers and Group Membership.

Accounting



The AMX NX Series Central Controllers log auditable events as defined in FIPS 800-53. Local, cryptographically protected audit logs, sufficient for 1440 hours of independent operation are stored in a syslog format. Access to audit logs is a separate privilege assignable to a role, which allows for an audit role.

Audit Logs can alternatively be securely sent to a centralized syslog server for enterprise installations. When Audit logs are enabled the NX Series Central Controller saves the following items to the audit log:

- Successful and unsuccessful attempts to access, modify, or delete privileges, security objects, security levels, or categories of information (e.g., classification levels)
- Successful and unsuccessful logon attempts
- Privileged activities or other system level access
- Starting and ending time for user access to the system
- Concurrent logins from different workstations
- Successful and unsuccessful accesses to objects
- All program initiations
- All direct access to the information system
- All account creations, modifications, disabling, and terminations
- All kernel module load, unload, and restart
- Events programmed in the workflow to be logged

PERIPHERAL TRUST

AMX peripheral devices are bound to a single Central Controller through ICSP. The Central Controller may be configured to require devices to be authenticated in order to connect to the system. ICSP logins are implemented similarly to Challenge Handshake Authentication Protocol (CHAP – RFC 1994) to verify the identity of the device using a 3-way handshake.

This is done upon initial link establishment, and MAY be repeated any time after the link has been established.

The authentication exchange is as follows.

- Device sends a Device Info message to the Central Controller.
- Central Controller sends an authentication challenge message to the device.
- Device responds with an authentication response message to the Central Controller.
- This consists of the credential pair encrypted with the public key of the Central Controller.
- Central Controller authenticates the device according to configured policy.
- Central Controller responds with an authentication acknowledge message to the device.
- Device sends the Device Info message again.

Mutual authentication (device authenticating a trusted Central Controller) is achieved through Internet Control System Protocol-Secure (ICSPS) (Section 2.4.2). The device initiates a TLS connection and verifies the Central Controller is a trusted device through Public Key Infrastructure (PKI) (x.509) certificate exchange. Once a TLS connection has been established the device authenticates with the Central Controller.

Peripheral Isolation
Dual Network Interface (NIC)

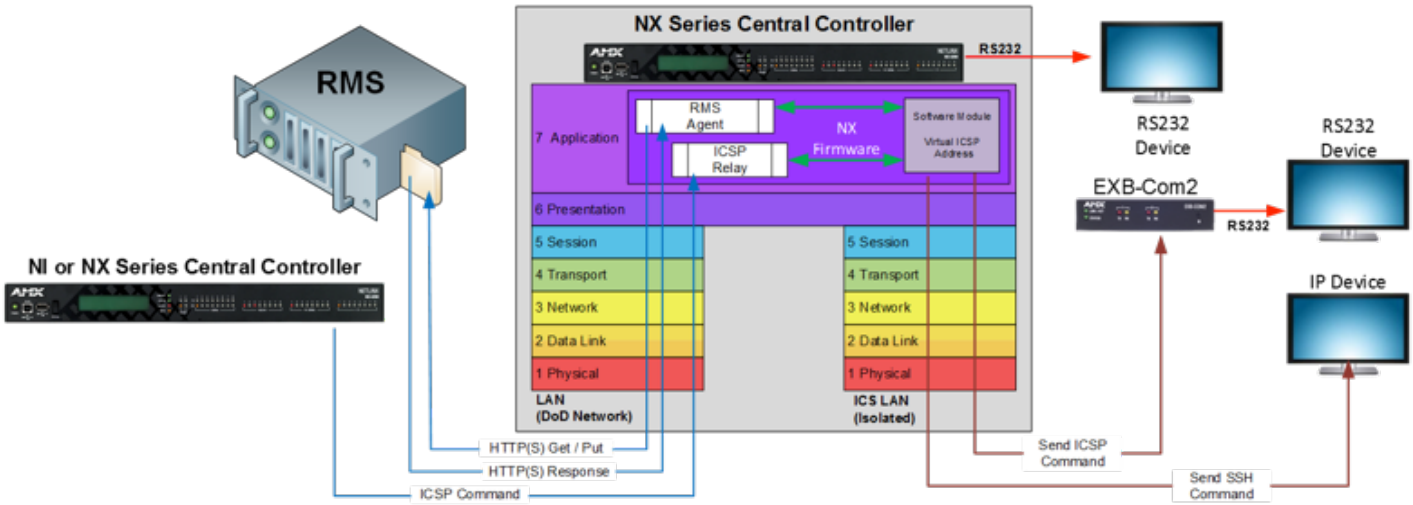
The integrated controllers in the AMX NX Series Central Controllers have two 10/100BaseT Ethernet interfaces. The first is intended for connection to the Data Network for external network communications such as database access or scheduling. This is referred to as the LAN port. The second, the ICSLAN is intended for communication with AV devices. In the case of the NX4200, the four (4) ICSLAN ports are unmanaged Ethernet switch ports on the ICSLAN local network for convenience in connecting ICSLAN devices.

These two Ethernet interfaces occupy separate logical address space and there is NO layer 1-5 communication possible between these two interfaces, including the possibility of a logical layer 3 (routing) path. This minimizes the possibility that any vulnerabilities on the ICSLAN can create a path to the data network.

ICSP Relay

AMX devices communicate with each other using a proprietary protocol called Internet Control System Protocol (ICSP). This protocol is tunneled over the Ethernet TCP/IP Network. ICSP is routable within AMX devices independent of transport medium. Each ICSP client device is logically bound to a single Central Controller. If a second Central Controller needs to communicate with a client device the ICSP communication is sent to the Central Controller the device is bound to and it is relayed to the client device through a Central Controller to Central Controller (CC2CC) connection.

As shown in the below, if a Central Controller needs to control or query a device on the ICSLan of another Central Controller, it will send an ICSP message using the ICSP address (D:P:S) of the device. The Central Controller for that device's ICSLan will receive the command\query on IP, completely de-encapsulate the IP communication and forward the data portion of the packet to the device. If the device is connected via IP, an entirely new Session will be created on the ICSLAN to forward the ICSP message to the device. If the device is not a native ICSP device, a virtual device in the ICSLan Central Controller will interpret the message and create the communication session (such as SSH) on the ICSLan interface.



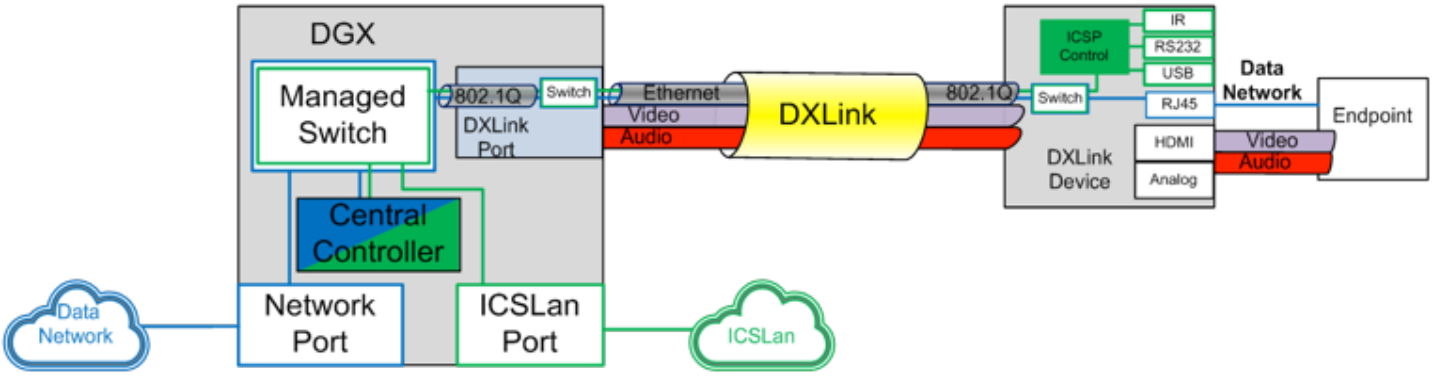
ICSLAN Devices

Any Ethernet device intended to be controlled by the Central Controller can be connected to the ICSLAN. This is particularly useful as a mitigation if the device to be controlled has a disallowed communications protocol such as Telnet. The device can be controlled via IP, but there is no logical network path to the data network.

Devices such as VTC Codecs which require an outside network connection for their application should not be connected to the ICSLAN Ethernet. The Central Controller may control them via RS232 connected to the ICSLAN, or via a routable network connection to the LAN via a secure communications protocol such as TLS or SSH.

ICSVLAN on DXLink Devices connected to DVX and DGX

The DGX100, DVX 22XX and DVX 32XX switchers Series Switcher features ICSVLAN which addresses the requirement to extend the enterprise data network to the DXLink Transmitter or Receiver, while isolating the control network (ICSLAN) from the data network. The DGX100 Series implements Virtual Local Area Network (VLAN) support within switches contained in the processor board, The DGX DXLink Input and Output Boards, and the DXLink Transmitters and Receivers. This allows the Network port on a DXLink Transmitter or Receiver to be assigned to the Data network, while still allowing isolated ICSLAN connection for device control and DXLink configuration and update.



The Ethernet port on the DXLink device may disabled or assigned to either the ICSLAN or the enterprise network.

INTER-DEVICE COMMUNICATION

Internet Control System Protocol (ICSP)

AMX devices communicate with each other using a proprietary low level protocol called Internet Control System Protocol (ICSP). This protocol can be carried over the Ethernet TCP/IP connection, RS232 PPP connection, and ICSNet connection to devices. ICSP is routable within AMX devices independent of transport medium. Each ICSP client device is logically bound to a single Central Controller. If a second Central Controller needs to communicate with a client device the ICSP communication is sent to the Central Controller the device is bound to and it is relayed to the client device through a Central Controller to Central Controller (M2M) connection.

Internet Control System Protocol- Secure (ICSPS)

ICSPS is a mechanism to tunnel ICSP though a TLS connection on port 1320. ICSPS requires the device to validate the Central Controller PKI certificate in order to establish the TLS connection. If the device is connected to the ICSLan, the Central Controller public certificate must be included in the device trust store since there will be no valid route to the Certificate Authority.

Legacy Encrypted ICSP

ICSP may also be encrypted where required by the environment. Encrypted ICSP uses a Challenge-Handshake Authentication Protocol (CHAP) with a three way handshake using the MD5 hash algorithm. The encryption is ARC4 with a commonly derived key, with no key information is passed between the hosts. The entire ICSP packet, including headers, is encrypted and the resulting data encapsulated in a new eICSP packet.

Encrypted ICSP has been maintained in the NX Series Central Controllers to support legacy devices which do not support ICSP.

Additional Security Features

The AMX NX Central Controller supports the following security standards:
X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate described in IETF RFC 6960 It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).

Certificate Revocation Lists (CRL) is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.

802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). PNAC provides the ability to grant or deny network access to devices wishing to attach to a LAN based on credentials tied to the

device rather than to a user. Until the device has been verified and permitted access, no network traffic is passed through the connected port, effectively keeping the device disconnected from the network.

FIPS 140-2 and FIPS 140-3 are U.S. government computer security standards used to approve cryptographic modules. The Central Controller settings allow for cryptographic strength to be set to “low” or “high”. The high setting disables all deprecated cypher suites per FIPS 140-2 or FIPS 140-3. In High Mode the following cypher suites are available:
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

About HARMAN Professional Solutions

HARMAN Professional Solutions (harmanpro.com) is the world’s largest provider of professional audio, lighting, video and control products. HARMAN’s best-in-class integrated solutions help customers to deliver the highest-quality results for concert tours, cinema, retail, corporate, government, education, large venues, hospitality and more. With brands that include AKG®, AMX®, BSS Audio®, Crown International®, dbx Professional®, JBL Professional®, Lexicon Pro®, Martin®, Soundcraft®, HARMAN Professional Solutions offers the most proven, innovative, and comprehensive solutions for the entertainment and enterprise markets. For more information, visit http://pro.harman.com/.

©2023 HARMAN. All rights reserved. Specifications subject to change.