IX Amplifier Series

Security precautions

At Dynacord, we understand the critical importance of cybersecurity in today's digital landscape. We recognize that securing a network, its devices, and the services it supports requires active participation from the entire supply chain and end-user organizations. Therefore, we are committed to providing our customers with the necessary resources and information to create a secure and resilient environment.

The IX amplifier series is designed for use in professional audio applications. It has a wide range of features, including many input and output channels, various mixing modes. Furthermore, it can act as a central place to aggregate and distribute control data in the network. Depending on the use case, you might want to implement just a subset or more than the given security measures. The first chapters of this guide elaborate on the various security controls that you should consider. In the second step, some best practices are mentioned.

1 Physical security

The first step in ensuring the security of the amplifier series is to ensure that it is physically secure. This also holds for other equipment being used in the system which are attached to the devices This means that devices should be kept in a secure location, and access to the device should be restricted to authorized personnel as much as possible. You may want to consider using locks or other physical security measures to prevent unauthorized access to the device.

2 Network security

The amplifiers are designed to be connected to a network, which means that it is vulnerable to various network-based attacks. To ensure the security of the device, you should take steps to secure your network. This may include using firewalls, setting up virtual private networks (VPNs), and implementing strong password policies.

2.1 Security

Security should be built up in layers. Network security is crucial: its main goal is to prevent unauthorized persons to access the environment. Only when unauthorized persons have breached through the network security layers, the security of the firmware and system itself (including hardening of the operating system, system authentication, and encryption) becomes important. This section describes several methods to harden the network and provide logical intrusion detection.

2.1.1 Use of VLANs

VLANs, or Virtual Local Area Networks, can be used to increase network security by isolating network traffic and limiting access to specific areas of the network.

Segmenting the network: VLANs can be used to segment the network into smaller, more manageable subnets, which can help to reduce the impact of attacks and limit the spread of malicious traffic.

Controlling access: VLANs can be used to control access to network resources by limiting which users or devices can access certain VLANs. For example, a VLAN can be created specifically for servers, and only authorized users or devices can be allowed to access that VLAN.

Enhancing monitoring: By segmenting the network using VLANs, network administrators can more easily monitor network traffic and detect any unauthorized access or suspicious activity.

2.1.2 Access Control Lists (ACL)

An access control list acts as a simplified firewall and allows system administrators to set rules for limiting the communication between network endpoints. Access control lists can be configured on most managed network equipment. It is recommended to check the product datasheet for the exact specifications. An example: 192.168.0.3 can communicate to 192.168.0.254 using port 3260. The communication on all other ports is prohibited.
As most access lists end with a "deny all other traffic" statement, they provide a very good first layer of defense against unauthorized network access by restricting the communication in the network.

2.1.3 MAC ACLs

MAC Access Control Lists (MAC ACLs) can be used in conjunction with VLANs to provide an additional layer of security to the network. MAC ACLs allow network administrators to control which devices are allowed or denied access to the network based on their MAC address.

When using VLANs, MAC ACLs can be applied to specific VLANs to further restrict access to the resources within that VLAN. For example, if a particular VLAN is dedicated to sensitive data, a MAC ACL can be created to only allow devices with authorized MAC addresses to access that VLAN.

MAC ACLs can be configured on a switch or router and are applied to a specific port or VLAN. When a device attempts to access the network through that port or VLAN, the switch or router checks the device's MAC address against the MAC ACL to determine if it is allowed or denied access.

2.1.4 Firewalls

A firewall has a similar function as an access control list: it restricts network traffic between network endpoints. On top of what an access control list can do, a firewall typically also performs "packet inspection". This allows a firewall to look at the content of the network traffic, verify if the right protocol is used, and if the traffic is matching the protocol specifications. As a result, it is not only able to check if traffic on port 3260 between the device and other devices is allowed, it is also able to check if the traffic matches the specification of the used protocol. Firewalls can be deployed as software only packages or combined hardware and software appliances. Well-known vendors include Cisco, Juniper Networks and Checkpoint.

2.1.5 Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection and Prevention systems go one step further compared to firewalls. These systems act as a "virus scanner" on the network. They can detect and block known, and unknown attack methods based on the signature and behavior of a specific attack. Well known vendors include McAfee, Cisco, Trend Micro and Fire Eye.

3 Software security

The software running on the Dynacord IX series should be kept up to date with the latest security patches and updates. You should also take steps to ensure that the device is not vulnerable to common software-based attacks.

4 Best practices

4.1 Limit internet access

Do not connect the system to the internet or open ports to the internet. The systems are designed to being used in local networks without being exposed to the internet.

4.2 Decommissioning

When you sell or decommission the device, make sure you set it to factory reset to clear all confidential data (config data including passwords of third-party APIs).

4.3 Port security

It is recommended to disable unused ports of network switches to avoid the possibility that equipment is connected that may compromise the system.

4.4 Wall panels

Wall panels are usually accessible for unauthorized people and therefore it would be easy to gain access to that specific network port.

Therefore, when using wall panels, we highly recommend using MAC-based VLAN assignment, which assigns the panel to a different VLAN depending on its MAC. Ideally combine this with a port security scheme like shutdown. I.e. when an unauthorized device attempts to connect to the port, the switch

should automatically disable the port, effectively preventing any traffic from passing through it. Furthermore, restrict the allowed MAC address allowed on that port only to the wall panel.

Finally, consider filtering out Dante traffic on that port, as Dante is inherently unsecure.

Also, consider hiding systems or elevated actions behind the PIN feature of the wall panels.

4.5 Lock Dante Ports

Unsecure Dante or AES67 audio connections are used both as inputs and as outputs. These Dante/AES67 connections are not authenticated and not encrypted. They form a security risk, as no precautions are taken against malicious or accidental attacks through their network interfaces. Only Dante devices that support Device Lock should be used. Device Lock allows you to lock and unlock supported Dante devices through a 4-digit PIN (Personal Identification Number). Make sure that the devices are locked when in normal operation. The Dante Controller is needed to set the PIN and setup the connections. Alternatively, when not in combination with the ARNI, consider using the Dante Domain Manager.

4.6 IX Amplifier series

Be aware that the IX amplifier series offer maximum compatibility with all networked audio devices to allow for fast and easy setup and maintenance, on the network. This means that these devices do not take any special precautions against malicious or accidental attacks via their network interfaces. Such attacks happen every day on the public internet. It is strongly recommended to use it in a safe and isolated network, meaning that no untrusted and unknown parties and hardware components can get access to the network. Furthermore, all parties of the network should not be connected to the internet or bridge to other networks.

An isolated network means that it is neither logically nor physically accessible to untrusted parties. In this specific case, if access to all network devices is physically restricted you have an isolated network.

However, devices located at the physical edge of the network are susceptible of being the entry for attackers. Especially wall panels or call stations are mostly installed in places that are accessible to the public. As these devices have to be connected to the same network to work properly, this also increases the risk of unwanted access to the network: people could try to disconnect the device and connect their own equipment to try to gain access to the network. If you have a higher security need, it is highly suggested to take specific security controls into account:

- Physically secure the wall panels by mounting them with e.g. resistorx screws
- At least use ACLs on the according ethernet ports. Only allow access to the network if the according MAC address is attached. Given another MAC address appears on that port, shut it down automatically.
- If present, use a firewall and / or intrusion prevention systems

As Dante by default is inherently insecure, make sure to filter all Dante (control / audio) traffic on ports used for the wall panels in both directions. Also Dante allows for further security mechanisms by using the Dante Domain Manager. Furthermore, restrict traffic to and from the wall panels to the following ports:

Origin	Destination	Destination Port	Protocol
WPN-1	IX	27999	Proprietary / Websocket / TCP
TPC-1	IX	55555 / 55556 / 55557	OCA / TCP

TPC-1 / WPN-1	IX	5350 / 5351	Bonjour / UDP
Webinterface	IX	80 / 443	HTTP and Websockets
Sonicue	IX	8090	HTTP for TaskEngine state
Third Party	IX	8989 / 8990	HTTP / Websockets / TCP OpenInterface
NTP-Server	IX	123	NTP

Also note that the IX series comes with a third-party TCP / HTTP interface which is disabled by default. These interfaces do not contain any sort of authentication or encryption.