Barco CTRL

Security Whitepaper

DATE 15/09/2023

AUTHOR **Timo Kosig** | Product Security Officer | timo.kosig@barco.com

https://www.barco.com/ctrl

Table of content

Security recommendations

This whitepaper includes security recommendations marked by a red shield icon, based on our experience and research. Following these is not mandatory, but highly recommended for optimal security. Look out for this red shield icon:

Security recommendation: Describes a setting or configuration that increases the security of the system.

Security at Barco

As a technology leader developing visualization solutions, including devices capable of connecting to the internet and related software, Barco is fully aware of the growing importance of corporate and product security.

At Barco, data governance is well managed, to protect our data and that of our customers and to comply with regulations like GDPR, and similar data privacy legislations outside the EU, such as HIPAA.

Information Security Management

Barco maintains an information security management system (ISMS) which complies with the ISO 27001 standard, covering policies, management involvement, business, and development processes, compliance with local laws, security awareness and security best practices.

In collaboration with the data protection officer, a growing number of high-risk third parties are assessed based on security and privacy requirements. In addition, our key vendors' external security activities are continuously monitored.

Gradually the scope of our ISMS and ISO/IEC 27001:2013 certification is being extended to contain all Barco processes, locations, and products. The products and locations already in scope are specifically mentioned on our certificate, which can be found on https://www.barco.com/en/about-barco/legal/certificates

Security Office

Barco's leadership has a clear commitment to cybersecurity, which translates into a Security Organization that operates along three lines of defense. Barco's Security Office, the second line of defense, has dedicated teams for driving Barco's cybersecurity program for both corporate and product security.

More information on Barco's cybersecurity can be found in our Trust Center: https://www.barco.com/eu-en/about/trust-center.

Barco's Secure Software Development Lifecycle

Our secure software development lifecycle follows the shift-left security approach: we aim to integrate security controls as early as possible in the design and development phases of our products.

This is industry best practice and becoming increasingly important to comply with regulations that focus on security by design, such as the United States Health Insurance Portability and Accountability Act (HIPAA), Medical Device Regulation (MDR), Radio Equipment Directive (RED) Delegated Act, …

To integrate these security controls, Barco uses source code management platforms, bug tracking systems, threat modeling, static application security testing (SAST), source code analysis (SCA) and compliance management tools, dynamic application security testing (DAST) and vulnerability scanners.

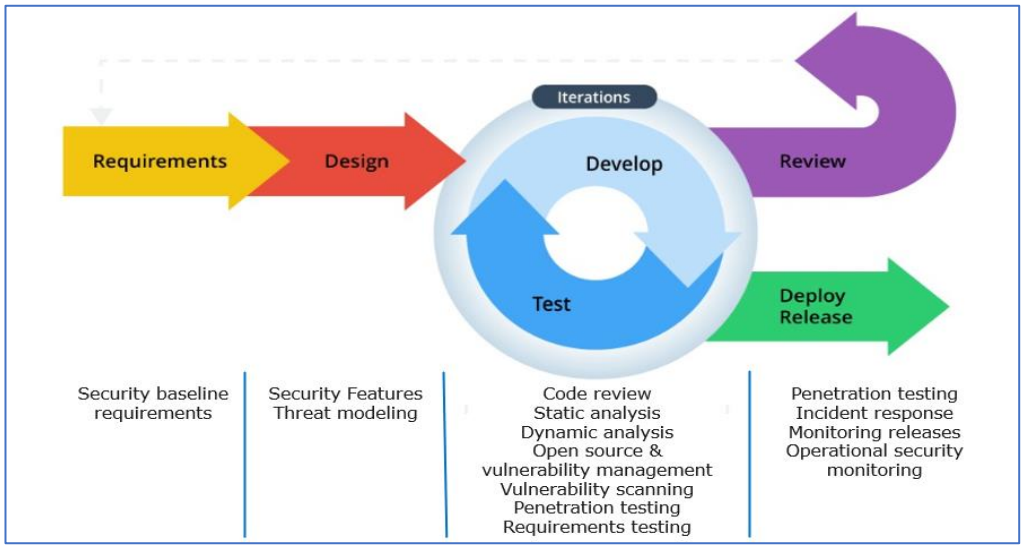
Furthermore, independent security experts are involved in training our developers and test the security of our products. Thanks to these efforts, Barco increasingly embraces the 'security by design' principle.

Over the last couple of years, Barco noticed an increase of market questions and requests concerning security, user scenarios, integration methods, etc. With all those topics in mind, we perform extensive threat modeling during our products' design and development phases.

Threat modeling is one of the most potent security engineering activities since it focuses on designing vulnerabilities as well as the threats that could exploit them. A design vulnerability is a hypothetical weakness within a system's design that could potentially be exploited. A threat is a potential for a malicious actor to exploit existing vulnerabilities.

Vulnerabilities can and should be solved, but threats can live on indefinitely or change over time and cannot be controlled by the people managing or using the device or system. Threat modeling facilitates a risk-based product development approach by uncovering risks related to threats and encouraging the use of secure design and development practices.

Threat modeling, therefore not only needs to focus on software, but also hardware and even production-related topics need to be covered to create a secure product in every aspect.



Product introduction

Barco CTRL is an innovative, scalable software platform for control rooms that simplifies workflows, deployment, and serviceability. Designed to uphold the highest levels of cybersecurity, Barco CTRL allows users to securely connect to their sources and interact with the content on any video wall or operator desk.

Although the system is very powerful, it is also simple to set up with a wizard guiding the installer through the configuration process. A single platform that serves both the video wall and operator desk, Barco CTRL extends the same intuitive look and feel over the complete control room and beyond.

Barco CTRL is fully scalable and grows with your needs. This means that by simply adding additional encoders and decoders, the solution can start small and potentially expand to a global system. Barco CTRL also takes all possible measures to prevent downtime (including redundancy options of critical components).

For Barco CTRL, we have chosen to follow a security-by-design and security-by-default approach, in order to be able to provide the highest levels of security in the default configuration and deployment of the solution.

Reconciling these increased security requirements with usability and user experience has always been challenging. Increasing security can result in poorer usability, while an exclusive focus on user experience and usability can result in a poorly secured product.

Finding a perfect balance between these three requires attention from the very start of a product lifecycle.

The Barco CTRL development teams follow the (secure) Software Development Life Cycle (SDLC) process, and during the initial stages of this process, the security aspect of the Barco CTRL solution was already accounted for and given top priority.

This focus on security ensures that the final product is a very user-friendly system that protects users of the system against malware, corporate espionage, and hackers at the same time.

Another important aspect that was taken into account from the early stages of the SDLC process is the privacy-by-design principle which aims to minimize or eliminate the amount of collected personal data (e.g., IP, username, MAC addresses).

What does the system look like?

The system is composed of encoders, a backend server appliance, and decoders.

The system supports various source types such as traditional AV sources, web sources, camera streams and virtual desktop sources (RDP, VNC). Encoders are optional and are only needed when traditional AV sources need to be integrated. All other source types only require a server and a decoder to be part of the system.

Where traditional AV sources are used, encoders convert baseband display signals from external systems to a bitstream that can be transferred over a network connection. At the same time, they allow for keyboard and mouse inputs to be fed back into the external system by emulating USB input devices.

The video bitstreams are directly sent to the decoders, which support both control desk and video wall use cases. The system operator interacts with the decoder system via a single connected keyboard and mouse, allowing control of all incoming signal sources, including web sources – such as dashboards – and remote desktop protocol (RDP, VNC) connections.

The backend server appliance stores the configuration of all connected systems. It allows for plug-and-play integration of additional encoder or decoder systems and offers a unified, web-based administration interface where system administrators can easily control the configuration of both signal sources and outputs.

What data needs to be protected?

The system contains credentials and system configuration data, such as credentials for connected web or RDP sources, certificates for identity verification of devices and services, and secrets for encrypting content in transit.

In many use cases, the media content transferred and shown by Barco CTRL can be of a restricted origin and needs to be protected from public exposure or even for internal stakeholders (classified data).

Where is the system physically located?

Barco CTRL is operated on-premises at the customer site in an environment with physical access controls. Encoders will be physically located with source systems (e.g., servers), whereas decoders can also positioned the control room itself. The backend server appliance can be located in any secured server room with access to the network. If the system is set up for high availability, additional server nodes can be in different physical locations to ensure redundancy.

Web and remote desktop (RDP, VNC) sources can be located anywhere, as long as a network

connection between the decoder and the source can be established.

Who is using and who is managing the system?

Operators use the system on a day-to-day basis. They configure their desks or video walls so that all relevant sources are grouped and displayed in a sensible fashion, allowing them to observe and interact with sources of different types and origins (server display outputs, web sources, RDP sources and video streams such as camera feeds) at the same time.

System administrators use the system to configure content sources, connected devices, security settings, user management, integration with external identity providers that are LDAP compliant such as Active Directory and perform maintenance tasks such as backup and restore and view diagnostic system data as well as perform system updates.

Product security

Layered approach

The cornerstone principle of information security is the "CIA triad": Confidentiality, Integrity, and Availability. Furthermore, additional security requirements such as Non-Repudiation, Authenticity and Reliability need to be met. All parts of a product or system must honor these requirements throughout the system's life cycle to guarantee a secure environment.

A network connected system can be divided into different layers: physical, network, host, and application layer. Mapping these four layers onto the security requirements will reveal how security is implemented in a system and reveal where safeguards are missing. The layered approach and the implementation of multiple safeguards to protect a system will ensure that in case one safeguard fails, another safeguard prevents compromising the system, providing a "Defense in depth" approach. The safeguards must correspond to and mitigate the threats identified in the threat modeling.

Authentication

Machine/Node Authentication

System devices (encoder, backend server, decoder) are shipped with a Barco-signed certificate by default. This certificate is used to verify the identity of a device that is added to the system to ensure only genuine, trustworthy Barco devices can be added to the system.

During initial installation, the server will automatically set up a new custom root certification authority (CA) that resides on the server. This PKI will be used to generate application certificates that will be installed on the devices and will be used for mutual TLS authentication and encryption between devices going forward.

This approach ensures that only genuine Barco devices can be added to a Barco CTRL installation and that once added, only devices belonging to the same Barco CTRL installation can communicate with each other.

An automatically created, self-signed certificate is used to secure the wall and desk user interfaces as

well as the administrative web interface. The user can upload a certificate signed by their own CA that will be used to secure those user interfaces.

Security recommendation: Upload a certificate signed by your own CA to ensure that connections to any Barco CTRL user interface will be verified as secure (e.g., when using a web browser to access the administration interface).

Person Authentication

The server has a default admin account which authenticates with a password. The password must be changed by the user at the time of installation. The new password must be at least 12 characters long and contain at least one upper case, one lower case and one special character. The new password must not match the username or have similarities to the last three used passwords. The account is temporarily locked for 10 minutes after two consecutive login failures. The password is stored on the server as a salted hash. The hash algorithm family used is SHA-2.

Regular system users authenticate via login/username and password. Barco CTRL supports integration with an external identity provider via LDAP v2/v3 over SSL (LDAPS). Internal user accounts will be supported in a future release.

Security recommendation: Configure the system to connect to your external identity provider via LDAP over SSL to ensure that the confidentiality of user data synchronized to Barco CTRL is guaranteed.

When an external identity provider is configured, authentication is handed off to the external identity provider; therefore, any relevant security functions, such as locking user accounts after several failed authentication attempts, password complexity requirements, password re-use requirements, etc., are handled by the external identity provider.

Security recommendation: Ensure that appropriate password complexity requirements, password re-use requirements and account locking rules are in place in your external identity provider, as it will be responsible for authentication and enforcement of associated requirements.

By default, external identity providers are configured such that user data is only retrieved and cannot be changed in Barco CTRL. This configuration can be changed to allow local changes of user attributes and passwords, which are then synchronized back to the external identity provider.

Role based access control (RBAC)

Barco CTRL supports RBAC by allowing system users to be assigned roles with specific rights. Roles can also be assigned to groups to which users can be added to simplify access rights management.

Existing roles

Operator	Allows the user to log into wall and desk user interfaces where the user can create and modify desk and wall layouts for content arrangement. The user is able to see content from pre-defined sources.
Administrator	Allows the user to log into the administrative web interface to access and change system configuration settings as well as user management and definition of content sources.

Security recommendation: When integration with an external identity provider is configured for administrative rights, make sure the local admin account is still properly managed as a fallback option in case the external identity provider is not available.

It is recommended to have two or more members of your organization assigned with administrative rights to guarantee operational continuity in case of absence.

Security recommendation: It is the responsibility of the customer/integrator to regularly perform an access control review and remove any unused accounts, roles, and privileges.

Privacy by design

Personally identifiable information is processed in alignment with GDPR, and care has been taken to ensure that only personal data is processed that is required for the installation and operation of Barco CTRL.

All data that is created/processed during operation is maintained locally on-premises and does not leave the customer environment.

Barco's product privacy statement outlines more details regarding privacy, including which personal data is collected for which purposes and Data Subject Rights.

You can find the Product Privacy Statement on the following website: https://www.barco.com/en/about-barco/legal/privacy-policy/product-privacy-statement.

Encryption at rest and in transit

Encryption of data at rest is facilitated by operating system-level encryption of hard disks of each system device. The encryption uses 256-bit cryptography and encryption keys are stored in a hardware root of trust.

Passwords required for access of content sources (e.g., web, camera, or RDP sources) are additionally also encrypted at the file system level.

All non-video data transmitted between system components is encrypted using TLS 1.3. For non-video data transmitted to/from external systems a fallback to TLS 1.2 is possible if TLS 1.3 is not supported by the external system. Video data in transit is encrypted using 128-bit cryptography.

The system administrator can add root certificates to a user trust store, which is being used for verification of the validity of the certificate that the external identity provider presents.

Usage of open-source

Barco CTRL makes use of multiple open-source software packages. Barco closely monitors these for any open-source licenses violating our own policies which would impact intellectual property and for new vulnerabilities detected in the used open-source packages.

If a vulnerability is detected or reported, it will be analyzed, and depending on the criticality and impact, it will be planned to be remediated in a future release.

Secure software upgrades

New software versions for the system are released at least every quarter. These new versions include next to new features, regular security fixes.

Should a security vulnerability require an intermediate release in between regular release cadence, then Barco's software development and release process can be adapted to this situation. This will be subject to a risk-based approach, which will consider the severity of the vulnerability that needs to be addressed and the impact on the product and its operation by the customer.

To protect the integrity of the upgrade files and the devices themselves, the software upgrade files are:

- Signed: to establish proof of origin, all firmware software files are digitally signed by Barco. Signature verification happens when installing new software upgrades.
- Encrypted: all software upgrade files are encrypted to protect the potentially sensitive content in the software upgrade file and prevent reverse engineering.

Security recommendation: To make sure that your installation is as secure as possible, it is highly recommended to keep your installation in sync with the latest release.

New security fixes are not backported to older releases but are deployed with future new releases. Therefore, it is important to keep your installation up to date.

Attack surface reduction

Care has been taken to reduce the system's attack surface as much as possible. Any unnecessary services have been disabled in the system. Users can only login into the system via wall and desk user interfaces or via the administrative web interface. Access to the operating system is not possible.

Network connectivity

Barco CTRL was designed with network segregation and isolation of media content in mind to allow system/network administrators and security personnel to deploy and maintain a secure environment for their control room.

Security recommendation: Deploy Barco CTRL in a segregated network. Utilize different VLANs for backend server and devices handling media content (encoder, decoder). Use a firewall configured to only allow outgoing connections from the media network.

The system's architecture does not require any incoming connections into the media network. All connections to the server will be initiated from encoder or decoder devices.

For an overview of the system's network communication and all ports used for inbound or outbound connections, please refer to our Network Design Guide (R591966) document here: https://www.barco.com/en/support/docs/r591966

Operating System

All devices of the system are built upon Linux-based operating systems.

While running on a Linux-based operating system, the devices that comprise Barco CTRL are appliances – they are fully hardened to not allow access to the operating system. Neither normal nor administrative users can log into the operating system and no additional software can be installed by users.

The devices utilize secure boot and will only boot disk images that have been digitally signed by Barco. The keys used to verify the authenticity of disk images are stored in the devices' hardware trusted platform module. Therefore, it is not possible to boot unauthorized software.

We do not allow 3rd parties to install software packages on top nor to replace our software with non-official binaries. Our software went through a process of functional validation, code review, and security checks. All software binaries are stored on a read-only file system, and additionally, all system devices check at boot time whether the file system on disk has not been tampered with.

This is done through a multistage process of secure boot, in which the CPU boot ROM or BIOS firmware verifies the signature of the bootloader. This bootloader verifies the signature of the Linux kernel, which, in turn, verifies the integrity of the read-only file system containing all the software binaries. The BIOS settings are password-protected to prevent secure boot and other security or performance-related settings from being disabled or changed.

Updates to the operating system are installed as part of the secure software upgrades. Barco CTRL uses Linux distributions that have support for the foreseeable future and closely follows operating system releases, patch releases, and security fixes of the upstream Linux distributions.

Physical security

Protecting the physical interfaces of devices is as important as protecting the other layers of the system. This concern was taken into account from the very first phases of the project, but it needs to be noted that Barco also depends on the hardware features that third-party suppliers provide.

Security recommendation: Depending on the risk profile of your usage of control room software, consider putting some or all system devices behind additional physical access controls, e.g., locked in a server room.

Shared responsibility model

Barco CTRL is an on-premises solution and is therefore operated using a shared responsibility model with both the customer and Barco having distinct responsibilities to ensure the continued security of the solution.

Barco as the manufacturer will provide a secure-by-design and secure-by-default solution. We will continuously monitor the product for security vulnerabilities and provide frequent patches and security updates whenever required. Barco will provide security incident notifications through the customer's MyBarco account and will also publish security bulletins on the Barco website when appropriate.

The customer is responsible for upholding the security of the deployed solution. This includes the following aspects:

- Ensuring that security configuration is only loosened when required by the deployment scenario and that other mitigating controls are put into place to offset any changes made that may weaken security.
- The responsibility for onboarding and offboarding users to the solution, while ensuring that adequate password strength and complexity, password re-use and account lockout configurations are in place that match the customer's policies.
- Timely installation of software updates and security patches that Barco provides.
- Ensuring the security of the network environment in which the system operates by employing network segregation and controlling and monitoring data flows using firewalls.
- Ensuring that the physical security of the different system components is adequate by placing them in locations with restricted access, which is granted for authorized personnel only.

Product Security Incident Response

As a global technology leader, Barco is committed to delivering secure solutions and services to our customers while protecting Barco's intellectual property.

When product security concerns are received, the product security incident response process will be triggered immediately. To address specific security concerns or report security issues with Barco products, please inform us via contact details at https://www.barco.com/psirt.

To protect our customers, Barco does not publicly disclose or confirm security vulnerabilities until Barco has conducted an analysis of the product and issued fixes and/or mitigations.

Closing

Barco CTRL was designed with security in mind during all stages of the Software Development Lifecycle. We hope this security whitepaper was able to provide the information you were looking for. If any questions might have been left unanswered or for application-specific support, please contact Barco Support via https://www.barco.com/support.

VERSION TRACKING NR: 1