Barco CTRL

# Sicher konzipiert, voreingestellt vertrauenswürdig

## Ein Leitfaden zur Sicherheit bei KVM-over-IT




Lesen ↓

# Sicherheit ist die Grundlage, keine Feature

Kontrollräume sind der Mittelpunkt kritischer Betriebsabläufe. Stromnetze, Verkehrsnetze, Notfallreaktionssysteme, Öl- und Gasinfrastruktur … In diesen Räumen getroffene Entscheidungen wirken sich konkret auf Menschen aus. Das macht sie zu einem attraktiven Ziel für jeden, der Störungen verursachen will.

Cybersicherheit in Kontrollräumen war noch nie so wichtig wie heute. Die Risiken waren noch nie so groß. Neue Vorschriften können Führungskräfte für Sicherheitsmängel persönlich haftbar machen. Die Angreifer werden immer raffinierter. Und die Konvergenz von IT und OT führt dazu, dass Hardware, die bisher immer auf einer digitalen Insel betrieben wurde, plötzlich mit der Außenwelt verbunden ist. Dadurch entstehen neue Angriffsflächen, die bei ihrer Entwicklung nie berücksichtigt wurden.

Barco CTRL wurde genau für diese Umgebung entwickelt. Als KVM-over IT-Plattform ist Sicherheit keine Zusatzfunktion. Sie ist auch keine nachträgliche Überlegung. Sie bildet die Grundlage, auf der alle anderen Fähigkeiten beruhen. Barco CTRL wurde von Grund auf nach den Prinzipien von „Security by Design" entwickelt. Das System wird von einem speziellen internen Sicherheitsteam unterstützt. Damit gibt Barco CTRL Organisationen die Gewissheit, ihre kritischen Betriebsabläufe mit den benötigten Netzwerken verbinden zu können – ohne dabei Tür und Tor für Bedrohungen zu öffnen, die sie sich nicht leisten können.



**Dieses E-Book beleuchtet zwölf Wege, mit denen Barco CTRL das Thema Sicherheit angeht – von der Architektur der Plattform selbst bis hin zum regulatorischen Umfeld, in dem es Organisationen unterstützt.**

# Inhalt


## Teil 1

**Sicherheit durch Design**

Security by Design und Zero Trust

Die 5 Säulen der Barco CTRL-Sicherheit

Keine offenen Türen

Voreingestellt sicher

## Teil 2

**Sicherheit im Betrieb**

Flexible Lizenzierung

Softwarebasierte Architektur und Ein-Klick-Upgrades

Skalierung ohne erneute Schulung

Offene APIs für die Integration von Drittanbietern

## Teil 3

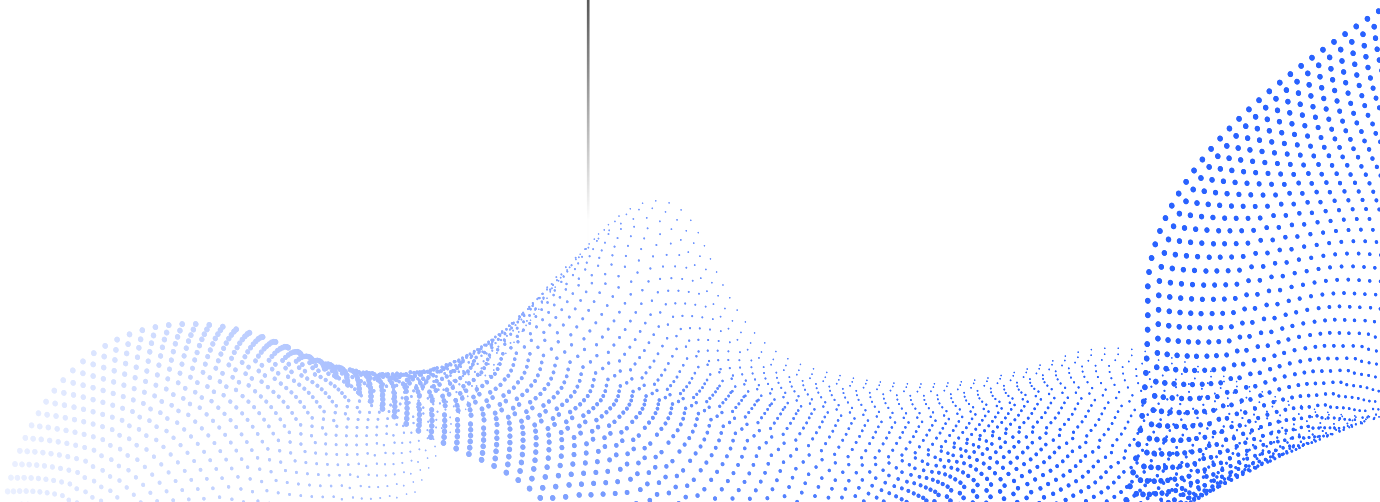
**Sicherheit im Kontext**

IT-OT-Konvergenz

Sicherheit trifft Flexibilität

Einhaltung gesetzlicher Vorschriften

Haftung und gemeinsame Verantwortung



# Teil 1
# Sicherheit durch Design

## 1. Security by Design und Zero Trust

Die meisten Sicherheitskonzepte gehen von einem Produkt aus und fügen diesem erst im Nachhinein Sicherheitsfunktionen hinzu. Barco CTRL ging den umgekehrten Weg. **Von der allerersten Entwurfsentscheidung an bildete Sicherheit das Fundament – nicht etwa eine Ebene, die nachträglich hinzugefügt wurde, sondern das Prinzip, das jede architektonische Entscheidung prägte.**

Dieser „Security by Design"-Ansatz wird durch eine Zero-Trust-Architektur ergänzt. In einem Zero-Trust-Modell wird standardmäßig nichts als sicher vorausgesetzt: weder Geräte, noch Benutzer, noch Netzwerkverbindungen. Jede Zugriffsanfrage wird authentifiziert und autorisiert, jeder Kommunikationskanal wird überprüft. Dies ist insbesondere in Kontrollräumen von Bedeutung. Dort können die Folgen erfolgreichen Eindringens weit über das IT-System selbst hinausreichen. Weitere bewährte Verfahren, darunter die „Shift-Left"-Methodik – bei der Sicherheitstests bereits früh im Entwicklungsprozess und nicht erst am Ende durchgeführt werden –, stellen sicher, dass Schwachstellen erkannt und behoben werden, bevor sie überhaupt in ein produktives System gelangen können.

**Das Ergebnis ist eine Plattform, die nicht nur behauptet, sicher zu sein, sondern die auch so aufgebaut ist, dass sie sicher ist.**



## 2. Die 5 Säulen der Barco CTRL-Sicherheit

Die Sicherheitsarchitektur von Barco CTRL basiert auf fünf klar definierten Säulen, von denen jede eine bestimmte Ebene des Systems abdeckt. Zusammen bilden diese fünf Säulen eine lückenlose mehrschichtige Verteidigungsstrategie.

1

**Das Identitätsmanagement** stellt sicher, dass nur autorisierte Benutzer und Geräte auf das System zugreifen können. Dazu kommen robuste Authentifizierungsmechanismen wie die Multi-Faktor-Authentifizierung (MFA) und die attributbasierte Zugriffskontrolle (ABAC).

2

**Der Kommunikationsschutz** verschlüsselt alle übertragenen Daten mithilfe von TLS 1.2 und 1.3 sowie mTLS, wobei eine zertifikatsbasierte Authentifizierung sicherstellt, dass jede Verbindung legitim ist.

3

**Der Systemschutz** deckt den gesamten Lebenszyklus der Plattform ab – von sicheren Boot-Prozessen, die das Laden nicht autorisierter Software verhindern, bis hin zu verschlüsselten Speichern und striktem Update-Management.

4

**Die Audit-Protokollierung** erstellt umfassende, manipulationssichere Aufzeichnungen aller Systemaktivitäten – Anmeldungen, Konfigurationsänderungen, Datenzugriffe – und liefert damit den Audit-Trail, der sowohl für die interne Governance als auch für externe Vorschriften erforderlich ist.

5

**Der Medienschutz** stellt sicher, dass Inhalte auf Geräteebene verschlüsselt und zugriffskontrolliert werden. Damit wird verhindert wird, dass Daten extrahiert werden können, selbst wenn ein physisches Gerät kompromittiert ist.

## 3. Keine offenen Türen

Einer der häufigsten Angriffsvektoren in jedem vernetzten System ist der Endpunkt – das einzelne Gerät, über das Benutzer mit dem Netzwerk verbunden sind. Offene Computer mit allgemeinem Verwendungszweck sind besonders anfällig: Sie können nicht autorisierte Software ausführen, unbekannte USB-Geräte akzeptieren und durch Benutzer kompromittiert werden, die Anwendungen außerhalb der zugelassenen Umgebung installieren.




Barco CTRL löst dieses Problem durch den Einsatz eines speziellen Appliance-Modells. **Die Decoder und Encoder, aus denen sich die CTRL-Hardware zusammensetzt, sind speziell entwickelte, abgesicherte Geräte, auf denen ausschließlich von Barco signierte Software ausgeführt wird.** Benutzer haben keinen Zugriff auf die Boot-Einstellungen. Nicht autorisierte Software kann nicht installiert werden. Das Systemdesign schließt von vornherein das Risiko aus, dass ein kompromittierter Endpunkt Malware in das System einschleust.

Dieser Ansatz ist besonders wirksam gegen Insider-Bedrohungen, eines der am meisten unterschätzten Risiken in kritischen Infrastrukturumgebungen. Die Angriffsfläche verringert sich drastisch, wenn die Hardware selbst bereits auf der Geräteebene unbefugten Zugriff verhindert. Das Appliance-Modell ist daher nicht nur eine Hardwareoption, sondern eine Sicherheitsstrategie.

## 4. Standardmäßig sicher

Ein System, das von Grund auf sicher entworfen ist, dessen Sicherheit jedoch erst durch umfangreiche Konfiguration aktiviert wird, ist nur so sicher wie die Person, die es konfiguriert. Menschliches Versagen bei der Einrichtung von Sicherheitsmaßnahmen ist eine der häufigsten Ursachen für Sicherheitslücken in bereits im Einsatz befindlichen Systemen – eine übersehene Einstellung, ein unverändertes Standardpasswort, ein unnötig offener Port.

Barco CTRL ist standardmäßig sicher. Das bedeutet, dass **das System bei der Bereitstellung bereits in seinem sichersten Zustand ist, ohne dass vom Installateur zusätzliche Sicherheitskonfiguration erforderlich ist.** Unnötige Services werden deaktiviert. Es werden keine Standard-Anmeldedaten verwendet. Alle Kommunikationskanäle sind ab dem Zeitpunkt, an dem das System online geht, verschlüsselt.

Dieser Ansatz beseitigt eine erhebliche Risikoquelle im Bereitstellungsprozess und stellt sicher, dass jede Barco CTRL-Installation – unabhängig vom technischen Fachwissen des Installateurs – auf derselben soliden Sicherheitsgrundlage basiert. Bei Bedarf kann die Sicherheit vom Benutzer etwas gelockert werden, um zum Beispiel Altsysteme zu integrieren. Dieses Bewusstsein macht jedoch einen großen Unterschied.



**Sicherheit, die von einer korrekten Konfiguration abhängt, ist Sicherheit, die versagen kann. Sicherheit, die bereits voreingestellt integriert ist, ist Sicherheit, die einfach funktioniert.**

Teil 2

# Sicherheit im Betrieb

## 5. Patch-Management einfach und flexibel

Verzögertes Patchen gehört zu den vermeidbaren Sicherheitsrisiken in kritischen Infrastrukturen. Gleichzeitig ist die regelmäßige Aktualisierung komplexer Systeme im 24/7-Betrieb eine Herausforderung: Ausfallzeiten, manuelle Prozesse und die Sorge vor Betriebsunterbrechungen führen häufig dazu, dass notwendige Updates verschoben werden.

Barco CTRL vereinfacht diesen Prozess grundlegend. **Sicherheitspatches und Systemupdates können zentral über die gesamte Installation verteilt werden und erreichen mit einem einzigen Vorgang die relevanten Geräte im Netzwerk.** Der Update-Prozess lässt sich dadurch mit minimaler Systemunterbrechung durchführen, ohne USB-Laufwerke, manuelle Aktualisierungen einzelner Komponenten oder lange Wartungsfenster.

So wird Patch-Management von einer aufwendigen Wartungsaufgabe zu einem **planbaren und effizienten Routineprozess**. Sicherheitsupdates können zeitnah eingespielt und Systeme zuverlässig auf einem aktuellen Softwarestand gehalten werden.

## 6. Das engagierte Barco-Sicherheitsteam

Sicherheit ist nur so stark wie die Menschen, die dahinter stehen. Viele Technologieanbieter betrachten die Produktsicherheit als eine Compliance-Funktion – ein Team, das vor der Veröffentlichung die Produkte überprüft und Zertifizierungen freigibt. Barco verfolgt einen grundlegend anderen Ansatz.

**In allen Entwicklungsteams der Barco Control Rooms Division sind Produktsicherheitsingenieure, Produktsicherheitsarchitekten und Security Champions direkt integriert.** Sicherheit wird nicht erst am Ende des Entwicklungsprozesses überprüft, sondern ist in jedem einzelnen Schritt dieses Prozesses präsent. Wöchentliche Sicherheitsbesprechungen stellen sicher, dass Schwachstellen erkannt und Abhilfemaßnahmen festgelegt werden – bevor sie ein bereitgestelltes System erreichen können.

Diese Philosophie geht über die interne Entwicklung hinaus. Das Sicherheitsteam von Barco tauscht sich regelmäßig mit Partnern und Kunden über komplexe Sicherheitsfragen aus, die über übliche Verkaufsgespräche hinausgehen. Es bietet dabei genau die fachkundige Beratung, die Organisationen benötigen, um ernste Sicherheitsherausforderungen in kritischer Infrastruktur zu meistern. Sicherheitskompetenz ist, mit anderen Worten, Teil des Produkts.

Immer auf dem neuesten Stand zu sein, ist in die Plattform integriert und nicht nachträglich hinzugefügt.

## 7. Eine spezielle Sicherheitsroadmap

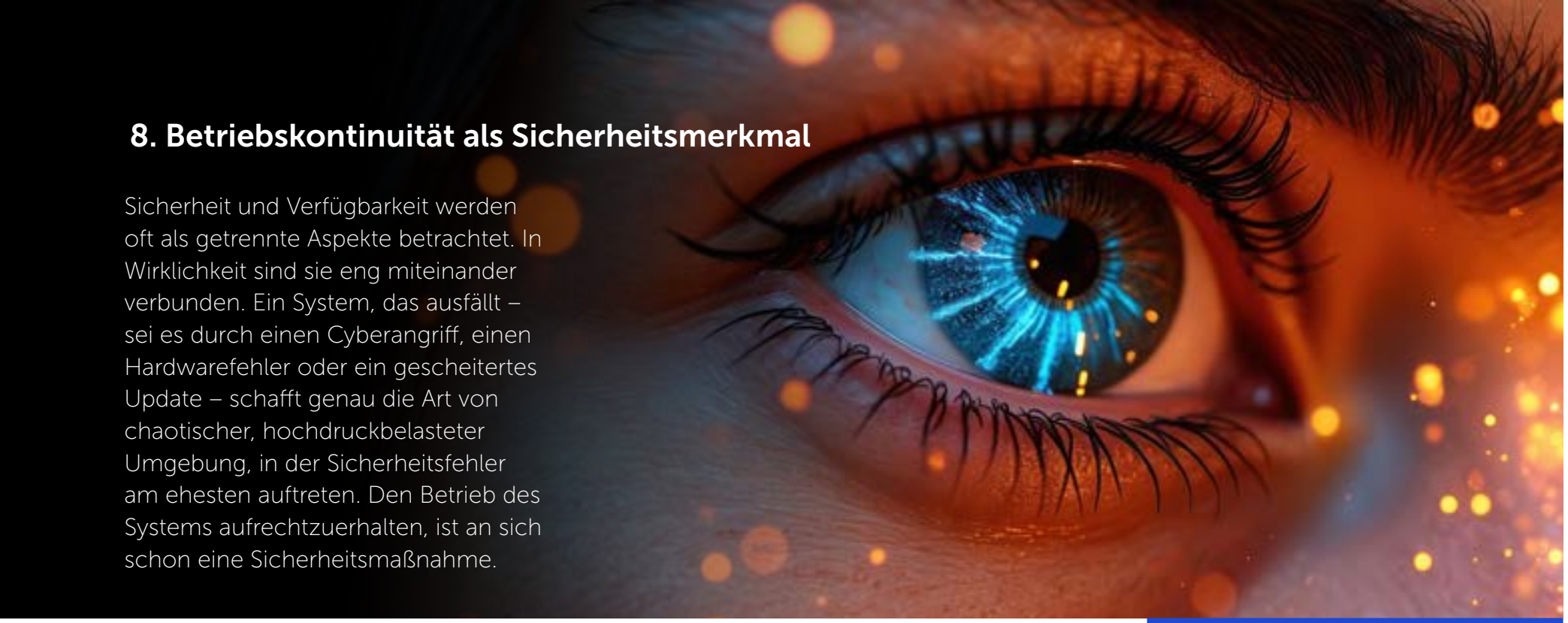
Cybersicherheit ist kein Endziel. Angreifer entwickeln sich weiter, Vorschriften ändern sich, und in Systemen, die gestern noch als sicher galten, werden Schwachstellen entdeckt. Eine Plattform ohne zukunftsorientierte Sicherheitsstrategie ist eine Plattform, die letztendlich zurückfällt.

**Barco CTRL verfügt über eine eigene Sicherheits-Roadmap, die sicherstellt, dass die Plattform während ihres gesamten Lebenszyklus an der Spitze der Cybersicherheit bleibt.** Dazu gehören regelmäßige Penetrationstests durch unabhängige Experten, die Zertifizierung nach ISO 27001 sowie ein proaktiver Prozess zum Schwachstellenmanagement, der Probleme behebt, bevor sie ausgenutzt werden können.

Die Roadmap trägt zudem den sich wandelnden rechtlichen Rahmenbedingungen Rechnung. Angesichts ständig neuer Vorschriften – von NIS2 und NERC-CIP bis hin zum Cyber Resilience Act der EU – sorgt Barco dafür, dass die CTRL-Bereitstellungen die neu hinzukommenden Standards einhalten oder sogar übertreffen.

**Mit Barco CTRL erhalten Kunden eine Plattform, die nicht nur heute sicher ist, sondern dies auch morgen und in den kommenden Jahren bleibt.**

ISO 27001 · NERC CIP · NIS 2 · CRA Cyber Resilience Act



## 8. Betriebskontinuität als Sicherheitsmerkmal

Sicherheit und Verfügbarkeit werden oft als getrennte Aspekte betrachtet. In Wirklichkeit sind sie eng miteinander verbunden. Ein System, das ausfällt – sei es durch einen Cyberangriff, einen Hardwarefehler oder ein gescheitertes Update – schafft genau die Art von chaotischer, hochdruckbelasteter Umgebung, in der Sicherheitsfehler am ehesten auftreten. Den Betrieb des Systems aufrechtzuerhalten, ist an sich schon eine Sicherheitsmaßnahme.

**Barco CTRL ist mit Server-Redundanz ausgestattet. Wenn diese Hardwarekomponente ausfällt, übernimmt automatisch eine Ersatzkomponente die Funktion. Dabei ist kein Benutzereingriff erforderlich.**
Auf der Softwareseite laufen alle Services in isolierten Containern auf dem Server – wenn ein Service ausfällt, kann er den Rest des Systems nicht beeinträchtigen. Dieselbe Isolierung wird auch auf Decoder-Ebene angewendet.

Ein einzelnes Problem an der Quelle kann nicht das breitere Hardwaregerät beeinträchtigen.
Diese Architektur gewährleistet, dass die Leitwarte auch im unwahrscheinlichen Fall eines Teilausfalls weiterhin betriebsfähig bleibt. Die Anwender behalten die Kontrolle. Entscheidungen können weiterhin getroffen werden. Das Sicherheitsniveau des Systems bleibt durchgehend erhalten.

**Resilienz und Sicherheit sind bei Barco CTRL zwei Seiten desselben Designprinzips.**

# Teil 3
# Sicherheit im Kontext

## 9. IT-OT-Konvergenz

Kontrollräume stehen an einem einzigartigen Scheideweg. Auf der einen Seite steht die IT-Welt – fortschrittlich, vernetzt, an häufige Updates und raschen Wandel gewöhnt. Auf der anderen Seite steht die OT-Welt – konservativ aus Gründen der Notwendigkeit. In ihr hat Stabilität oberste Priorität und Ausfallzeiten können katastrophale Folgen haben. Diese beiden Welten haben ein grundlegend unterschiedliches Verhältnis zur Sicherheit. Sie zusammenzuführen, ohne dabei bei beiden Kompromisse einzugehen, ist eine der entscheidenden Herausforderungen für moderne kritische Infrastruktur.

**Als KVM-over-IT-Plattform ist Barco CTRL so konzipiert, dass es in beiden Umgebungen zuverlässig und sicher funktioniert.** Es lässt sich nahtlos in die IT-Infrastruktur integrieren und übernimmt deren Sicherheitsrichtlinien, Identitätsmanagement sowie Überwachungstools. Zugleich berücksichtigt es die betrieblichen Anforderungen von OT-Umgebungen – indem es Sicherheitsmaßnahmen bereitstellt, die transparent im Hintergrund arbeiten, ohne die Anwender in ihrer Arbeit zu beeinträchtigen, deren Fokus auf dem Betrieb selbst liegen muss.

Dieses Gleichgewicht ist nicht leicht zu erreichen, und es entsteht nicht von selbst. Dies erfordert ein tiefgehendes Verständnis beider Bereiche – ein Verständnis, das auf mehr als drei Jahrzehnten Erfahrung in Kontrollräumen beruht. Und dieses Verständnis ist mit einer Sicherheitsphilosophie kombiniert, die hervorragende operative Leistung und Cybersicherheit als sich ergänzende und nicht als konkurrierende Ziele betrachtet.



## 10. Sicherheit trifft Flexibilität

Die beste Sicherheitsmaßnahme ist die, die Anwender kaum bemerken. Sicherheitsmechanismen, die Arbeitsabläufe verlangsamen, wiederholte Authentifizierungen erfordern oder legitime Zugriffe erschweren, sorgen nicht nur für Frustration. Sie können auch dazu führen, dass Anwender nach Umgehungen suchen und dadurch neue Sicherheitsrisiken entstehen.

Barco CTRL folgt deshalb dem Grundsatz, dass Sicherheit den Betrieb **ermöglichen und nicht behindern** sollte. Die Zero-Trust-Architektur arbeitet transparent im Hintergrund und überprüft jede Verbindung, ohne zusätzliche Hürden für die Anwender zu schaffen. Die Multi-Faktor-Authentifizierung lässt sich in bestehende Identitätsanbieter integrieren, sodass vorhandene Anmeldedaten weiter genutzt werden können. Gleichzeitig erfolgt die Audit-Protokollierung kontinuierlich und ohne Eingreifen des Anwenders.

So entsteht **konsequente Sicherheit ohne unnötige Komplexität**: Sicherheitsmaßnahmen werden an die betrieblichen Arbeitsabläufe angepasst und nicht umgekehrt.

Technologie sollte im Kontrollraum unterstützen, nicht ablenken. Barco CTRL gibt Anwendern die Sicherheit und Zuverlässigkeit, die sie benötigen, um sich vollständig auf den Betrieb zu konzentrieren.



## 11. Einhaltung gesetzlicher Vorschriften



**Das regulatorische Umfeld für kritische Infrastrukturen verändert sich rasant, und die Folgen einer Nichteinhaltung sind nicht mehr nur finanzieller Natur.** Die NIS2-Richtlinie verpflichtet Organisationen in kritischen und wichtigen Sektoren zur Umsetzung umfassender Maßnahmen zum Cybersicherheits-Risikomanagement, wobei die Führungskräfte persönlich für die Einhaltung der Vorschriften durch ihre Organisation verantwortlich sind. Verwaltungsstrafen können bei wesentlichen Unternehmen bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes betragen.

Der EU Cyber Resilience Act, der im Dezember 2027 in Kraft tritt, verpflichtet Hersteller dazu, Schwachstellen zu beseitigen und über den gesamten Lebenszyklus eines Produkts hinweg Sicherheitsupdates bereitzustellen. Dies bringt neue Verpflichtungen für Technologieanbieter mit sich – Verpflichtungen, die Barco bereits vor Ablauf der Frist in die CTRL-Plattform integriert hat. Branchenspezifische Vorschriften wie NERC-CIP für das nordamerikanische Stromverbundnetz werden ebenfalls umgesetzt, um die Verfügbarkeit kritischer Infrastruktur zu gewährleisten. Und die Zertifizierung gemäß ISO 27001 belegt zudem, dass die Sicherheitsmanagementprozesse von Barco international anerkannten Standards entsprechen.

Für Unternehmen, die Barco CTRL einsetzen, bedeutet das die Entscheidung für eine Plattform, die bereits auf die zukünftigen regulatorischen Anforderungen abgestimmt ist – und nicht für eine, die bei Inkrafttreten neuer Vorschriften erhebliche Nacharbeiten erfordert.

# 12. Haftung und gemeinsame Verantwortung



Bei Sicherheitsverletzungen in Kontrollräumen ist die Frage der Verantwortung selten einfach zu beantworten. **Die Haftung verteilt sich auf eine Kette von Beteiligten: Der Hersteller, der die Plattform erstellt hat, der Integrator, der sie eingesetzt hat, und der Endkunde, der sie betreibt.** Jeder hat bestimmte Pflichten, und jeder kann zur Rechenschaft gezogen werden, wenn diese Pflichten nicht erfüllt werden.

Von den Herstellern wird erwartet, dass sie Sicherheitslücken umgehend beheben und Sicherheitsupdates bereitstellen. Integratoren sind dafür verantwortlich, die Verfügbarkeit dieser Updates zu kommunizieren und die Kunden bei der Implementierung zu unterstützen. Endkunden sind dafür verantwortlich, Patches rechtzeitig zu installieren – eine Verantwortung, die bei Vernachlässigung zu einem Haftungsrisiko wird. Gemäß den neuen Vorschriften wie NIS2 und der EU-Produkthaftungsrichtlinie werden diese Verpflichtungen gesetzlich durchsetzbar und sind nicht mehr nur vertraglicher Natur.

Barco setzt dieses Modell der geteilten Verantwortung aktiv um. Die Kombination aus automatisiertem Patch-Management, klaren Sicherheitsrichtlinien für Integratoren und Kunden sowie einem proaktiven Schwachstellenmanagement soll es allen Beteiligten in der Kette so einfach wie möglich machen, ihren Verpflichtungen nachzukommen. Sicherheitsverantwortung ist im besten Fall ein gemeinsamer Anreiz – und Barco CTRL wurde entwickelt, um diese Anreize über die gesamte Wertschöpfungskette hinweg aufeinander abzustimmen.

# Fazit: Sicherheit als Grundlage, nicht als Feature

In Umgebungen mit kritischer Infrastruktur ist Sicherheit nicht optional und nicht verhandelbar. Die Folgen von Sicherheitsverletzungen – Betriebsstörungen, Reputationsschäden, behördliche Sanktionen und in den schwerwiegendsten Fällen sogar Schäden in der physischen Welt – können so gravierend sein, dass Cybersicherheit als grundlegende Anforderung behandelt werden muss.

Barco CTRL wurde unter Berücksichtigung dieser Tatsache entwickelt. **Von den Security-by-Design-Prinzipien, die die Architektur des Systems geprägt haben, über die fünf Sicherheitssäulen, die jede Ebene des Systems schützen, bis hin zum engagierten Team, das das Sicherheitsniveau des Systems kontinuierlich aufrechterhält und weiterentwickelt: Sicherheit ist das Fundament von Barco CTRL!**

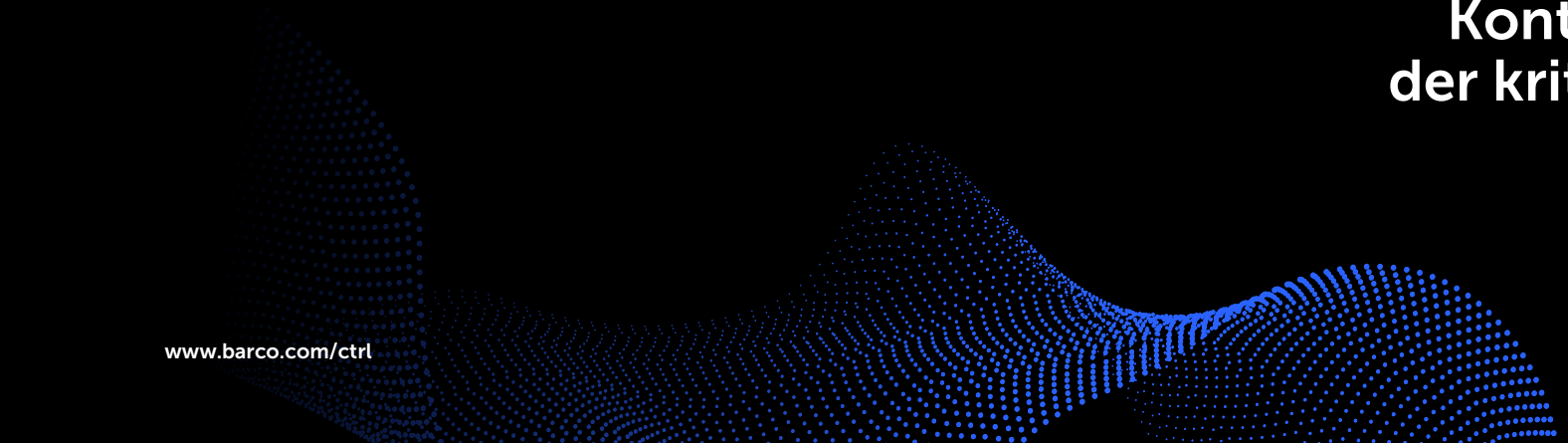
Zugleich ist sich Barco CTRL bewusst, dass Sicherheitsmaßnahmen, die Betriebsabläufe behindern, umgangen werden. Die Plattform ist so konzipiert, dass sie ebenso unauffällig wie robust ist – sie schützt Anwender, IT-Manager und Organisationen, ohne jemals die zu erledigende Arbeit zu behindern.

Sind Sie bereit, Barco CTRL in Aktion zu erleben?

**Fordern Sie Ihre persönliche Demo an**

Erfahren Sie, wie Barco CTRL Ihren Kontrollraum vom ersten Tag an vereinfacht.

**Heutzutage ist die Kombination aus kompromissloser Sicherheit und müheloser Anwendbarkeit der einzige akzeptable Standard für eine Kontrollraumplattform, der kritische Infrastruktur anvertraut wird.**



www.barco.com/ctrl

BARCO