

AMOSSYS

BARCO

**CSPN SECURITY TARGET CX-50
GEN2 VERSION 02.20.02.0027**

BARCO

2026-05-13

Version 1.07

AMOSSYS

11 Rue Maurice Fabre

35000 Rennes

SAS au capital de 38 000 €

SIREN 493 348 890

TVA FR 21 493 348 890

www.amossys.fr

DOCUMENT HISTORY

Version	Author	Description	Date
0.10	Amossys	Document creation	2024/02/08
0.20	Amossys	Corrections	2024/02/20
0.30	Amossys	Corrections	2024/03/04
0.40	Amossys	Corrections	2024/03/14
1.00	Amossys	Final version	2024/03/22
1.01	Amossys	TOE version and COTS update	2024/10/14
1.02	Amossys	Assumptions update	2024/11/21
1.03	Amossys	SF.4 update according to ANSSI remarks	2024/11/25
1.04	Amossys	SF.4 update according to ANSSI remarks	2025/09/30
1.05	Amossys	SF.4 update according to ANSSI remarks	2025/10/08
1.06	Amossys	TOE version and COTS update	2025/12/23
1.07	Barco	Redacted for publication	2026/05/13

SUMMARY

1. INTRODUCTION	4
1.1 Subject of the document	4
1.2 Product identification	4
1.3 References	4
1.4 Glossary	4
2. PRODUCT DESCRIPTION	5
2.1 General description	5
2.2 Principle of operation	5
2.3 Dependencies description	6
2.4 Technical operating environment	7
2.4.1 Compatible or dedicated equipment	7
2.4.2 Operating system selected	7
2.5 Evaluation scope	7
2.5.1 Scope	7
2.5.2 Evaluation platform	8
3. SECURITY PROBLEM	10
3.1 Product users	10
3.2 Sensitive assets	10
3.3 Environmental assumptions	11
3.4 Threats	11
3.5 Security functions	12
3.5.1 Operational functions	12
3.5.2 Security Functions	12
3.5.3 Disabled Functions	13
3.6 Tracings	14
3.6.1 Threats and sensitive assets	14
3.6.2 Threats and means exploited by the threatening agents	15
3.6.3 Threats and security functions	16

1. INTRODUCTION

1.1 Subject of the document

This document has been written for the CSPN certification scheme promoted by the ANSSI, for the product **CX-50 Gen2**, developed by .

This document is subject to **AMOSSYS** technical and quality controls and validation. Updates of this document are done by **AMOSSYS** project team.

1.2 Product identification

Developer	BARCO N.V. Beneluxpark 21 8500 Kortrijk Belgium	
	https://www.barco.com/	
Link to the developer		
Commercial name	CX-50 2 nd generation	
	Base Unit	02.20.02.0027
Evaluated version	Button	04.21.0
	Application	04.37.5

1.3 References

For the writing of this document, the following documents were used:

Table 1 - References

Reference	Description
[USER-GUIDE]	"R5900095_13_UserGuide.pdf", ClickShare CX-50
[INSTALL-GUIDE]	"R5900096_11_Installation.pdf", ClickShare CX-50
[SEC-CLICKSHARE]	"TDE10355_01_WhitePaper.pdf", Security Whitepaper ClickShare Conference and ClickShare Present
[NET-CLICKSHARE]	"TDE10396_06_WhitePaper.pdf", Network Deployment Guide

1.4 Glossary

Table 2 - Glossary

Acronym	Definition
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	<i>Application programming interface</i>
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
COTS	<i>Commercial Off-The-Shelf</i>
IP	<i>Internet Protocol</i>
PKI	<i>Public Key Infrastructure</i>
TOE	<i>Target Of Evaluation</i>
USB	<i>Universal Serial Bus</i>

2. PRODUCT DESCRIPTION

2.1 General description

The ClickShare CX-50 Gen2 is an award-winning wireless meeting room system for easy video conferencing, collaboration and presentation in the modern workplace. It seamlessly connects your laptop to the room display, audio and video equipment in any conference room, so you can start your meeting in less than 7 seconds with just one click via the ClickShare Button or App.

ClickShare enables wireless conferencing in large meeting spaces and board rooms. When you walk into the meeting room, ClickShare automatically connects you to room devices like cameras, mics, speakers, sound bars and displays.

It facilitates hybrid meetings for employees and guests, for up to 32 people, at the click of a button or the ClickShare desktop and/or mobile application.

The ClickShare CX-50 Gen2 consists of a Base Unit, a button and an application.



Figure 1 - Base Unit and two buttons

There are two main usage scenarios:

- Every button contains a copy of the application. When the user plug in the button, it launches the embedded client application with preconfigured elements;
The user launches the client application directly from its computer and manually selects the Base Unit to connect.

In addition, the product allows for simple, intuitive content sharing from your smartphone or tablet via Android and iOS applications. These applications and their features are not in the scope of evaluation.

2.2 Principle of operation

The Base Unit receives the wireless input from the buttons and controls the content of the meeting room display and the sound of the meeting room's audio system.

The installation step is as follows:

- Install the Base Unit in the meeting room (standalone or network integration);
- Connect the video signal between the Base Unit and the display;

- Connect the audio devices via USB or jack if any to the Base Unit;
- Connect the USB camera to Base Unit;
- Optional: connect a network cable between the Base Unit and local network;
- Configure devices (via ClickShare Configuration, Rest API or XMS);
- Pair buttons with the Base Unit;

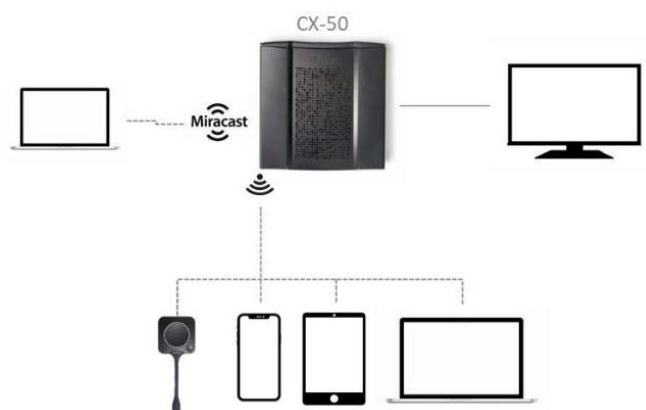


Figure 2 – Clickshare environment

The administrator can configure the Clickshare Base Unit through a web Configurator or REST API. Valid credentials are required to access them. The following functions can be configured:

- Enable automatic updates (If outbound connectivity is in place, automatic upgrades can be downloaded and installed via our public upgrade service.);
- Personalization (room name for example);
- Security-level management: there are three levels of security in the Base Unit. After each modification, the buttons need to be paired with the Base Unit.
- Modification of the user passwords;
- Log management;
- Certificate management (Configurator and REST API).

Secure communication configuration:

Wireless: WPA2-PSK;

- Wired or wireless: 802.1X.

Connecting the Base Unit to the internet is optional and a PKI is used for cryptographic elements.

The TOE supports two types of Wi-Fi connectivity, the button/app can either directly connect to the Base Unit internal access point or both the button/app and the Base Unit can use an external access point.

2.3 Dependencies description

No dependence is necessary for the functioning of the TOE.

2.4 Technical operating environment

2.4.1 Compatible or dedicated equipment

The Base Unit runs a Linux operating system and the Button runs a Real Time OS.

The ClickShare application runs on:

- Windows 10 or higher;
- MacOS 11 and higher;
- Android v11 and higher;
- iOS 14 and higher.

The application for Windows and Mac is identical from a feature perspective (except for extended desktop functionality on Windows), but technical implementation (use of screen scraping techniques, audio/video libraries) is slightly different. For the mobile apps, they have the same feature set, but different implementations.

The minimum system requires for a smooth experience with Microsoft Teams or Zoom is:

- Intel i3 dual-core processor;
- 8GB RAM;
- OS: Windows 10 latest build or Mojave latest build.

The recommended system requires is:

- Intel i5 dual-core processor;
- 8GB RAM;
- OS: Windows 10 latest build or macOS latest build.

2.4.2 Operating system selected

The client machine is an up-to-date Windows Workstation (Windows 11).

2.5 Evaluation scope

2.5.1 Scope

The scope of the evaluation is composed of:

- ClickShare button;
- Base Unit;
- Windows application;
- Communications.

The cloud connectivity, the Desktop App for macOS and the additional mobile application are out of the scope of evaluation.

The configuration of the evaluated product is presented in the following table.

Table 3 – Evaluated product configuration

Component of the overall system	Included in the	Not evaluated (TOE environment)
---------------------------------	-----------------	---------------------------------

		evaluation target (TOE)	Assumed to be trusted	Is a potential attacker
Base Unit version 02.20.02.0027	Firmware	✓		
	Operating system		✓	
	Cryptographic functions	✓		
Button Version 04.21.0	Firmware	✓		
	Operating system		✓	
Application Version 04.37.5	Windows Desktop	✓		

2.5.2 Evaluation platform

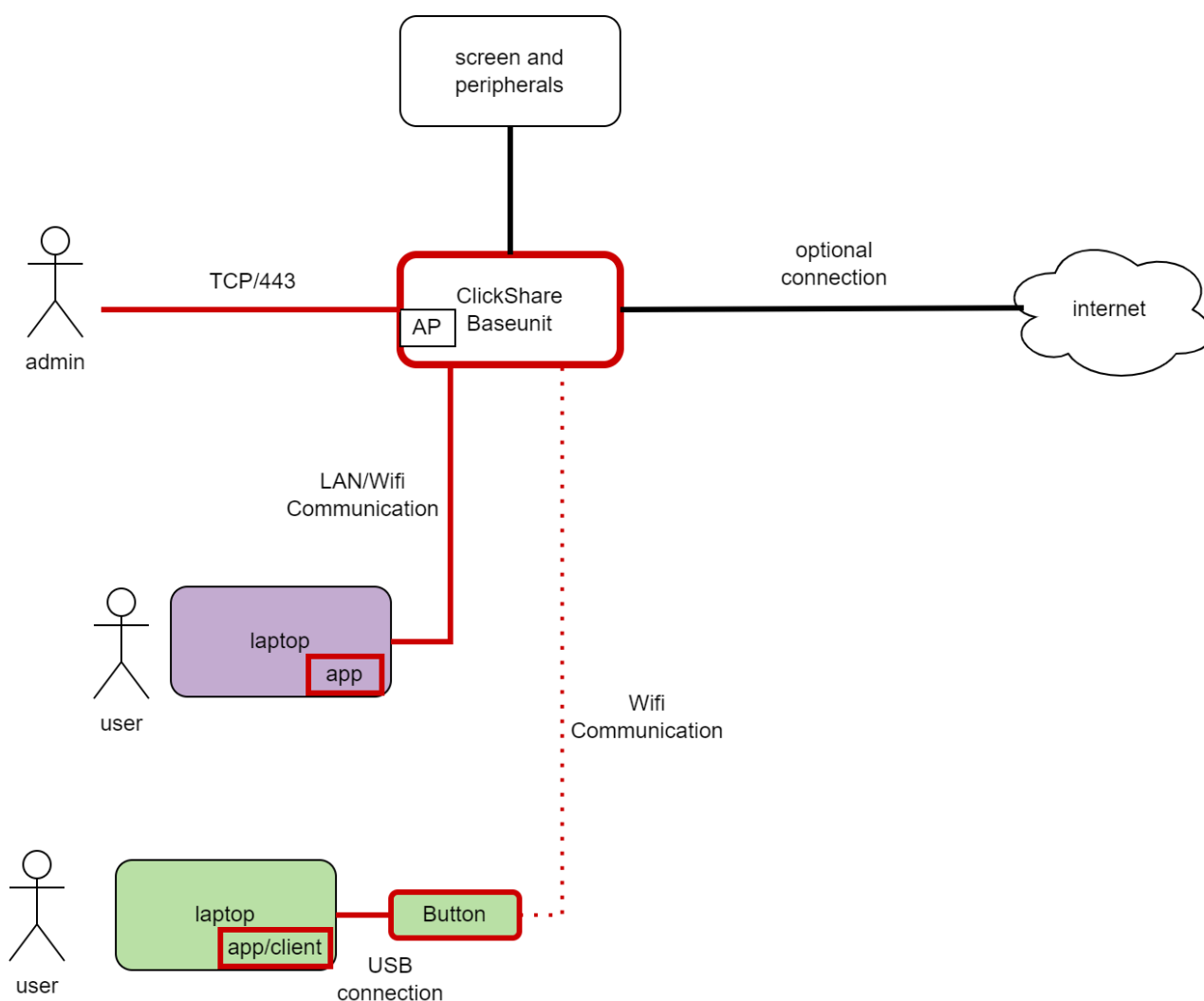


Figure 3 - Evaluation platform (evaluated elements and communications in red)

In the context of the evaluation, the button/app connect to the Base Unit through its internal access point.

The green and purple square represents two similar use cases of the TOE, they are both evaluated. The former plugs the button which automatically connect to the Base Unit while the latter must first configure the client application.

3. SECURITY PROBLEM

3.1 Product users

By definition, users refer to people and application services that interact with the evaluated product. The following roles should be considered in the security evaluation:

User: TOE users, using the services offered by ClickShare;

Administrator: Administrator in charge of the administration of the TOE.

3.2 Sensitive assets

By definition, a sensitive asset is data (or function) deemed to be of value by the TOE. Its value is estimated according to security criteria (also called security needs): availability, integrity, confidentiality, and authenticity. The sensitive assets of the TOE are as follows:

SA1. Host system

The host systems of the Clickshare Button, the Base Unit and the client computer.

Security requirements: integrity.

SA2. Network traffic

All communications between the Base Unit, the administrator and the client.

Security requirement(s): availability, integrity, confidentiality and authenticity.

SA3. Logs

The events logged by the TOE in the Base Unit.

Security requirement(s): availability and confidentiality.

SA4. Cryptographic material

The data transmitted is protected by cryptographic mechanisms.

Security requirement(s): availability, integrity and confidentiality.

SA5. Authentication data

The web configuration interface credentials and device pairing authentication data.

Security requirement(s): integrity, confidentiality.

SA6. Business data

Client data shared on the solution.

Security requirement(s): availability, integrity and confidentiality.

SA7. Configuration

The configuration of the ClickShare Base Unit.

Security requirement(s): availability, integrity.

3.3 Environmental assumptions

An assumption is a statement on the context of the use of the TOE or on the TOE environment. Regarding the current context, only one assumption is relevant:

H1. Secure environment

The PKI infrastructure is hosted on internal premises, physically separated from the corporate network and situated in a restricted area with physical access control.

H2. Administrator

The TOE administrators are trained in good security practices and use of the TOE.

3.4 Threats

By definition, a threat is an action or event that may affect the security of the TOE. The threat agents to be considered for the evaluation are the following:

An attacker on the network who can try to intercept the communications;

A local attacker with short timed physical access to the button and Base Unit;

An attacker with a low privileged account who can try to elevate its rights.

Consequently, the TOE must resist these threatening agents as well as the software and hardware means implemented by them. These means are the following.

Table 4 – Means deployed by the threatening agents

Means used by the threatening agents	Means applied		TOE resistant to an attacker	
	Software	Hardware	Local	Remote
Changing the firmware on the button	✓	✓	✓	
Changing the firmware on the Base Unit	✓	✓	✓	
User session vulnerability	✓			✓
Network vulnerability	✓			✓

The threats to the sensitive assets of the TOE are the following:

T1. Log data alteration

Logging data is corrupted or deleted (by an attacker to hide illegitimate actions).

T2. Cryptographic elements access or modification

An attacker manages to access or modify the cryptographic keys handled by the TOE.

T3. Communication compromised

An attacker manages to modify or capture the content of communications between the TOE and other components.

T4. Session theft

An attacker manages to steal a legitimate user session in order to impersonate user identity.

T5. Configuration corruption

An attacker manages to corrupt TOE configuration in order to downgrade its security.

T6. Firmware modification

An attacker manages to corrupt the button/Base Unit firmware in order to downgrade its security.

T7. Authentication theft

The attacker succeeds in authenticating himself without credentials or theft credentials.

3.5 Security functions

3.5.1 Operational functions

The operational functions are set of functions that are active and implemented by the TOE to ensure its operation and respond to the need for which it was developed. These operational functions will not be evaluated for compliance, but will be considered a potential attack vector on the TOE.

The operational function of the TOE is the security functions identified below:

OF1. Share content

The TOE allows data to be easily shared between users using a button.

OF2. Conference service

The TOE facilitates the use of microphones and cameras during the video calls.

OF3. PresentSense

The TOE uses PresentSense to detect the Base Unit / Meeting room.

3.5.2 Security Functions

The security functions are the technical measures and the mechanisms enforced by the TOE to protect the sensitive assets from the threats. The security functions of the TOE are:

SF1. Identification, authentication and users access control

The Base Unit receives button and application communications. The button communicates with the Base Unit via Wi-Fi. Data is delivered in real time, there is no-volatile memory. Content which is being shared is never stored, not on Base Unit level, nor on Button level. The ClickShare Base Units and Buttons contain a device certificate, which is provisioned during manufacturing of the device and is stored in encrypted format in non-erasable memory on the device. There is mutual authentication between ClickShare Button and Base Unit.

Authentication is needed to connect to the Configurator web interface. The default credentials are admin/admin. However, during the first connection, the administrator must set a new password. The ClickShare Configurator login uses a session, bound to a cookie that stays valid until logout or expiration.

SF2. Communications Security

Communications between the Base Unit and the ClickShare Configurator rely on TLS. TLS cipher suites and versions are configured to resist the latest known attacks.

User apps communicate with the Base Unit at the application layer via TLS.

SF3. Logging

The logging function records the actions performed on the TOE and the security events related, both for the button and for the Base Unit. Logging is carried out via a TLS connection.

Logging is based on rsyslog, in syslog format. Storage is limited to 20 log files of 2 Mb in compressed size.

It is possible for the TOE administrator to view the action log. It is also possible for the administrator to export the logs.

SF4. Self-protection

The ClickShare button is using secure boot and contains two partitions. If a partition is corrupted, the button will not boot that partition and will revert to the secondary one. If the two partitions are corrupted, the button will not boot at all and will no longer be usable. If a button does not boot, it cannot connect to the Base Unit and by this way, a user can be informed that a button is corrupted. The Base Unit uses the same procedure, it has two partitions.

SF5. Update

When an external storage device is connected via USB, the top directory will be scanned for a firmware update image. If this file is found, the Base Unit will attempt to upgrade. This upgrade can only be successful if the firmware is correctly encrypted and signed. In all other cases, connecting USB devices will result in no action.

The button and the Unit Base have two partitions for the update firmware. If the update fails, the second partition allows you to go back.

3.5.3 Disabled Functions

Deactivated functions are a function considered to be outside the scope of the evaluation (outside the TOE) and not accessible to an attacker. These functions will not be considered during the evaluation. The disabled functions of the TOE are the following:

DF1. Sharing by other applications

Sharing by AirPlay, Google Cast or Miracast is considered out of scope.

DF2. Room Systems

Connect a room system over USB. ClickShare will pass the peripherals to the room system in case the room system is in use and it will use them itself in case the user is using ClickShare.

DF3. SNMP

SNMP collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

DF4. XMS

When your device is not registered and connected to the cloud service, the following message will be displayed: "Device has not been added to XMS cloud".

DF5. Blackboarding

Blackboarding allows you to use the meeting room's touchscreen as a writing board to write or sketch ideas on.

3.6 Tracings

3.6.1 Threats and sensitive assets

The following table traces back the sensitive assets to the threats (letters "V", "I", "C", "A" meaning respectively Availability, Integrity, Confidentiality, Authenticity).

Table 5 – Covering of the sensitive assets by the threats

	SA1. Host system	SA2. Network traffic	SA3. Logs	SA4. Cryptographic material	SA5. Data of authentication	SA6. Business data	SA7. Configuration
T1. Log data alteration			VC				
T2. Cryptographic elements modification				VIC	I	IC	
T3. Communication compromised		CIVA					
T4. Session theft					C	A	
T5. Configuration corruption							AI
T6. Firmware modification	I						
T7. Authentication theft					CI		

3.6.2 Threats and means exploited by the threatening agents

The following table presents the coverage of the means exploited in relation to the identified threats.

Table 6 – Coverage of the means exploited in regards to the threats

	Changing the firmware on the button	Changing the firmware on the Base Unit	User session vulnerability	Network vulnerability
T1. Log data alteration				✓
T2. Cryptographic elements modification			✓	
T3. Communication compromised				✓
T4. Session theft			✓	
T5. Configuration corruption			✓	
T6. Firmware modification	✓	✓		
T7. Authentication theft			✓	

3.6.3 Threats and security functions

The following table back the security functions to the threats.

Table 7 – Covering of the threats by the security functions

	SF1. Identification, authentication and users access control	SF2. Communications Security	SF3. Logging	SF4 Self-protection	SF5. Update
T1. Log data alteration			✓		
T2. Cryptographic elements modification	✓	✓			
T3. Communication compromised		✓			✓
T4. Session theft		✓			
T5. Configuration corruption					✓
T6. Firmware modification				✓	
T7. Authentication theft	✓				

End of the document
