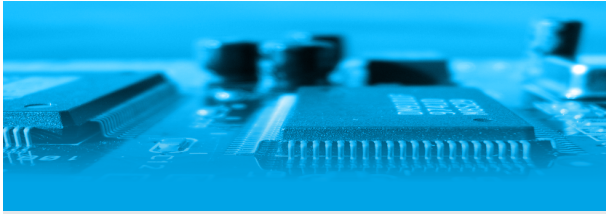


PRODUCT DATASHEET



Highlights

ERGONOMY

The ergonomy of the 7-inches touchscreen allows to operate most of the common actions in 2 or 3 clicks.

IDENTIFICATION AND AUTHENTICATION

The identification of the users is made by the reading of an RFID usercard on the reader.
It can be reinforced by the personalized pin code access and centralized by MICROSESAME.

ANSSI REDIRECTED SECURITY

The reader can read secured usernames (or UID)/ The reading key is downloaded via MICROSESAME CUBE and is locked in an HSM EAL5+ ANSSI certified "safe deposit box" integrated in the keyboard.

The IP network in which the intrusion exploitation terminal is connected to is cyber-secured in TLSv1.3 (via PKI certificate of the final client). It's the identical solution as the one which is ANSSI certified.

Main features

- Directly connected to the IP network
- Multi-central exploitation via its "master" TILLYS
- Alarm display functions & real-time defaults
- "Ready for monitoring" anticipates monitoring problems, siren shutdown, dot ejection, waiver / postponement of monitoring, siren / dots inhibition, event history viewing, intrusion profile creation
- Transmission of alarms, events and remote controls to/from the remote operator in SIA DC-09
- Can be configured to manage only some of the 32 detector groups of its TILLYS master controller
- Enable/disable only authorized groups on the control panel for the identified user
- Integrated test and maintenance tool with real-time diagnostics of installation, points, sirens etc...

TACTILLYS IP CUBE

Intrusion CUBE operating terminal



Fingertip control of your TACTILLYS IP CUBE

Intrusion CUBE offers cybersecurity, ergonomy and functional power.
Its exploitation terminal, the TACTILLYS IP CUBE screen, is directly connected to the IP network, communicating dot by dot with only one TILLYS CUBE plant that can only be the "master" of multiple others TILLYS CUBE. So the screen can manage multi-plants groups of detectors by this "master" plant.

TACTILLYS IP CUBE allows its users to operate the majority of the daily operating actions in 2 or 3 clicks.

It integrates multiple functions for the management and the intuitive setting and the monitoring of intrusion, as well as a testing and diagnostics for the maintenance of the installation.

The most important characteristics of its associated TILLYS CUBE plant:

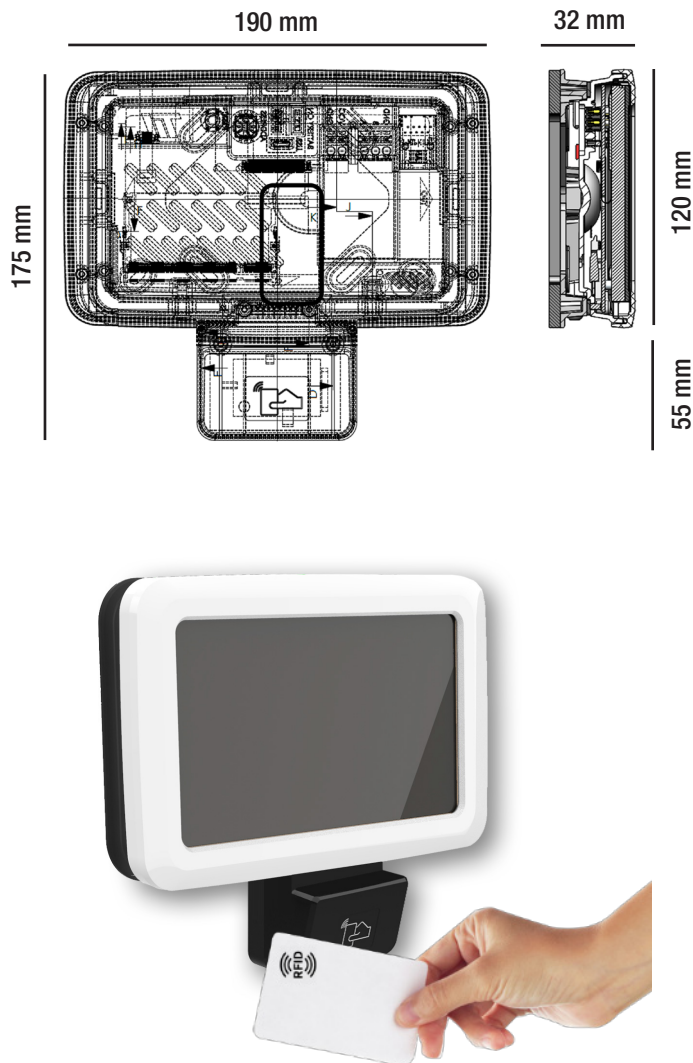
- Up to 32 groups of detectors and up to 768 physical detectors.
- No limit of number of TACTILLYS-IP CUBE operating screens
- No limit to intrusion profiles.
- Each TILLYS CUBE operates exclusively in one only mode, up to choice: Intrusion CUBE (from the MS 2024) or Intrusion V1.
- Automatic alarm inhibition based on hierarchy (ex: default com TILLYS inhibits default detector).

GTB, INTRUSION AND ACCESS CONTROL INTEGRATED SYSTEM

SUPERVISION SOFTWARE	AUTOMATE TILLYS CUBE	TACTILLYS IP CUBE	EVOLUTION READERS	SENSORS AND CONTACTS
MICROSESAME CUBE				

TACTILLYS IP CUBE

Dimensions



References

- **CDA00TY2025-BBIP** : Deployed touchscreen TACTILLYS IP CUBE for TILLYS CUBE - 7-inches - colored - horizontal mounting - for Intrusion CUBE exploitation
- **LEC05XF0200-NB6** : Reader EVOLUTION module- Integrated under the display of the TACTILLYS (IP) CUBE - For secured MIFARE/DESFIRE badges UID number - Black - **MANDATORY** for TACTILLYS IP CUBE

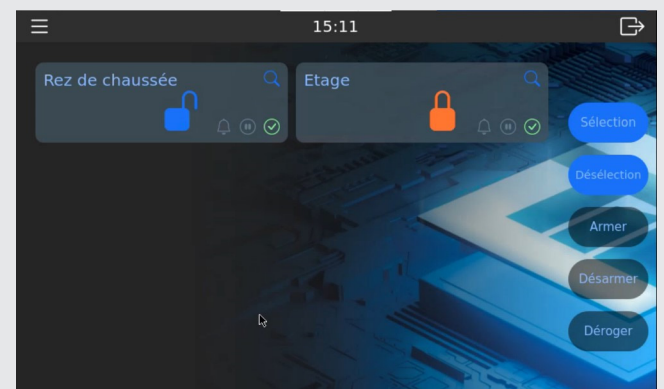
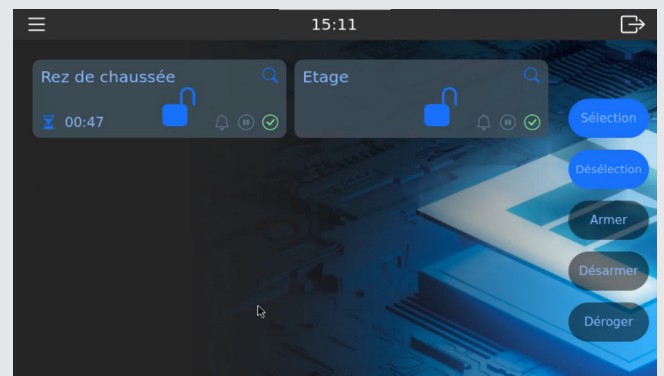
fpr_TACTILLYS-IP-CUBE - 04/08/2025

Informations non contractuelles,
susceptibles de modifications sans préavis.



Technical details

- **Power supply** : 12 to 28 VDC
- **Consumption** : 150 mA with a reader module and inactive screen, 300mA with a reader module and an active screen
- **Horizontal screen dimension + module reader** : 175 x 190 x 32 mm
- **Display** : 7-inches capacitive color display screen, 800 x 480 pixels
- **Connections** : Ethernet 10/100 Mbits @IP fixe (TLSv1.3 with certificate) + 1 micro-USB port for the firmware updates. IP connection with the TILLYS CUBE linked (associated).
- **Badge technologies** : ISO14443-A : DESFIRE EV1/2/3 native, or emulated EV1, UI or secured by a key in the crypto processor HSM EAL5+. Authentication of the users by badge or by badge + personalized keyboard code.
- **Reading distance** : Up to 5 cm
- **MICROSESAME compatibility** : MS >= 2024.2
- **TILLYS compatibility** : TILLYS CUBE, firmware >= 7x
- **TILLYS history** : Up to 10000 intrusion events, transmission links, requests audits and source of the events (tracking)
- **Mount** : Wall-mounting with 4 projecting screws or a flush-mounting box
- **Protection** : Self-protection against tampering by acceleration meter
- **Acoustic signaling** : Integrated speaker



Contact : sales@hirschsecure.com
www.til-technologies.com / www.hirschsecure.com