

# Oxtopus at the forefront of safety with 802.1X standard

Occitaline now equips all of their Oxtopus routers with the IT 802.1X authentication to ensure the security of the entire BMS.

## Cyber security, a central concern

Recent waves of computer attacks on companies and their facilities have proven that no one is now safe. Launched randomly, they attacked big companies, SMEs, institutions and sensitive places such as hospitals, highlighting the need for a real protection.

## Occitaline adopts 802.1X protocol to equip their routers range

Occitaline, a Toulouse-based manufacturer of BMS infrastructure products, has been developing for several years, solutions for BMS cybersecurity.

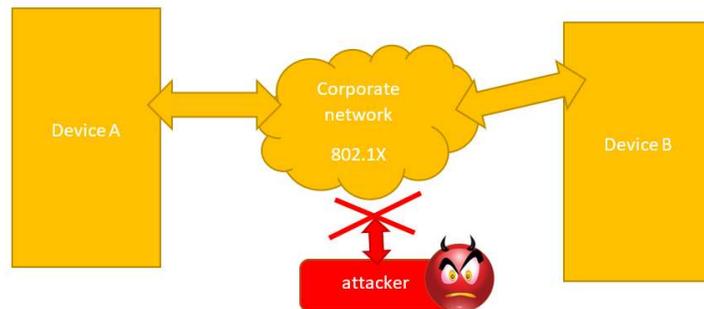
Before introducing their Ox-Bras in Paris IBS fair 2021, Occitaline decided to equip their entire range with the 802.1X, the reputed standard for authentication. Oxtopus is the first BMS router to achieve such a high level of cybersecurity.

## How does 802.1X authentication work?

BMS network remains the weak point in technical facilities. The principle of 802.1X is to ask a server for permission to enter a network. Without this authorization, no traffic is possible.

The authorizations are managed centrally by the IT Directors, guarantors of the network security.

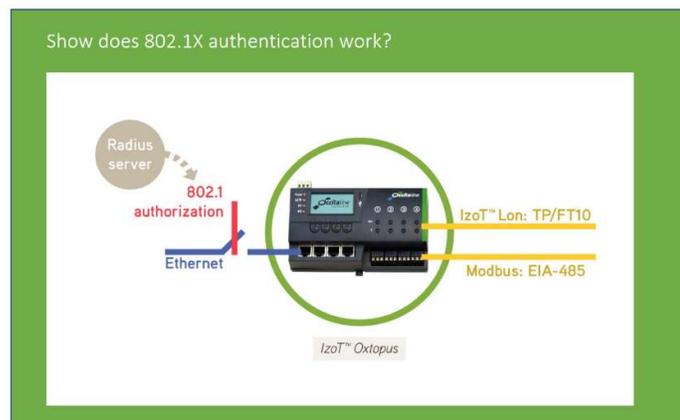
The 802.1X operates over all access points of the enterprise network: an un-authenticated device cannot enter the network and all connected devices are protected.



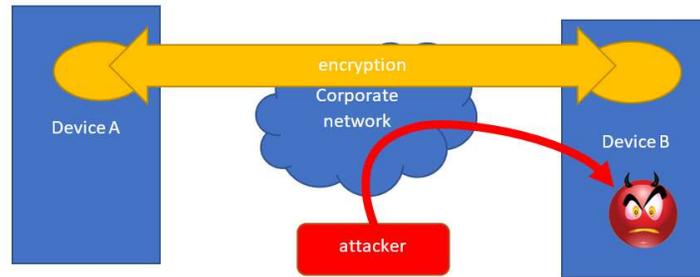
## 802.1X Oxtopus routers protect the company's network

For sensitive installations using the 802.1X protocol, it is now possible to install Oxtopus routers which are placed at the same level of security as other IT products.

The Oxtopus connects twisted pair of the field with the IP to LonWorks, BACnet, Modbus and IzoT protocols. Since attacks from field network are impossible, Oxtopus protects both BMS and the company's network.



By comparison, some protocols use encryption to operate a secure exchange between two applications (e.g. HTTPS). However, neither the equipment nor the network is protected from intrusions with this approach. This technique is only efficient to protect the applications, they are the only ones to benefit from encryption.



## Biography: Daniel Zotti, a singular story of a LON's pioneer

President of LonMark Francophone, Daniel Zotti was one of the founders of the association in 1994, he is also a member of LonMark International Board of Directors.

Member of TC247/WG4, standard-setter of the protocols used in BMS, he is also a member of the NGO eG4U (e-green for users) to defend the users' interests in IT networks, as well as a member of several working groups like IPV6, Smart M2M with ETSI, the standard-setter for radio and wire telecommunications, but also for their uses in the Smart City and Smart Building.

As member of the SBA (Smart Building Alliance), Daniel Zotti is part of the working groups on BOS/BIS and BMS protocols.



Founder and CEO of Newron System, a software company for building automation using LonWorks, BACnet, KNX, Modbus, its sale in 2013 to ABB Group allows the creation of Occitaline which becomes the French manufacturer of multi-protocol infrastructure products IP, LonWorks, BACnet, Modbus. For more than three years, Occitaline has been developing future infrastructure products that combine cybersecurity and building automation.

More information about Occitaline and Oxtopus on [www.occitaline.fr](http://www.occitaline.fr)

For interview requests, please contact us: [info@occitaline.fr](mailto:info@occitaline.fr) or +33 (0)5 34 28 12 24

Occitaline - 13 rue Antoine de Lavoisier - 31830 Plaisance du Touch - France