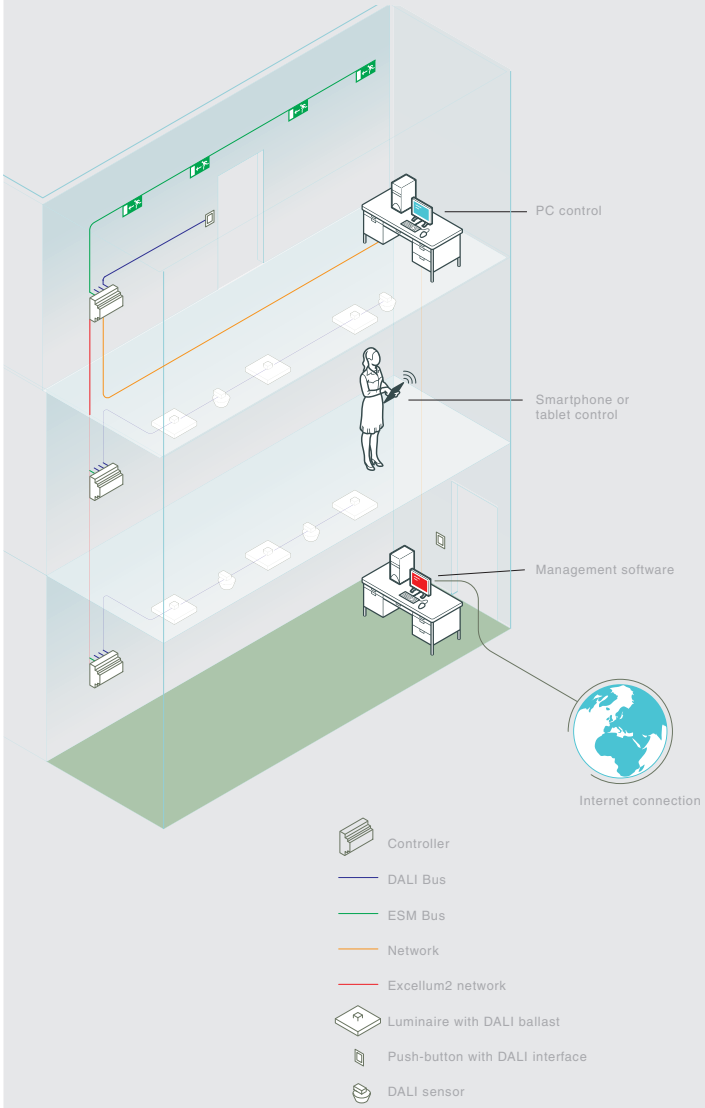
EXCELLUM2: NETWORK SECURITY

INTRODUCTION

Excellum2 is a light management system that controls general and emergency light luminaires in combination with sensors, push buttons and advanced software with the goal to save energy, increase comfort for the users and add flexibility for building managers.
The system provides a web-based interface to interact with users so there is no to install additional software. The look and feel of the interface is optimized depending on the used hardware (e.g. tablets, smartphones or PC's) and on the user's role and access rights (e.g. employees, maintenance staff).
The system implements security rules to ensure that only authorized users can access the interface, that such connection cannot be forced and that none of this communication is accessible for others.

This document gives you an answer to the key question "Is it safe to connect the Excellum2 system to my network?"
First we will take a closer look on the basic mechanism of security measures. Then we go more in detail to the communication flow and finally we look into the different levels of security.



SECURITY MEASURES

The Excellum2 solution is built up by connecting the lighting elements (luminaires, sensors, etc) on controllers using DALI and ESM field busses (blue and green lines on the image) and connecting controllers to each other in a TCP/IP network (red lines on the image). To allow access to the users, the system needs to be connected to the corporate network by using an Ethernet port on one of the controllers (orange line on the image). These ports only allow requests from a limited set of port numbers and use several security protocols.

In a configuration with multiple Excellum2 controllers, the Excellum2 network can be isolated from the rest of the network as the controllers have dual Ethernet interfaces, with daisy chain ability, as shown in the system topology image (see left).
Only one controller is connected to the corporate network, to provide user access. This configuration provides additional security, as the communications between different controllers is totally separated from the corporate network. This also ensures tight performance metrics, as problems on the corporate network - like congestion or network outages - remain on the corporate network.

The system uses an embedded operation system and TCP/IP stack that is tailored to only allow access to public parts of the light systems and avoid back doors and network weaknesses. All TCP/IP ports are closed, except those needed to allow the users to operate and configure the system.

ETAP
EXCELLENT LIGHTING, SAVING ENERGY

EXCELLUM2: NETWORK SECURITY

The system only uses a standard HTTP (Hyper Text Transfer Protocol) port, so all other protocol ports are closed or set unavailable.

The data is stored in an encrypted form on the controller. So even when someone would have access to the operating system of the controller, this data is unreadable without the correct decryption key.
Passwords are not stored at all, only a hash of the password is stored. This is the same mechanism as used in all major operating systems and also on PIN-protected cards like debit and credit cards.

SECURE COMMUNICATION FLOW

When a client establishes a connection to the controller, he needs to identify himself by using a login and password. After a successful authentication on the controller, a temporary connection will be established between the controller and the local equipment.
The user communicates with the controller using HTTP for loading the interface on the local device, but all information is transferred in encrypted form.

DIFFERENT SECURITY MEASURES

- Measure 1: Separation
  The Excellum2 controller separates the system network from the corporate network, so that the critical traffic is isolated. Performance is guaranteed and potential threats are confined.
- Measure 2: Encryption
  All sensitive information exchange between the remote user and the controller is encrypted. This prevents outside modification of the data as well as eavesdropping (or listening-in).
- Measure 3: Connection flow
  The connection must always be initiated from user towards the controller, obliging authentication. This means that any spurious attempt to issue a command or access data will not be executed if the flow is not accomplished.
- Measure 4: Closed Authentication
  Passwords are never transmitted in the network.

CONCLUSION

The Excellum2 system offers the advantage of local web access which does not need software installation and at the same time maintains the safety and integrity of your network.
The infrastructure topology and password architecture prevents unauthorized access to the controller from and to your network.
The connection flow prevents a forced connection to the system.
The combination of our measures tackles the risk of unauthorized access to your network on every level.

UK
ETAP NV
Progress Business Centre – 7 Whittle Park Way
Slough – Berkshire – SL1 6DQ
Tel.+44 (0)1628559650 – Fax +44 (0)1628559012
e-mail: enquiries@etaplighting.com – www.etaplighting.com

ETAP EXPORT DEPARTMENT
Antwerpsesteenweg 130
B-2390 Malle – BELGIUM
Tel. +32 (0)3 310 02 11 – Fax +32 (0)3 311 61 42
export@etaplighting.com

ETAP
EXCELLENT LIGHTING, SAVING ENERGY