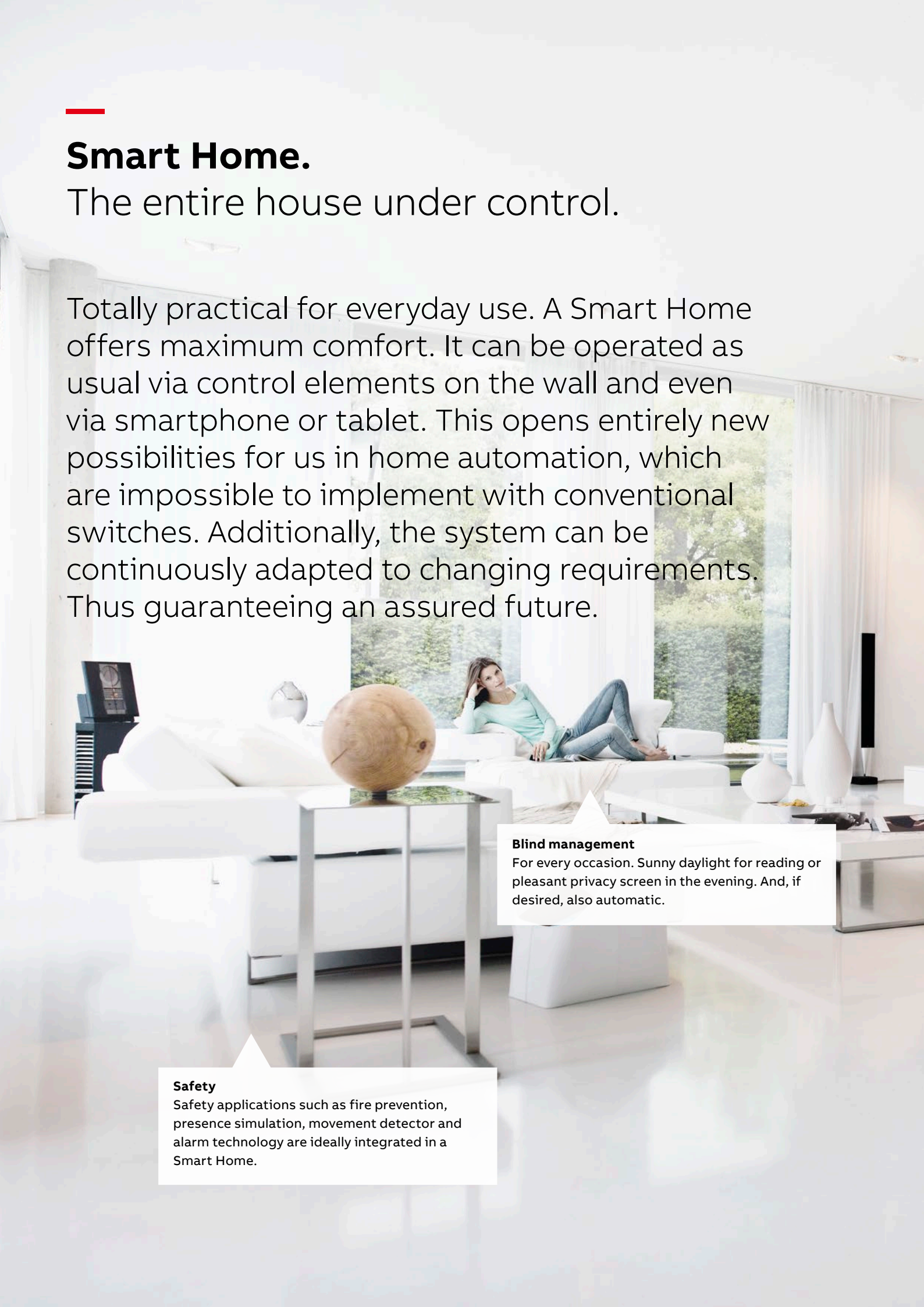
LIVING SPACE® | SMART HOME

Smart Home

Guide for network security in building systems control.

Smart Home.
The entire house under control.

Totally practical for everyday use. A Smart Home offers maximum comfort. It can be operated as usual via control elements on the wall and even via smartphone or tablet. This opens entirely new possibilities for us in home automation, which are impossible to implement with conventional switches. Additionally, the system can be continuously adapted to changing requirements. Thus guaranteeing an assured future.



Blind management
For every occasion. Sunny daylight for reading or pleasant privacy screen in the evening. And, if desired, also automatic.

Safety
Safety applications such as fire prevention, presence simulation, movement detector and alarm technology are ideally integrated in a Smart Home.

Lighting
In a Smart Home it is easy to create different atmospheres with light – from romantic to cosy. With a press of a button a variety of lamps change not only their luminance but, if desired, also their colour.

Scenes
Dining, watching a film or simply relaxing – during various activities, or inactivity, we have different perceptions about perfect light, temperature and privacy screen. With the scene function the desired atmosphere is available with just a press of a button.

Multimedia
Convenient use of everything, even networking. Whether Smart TV, Hi-Fi system, computer or tablet.

Room temperature
No matter how warm you like it, when you are not at home the heating can remain off. And, in a Smart Home, it also does it.

A Smart Home needs safety. Detecting risks early.

Today intelligent building automation is an integral part of modern electrical installation. The house is perceived as living space and is to be adapted to the individual requirements. And here the preferences of the net-worked home are obvious: IP camera, lighting or heating can be operated via smartphone or tablet – even while travelling. What is also important here is to properly protect ones data, in order to minimize risks.

For ABB and Busch-Jaeger the safety of its customers is of the utmost importance. Therefore we always check the IP safety of components for the building systems technology in different test configurations. However, to really reduce the risks of a Smart Home to a minimum, it additionally requires the cooperation of the electrical fitter and the end customer, since the correct installation and the choice of passwords are an integral part of safety.

Glimpses into private life

As soon as elementary elements of one's privacy, such as doors, windows or cameras, are linked via the Internet, comprehensive protection becomes of vital importance. Especially when the user can access the surveillance cameras while travelling, there is the risk that third parties may also read these data. Also the interception of simple control signals, such as switching lights on and off, bears the risk of revealing your habits which burglars could make use of.

Foreign control of your home

If a third party succeeds in hacking into a Smart Home system, there is also the risk of foreign control and reprogramming. This would cause a large part of the added value created by the electrical fitter to be lost, and the system may have to be reprogrammed.

Free choice.
Live as your heart desires.

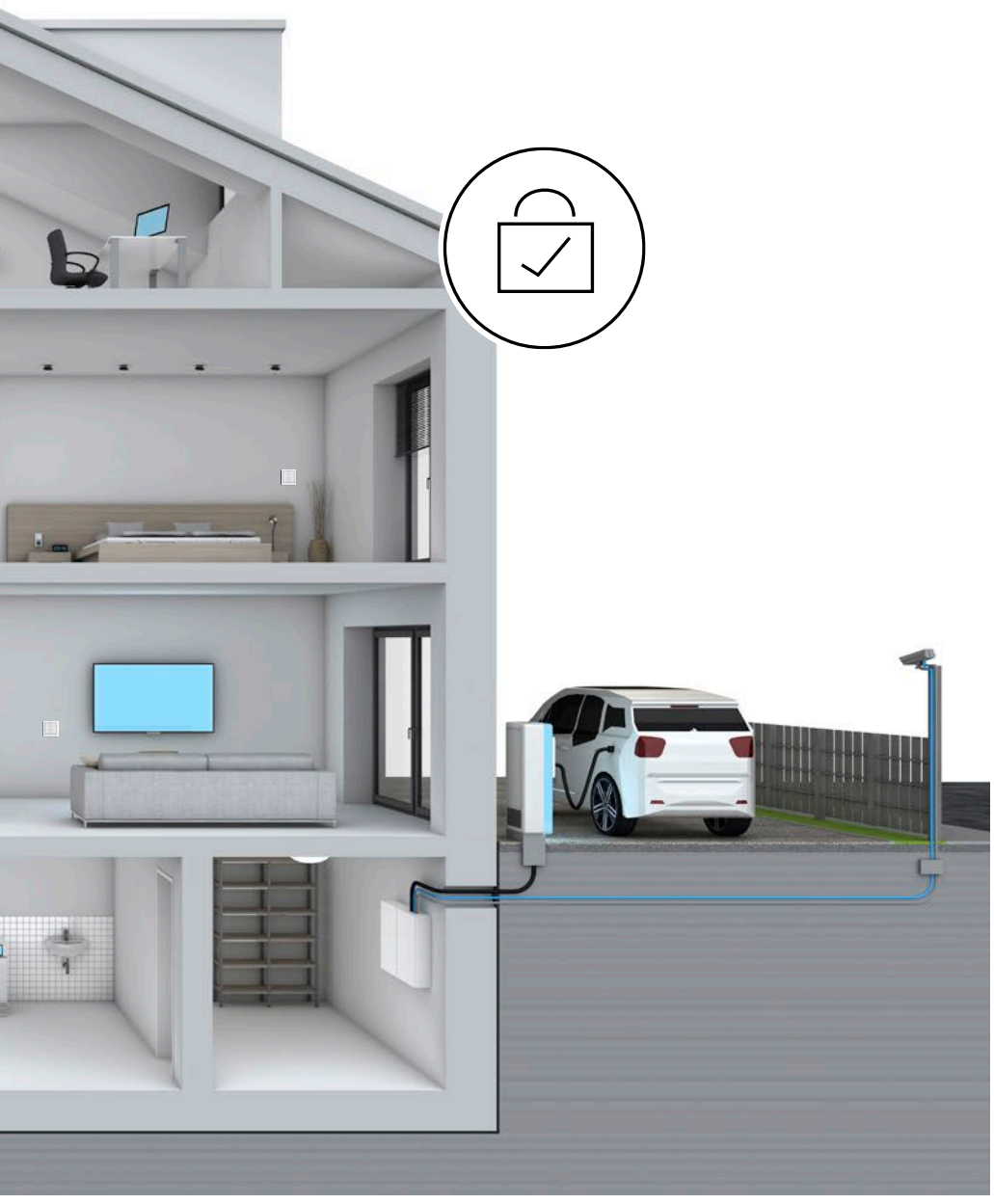
Increase of safety. Smart Home systems make planning, installation and programming by qualified professionals necessary. Generally it is recommended to consult an electrical installer or system integrator for the building automation. Several tips about safety need to be observed during the implementation.

Installation of cables and devices

- As a general rule, applications and devices should be permanently installed to prevent their easy removal and thereby allow access to unauthorized persons to the system.
- The cable ends should not be visible or project out from the wall, neither inside nor outside the building.

Anti-theft facility

Anti-theft facility should be used (securing by means of screws, only removable with tools, high withdrawing forces).



Device password
Use a password if supported by the device. A password prevents unauthorized access to the device.

Areas with limited protection

- Bus lines in outdoor areas represent an increased risk. Here the physical access to the KNX Twisted Pair cable should be made exceptionally difficult.
- If possible, no network lines should be laid outdoors
- Outdoor devices should be protected against unauthorized dismantling.
- Devices installed in areas with limited protection (outdoors, underground car park, WC, etc.) can be designed as independent line for additional protection. The activation of the filter chart in the line coupler prevents attackers from gaining access to the entire system.

Smart Home Network.
Minimizing risks.

Separate LAN-/WLAN network
- For building automation a separate LAN or WLAN network with its own hardware (router, switches, etc.) should be used.
- Provide adequate WLAN cover. For this, additionally installed WLAN Access Points are of assistance.

Use safety mechanisms for IP networks
- Use anti-virus software and firewall
- Encryption of wireless networks (WPA2 or higher)
- Use safe passwords
- Use MAC filter

Safe password
Passwords protect numerous sensitive data coming from us, misuse is often very difficult or even impossible to rectify. The characters of a safe password are described in the following.

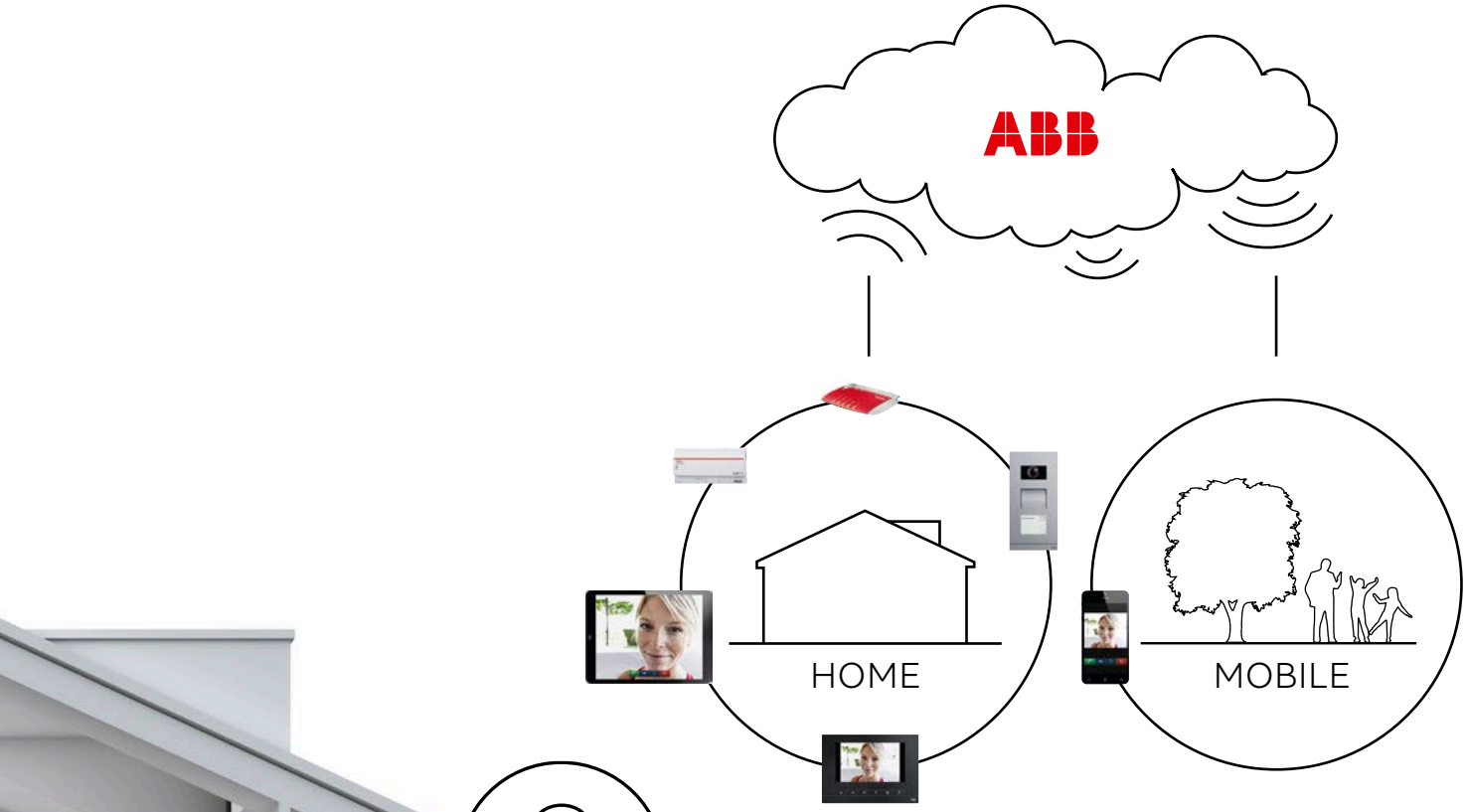
The rules for a safe password:
- The password must consist of at least 8 characters.
- It should contain at least 2 special characters, a number, a small letter and a capital letter.

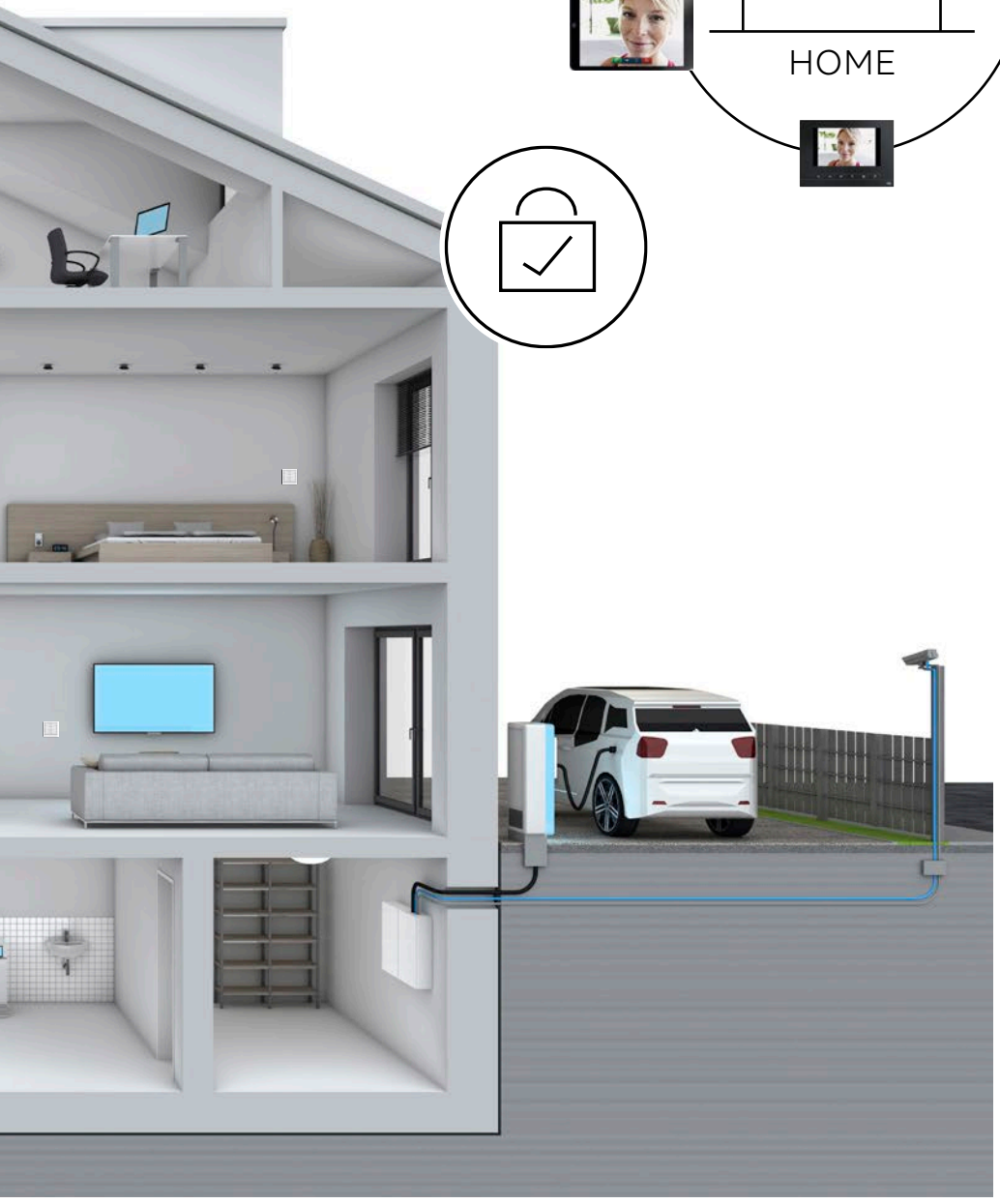
Password managers
If you find it difficult to remember countless passwords, password managers can serve as a memory aid.

Password managers use a safe method to store user names and passwords which you use for accessing websites, and they insert them automatically during your next visit.

In addition to a safe password one should also use the multi-factor authentication. For this a second – temporary – code is mostly used. Apple, Facebook, PayPal and other Internet service providers offer this option.

myABB-LivingSpace





Remote access

- KNXnet/IP routing and KNXnet/IP tunnelling are not safe for use on the Internet since they use a protocol that is not encrypted.
- No ports of routers are to be opened in the direction of the Internet: This prevents KNX communication from becoming visible on the Internet.
- A VPN tunnel or myABB-LivingSpace is recommended for gaining remote access. The myABB-LivingSpace portal is a service of ABB which guarantees the utmost operating comfort for remote access with smartphone and tablet. The end customer does not need a DynDNS account. A connection is established through a cloud by registering and logging in at myABB-LivingSpace: https://my.abb-livingspace.com

Smart Home.
A good feeling.

A Smart Home is intelligent and comfortable. If it is protected correctly against third-parties it can be enjoyed without hesitation – and that from everywhere. The more complex the technical systems and the further the advancement of digital networking, the more critical must the connected safety aspects be considered.

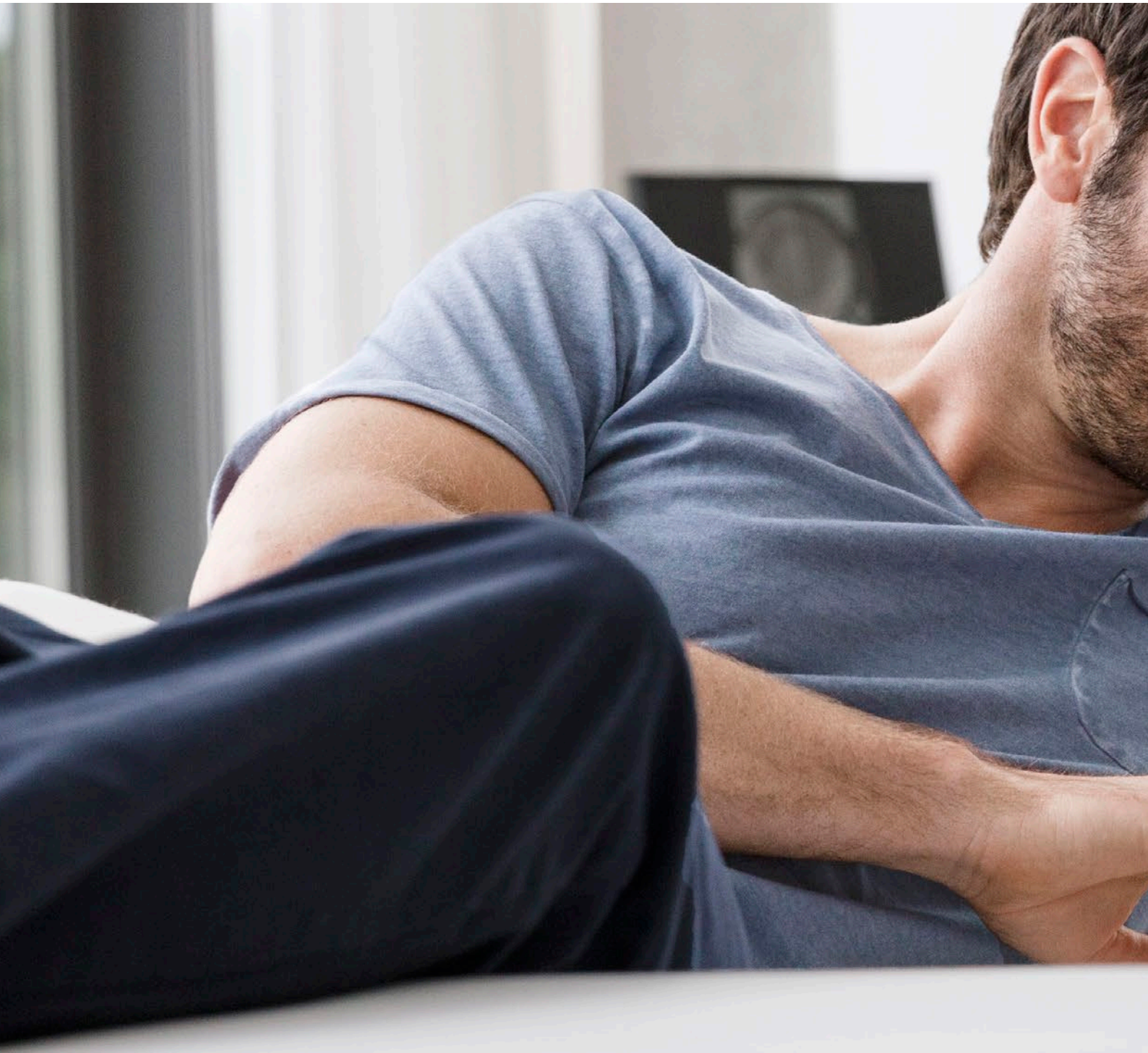


ABB-free@home® is now VDE-certified.
Both the cabled and the wireless components of ABB-free@home®, the ABB-free@home® app of the iOS and Android version, and the remote access via myABB-LivingSpace have been tested by the VDE with regard to the security of information and have passed it as being secure. This enables users to enjoy the entire diversity of the Smart Home functions – even when travelling.

—
new.abb.com/buildings

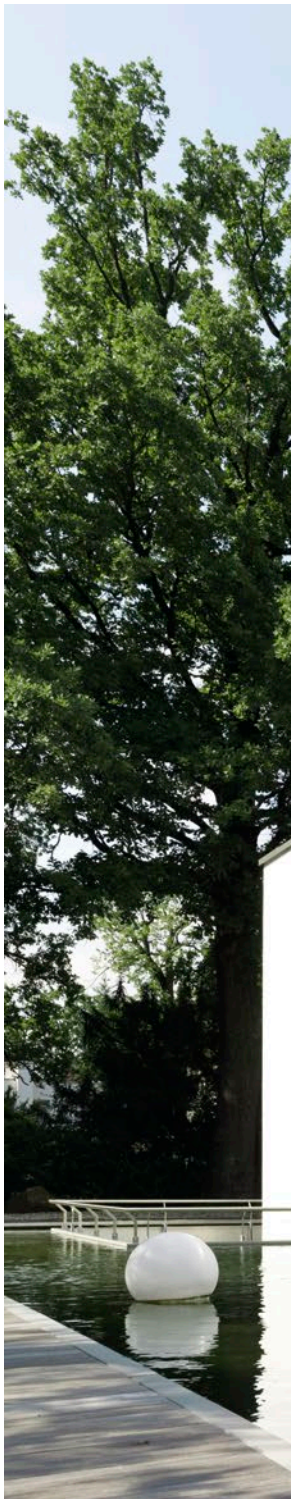
A member
of the ABB Group

Busch-Jaeger Elektro GmbH
P.O. Box
58505 Lüdenscheid
Germany

Freisenbergstraße 2
58513 Lüdenscheid
Germany

www.busch-jaeger.com
info.bje@de.abb.com

Central sales service:
Phone +49 (0) 2351 956-1600
Fax +49 (0) 2351 956-1700



9AKK106713A5111/5.17/0502-D, dpi 419688

© Copyright 2017 ABB. All rights reserved.
Specifications subject to change without notice.