
zencontrol

Security

With the rise of IoT and cloud connected devices, security has been continually overlooked

Adequate security is a must for connected systems

- Many control system are already exposed
- Many connect through an Ethernet gateway with zero protection
- Many use TeamViewer or other remote connection software
- Most sites can be comprised easily

The risk of IoT

- 2016 saw botnets using the Mirai exploit to compromise devices and produce large scale DDoS attacks (Distributed Denial of Service attacks)

- A DDoS attack can be used to take down websites and other online services

- DDoS attacks built on the Mirai exploit are based on vulnerabilities in an outdated operating system used in many embedded devices

The risk of IoT

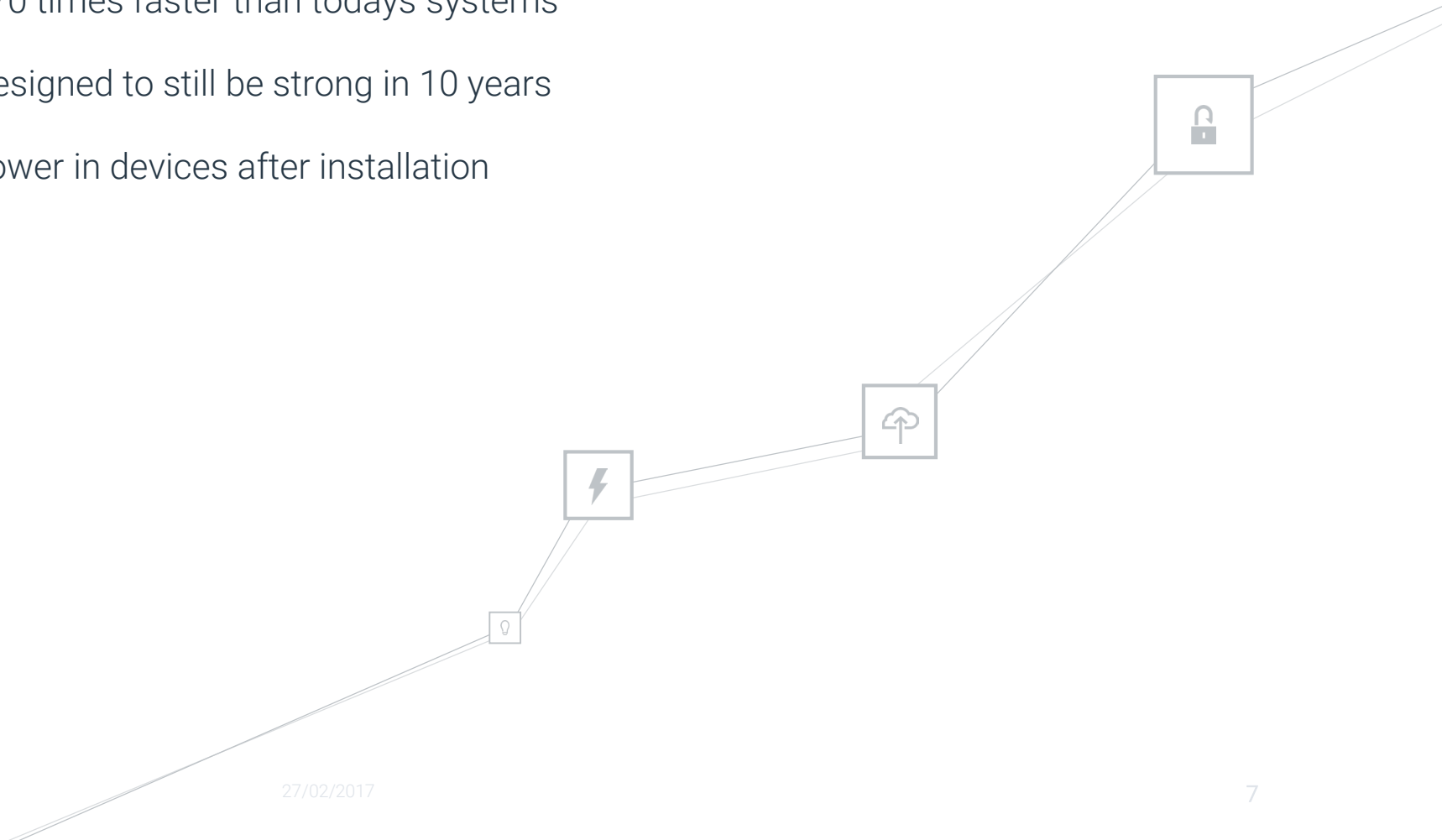
- Due to limited processing power and lazy software development many IoT devices such as webcams and network equipment have not implemented or have outdated encryption
- Many have implemented security flaws or have hardcoded security keys and credentials
- FTC has outstanding lawsuits with companies such as D-link for negligent security practices
- The sheer number of IoT devices, if vulnerable, can create large issues if not handled correctly
- Unprotected systems can expose data, provide unauthorised access and put users at risk of malware or allow illegal activity

Why?

- A high level of processing power is required to encrypt sufficiently (on all devices)
- Processing power cost $$ and many devices do not have the budget
- Implementing correct systems is costly (labour) and time consuming
- Control system companies and IoT suppliers don't have resources to implement security correctly. Typically they lack the budget & skilled people

Risk

- Processing power doubles every 18 months making it easier to break cryptos
- In 10 years computers will be 70 times faster than todays systems
- Security systems need to be designed to still be strong in 10 years
- Cannot increase processing power in devices after installation

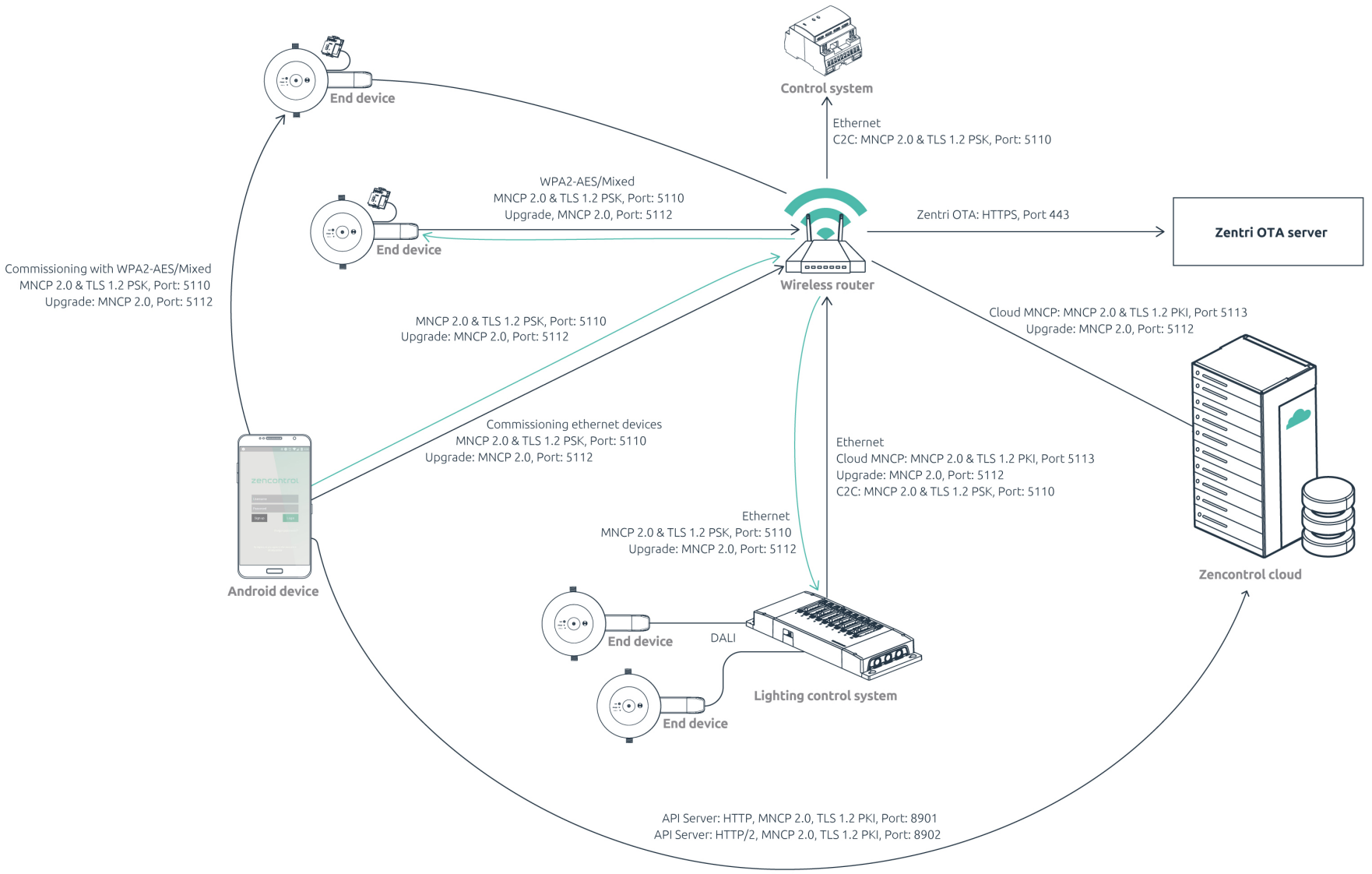


zencontrol security

zencontrol device security

- Devices include enterprise grade encryption
- Devices are upgradeable, new exploits will be patched and protected against
- Every individual device programed with unique and strong 32byte encryption key
- Local communications use TLS 1.2 PSK
- Cloud communications use TLS 1.2 PKI (4096 RSA)
- TLS 1.2 stack developed and backed by ARM
- Password/credential storage hashed and salted

System overview



Secure practices

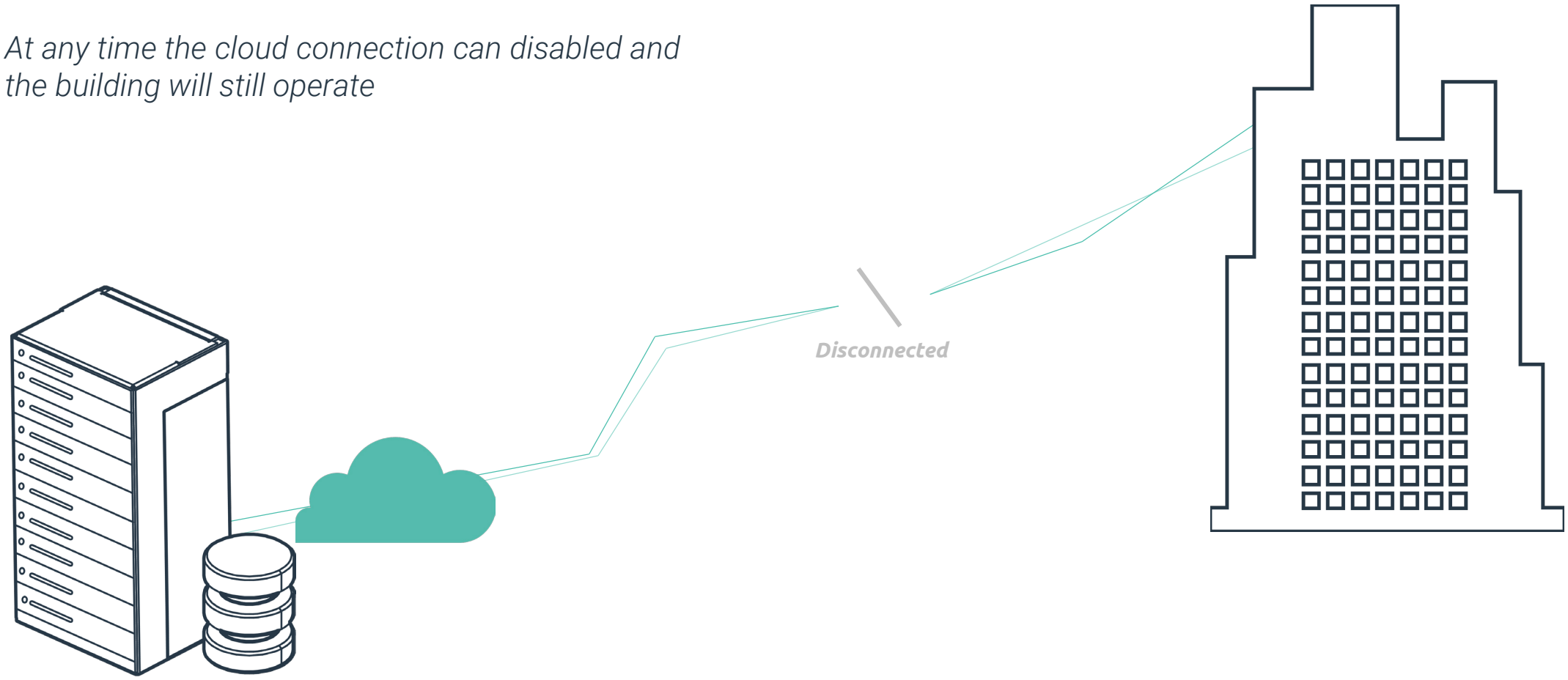
- Local servers abide by local privacy laws
- Access control list which ensures only the correct users can access sensitive information
- Private keys are not stored in firmware or firmware repository
- Security is built in from day 1, zencontrol is secure from installation
- Authentication tokens are per device/API-client allowing auditing and per device access revoking capabilities
- Cryptographically signed firmware security updates can be pushed remotely as a response to security issues

zencontrol does not take security lightly. Practises and implementation help ensure that zencontrol networks stay strong well into the future

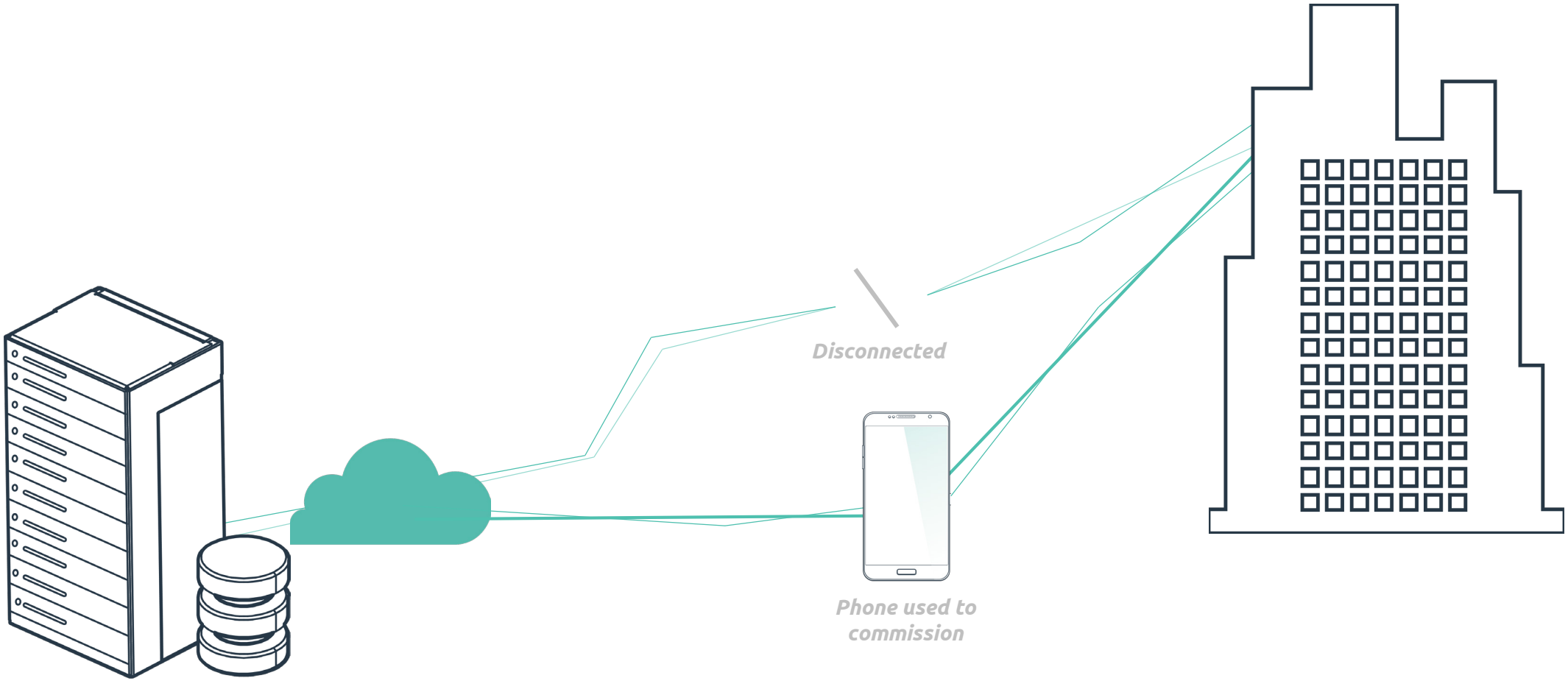
…but

…zencontrol systems still run without the cloud

At any time the cloud connection can disabled and the building will still operate



Users can still use cloud to commissioning and setup



zencontrol.secured