STORMSHIELD

Different strategies for actively reducing the network attack surface

Source: Reddit
www.reddit.com/r/talesfromtechsupport/comments/6ovy0h/how_the_coffeemachine_took_down_a_factories/

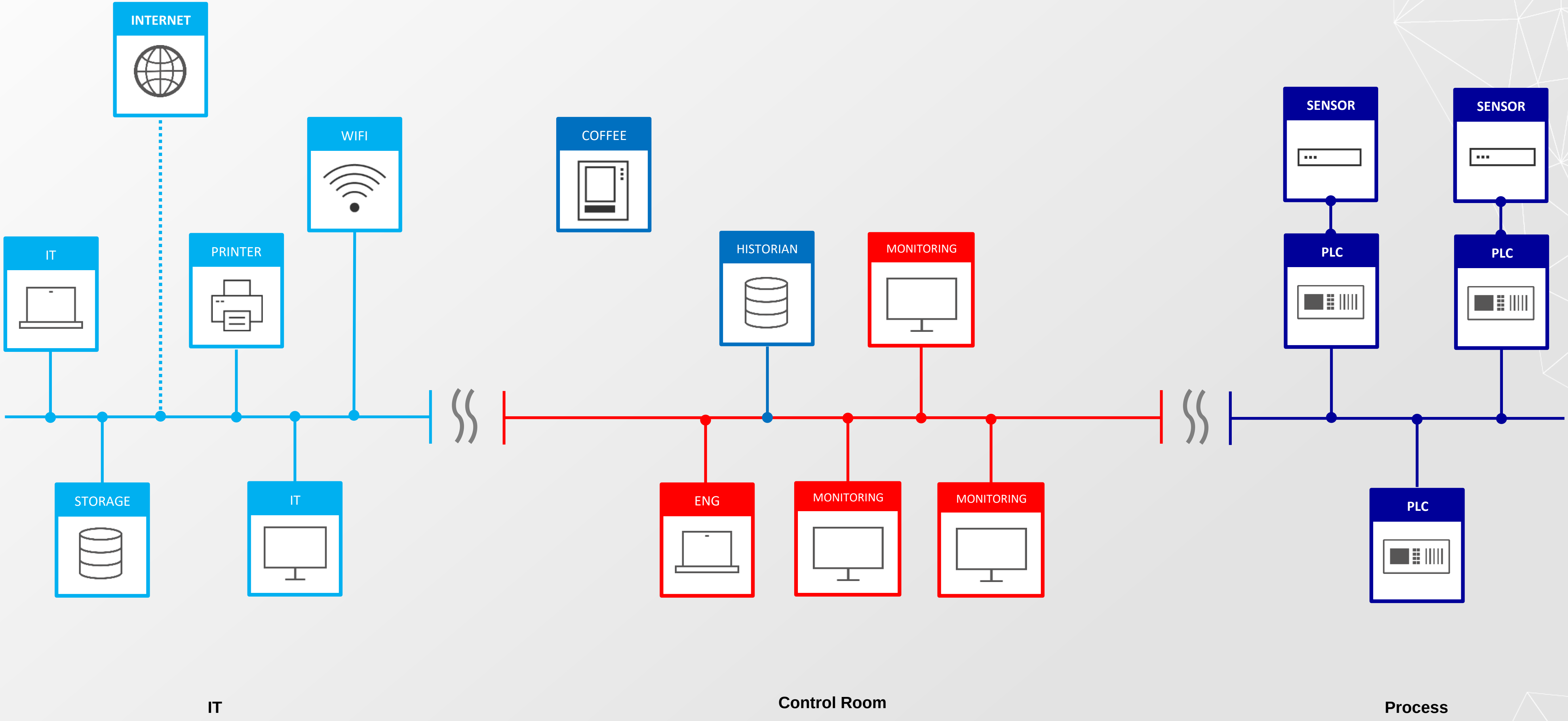
Attack Surface

attack surface – the sum of the potential exposure area that could be used to gain unauthorized entry to any part of a **digital landscape**. This area usually includes perimeter **network** hardware (such as **firewalls**) and **web servers** (hardware that hosts Internet-enabled **applications**). It can also include extended areas of the landscape such as external applications, supplier services and mobile devices that have permission to access information or services of value.

source: The Cybersecurity to English Dictionary

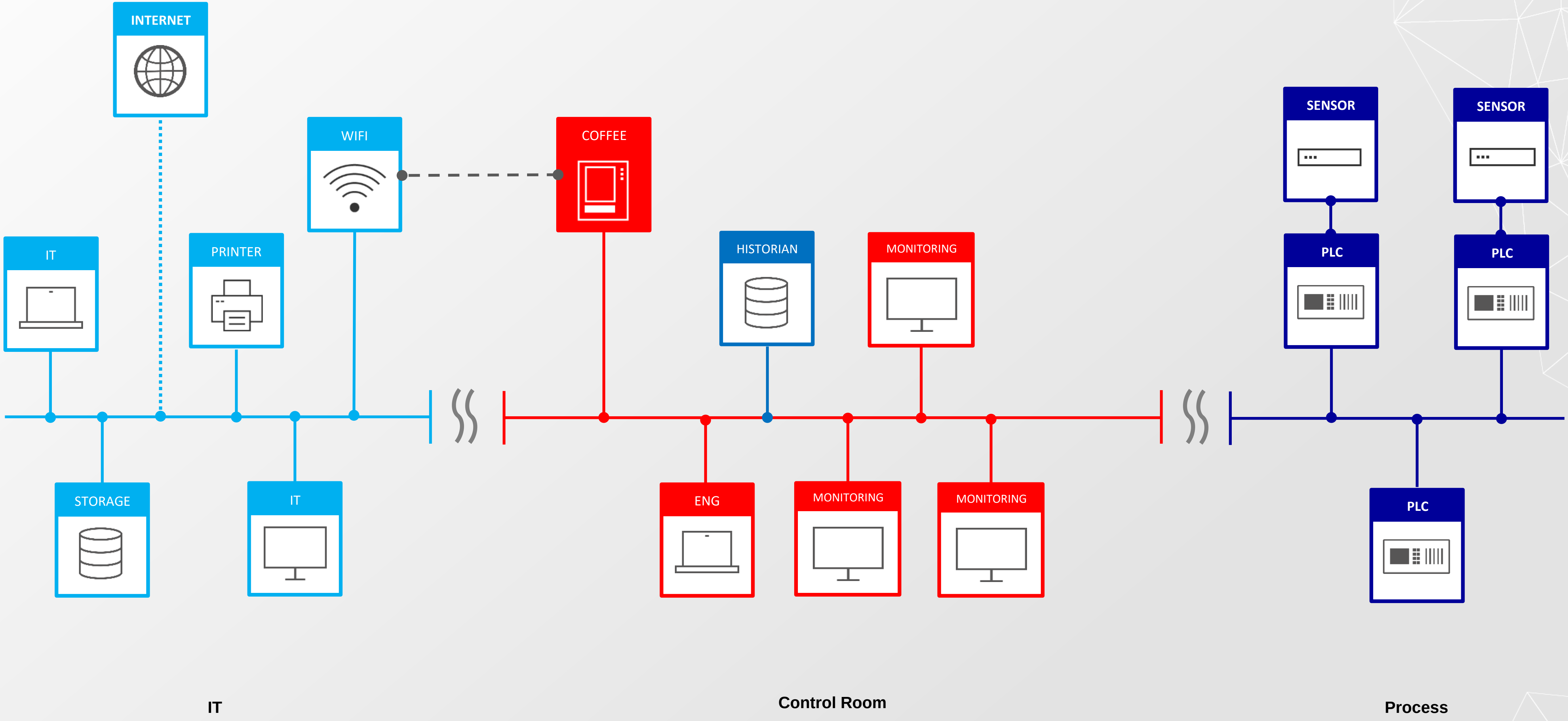
How the coffee machine took down a factory

Reddit



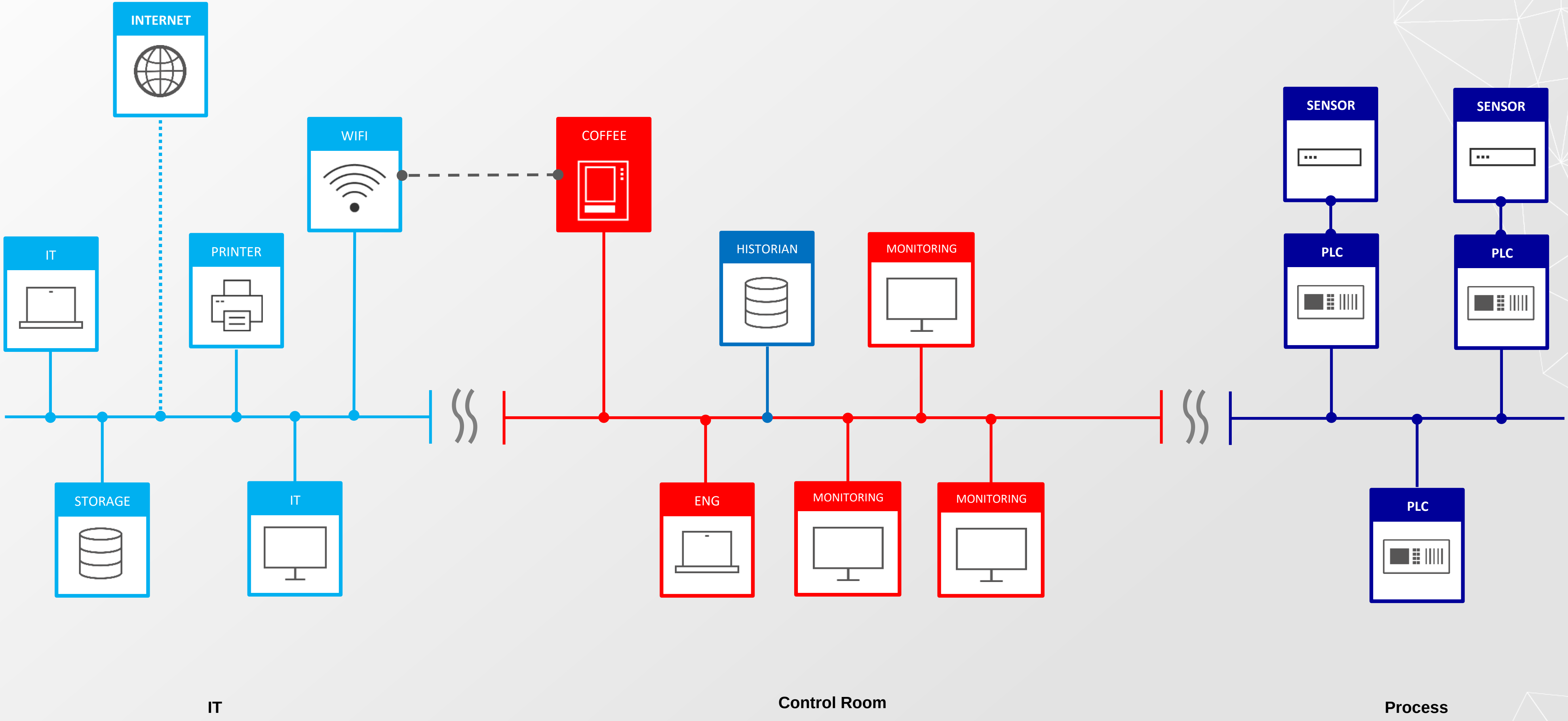
How the coffee machine took down a factory

Reddit



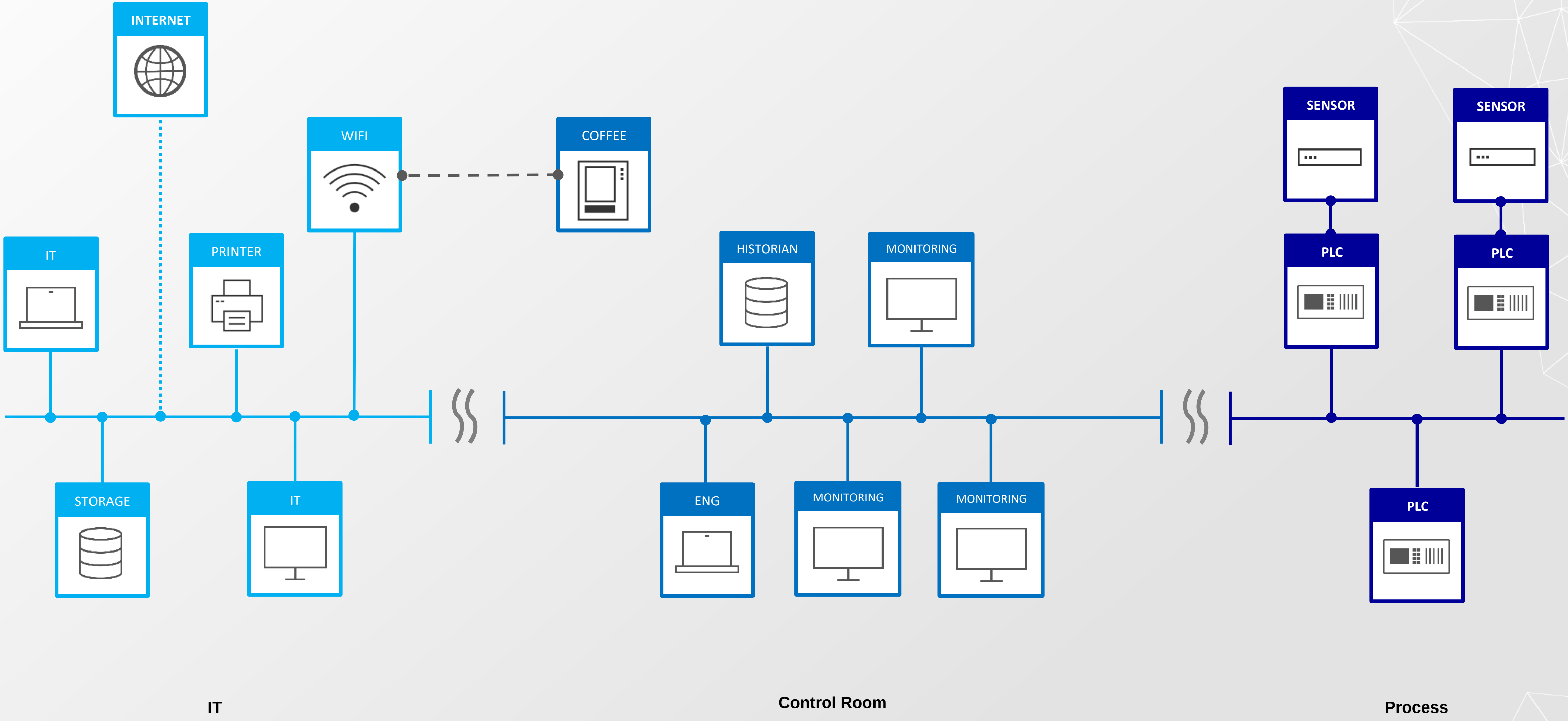
How the coffee machine took down a factory

Reddit



How the coffee machine took down a factory

Reddit



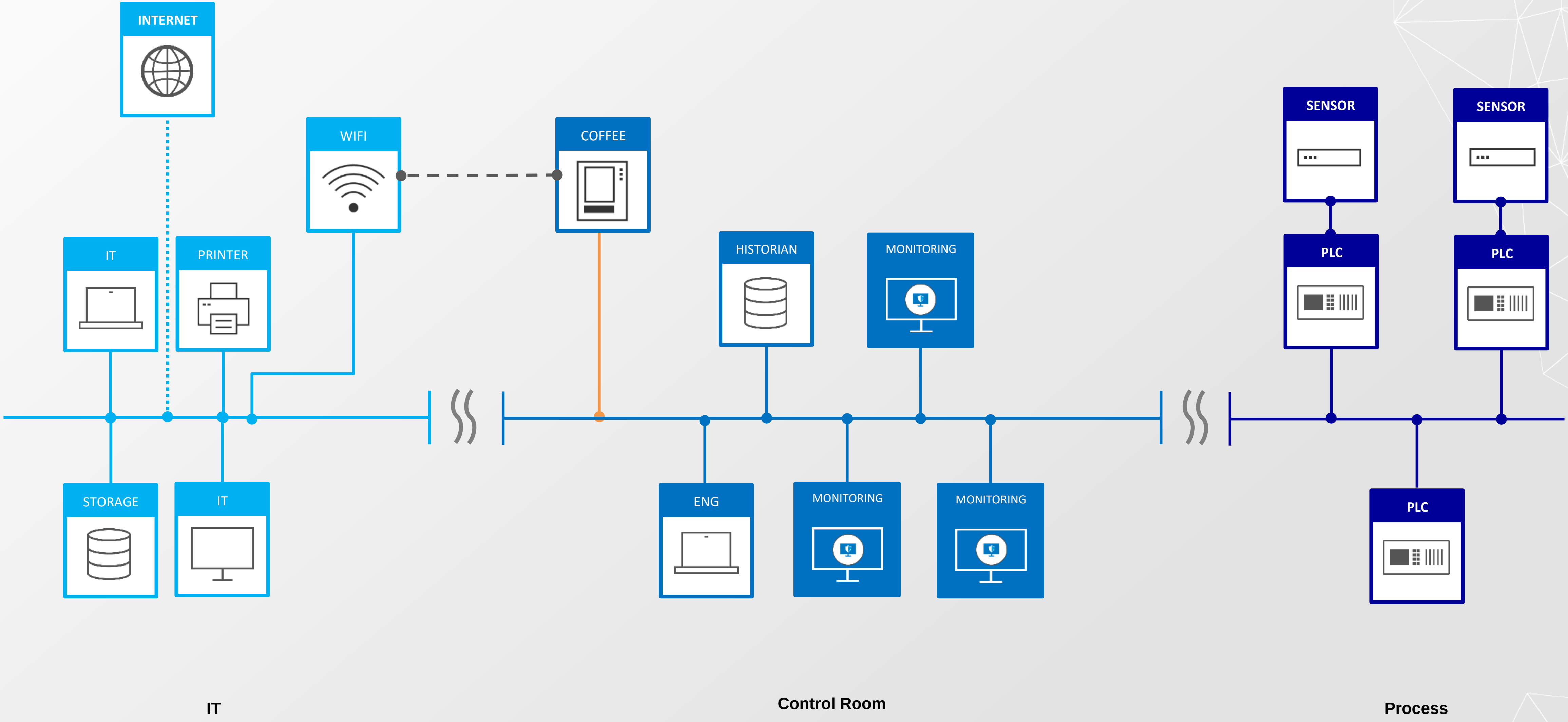
Endpoint Protection

endpoint protection – a term used to describe the collective set of security software that has become standard for most user-operated **digital devices**. The security software may include **anti-malware**, a personal **firewall**, intrusion prevention software and other protective programs and processes.

source: The Cybersecurity to English Dictionary

STORMSHIELD

Protecting the Endpoint



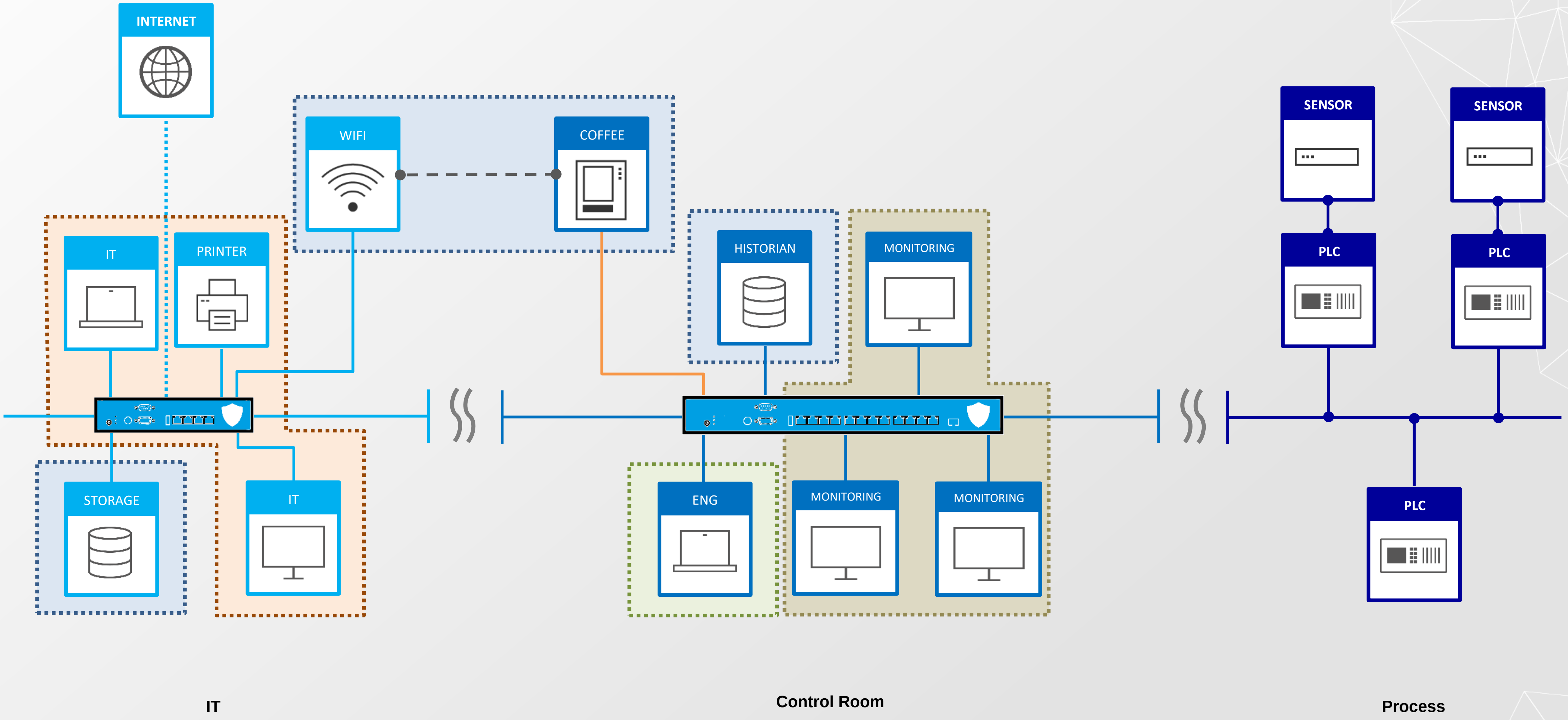
Network Segmentation

Network segmentation

Splitting a single collection of devices, wiring and applications that connect, carry, broadcast, monitor or safeguard data **into smaller sections**. This allows for more discrete management of each section, allowing **greater security** to be applied in sections with the highest value, and also permitting **smaller sections to be impacted in the event of a malware infection** or other disruptive event. .

source: The Cybersecurity to English Dictionary

Enabling Network Segmentation



Network protection

the defensive and protective measures taken to secure a specific set of interconnected **devices**. **Firewalls** are an example of a network protection technology.

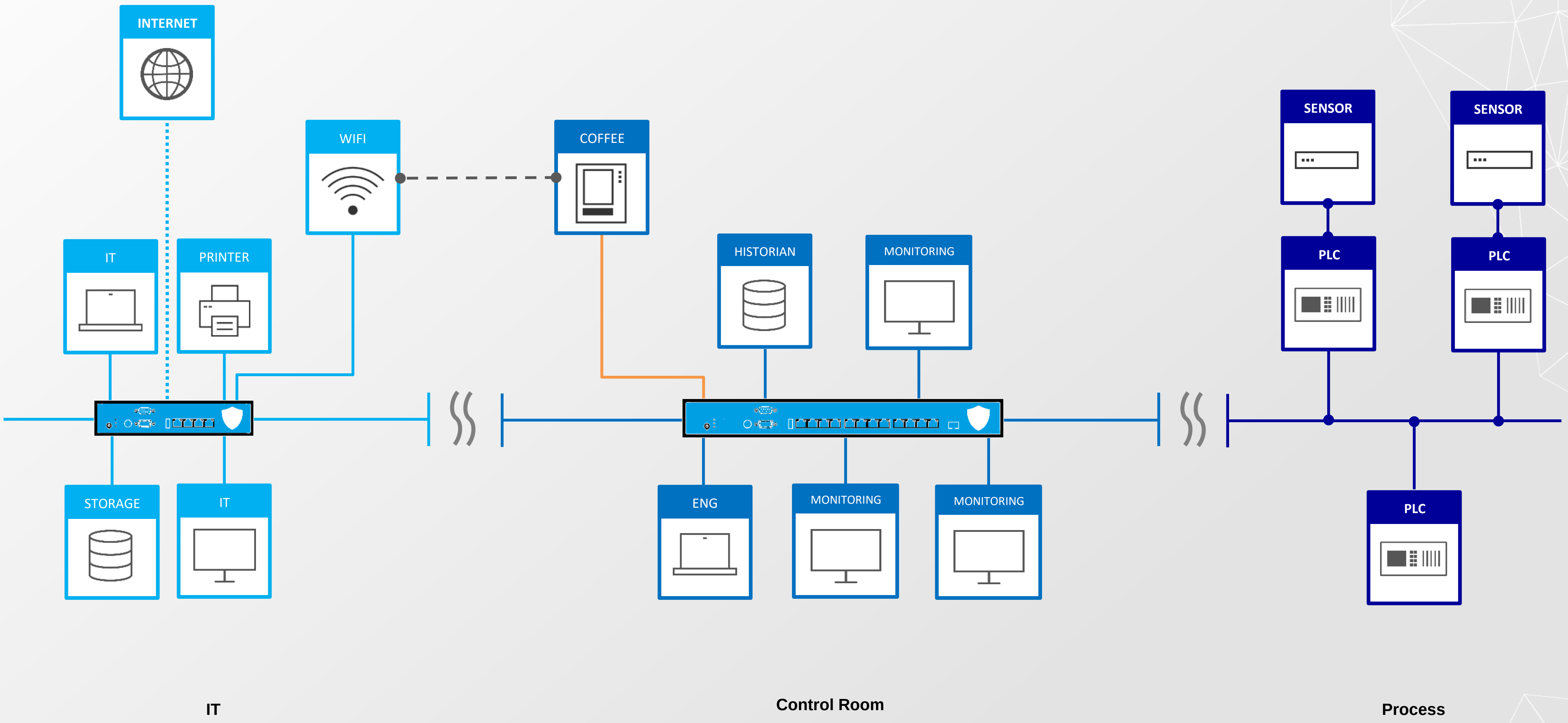
source: The Cybersecurity to English Dictionary

Deep packet inspection

(DPI, also called **complete packet inspection** and information extraction or IX) is a form of computer network packet filtering that examines the data part (and possibly also the header) of a packet as it passes an inspection point, **searching for protocol non-compliance, viruses, spam, intrusions**, or defined criteria to decide whether the packet may pass. […]

source: Wikipedia

Enabling Network Protection and Deep Packet Inspection

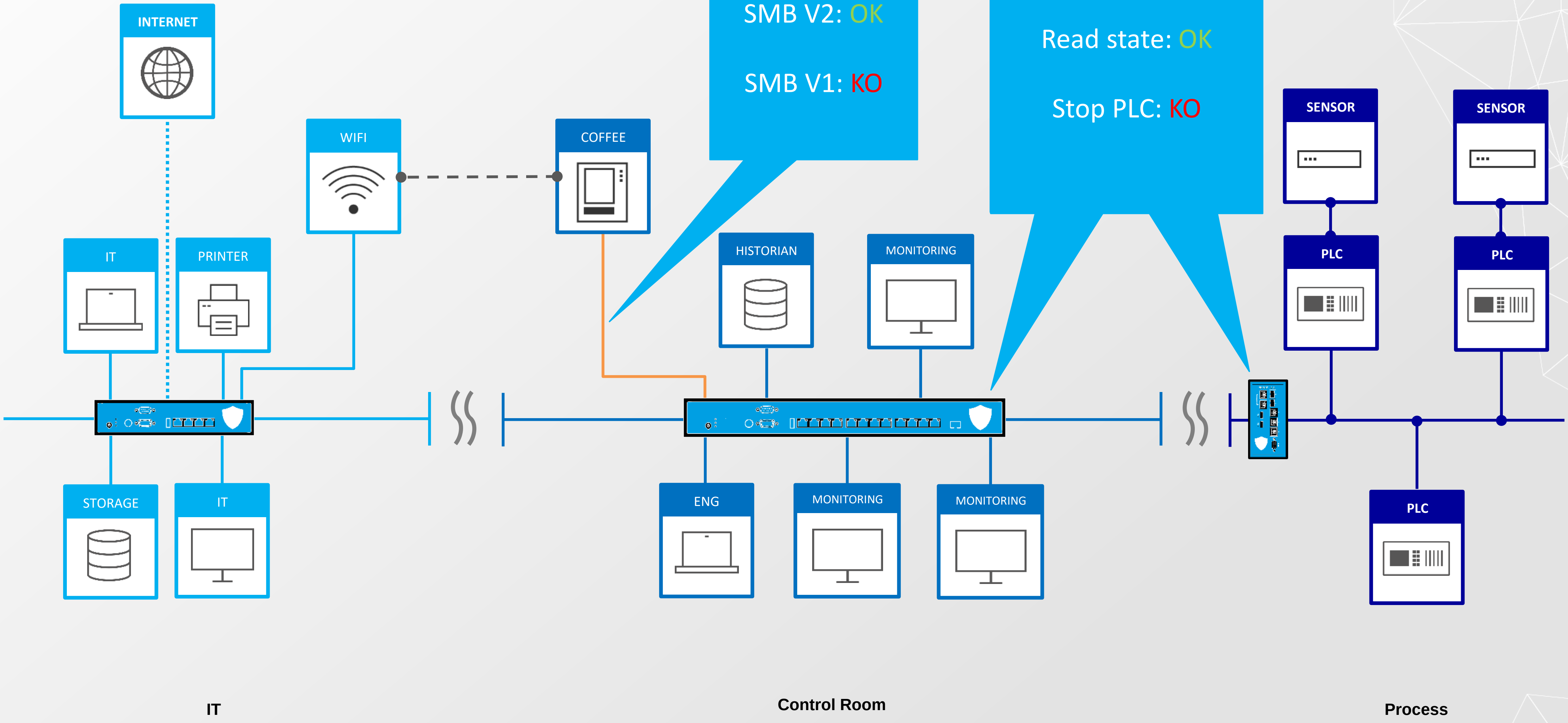


Application Network Communication Control

The ability to ensure that only predefined or **pre-allowed messages can go through** protection inspection points.

source: None

Enabling Application Network Communication Control



SMB V2: OK

SMB V1: KO

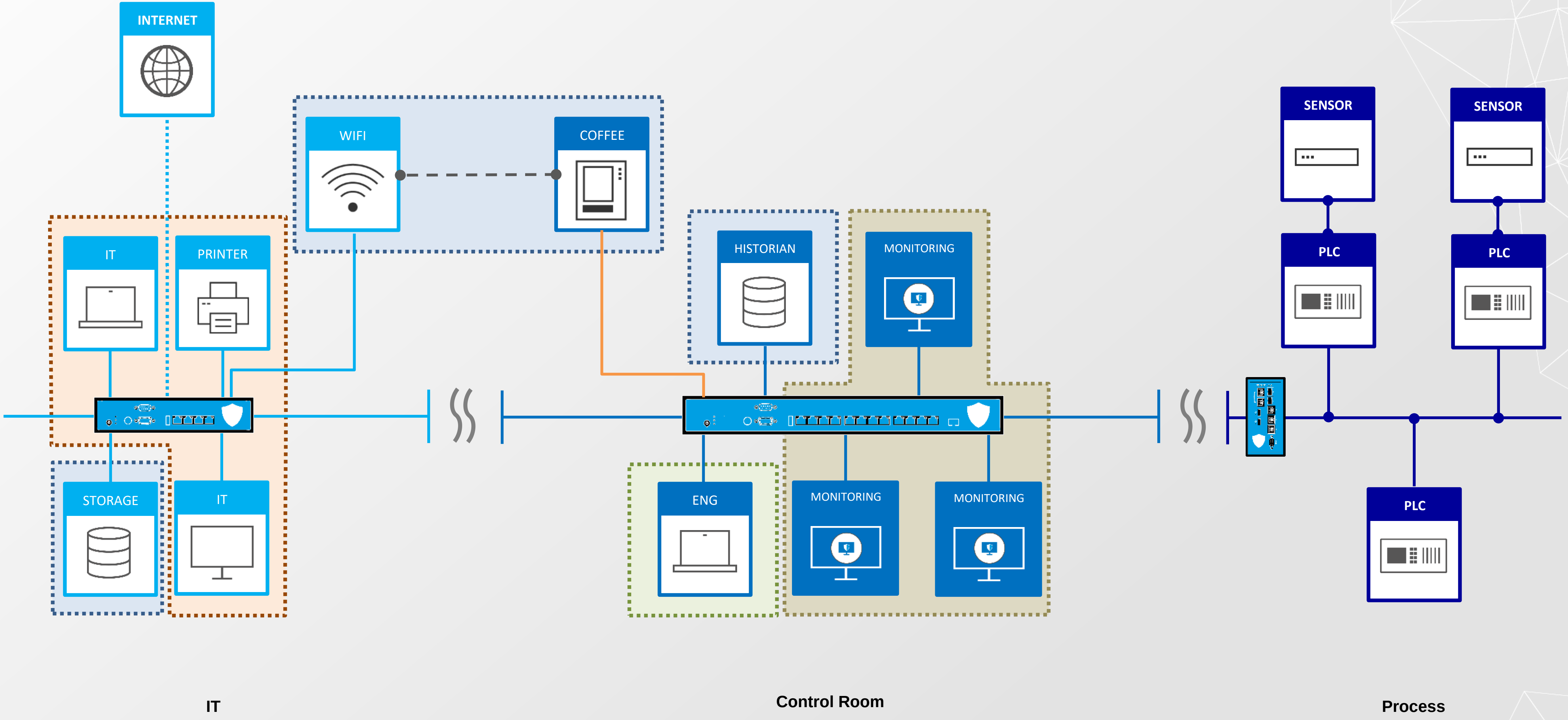
Read state: OK

Stop PLC: KO

Stop coffee

Conclusion

The more strategies you apply, the safer you are



STORMSHIELD

Q&A

robert.wakim@stormshield.eu
www.stormshield.com