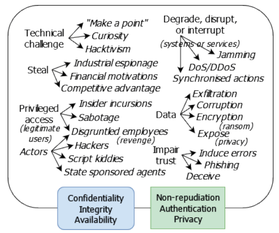
Cybersecurity of Active Buildings

ACTIVE BUILDING CENTRE RESEARCH PROGRAMME

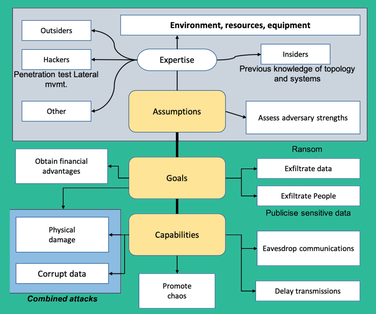
Research topics

- Threat Modelling Active Buildings
- Assessing vulnerabilities in threat-based approaches (MITRE's ATT&CK framework, and ATT&CK for ICS)
- Co-simulation: stressing the infrastructure by emulatin cyber-attacker
- Modelling and evaluation of adversarial behaviour
- Scaled models running microcontrollers that mimic an operational Active Building

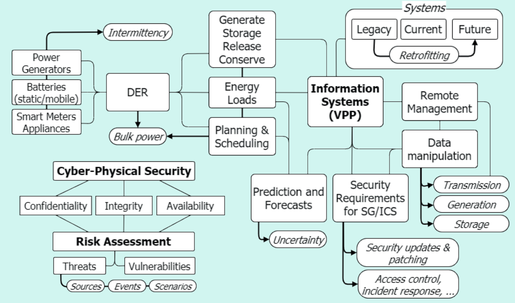
Major drivers and actors in cyber-security



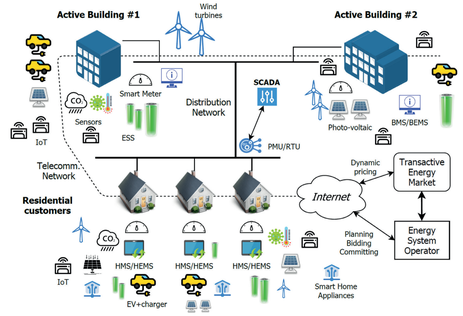
AGC Model



Cyber-Physical Systems to support the Active Buildings business proposition

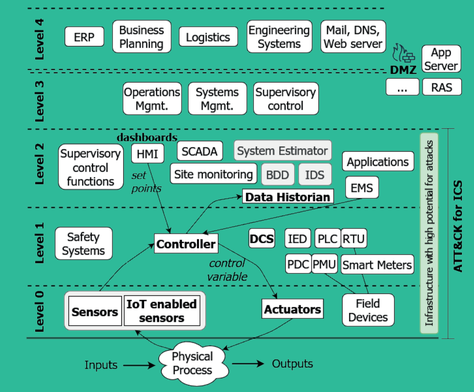


Attack surface of Active Buildings (a brief excerpt)

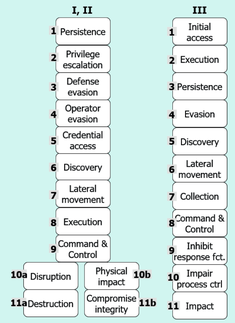


A myriad of components with telecommunication capabilities are distributed across the infrastructure. Timely control, detection, identification, and mitigation are in place to ensure smooth operations. Intrusion Detection Systems (IDS), latest vulnerabilities databases, continuous logging, and detecting bad data before feeding Information Systems help thwarting cyber-attacks, among other measures.

'Adapted' Purdue Enterprise Reference Architecture Model (PERA)



Usual attack Cyber Kill Chains in TTPs and attack vectors in ICS



Adversaries use distinctive attack vectors to invade systems and establish footholds. Threat hunting approaches allow to explore the vulnerabilities state space and devise measures to detect and contain attacks before they spread over other systems.

MITRE's Tactics, Techniques, and Procedures (TTP) employed by adversaries in the ATT&CK for ICS framework. These vulnerabilities databases contain documented attacks perpetrated by adversarial groups over the Internet for the past years and may guide mitigation actions.

Ricardo M. Czekster • Newcastle University
Walter A. Bassage • University of Sheffield

Newcastle University
The University Of Sheffield.
UK Research and Innovation
INDUSTRIAL STRATEGY