Building automation systems (BAS) are concerned with control and monitoring of buildings, while aiming to achieve different goals such as:

- provide safety for inhabitants (e.g. by integrating fire alarm systems or physical access control),
- control the climate in the building/supervise and control the heating, ventilation, and air conditioning equipment
- perform facility management (indicate problem by generating reports, graphs and annunciating alarms)
- perform energy management strategies to reduce operating and energy costs

Security in building automation systems

Building automation systems dethaw the aspect of security as they originated at the time when security was not an utmost concern. Some security challenges concerned with building automation systems (Granzer et al., 2010) are:

- Network attacks: Manipulation, fabrication or interruption of the transmitted data over the network
- Device attacks: Software level: code injection, exploiting algorithm; Physical level: component replacement, microprobing
- Network steganography: Hidden exfiltration of sensor data (e.g. monitoring of inhabitants or employees) (Wendzel, 2012)

Virtual Testbed

**Major goal:** Allow teaching of BAS fundamentals and BAS security for students and employees in a highly configurable way without requiring expensive BAS hardware.

**Defensive mechanism:** Traffic Normalization
We realized traffic normalization as a protection measure for one of the widely used BAS protocols BACnet.
- Sits on the communication path between the BACnet devices and monitors the traffic exchanged between the devices in order to detect anomalies
- Reports malicious activity and perform actions (drop/modify) as per normalization rules

**Benefits:**
- Very simple, cheap solution and available as open source
- Easy to get hands-on with the logic and code
- Dynamically show the behavior and relationship of the components involved
- Comprehensive testing can be done effectively without damaging the real hardware
- Results in reduced training time
- Efficient monitoring of network flow with the help of Wireshark