Covert Channels and their Prevention in Building Automation Protocols – A Prototype Exemplified Using BACnet

Steffen Wendzel[1,2], Benjamin Kahler[2], Thomas Rist[2]
[1]University of Hagen / [2]Augsburg University of Applied Sciences

2nd Workshop on Security of Systems & Software Resiliency
November 20, 2012, Besançon

Outline

IT4SE

- Covert/Side Channels and Active Wardens
- Building Automation Systems and BACnet
- Covert/Side Channels in BAS
- Building-aware Active Warden
- Covert Channels in BACnet
- Prevention of BACnet-based Covert Channels
- Conclusion & Future Work

Covert Channels

- A communication channel not designed to be used for a communication
  - Presented by Lampson in 1973
- CCs break mandatory security policies
  - Multi-Level Security (MLS) → Bell-La Padula
- Timing and Storage Channels
- Can be used to exfiltrate confidential data from networks

Active Wardens

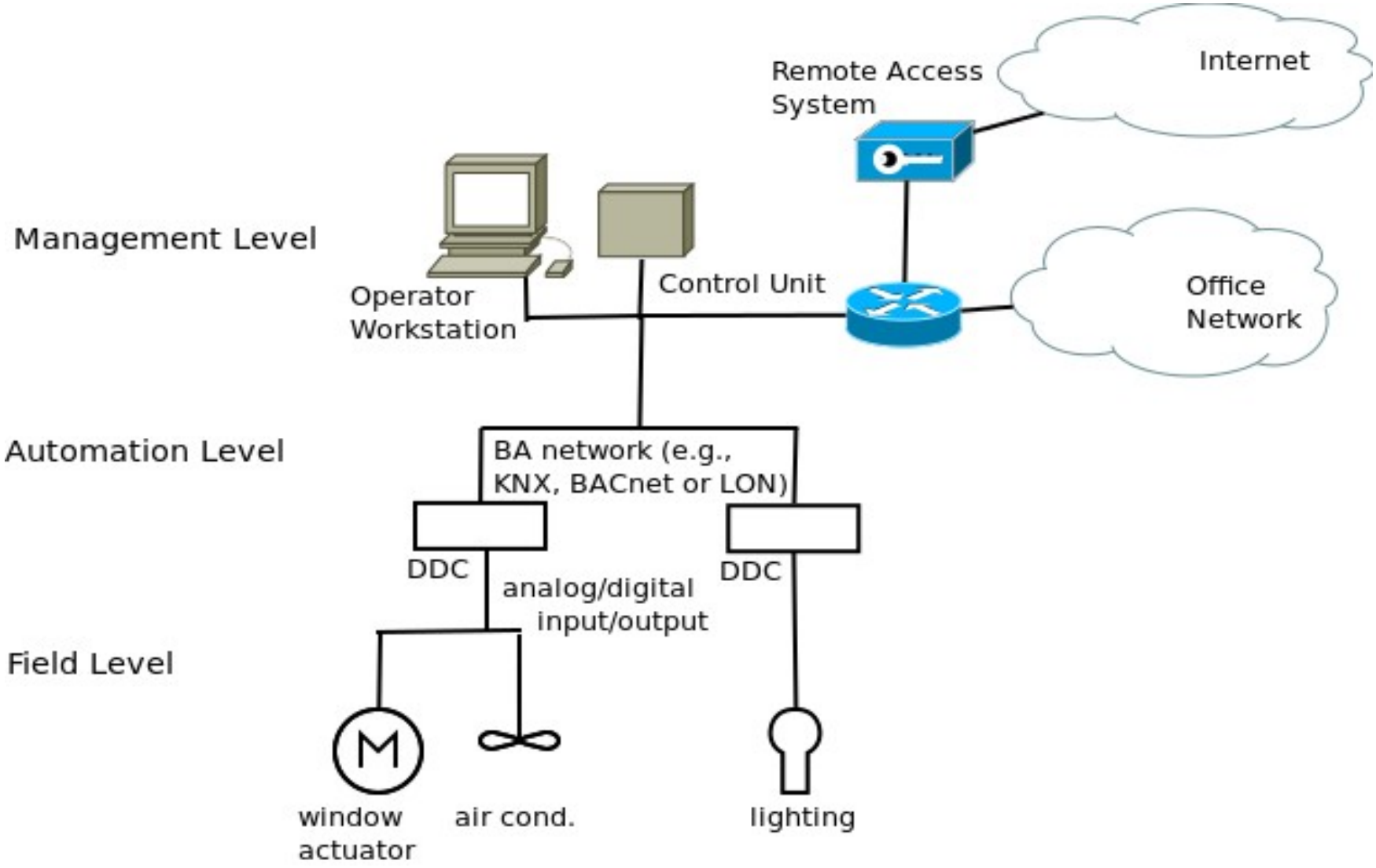
- **Passive** wardens try to detect steganographic elements within information transfers
- **Active** wardens try to remove such steganographic elements
  - Like OpenBSD pf scrubbing or Snort normalizer

Building Automation Systems

- Early systems: HVAC
  - **H**eating/**V**entilation/**A**ir-**C**onditioning
- Today used for nearly everything
  - Ambient Assisted Living (AAL)
- Various low-level protocols
  - e.g., EIB/KNX, BACnet, proprietary protocols

HomeMatic Central Control Unit (CCU)

Building Automation Systems



BACnet

IT4SE

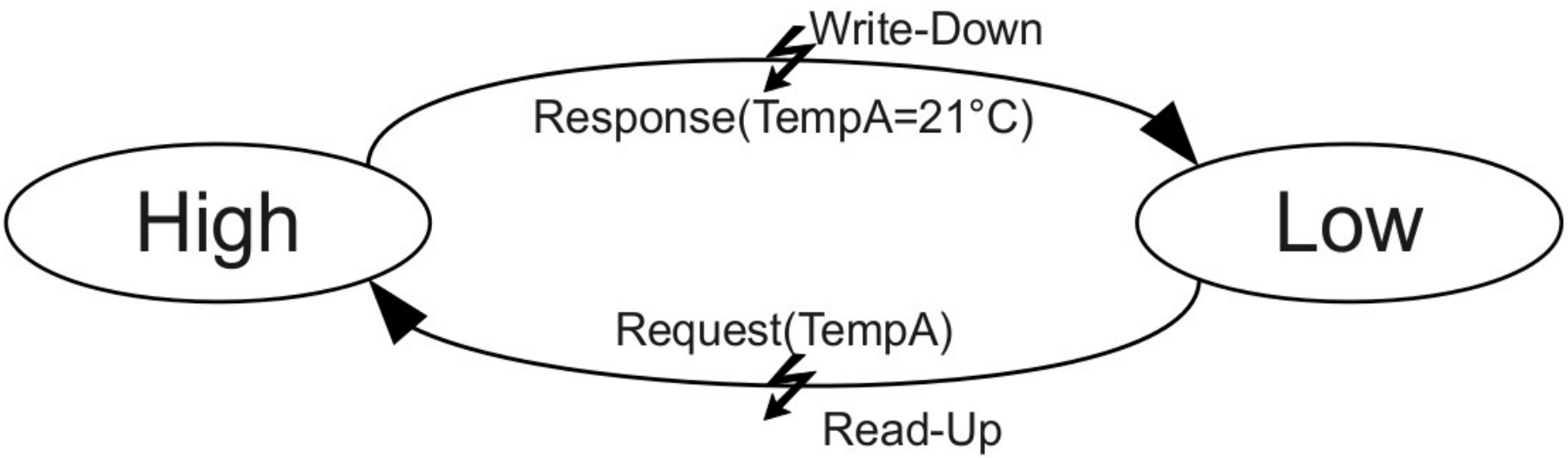
- Selected BACnet (*Building Automation and Control Network*) due to its popularity
- Developed by ASHRAE[1]
- BACnet comprises its own protocol stack (OSI layers 1-3 and 7)
- Open OSI standard since 2003
- One of the most important BAS protocol suites (e.g., used in German Parliament building)

[1] American Society of Heating, Refrigeration, and Air-Conditioning Engineers

Covert/Side Channels

- **Side Channel:**
  - **Unintentional** sender (information leak), intentional receiver
- **Covert Channel:**
  - **Intentional** sender, intentional receiver
- Monitoring of inhabitants, employees, …
- Bypassing enterprise network security means by leaking confidential information through the BAS

Read-Up/Write-Down in BAS

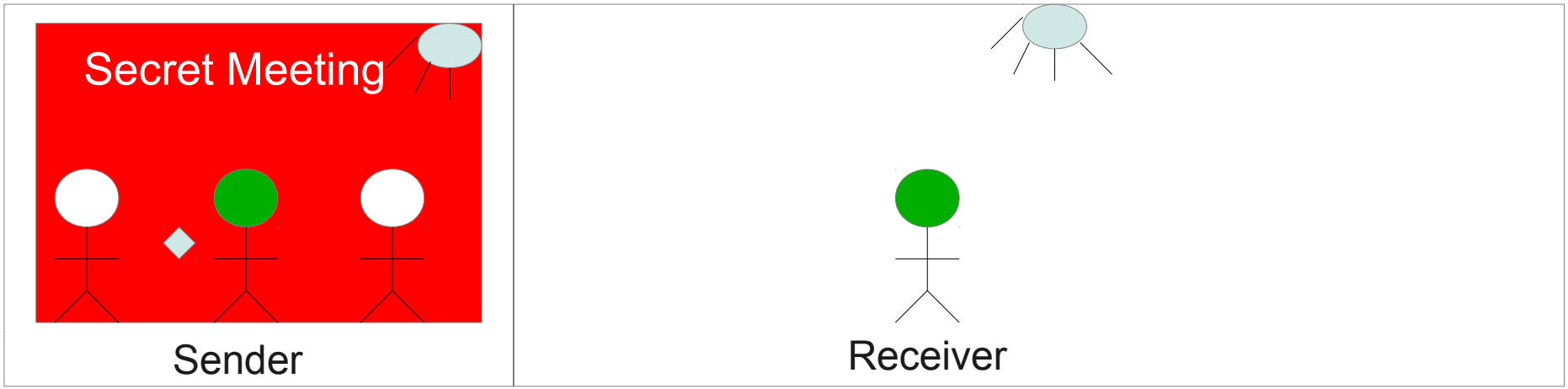


Example:
Side Channel in BAS

- **Passive** monitoring of all events within the BAS network
- **Active** information request of unintentional leaked information via middleware
  - Is my boss currently in his office? If not, I could try to steal a secret document.
  - Idea: Request BAS information such as
    - lighting on/off, room temperature, …

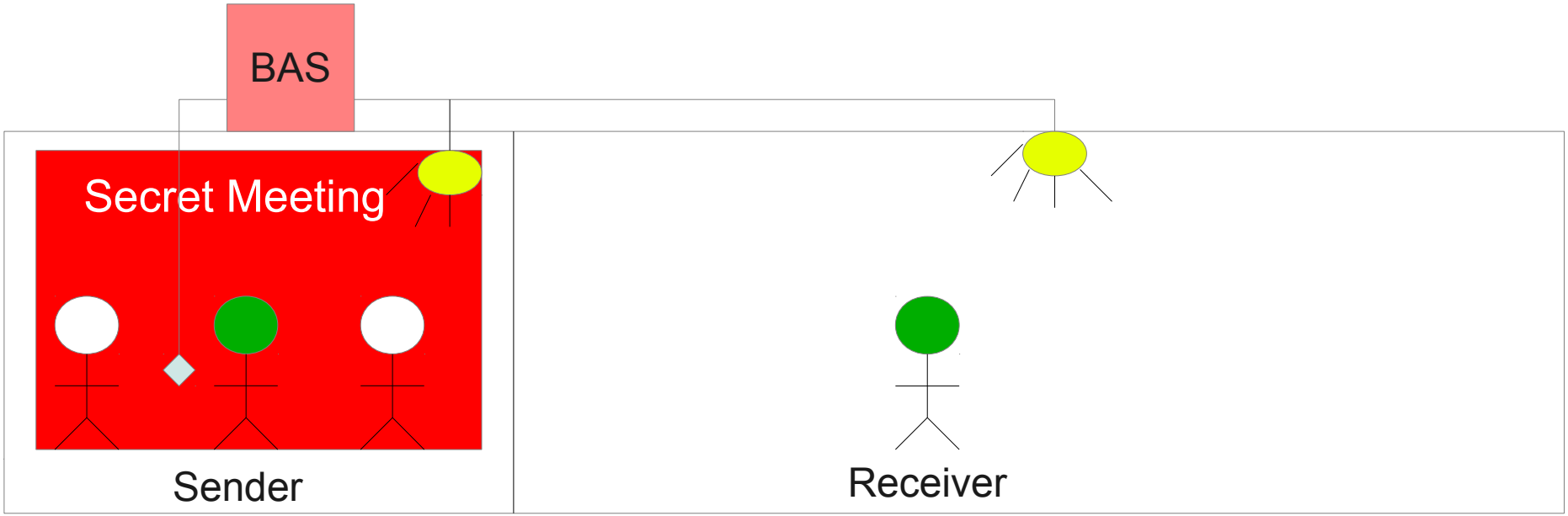
Example:
Covert Channel in BAS

- Collaborative information transfer violating a mandatory access policy
- Example: Papal Conclave



Example:
Covert Channel in BAS

- Collaborative information transfer violating a mandatory access policy
- Example: Papal Conclave



High/Low Covert Channels

IT4SE

- High-level Covert Channels are
  - based on the interaction with the BAS

    → Building-aware active warden
- Low-level Covert Channels
  - embed hidden data in BAS network protocols

    → introduction of MLS into BAS network environment

Building-Aware Active Warden

IT4SE

- Based on a previous development
  - „HASI“ (*Home Analytical System Interface*)
  - Middleware (initially developed by student project group)
  - Supported HomeMatic by eq-3 and CurrentCost
  - No mentionable security features
  - Web-based Interface (the only „App“)

Nabaztag Rabbit ™ and CurrentCost

Active Warden Concept

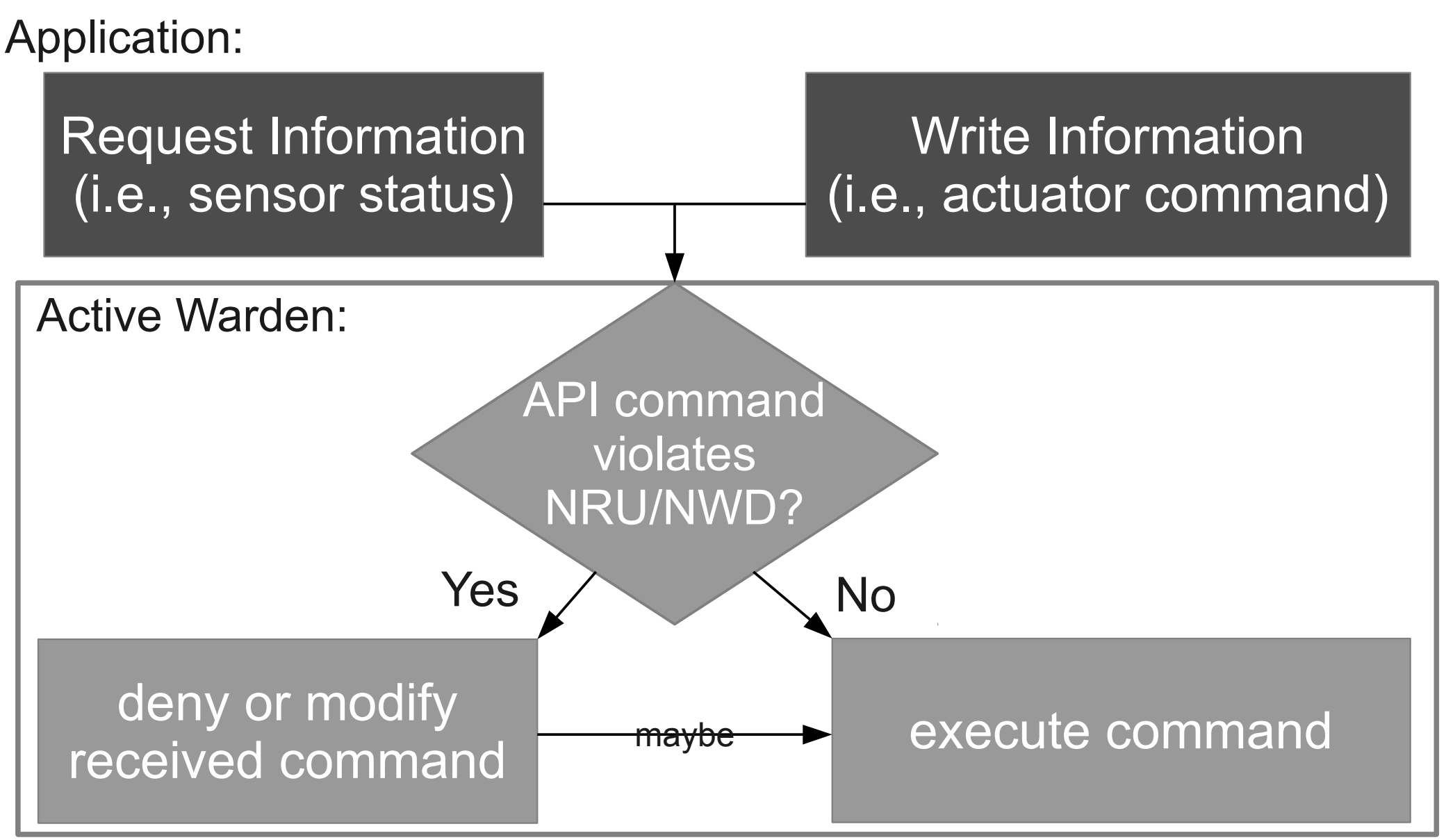
- employee should not have read access to BAS data of the manager's office
- member of papal conclave should not have write access to actuators in other rooms but the election room

Building-aware Active Warden

- Solution: **MLS** in a **building-aware** Act.Warden
  - Employee will get no read-up access to the manager office BAS devices
  - Member of papal conclave will be unable to control devices in the the covert channel receiver's room
- Our active warden must have a database containing all person's and device's security levels

Active Warden Concept

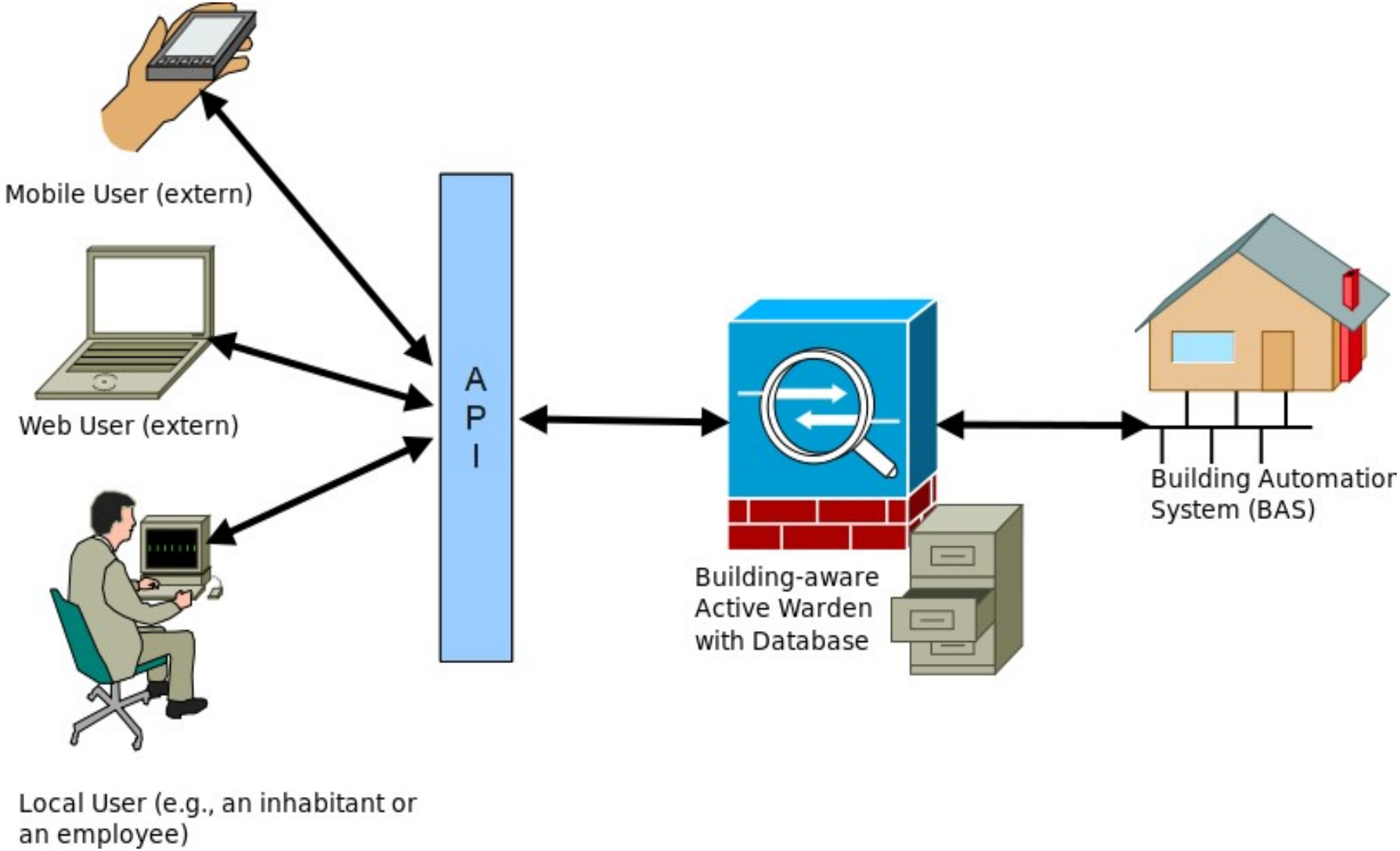
IT4SE



Active-Warden Concept

IT4SE

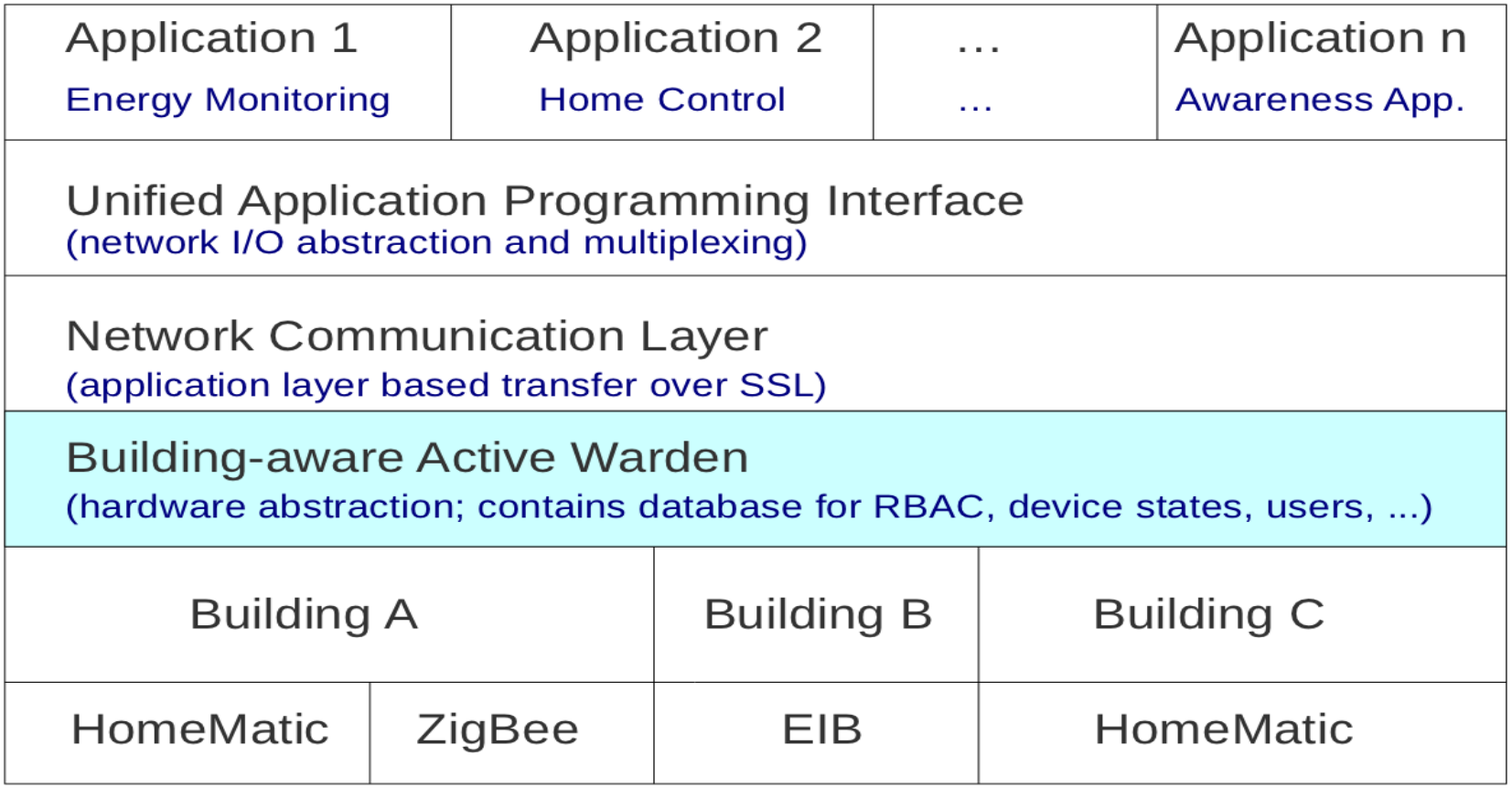
Location of the Building-aware Active Warden:



Active-Warden Concept

IT4SE

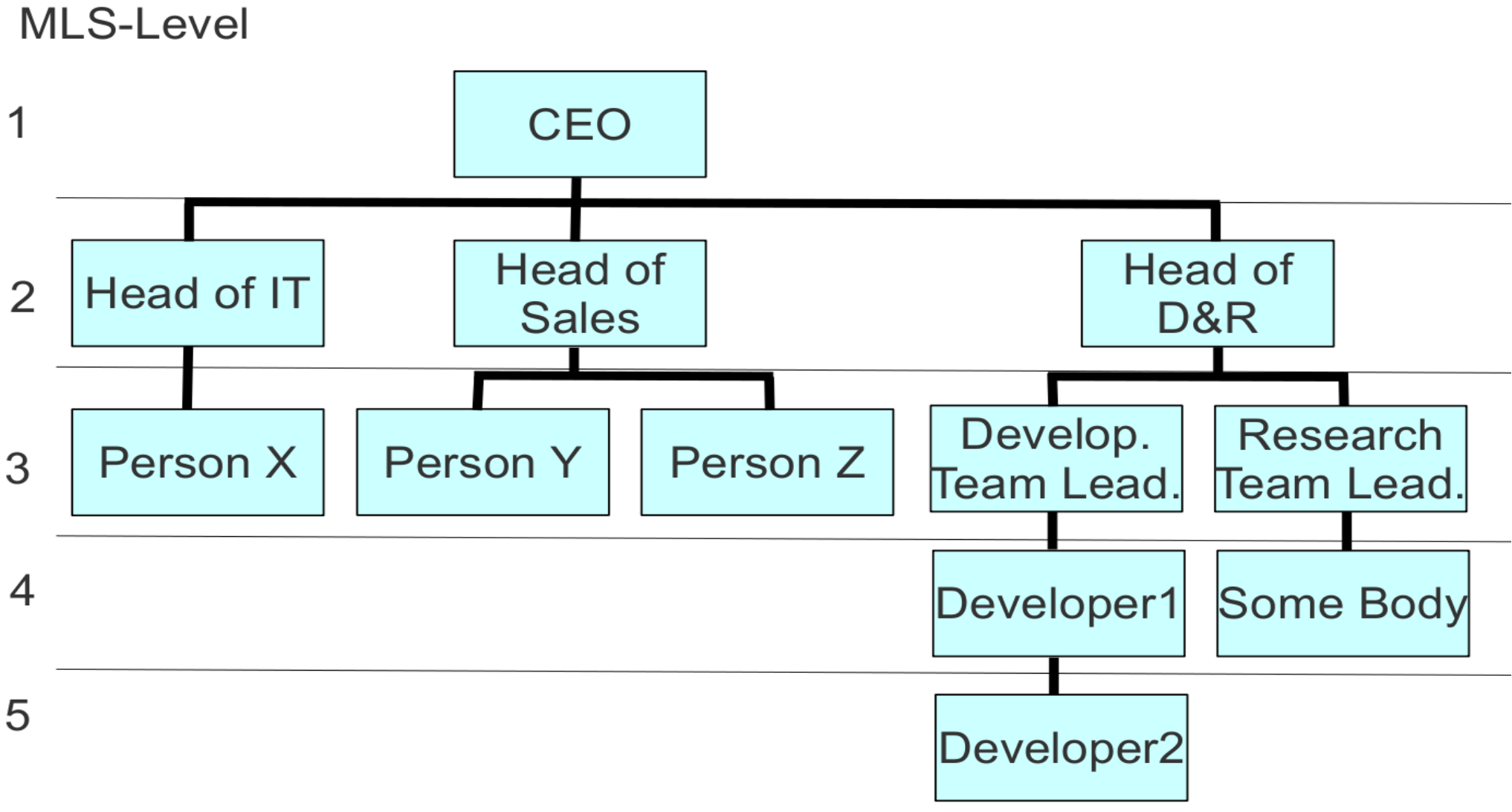
- Extend existing middleware with MLS
- RBAC was already implemented → we only added MLS levels and NRU/NWD rules



Active-Warden Concept

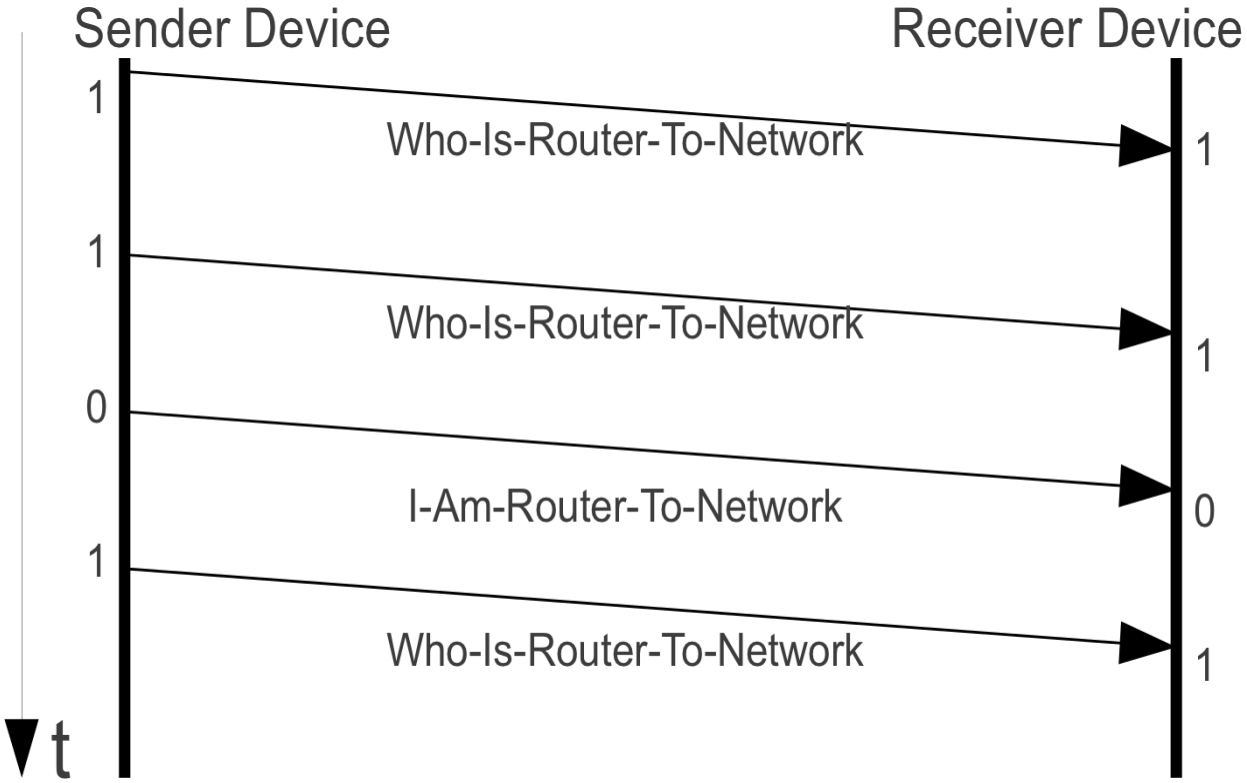
IT4SE

- MLS levels based on the organizational chart



Examples for Covert Channels in BACnet

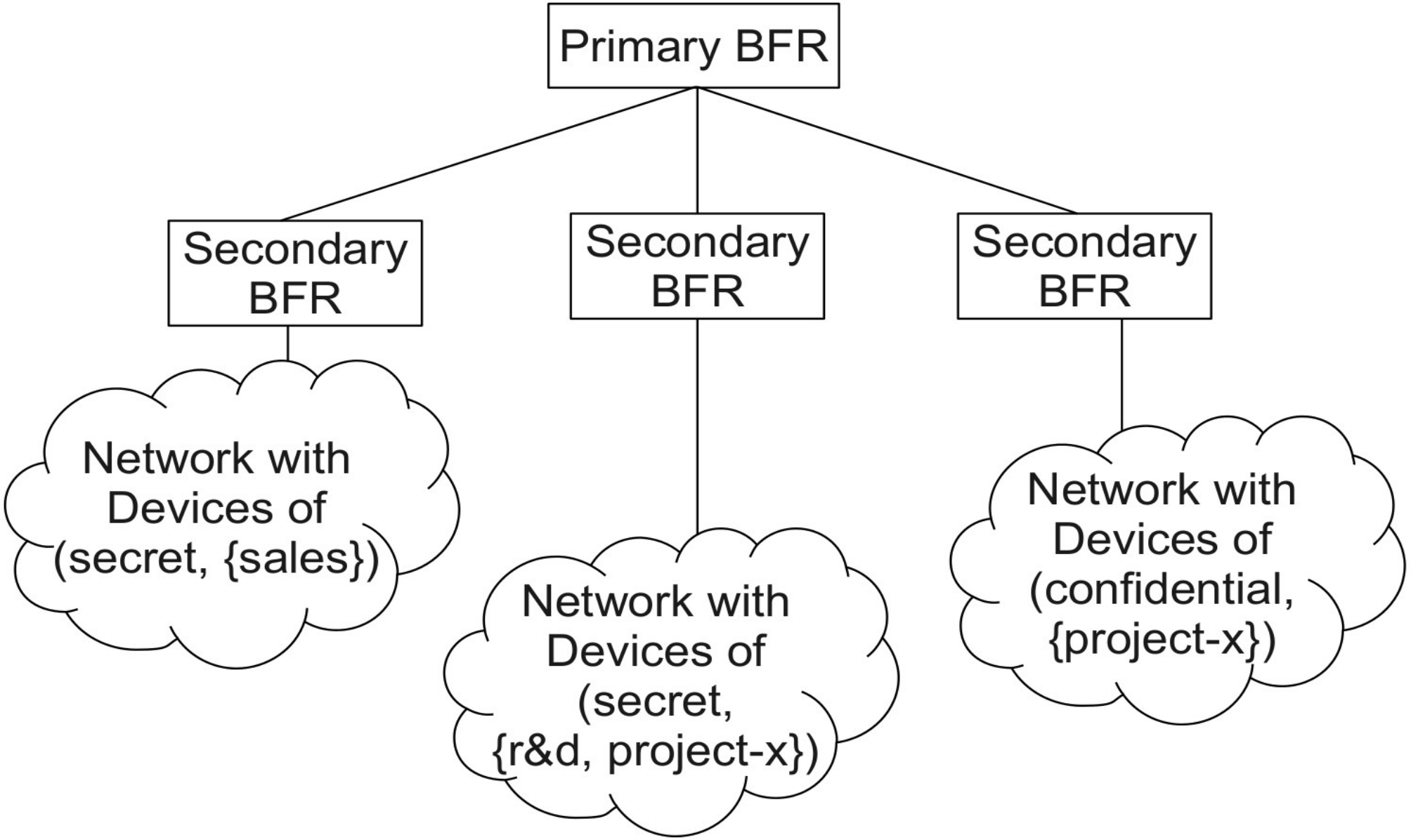
- Covert Storage Channel
  - Use n BACnet message types to transfer ld n bit/pkt
- Covert Timing Channel
  - Modify inter-arrival times of a selected message



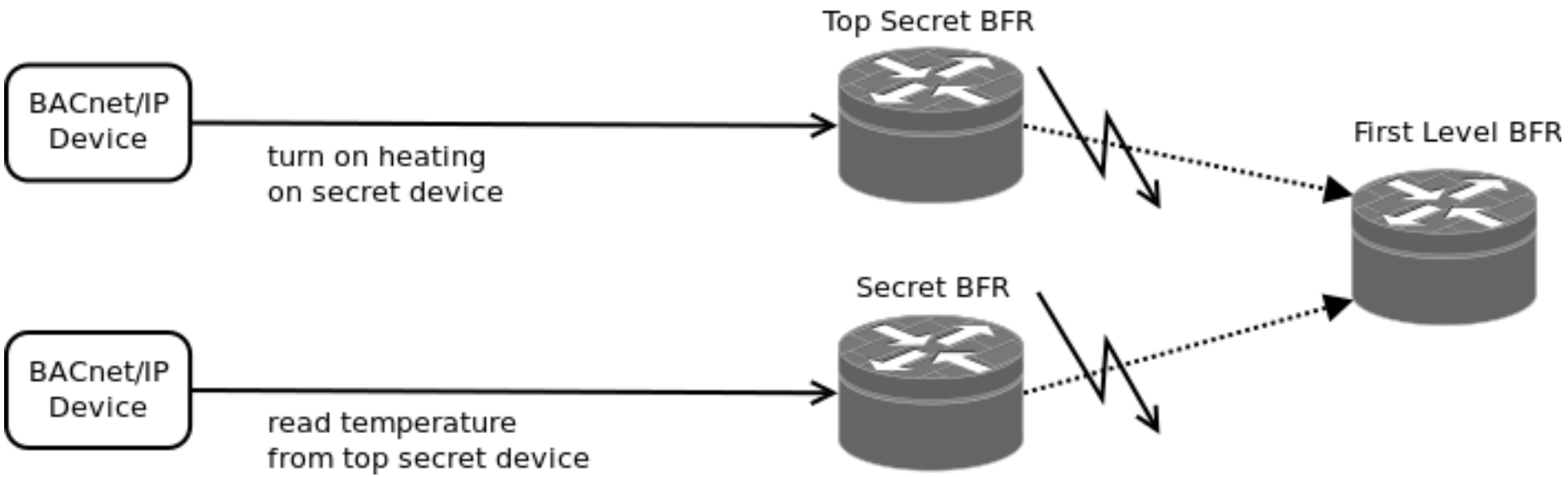
BACnet CC Prevention

- Idea: Introduce topological changes in the BACnet environment
  - Separate networks into different MLS areas, e.g. one network for (Top Secret, {management}).
  - Use the **BACnet Firewall Router** (BFR) to prevent traffic that violates the security policy
    - BBMD → Internet connectivity
    - NAT

MLS-BACnet Topology



MLS-BACnet Topology

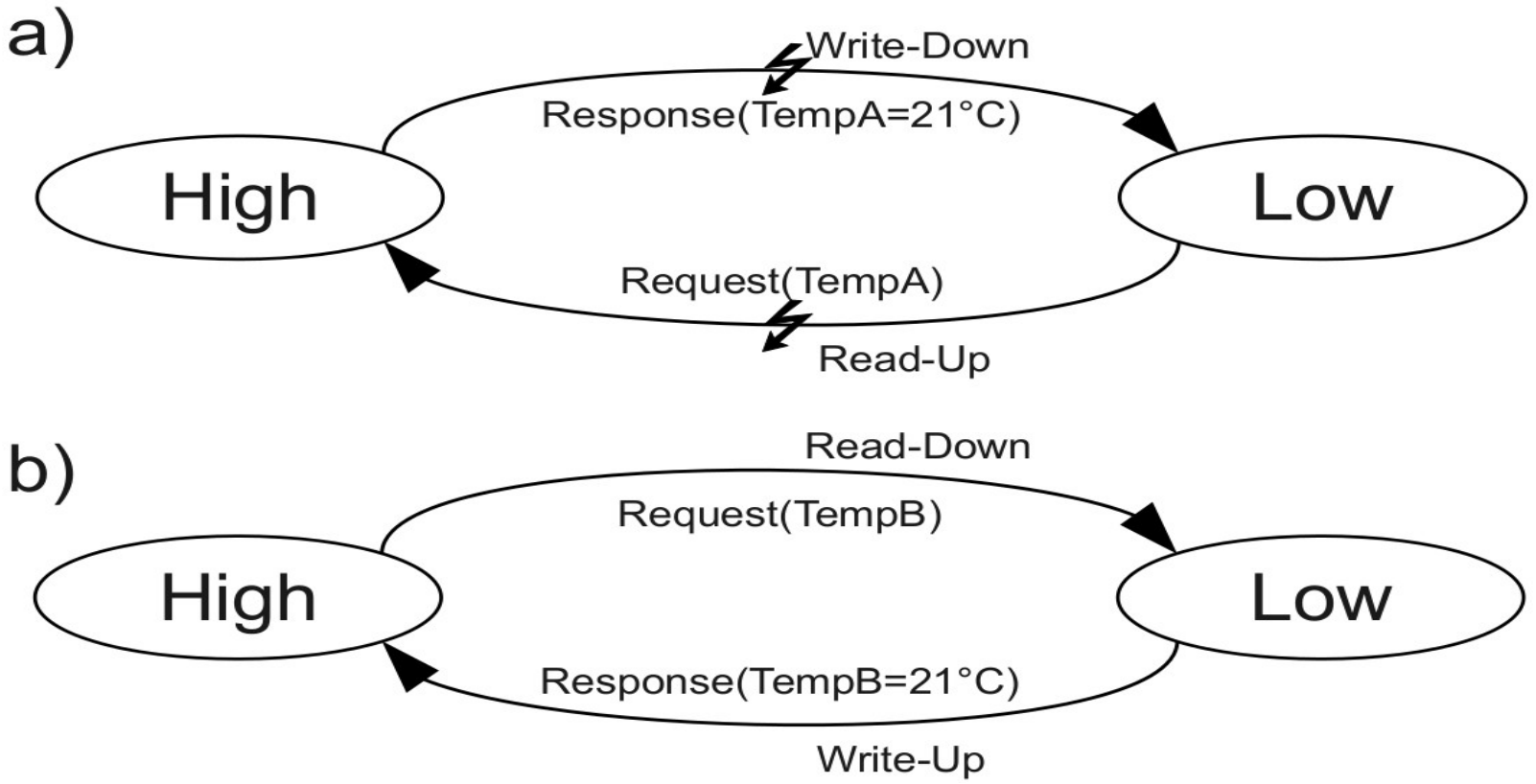


Results

- Configuration complex due to over-engineered BFR design
- BFR currently not able to filter all potential covert channel messages
- No new BFR releases since 2004
- Management level not taken into account (BFRs must be configured to allow bi-directional communication with the management layer)
- Primary level BFR is a single point of failure

Results

- Read-ups and Write-downs are easy to block for high-level covert channels (a) but hard to block for low-level covert channels (b):



Future Work

- Present/detect/limit/prevent low-level covert/side channels in other building automation protocols
  - e.g. in EIB/KNX or in LON
- Are protocol hopping covert channels (PHCC) useful in BAS?

Are there any Questions?

Image Source: Amazon

post-conference comments

- This research was supported by the IT4SE research cooperation (NZL 10/803 IT4SE) under the APRA initiative funded by the German Federal Ministry of Education and Research.
  - http://www.it4se.net

- Own related work for additional information:
  - Steffen Wendzel: Covert and Side Channels in Buildings and the Prototype of a Building-aware Active Warden, First IEEE International Workshop on Security and Forensics in Communication Systems (SFCS 2012), pp. 8339-8344, Ottawa, Canada, 2012.
  - Thomas Rist, Steffen Wendzel, Masood Masoodian, Elisabeth André: Next-Generation Home Automation Systems, In: Kempter G. & Weidmann K.H. (Hrsg.) Techniken fü Menschen im nächsten Jahrzehnt -- Beiträge zum Usability Day X, Pabst Science Publishers, pp. 80-87, 2012.
  - Steffen Wendzel, Thomas Rist, Elisabeth André, Masood Masoodian: A Secure Interoperable Architecture for Building-Automation Applications, in Proc. 4th Int. Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), pp. B:1-B:5, Barcelona, Spain, 2011.
  - Thomas Rist, Steffen Wendzel, Masood Masoodian, Paul Monigatti, Elisabeth André: Creating Awareness for Efficient Energy Use in Smart Homes, In Proc. Intelligent Wohnen. Zusammenfassung der Beiträge zum Usability Day IX, Dornbirn, Austria, Feuerstein Gerhild, Ritter Walter (Hrsg.), pp. 162-168, 2011.
  - More of our publications regarding network covert channels: http://www.wendzel.de/publications/