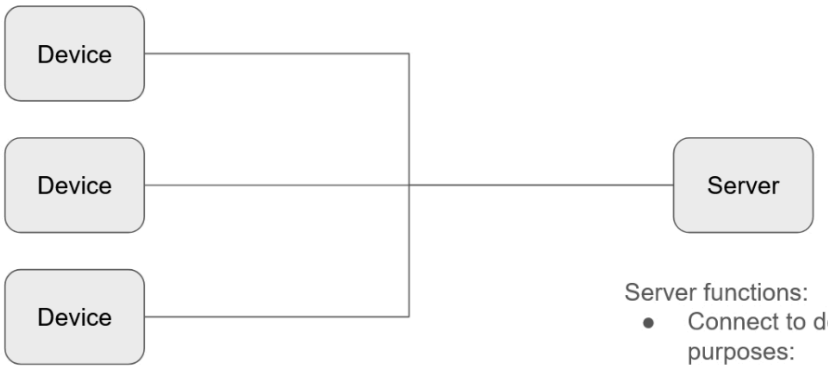

Server functions:

- Connect to device for data collection purposes:
  - Receive collected data
- Connect to device for admin purposes:
  - Change data collection configuration
  - Update device software
  - Disable device

Device functions:

- Collect data
- Listen to connection from server for data collection purposes:
  - Send collected data
- Listen to connection from server for admin purposes:
  - Change data collection configuration
  - Update device software
  - Disable device

Architecture of embedded devices and server

Possible assets in the architecture:

- Device firmware
- Server firmware
- Communication protocol

Stride analysis

Device firmware

STRIDE	THREAT	MITIGATION
Spoof	An attacker might try to impersonate a device to gain access to the network	Server should have a whitelist containing only the trusted devices so no fake ones can access the architecture
Tampering	Collected data could be modified	Implement secure boot on the devices so only trusted firmware can run + implement memory protection so no outside influence can modify device memory
Repudiation	No device authentication means an attacker can insert data on the network, and there is no way to know from which device it can	Data being collected and sent by devices should contain identifiers and timestamps to determine origine
Information Disclosure	Data saved locally on device could get extracted	Encrypt device flash memory + only make it accessible by secured code + store secrets separately and with restricted access
Denial of Service	Unauthorized command to disable device can stop data collection	Notify server of disabled devices and keep so restart can be handled by server + strong authentication and privilege requirements for critical commands
Escalation of Privilege	N/A	N/A

Server Firmware

STRIDE	THREAT	MITIGATION
Spoof	Imitate server so devices connect to malicious server instead of trusted server	Verification of server identity on devices so they can only connect to trusted server
Tampering	Modify update images for devices to contain malicious firmware	Used signed images and secure boot on devices
Repudiation	No logging on issued commands can make it hard to determine when or why devices configurations change or commands have been sent to device	Log incoming commands on devices and outgoing on the server + include timestamps and identifiers to determine their source
Information Disclosure	Unauthorized reading of data from server memory	(if possible) secure physical location of server to prevent physical access to hardware. + lock data with read protection so only trusted code can access and handle data
Denial of Service	Overload server by connection many devices and sending too much data	Validate devices on network and limit input rate
Escalation of Privilege	Stored data getting accessed by unauthorized code	Limit access to memory

Communication protocol

STRIDE	THREAT	MITIGATION
Spoof	N/A	N/A
Tampering	Man in the middle attack that changes data going over the network	Encrypt and authenticate communications with e.g. TLS
Repudiation	Messages over network get lost or maliciously deleted	Work with protocol that has acknowledgement system
Information Disclosure	Attacker listening in on network communication	Encrypt data over network
Denial of Service	Overloading network by spamming it with communication	Only allow input from a limited number of trusted sources
Escalation of Privilege	N/A	N/A