# “My Device, My Home”: Gaining Control in Smart Home Ecosystems

- ## Empirical Context

  In the fragmented landscape of the Smart Home, users strive to build Home Assistant by bypassing official limitations and unlocking additional features for control. This involves navigating “backroads” of local control, such as hacking Aqara Gateways for custom Zigbee access or forcing Xiaomi Miot into local Wi-Fi integration. Simultaneously, users construct digital “highways” to bridge closed clouds, exemplified by the unofficial Alexa Media Player API and Ring-MQTT integrations that force proprietary security cameras into open platforms.

- ## Problematization: The Battle for Control

  This thesis explores the inherent tension between manufacturer constraints and user community. This is a constant “cat and mouse” dynamic of firmware locks and community bypasses (e.g., unlocking Telnet ports). The research addresses a critical gap by moving beyond Open-source Software studies to investigate the specific phenomena of firmware hacking and hardware appropriation in consumer IoT.

- ## Task Description

  Your task is to analyse how online communities collaborate to “unlock” device potential and maintain these interoperability roads against vendors. Using Netnography, you will observe these interactions within their natural habitats, GitHub Issues, Home Assistant Forums, and Discord. You are tasked to sense their behaviour and draw out their community “pattern” as a process.

  Theoretically, the community effort to gain control can be seen as a form of value creation for their own benefits (and destruction in the eyes of manufacturers). On the opposite side, manufacturer constraints (value creation for them) can be seen as value destruction to users.

- Supervision
  - Supervisor: Univ.-Prof. Dr. Stefan Thalmann and Tong Li, Ph.D.