UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2025 Lukáš Drechsler

Univerzita Pardubice

Fakulta ekonomicko-správní

Zabezpečení domácnosti pomocí Smart home systému

Bakalářská práce

2025 Lukáš Drechsler

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lukáš Drechsler**
Osobní číslo:	**E22434**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Zabezpečení domácnosti pomocí Smart home systému**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je vytvořit funkční zabezpečovací systém domácnosti, který je nezávislý na konkrétním výrobci jednotlivých prvků.

Osnova:

- Popis současných Smart home systémů a jejich možností použití pro zabezpečení domácností.
- Popis objektu určeného k zabezpečení a analýza rizik.
- Návrh zabezpečení objektu.
- Konfigurace zabezpečení objektu.

Rozsah pracovní zprávy: **Cca 35 stran.**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: CERM, 2018. ISBN 978-80--7204-967-7.
CHOU, Timothy. *Precision: Principles, Practices and Solutions for the Internet of Things*. Lulu.com, 2016. ISBN 978-1-329-84356-1.
VALEŠ, Miroslav. *Inteligentní dům*. Vyd. 1. Brno: ERA group spol. s.r.o., 2006. ISBN 80-7366-062-8.

Vedoucí bakalářské práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2024**
Termín odevzdání bakalářské práce: **30. dubna 2025**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

prof. Ing. Jitka Komárková, Ph.D. v.r.
garant studijního programu

V Pardubicích dne 1. září 2024

Prohlašuji:

Práci s názvem Zabezpečení domácnosti pomocí Smart home systému jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 04. 2025

Lukáš Drechsler v.r.

ANOTACE

Bakalářská práce se zabývá návrhem a realizací systému zabezpečení bytu s využitím open-source platformy Home Assistant. Cílem práce je vytvořit cenově dostupné, modulární a na cloudu nezávislé řešení, které umožní efektivní ochranu domácnosti před neoprávněným vstupem, požárem či únikem vody. V práci jsou popsány jednotlivé typy senzorů a detektorů, použité komunikační protokoly i postup implementace celého systému do reálného prostředí. Výsledné řešení je porovnáno s komerčně dostupnými systémy a zhodnoceno z hlediska efektivity, rozšiřitelnosti a praktického využití.

KLÍČOVÁ SLOVA

chytrá domácnost, Home Assistant, zabezpečení, senzory, open-source, automatizace, IoT

TITLE

Home security using smart home systems

ANNOTATION

The bachelor thesis focuses on the design and implementation of an apartment security system using the open-source platform Home Assistant. The aim of the work is to create a cost-effective, modular, and cloud-independent solution that enables efficient protection of the household against unauthorized access, fire, or water leakage. The thesis describes various types of sensors and detectors, the communication protocols used, and the implementation process in a real environment. The resulting solution is compared with commercially available systems and evaluated in terms of efficiency, scalability, and practical usability.

KEYWORDS

smart home, Home Assistant, security, sensors, open-source, automation, IoT

Poděkování

Chtěl bych srdečně poděkovat panu doc. Miloslavu Hubovi, Ph.D., za jeho odborné vedení, podporu a cenné rady během celého procesu zpracování této bakalářské práce. Jeho trpělivost, ochota vždy pomoci a sdílet své znalosti byly pro mě nesmírně cenné.

Velké díky patří také mé rodině, která mě vždy podporovala, ať už morálně, nebo trpělivým snášením všech experimentů a testování zařízení, které jsem realizoval v rámci této práce. Bez jejich neustálé podpory a pochopení bych tuto práci nikdy nemohl dokončit.

A nakonec bych rád poděkoval všem, kteří mě v průběhu studia jakýmkoli způsobem podporovali, věnovali mi svůj čas a energii. Vaše pomoc a víra ve mě byly pro mě velkou motivací.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek a značek

API	Application Programming Interface
DALI	Digital Addressable Lighting Interface
DHCP	Dynamic Host Configuration Protocol
DMX	Digital Multiplex
DNS	Domain Name System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol
KNX	Konnex
MQTT	Message Queuing Telemetry Transport
NAT	Network Address Translation
PIR	Passive Infrared
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network

Úvod

S rostoucím rozvojem moderních technologií se stále více domácností obrací k inteligentním systémům, které zvyšují nejen komfort uživatelů, ale i jejich bezpečnost. Zatímco dříve bylo zabezpečení domácnosti doménou specializovaných firem, dnes je díky otevřeným softwarovým platformám a široké nabídce dostupných senzorů a zařízení možné realizovat takové řešení i svépomocí. Smart home systémy umožňují automatizaci různých procesů v domácnosti – od ovládání osvětlení, vytápění či multimédií až po pokročilé zabezpečení proti vloupání, požáru či úniku vody.

Cílem této bakalářské práce je navrhnout a implementovat systém pro zabezpečení bytu s využitím open-source platformy a běžně dostupných komponent. Důraz je kladen na cenovou dostupnost, otevřenost systému, modularitu a možnost provozovat jej bez závislosti na cloudových službách třetích stran. Součástí práce je také výběr vhodných senzorů a komunikačních protokolů, návrh řešení pro konkrétní bytovou jednotku, jeho realizace a vyhodnocení funkčnosti v reálném provozu.

Téma této práce reflektuje aktuální trend rostoucího zájmu o chytré domácnosti a přináší praktické řešení, které může být inspirací pro uživatele hledající flexibilní a bezpečný způsob ochrany svého majetku bez nutnosti investic do drahých komerčních systémů.

1. Smart home

Smart home je byt vybavený technologiemi, které jsou součástí počítačové sítě a komunikující i mezi sebou. Může být tvořen uzavřenými celky – samostatná čidla s přímo připojenými koncovými prvky – např. pohybové čidlo řídící osvětlení. Může však jít i o komplexní systémy, v nichž jednotlivé prvky komunikují mezi sebou a vyhodnocují celou řadu podnětů. Vyhodnocení může probíhat přímo koncovými prvky, anebo centrální jednotkou, která prvky řídí. [21]

1.1 Základní přehled Smart home systémů

1.1.1 Loxone

Centralizovaný systém rakouské společnosti Loxone Electronics GmbH umožňuje komplexní automatizaci domácnosti. Umožňuje integraci různých spotřebičů i bezpečnostních prvků v rámci jednoho systému. Na rozdíl od některých jiných platforem je zcela nezávislý na cloudových službách – veškeré řízení probíhá pouze lokálně prostřednictvím tzv. Miniserveru, který je centrální jednotkou celého systému. Centrální jednotka je ovládána prostřednictvím aplikace a multifunkčních tlačítek umístěných v domě. [9]

Systém využívá vlastní komunikační technologie Loxone Tree (pro kabelové zapojení) a Loxone Air (pro bezdrátové připojení). Dále je možné pomocí rozšiřujících modulů (extensions) připojovat zařízení využívající další technologie (např. DALI, DMX, KNX). Díky tomu umožňuje širokou integraci zařízení dalších výrobců. [10] Na rozdíl od spotřebitelsky orientovaných systémů není Loxone určen pro samostatnou instalaci – konfiguraci může provádět pouze vyškolený odborník. Běžní uživatelé tedy nemohou provádět změny v nastavení sami.

Z pohledu zabezpečení domácnosti tento systém nabízí celou škálu prvků od chytrých zámků po interkomy. Systém nedisponuje nativní podporou kamerových systémů, ale po vhodném síťovém nastavení je možné integrovat IP kamery. V tomto scénáři pak systém Loxone slouží pouze jako zobrazovací aplikace, ale záznam a zpracování obrazu musí probíhat v samostatném kamerovém systému.

1.1.2 Control4

Control4 představuje centralizovaný systém, který umožňuje integraci celé řady zařízení (např. osvětlení, vytápění, audia, kamer, žaluzií) do jednoho ovládacího panelu. Nevýhodou tohoto systému je jeho vysoká pořizovací cena. Control4 je svojí variabilitou vhodný nejen pro domácnosti, ale i pro komerční prostory.

Uživatelé mohou svůj Smart home ovládat prostřednictvím ovládacího panelu v podobě upravitelného dotykového displeje, mobilní aplikace nebo prostřednictvím integrace hlasových asistentů, jako jsou Google Asistent, Amazon Alexa apod. Mezi výhody systému patří podpora zařízení třetích stran, zejména díky podpoře rozšířených technologií pro IoT, jako jsou WiFi, ZigBee, Z-Wave, DALI a KNX.

Do jisté míry nevýhodou systému je, že konfiguraci může provádět pouze certifikovaný pracovník. Na druhou stranu toto opatření zajišťuje konzistenci a bezpečnost systému, které by mohly být neodborným zásahem ohroženy. Z oblasti zabezpečení systém umožňuje detekci otevření oken, únik plynu, vody, kouře, vloupání a dalších potenciálně nežádoucích událostí. Mezi užitečné funkce patří i simulace přítomnosti obyvatel v době jejich nepřítomnosti. Díky této funkci je možné snížit riziko vloupání během delší nepřítomnosti, například v době dovolené či hospitalizace. Vzdálený monitoring a správa domu, bytu či jiných prostor jsou zajištěny prostřednictvím cloudu a mobilní aplikace.

1.1.3 Tuya

Tuya je celosvětově rozšířeným cloudovým řešením, jehož velkou předností je, že umožňuje výrobcům chytrých zařízení snadnou integraci jejich produktů do platformy. V současné době využívají platformu Tuya vývojáři a firmy ve více než 200 zemích světa jako řešení pro integraci vlastních chytrých zařízení. Díky této široké rozšířenosti systém dokáže integrovat celou řadu zařízení – od běžných spotřebičů po chytré zámky a kamerové systémy. [20]

Platforma je zaměřena na tzv. plug and play řešení – tedy na taková zařízení, která lze snadno připojit a používat bez složitého nastavování. Proto naprostá většina kompatibilních produktů funguje bezdrátově, nejčastěji prostřednictvím WiFi. Tato zařízení jsou pak ovládána prostřednictvím cloudu, anebo v rámci lokální sítě pomocí mobilní aplikace. Vedle WiFi zařízení je možné do systému integrovat také produkty využívající Bluetooth nebo ZigBee. V těchto případech je nutné použít tzv. bridge – zařízení, které propojuje různé komunikační protokoly a zajišťuje připojení k internetu přes WiFi nebo Ethernet. I tato varianta však

vyžaduje přístup ke cloudové platformě. Tento systém umožňuje integraci s hlasovými asistenty a nabízí vzdálený přístup prostřednictvím cloudových služeb [20]. Z hlediska bezpečnosti však představuje určitou nevýhodu jeho závislost na cloudu – v případě výpadku této služby není možné systém na dálku ovládat ani monitorovat stav připojených zařízení. Přesto se jedná o jeden z nejrozšířenějších smart home systémů, a to především díky velmi nízkým pořizovacím nákladům a snadné konfiguraci, kterou zvládne i běžný uživatel pomocí mobilní aplikace dostupné pro Android a iOS.

1.1.4 openHAB

Otevřená platforma openHAB podporuje celou škálu zařízení od běžných spotřebičů a osvětlení až po chytré zámky a kamerové systémy. Celý systém je vyvinut v programovacím jazyce Java, což umožňuje její provozování na různých operačních systémech (Linux, Windows, macOS nebo jako kontejner v Dockeru). Hardwarově je platforma nenáročná, a tak je možné ji provozovat i na minipočítačích jako Raspberry Pi, pro které existuje i připravený image. [12]

Celý systém je možné rozšiřovat řadou doplňků, které lze instalovat prostřednictvím webového rozhraní, kde také probíhá i konfigurace. Díky doplňkům systém podporuje celou řadu protokolů, jako jsou DALI, ZigBee či KNX. Ovšem připojení těchto zařízení se neobejde bez přídavného hardwaru, např. ZigBee dongle, DALI master hat apod. [11]

OpenHAB je zcela nezávislý na cloudových službách, ale umožňuje propojení se systémy jako Google Home nebo Apple HomeKit [13]. K tomu, aby systém mohl být připojen k těmto cloudovým službám, je potřeba buď připojení pomocí bezplatného konektoru provozovaného společností openHAB Foundation e.V., nebo vystavení systému přímo do internetu. Pro přímé vystavení systému do internetu je potřeba pevná IP adresa poskytnutá poskytovatelem internetového připojení a správné nastavení firewallu routeru. Tento krok však zvyšuje riziko napadení systému.

1.1.5 Home Assistant

Home Assistant je jedním z projektů Open Home Foundation, jejímž cílem je ochrana soukromí uživatelů Smart home systémů. Díky široké komunitě a podpoře tisíců zařízení poskytuje bezpečné a flexibilní řešení pro řízení a automatizaci různých prvků chytré domácnosti včetně jejího zabezpečení. Home Assistant umožňuje integraci různých zařízení využívajících technologie, jako jsou ZigBee, Z-Wave, MQTT, WiFi a další.

Pro provoz aplikace není kladen vysoký nárok na hardware. Lze jej díky tomu spustit například jako Docker kontejner, instalovat jako balíček do systému Linux nebo využít samostatný operační systém Home Assistant OS, který je vhodný i pro minipočítače jako Raspberry Pi. [8].

Systém je nezávislý na cloudu, dokonce ho lze provozovat tak, že nebude mít přístup k internetu. Přístup do systému je možný pomocí webového rozhraní nebo pomocí mobilní aplikace. Je podporováno i dvoufázové ověřování, například pomocí Google Authenticator nebo Microsoft Authenticator. Při připojení do cloudu nebo v případě statické veřejné IP adresy je možné do systému přistupovat i vzdáleně a využívat funkce hlasových asistentů. Systém podporuje připojení vlastních aplikací a zařízení prostřednictvím otevřeného rozhraní (API) – například senzorů postavených na programovatelných modulech, jako je ESP32.

1.2 Technologie používané v chytrých zabezpečovacích systémech

1.2.1 Senzory

Senzory hrají klíčovou roli v zabezpečení domácnosti. Pro ochranu perimetru bytu jsou v současnosti používány detektory otevření dveří a oken a detektory tříštění skla K detekci pohybu osob uvnitř prostoru slouží nejčastěji PIR senzory (na principu infračerveného záření), mikrovlnné senzory (využívající odraz elektromagnetických vln), případně jejich kombinace v tzv. duálních senzorech. [4]

V oblasti požární bezpečnosti jsou využívány různé typy detektorů – kouře, plynu, teploty, plamenů a oxidu uhelnatého. Při výběru senzorů je potřeba zohlednit prostředí, v němž budou použity – např. zda je v domácnosti zaveden plyn, nachází se zde karma nebo plynový kotel. [3]

Proti riziku vytopení lze instalovat senzory úniku vody, které je možné umístit k pračkám, vodovodním hadičkám nebo dalším rizikovým místům. V kombinaci s elektromagnetickým uzávěrem přívodu vody může systém na případný únik automaticky zareagovat a zabránit tak větším škodám.

1.2.2 Komunikační protokoly

Komunikační protokoly určují způsob, jakým se jednotlivá zařízení připojují do systému chytré domácnosti. Lze je rozdělit na dvě velké skupiny – protokoly pro bezdrátové připojení a pro sběrnicové připojení. Pokud je byt teprve budován nebo prochází rekonstrukcí, nabízí

se možnost využití sběrnicového protokolu. V již hotových interiérech bývá praktičtější volit bezdrátové řešení, jelikož vyžaduje jen minimální zásah do stávající elektroinstalace.

Mezi běžně užívané protokoly pro bezdrátovou komunikaci patří:

- Zigbee

  Nízkopříkonový protokol pracující na frekvenci 2,4 GHz s podporou mesh sítě, kde zařízení mohou přeposílat signál a rozšiřovat tak pokrytí. Využívá se pro senzory a detektory, řízení osvětlení, chytré elektroměry, řízení vytápění a další.

- Z-Wave

  V rámci EU pracuje na frekvenci 868 MHz a díky nižšímu kmitočtu má lepší průchodnost signálu přes zdi. Stejně jako Zigbee využívá mesh síť, ale zařízení bývají dražší a nabídka omezenější kvůli licencování technologie.

- WiFi

  Umožňuje přímé připojení zařízení k routeru, čímž odpadá nutnost použití centrální brány. Hlavní nevýhodou je vyšší spotřeba energie, což omezuje použití bateriově napájených senzorů. WiFi se používá například u chytrých zásuvek, IP kamer nebo světel. Mezi nevýhody také patří, že zařízení se často připojují ke cloudu výrobce, takže mohou být potenciálně nebezpečná. Řešením bývá vytvoření samostatné VLAN (virtuální lokální sítě), která tato zařízení oddělí od zbytku domácí sítě a tím zvýší úroveň bezpečnosti.

- Bluetooth Low Energy (BLE)

  BLE je vhodný pro krátké vzdálenosti a aplikace s nízkou spotřebou energie. Uplatňuje se například u teplotních senzorů, chytrých zámků nebo zdravotnických přístrojů.

- MQTT

  Protokol pro výměnu zpráv mezi zařízeními, často využívaný u modulů s ESP32 a v projektech domácí automatizace typu „udělej si sám“ (DIY). Komunikace probíhá prostřednictvím tzv. MQTT brokera (např. Mosquitto), který zajišťuje přenos zpráv mezi zařízeními. Výhodou tohoto protokolu je nízká latence, tedy velmi rychlá reakce systému, a vysoká škálovatelnost, což přináší možnost snadno přidávat další zařízení bez ztráty výkonu.

Do kategorie sběrnicových protokolů řadíme:

- KNX

  Otevřený standard pro automatizaci budov, umožňuje řízení osvětlení, vytápění, ventilace, alarmů a dalších systémů. Funguje na sběrnicové architektuře, kde jednotlivá zařízení komunikují po společné lince, a s decentralizovaným řízením – zařízení pracují samostatně bez potřeby centrálního řídicího prvku. Pro propojení s dalšími systémy (například mobilní aplikací) je zapotřebí tzv. KNX IP brána, která umožní přenos dat do počítačové sítě. Výhodou je spolehlivost a rozšiřitelnost, nevýhodou vyšší pořizovací náklady a složitější instalace.

- DALI

  Standard pro digitální řízení osvětlení, který umožňuje například plynulé stmívání, nastavování světelných scén (např. pro různé denní doby) a získávání informací o stavu jednotlivých svítidel – například zda jsou zapnutá nebo jaký mají jas. Používá se v komerčních i rezidenčních budovách.

- DMX

  Komunikační protokol určený především pro řízení scénického a architektonického osvětlení. Umožňuje precizní ovládání světelných efektů – například RGB svítidel, LED pásků nebo reflektorů Pro propojení s dalšími systémy se běžně využívají speciální převodníky, tzv. brány (např. Art-Net), které převádějí DMX signál do počítačové sítě. Hlavní výhodou protokolu je rychlá a přesná komunikace s osvětlením, nevýhodou je však omezená možnost zpětné komunikace, kdy zařízení obvykle neposkytují informace o svém aktuálním stavu zpět do systému.

2. Současný stav zabezpečovaného bytu

Byt, který byl pro návrh zabezpečení vybrán, je typickou bytovou jednotkou v cihlovém domě, což dobře odpovídá prostředí, ve kterém jsou chytré technologie v oblasti zabezpečení běžně využívány. Výběr tohoto konkrétního bytu umožňuje reálné testování a praktickou implementaci vybraných bezpečnostních prvků, jako jsou detektory kouře, úniku plynu, pohybové detektory, detektory otevření dveří apod.

Byt představuje několik bezpečnostních rizik, například možnost úniku plynu nebo neoprávněný vstup přes balkon či dveřmi. Vzhledem k velmi omezeným možnostem instalace kabelových rozvodů je preferováno použití bezdrátových technologií. To odpovídá běžné praxi při dodatečném zabezpečování již existujících objektů.

Dalším důvodem pro použití bezdrátových technologií je možnost integrace se stávajícím Home Assistant. Tím lze efektivně rozšířit chytrou domácnost o bezpečnostní funkce bez nutnosti zásahu do elektroinstalace. Zvolený byt tak poskytuje vhodné podmínky pro ověření funkčnosti systému v reálném prostředí a zároveň slouží jako praktická demonstrace možností zabezpečení domácnosti pomocí běžně dostupných technologií.

2.1 Charakteristika zabezpečovaného bytu a jeho specifik

Byt, který je předmětem návrhu zabezpečení, se nachází v prvním patře cihlového domu v klidné části Prahy. Kromě jedné strany je kolem domu dvůr s vjezdem do garáží, díky čemuž se okna nacházejí ve výšce odpovídající druhému až třetímu nadzemnímu podlaží.

Jedná se o byt s dispozicí 3 + 1, s balkonem a o celkové rozloze 79 m^2. Vstup do bytu vede z uzamčené společné chodby, která je zabezpečena elektronickým vrátným s čipovým přístupem. Ve vstupním prostoru domu je umístěna maketa bezpečnostní kamery. Žádný další bezpečnostní systém, jako např. bezpečnostní kamery na chodbách, zde není instalován.

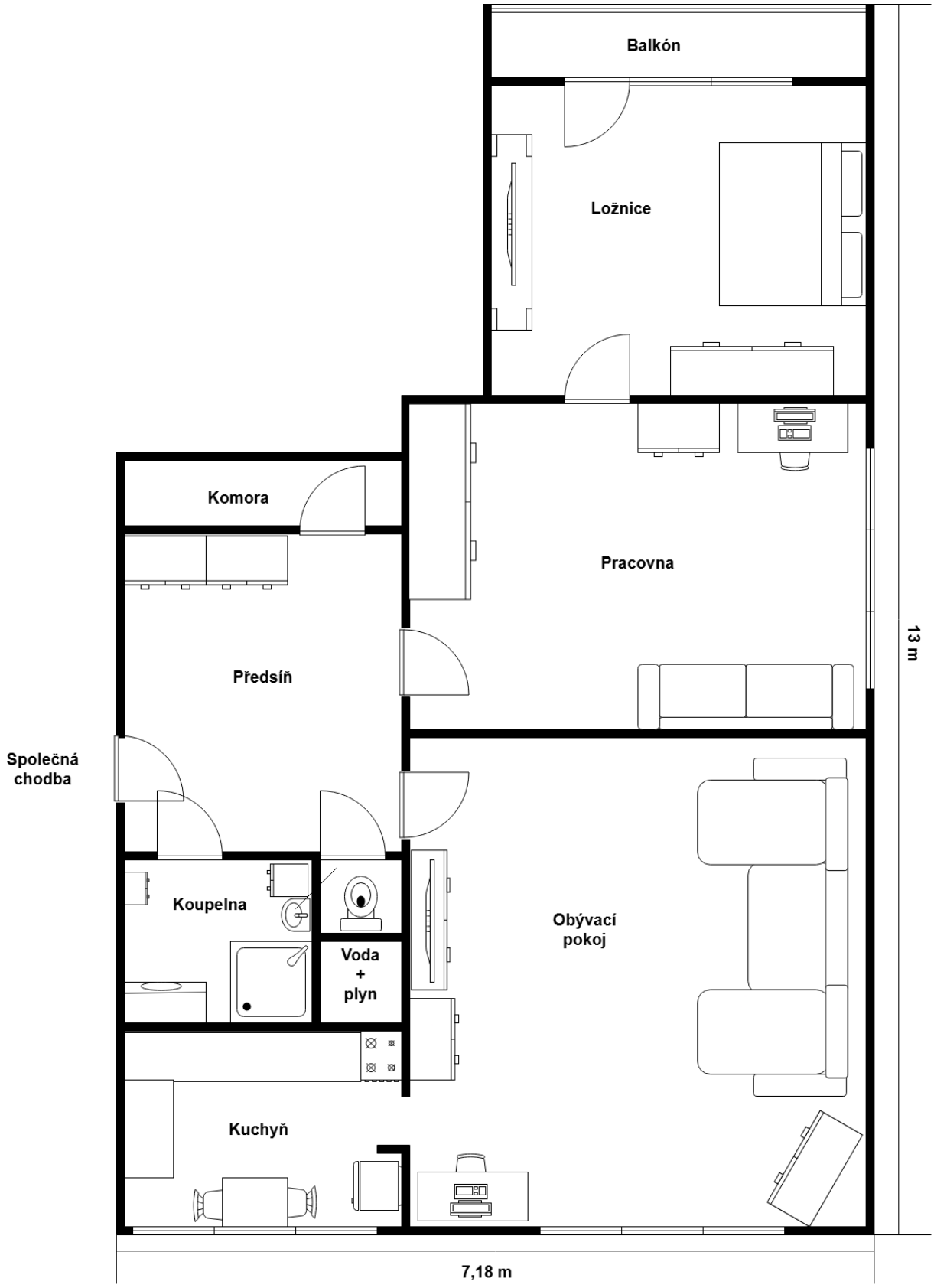
2.1.1 Přístupové body a kritická místa

Vstupní dveře jsou standardní bezpečnostní dveře s ocelovou výztuží a tříbodovým zámkem. Dveře nejsou vybaveny žádným čidlem detekujícím jejich otevření.

Byt má celkem čtyři okna, která jsou rozmístěna na třech různých stranách domu. Tři okna ze čtyř směřují nad vjezdy do garáží, díky čemuž jsou ve výšce osm metrů nad úrovní terénu. Za potenciálně rizikové lze považovat okna v ložnici, která vedou na nezasklený balkon

umístěný ve výšce přibližně 3 metry nad zemí. Balkon směřuje do ulice a je zapuštěný do konstrukce domu. Balkon je samostatně oddělený, pod ním se nacházejí pouze okna – v nižším podlaží domu balkony nejsou. Před domem se nachází husté křoví, v blízkosti balkonu se nachází okap a bleskosvod, které by teoreticky mohly usnadnit přístup do bytu.

Do bytu je přiveden plyn, který slouží pouze pro provoz plynového sporáku. Uzávěry vody a plynu se nachází v prostoru za toaletou. Obrázek 1 vyobrazuje orientační plánek zabezpečovaného bytu.



Obrázek 1: Orientační plánek zabezpečovaného bytu, Zdroj: vlastní

2.1.2 Specifika ovlivňující návrh zabezpečení

V bytě jsou staré hliníkové rozvody elektřiny, což znemožňuje instalaci sběrnicových systémů. Z tohoto důvodu je nutné zvolit bezdrátové řešení, které nevyžaduje zásah do stávající elektroinstalace.

Hlavní jistič bytu se nachází v rozvodné skříni ve společné chodbě, přičemž rozvodná skříň není nijak zajištěna. Ve stejné skříni je také umístěno kabelové vedení pro připojení k internetu, které je tím pádem rovněž přístupné zvenčí.

V domácnosti již je nainstalován systém chytré domácnosti Home Assistant, který je vybaven ZigBee donglem pro ovládání osvětlení v bytě. Navrhované bezpečnostní řešení musí být s touto stávající instalací plně kompatibilní, aby bylo možné zachovat jednotnou správu všech zařízení domácnosti v rámci jednoho systému.

2.2 Analýza rizik

Vzhledem k charakteru běžného bytového domu v Praze, který se nenachází v oblasti se zvýšeným rizikem kriminality ani výskytem živelních událostí, je v této práci zvolen zjednodušený přístup k analýze rizik, reflektující reálné podmínky daného prostředí. Důraz je kladen především na identifikaci klíčových aktiv z pohledu obyvatel bytu a na vyhodnocení rizik a rovněž na rizika, která tato aktiva či samotné obyvatele mohou bezprostředně ohrozit.

2.2.1 Identifikace aktiv

Pro identifikaci primárních aktiv byl proveden strukturovaný rozhovor s dospělými členy zabezpečované domácnosti. S cílem minimalizovat zátěž respondentů byla délka rozhovorů omezena na maximálně 10 minut. Na základě získaných odpovědí byla identifikována následující primární aktiva:

- bezpečnost obyvatel,
- dostupnost systému,
- fyzické vybavení domácnosti.

Mezi podpůrná aktiva bylo zařazeno následující:

- hardware (čidla, server, síťová infrastruktura),
- software (Home Assistant, Zigbee2MQTT),
- komunikační kanály (lokální síť, Zigbee),
- přístupové údaje (přihlašovací údaje, dvoufázové ověřování).

2.2.2 Identifikace hrozeb

Hrozby týkající se bezpečnosti obyvatel a vybavení domácnosti úzce souvisí s dostupností a spolehlivostí Smart home systému. Na základě identifikace aktiv a analýzy prostředí byly určeny následující klíčové hrozby:

- vloupání do bytu,
- vznik požáru v bytě,
- únik plynu z plynového sporáku nebo nebo z přívodního potrubí,
- únik vody,
- výpadek elektřiny,
- selhání senzorů,
- kybernetický útok,
- neoprávněný přístup do systému,
- zavlečení škodlivého softwaru (malware, ransomware).

2.2.3 Hodnocení rizik

Pro ohodnocení výskytu jednotlivých rizik byla použita následující stupnice:

- Vysoká pravděpodobnost – riziko je velmi pravděpodobné a může nastat opakovaně.
- Střední pravděpodobnost – riziko se může vyskytnout, ale není běžné.
- Nízká pravděpodobnost – riziko je nepravděpodobné nebo vzácné.

Dopad jednotlivých rizik byl stanoven subjektivně na stupnici:

- Vysoký dopad – pokud nastane, má závažné důsledky (např. ohrožení života, velká finanční ztráta, ztráta kontroly nad systémem).
- Střední dopad – důsledky jsou nepříjemné, ale ne fatální (např. dočasná nefunkčnost systému, potřeba zásahu uživatele).
- Nízký dopad – důsledky jsou minimální, snadno řešitelné.

Pro celkové hodnocení rizika byla sestavena následující matice rizik:

Tabulka 1: Matice rizik

Pravděpodobnost/Dopad	**Nízký**	**Střední**	**Vysoký**
Vysoká	Střední	Vysoké	Kritické
Střední	Nízké	Střední	Vysoké
Nízká	Nízké	Střední	Vysoké

Zdroj: vlastní

Na základě dat z Českého statistického úřadu a dat získaných strukturovaným rozhovorem s dospělými členy zabezpečované domácnosti byla sestavena hodnoticí tabulka:

Tabulka 2: Hodnocení rizik

Riziko	**Pravděpodobnost**	**Dopad**	**Celkové riziko**
Vloupání do bytu	Nízká	Vysoký	Střední
Vznik požáru v bytě	Nízká	Vysoký	Střední
Únik plynu	Nízká	Vysoký	Střední
Únik vody	Nízká	Vysoký	Střední
Výpadek elektřiny	Střední	Nízký	Nízké
Selhání senzorů	Střední	Vysoký	Vysoké
Útok na síť	Vysoká	Vysoký	Kritické
Neoprávněný přístup do systému	Vysoká	Vysoký	Kritické
Malware a ransomware	Střední	Vysoký	Vysoké

Upraveno podle [5], [6]

Legenda k tabulce hodnocení rizik:

- Kritické – vyžaduje okamžitá opatření, protože hrozba je reálná a má fatální dopady.
- Vysoké – je nutné zavést preventivní opatření, protože riziko je významné.
- Střední – riziko je třeba monitorovat a případně řešit.
- Nízké – riziko není zásadní, opatření nejsou prioritní.

2.2.4 Interpretace výsledku analýzy rizik

Výsledná analýza rizik identifikovala klíčové hrozby související se zabezpečením chytré domácnosti. Hodnocení kombinovalo pravděpodobnost výskytu jednotlivých rizik a jejich dopad, čímž bylo možné stanovit celkové riziko (viz tabulka 2).

Kritická rizika představují nejzávažnější hrozby, které mají vysokou pravděpodobnost výskytu a významný dopad na bezpečnost systému nebo celé zabezpečované domácnosti a jejích obyvatel. Mezi ně patří:

- Útok na síť – nedostatečné zabezpečení domácí sítě může vést k odposlechu dat včetně získání přihlašovacích údajů k systému Home Assistant. Riziko je obzvlášť akutní, jelikož systém aktuálně nemá aktivní šifrované připojení pomocí HTTPS.
- Neoprávněný přístup do systému – slabé přihlašovací mechanismy umožňují útočníkům snadno získat kontrolu nad celým systémem.

Rizika s vysokým dopadem, ale malou pravděpodobností výskytu mohou mít závažné důsledky. Na základě tabulky Hodnocení rizik se jedná o:

- Vloupání do bytu – přestože pravděpodobnost vloupání je nízká, dopad je extrémně vysoký, protože může vést nejen k materiálním škodám, ale i k újmě obyvatel.
- Požár bytu – při požáru bytu je dopad ještě vyšší než u vloupání, zde kromě materiálních škod může dojít i k újmě na životech a zdraví obyvatelů, a to nejen monitorovaného bytu, ale i bytů okolních.
- Únik plynu – při úniku plynu se zvyšuje riziko vzniku požáru nebo výbuchu, což má opět vysoký dopad. Při časné detekci se dá vzniku škod zabránit.
- Únik vody – při úniku vody hrozí pouze materiální škody, ale včasnou detekcí je lze minimalizovat.

Rizika s vysokým dopadem, ale s menší závažností nepředstavují přímou újmu na majetku nebo zdraví obyvatel zabezpečovaného bytu. Pokud k nim však dojde, mohou nepřímo přispět k tomu, že se naplní (realizují) jiná, závažnější rizika. Jedná se o následující rizika:

- Selhání senzorů – pokud dojde k poruše senzoru nebo např. vybití jeho baterie, systém ztrácí schopnost detekovat hrozby a nedokáže jim účinně předcházet nebo minimalizovat jejich dopad.
- Malware a ransomware – infekce škodlivým softwarem je sice málo pravděpodobná, ale v jejím důsledku může dojít k úplné ztrátě kontroly nad bytem.

Rizika s nízkým dopadem sice mohou negativně ovlivnit chování systému a bezpečí obyvatel, ale dopad je pouze dočasný a jeho odstranění je snadné nebo se provede automaticky po skončení realizace rizika:

- Výpadek elektřiny – během výpadku elektřiny mohou být funkce Smart home systému nedostupné, ale po jejím opětovném připojení se všechny funkce automaticky vrací do normálu.

2.3 Nedostatky stávajícího řešení

Současné řešení chytré domácnosti v analyzovaném bytě využívá Home Assistant jako centrální řídicí systém pro ovládání osvětlení (jsou instalovány chytré žárovky), přičemž další prvky domácnosti, například detektor plynu a WiFi zásuvky, nejsou do systému integrovány. Systém sice umožňuje základní úroveň automatizace, ale obsahuje několik zásadních nedostatků v oblasti bezpečnosti a funkcionality, které mohou negativně ovlivnit, jak schopnost chránit domácnost, tak spolehlivost a uživatelský komfort celého řešení.

2.3.1 Omezení stávajícího řešení

Aktuálně je Home Assistant dostupný pouze prostřednictvím nezabezpečeného protokolu HTTP. To vytváří potenciální riziko, že přihlašovací údaje do systému budou zachyceny útočníkem, který by následně mohl získat kontrolu nad systémem. Navíc Home Assistant není chráněn dvoufázovým ověřováním, což znamená, že při případném úniku hesla nebo jeho prolomení by útočník získal kontrolu nad systémem chytré domácnosti. Systém je aktuálně dostupný pouze z lokální sítě, takže z něj není možné zasílat notifikace a vzdáleně kontrolovat stav domácnosti.

Do systému nejsou integrovány žádné detektory, což znemožňuje provádět bezpečnostní automatizace – například vypnutí zásuvek při detekci úniku plynu, vody nebo kouře a zaslat o tom notifikaci. Rovněž chybí jakákoli kontrola pohybu osob po bytě a kontrola vniknutí do objektu.

2.3.2 Výzvy zabezpečení

Z pohledu softwarového řešení je potřeba v systému nastavit šifrované připojení pomocí HTTPS, zavést dvoufázové ověřování, umožnit vzdálený přístup do systému. Ten následně umožní zasílání notifikací na zařízení mimo lokální síť.

V oblasti hardwaru je nutné doplnit systém o senzory a další prvky umožňující efektivní řízení bezpečnosti v objektu s podporou systému Home Assistant a pořízení UPS pro zajištění chodu systému při výpadku elektřiny.

3. Návrh řešení zabezpečení bytu

3.1 Požadavky na systém

Požadavky na systém vycházejí z analýzy rizik, která identifikovala potenciální hrozby, jejich pravděpodobnost a dopad na bezpečnost domácnosti. Na základě těchto zjištění byl stanoven soubor opatření, která minimalizují pravděpodobnost vzniku těchto rizik nebo jejich následky.

Dále jsou požadavky ovlivněny konkrétními potřebami a preferencemi obyvatel bytu. Každá domácnost má odlišné nároky na zabezpečení – například některé osoby preferují vysokou úroveň automatizace a vzdálenou správu, zatímco jiné dávají přednost jednoduchým systémům s minimálními zásahy do každodenního života. Obyvatelé mohou také klást důraz na uživatelskou přívětivost systému, například na snadné ovládání přes mobilní aplikaci nebo hlasové příkazy.

Třetím faktorem ovlivňujícím návrh jsou specifika samotného bytu, jako je jeho dispozice, typ konstrukce a dostupná infrastruktura. Například rozmístění senzorů a kamer je ovlivněno počtem vstupních bodů, velikostí místností a možnými slepými místy v pokrytí. Důležitým aspektem je také dostupnost a stabilita připojení k internetu a napájení, protože některé části zabezpečovacího systému mohou vyžadovat redundantní řešení (např. záložní bateriové napájení).

Výsledkem je soubor požadavků, který zajistí optimální úroveň zabezpečení při zachování uživatelského komfortu a technické proveditelnosti v rámci konkrétního prostředí.

3.1.1 Funkční požadavky

Na základě rozhovorů s dospělými obyvateli zabezpečovaného bytu byly definovány klíčové funkční požadavky, které reflektují jejich reálné potřeby a očekávání od Smart home systému:

- vzdálený přístup do systému a vzdálená kontrola domácnosti,
- detekce neoprávněného vstupu do bytu,
- zasílání notifikací v případě nečekaných událostí,
- automatické reakce systému,
- monitorování stavu domácnosti (sledování teploty, vlhkosti, detekce kouře, plynu, vody v okolí potrubí),
- řízení uživatelských práv.

3.1.2 Technické požadavky

Na základě funkčních požadavků a požadavků obyvatel bytu byly stanoveny následující technické požadavky:

- lokální server bez závislosti na cloudu,
- podpora bezdrátových protokolů (WiFi, Zigbee),
- zajištění dostatečného pokrytí signálem po celém bytě,
- redundance kritických komponent,
- zavedení šifrované komunikace (HTTPS),
- dvoufázová autentizace.

3.2 Výběr technologií

Při výběru technologií bylo nutné zohlednit specifika zabezpečované domácnosti, která významně ovlivňují možnosti instalace a provoz Smart home systému. Jedním z hlavních omezení je nemožnost využití kabelových rozvodů, což vylučuje použití tradičních bezpečnostních systémů, jako jsou alarmy využívající drátové sběrnice a pevně zapojené senzory. Z toho důvodu bylo nutné zvolit bezdrátová řešení, která umožňují libovolné umístění senzorů bez stavebních úprav.

Dalším zásadním faktorem jsou silné zdi a stavební materiály, které mohou výrazně tlumit signál bezdrátových technologií, zejména u technologií využívajících vyšší frekvenční pásma, jako např. Bluetooth. Z tohoto důvodu byl výběr technologií omezen pouze na WiFi a Zigbee, jelikož v bytě již existuje kvalitní pokrytí WiFi signálem zajištěné dvěma vysílači WiFi signálu pracujícími v režimu mesh. Tyto jednotky si mezi sebou předávají připojená zařízení tak, aby při jejich přesunu nedocházelo k výpadkům připojení. Zigbee technologie rovněž využívá síťovou topologii typu mesh, kdy všechna zařízení připojená k napájení (např. Zigbee žárovky, zásuvky, spínače) fungují jako opakovače signálu. Díky tomu vzniká spolehlivá síť pokrývající celý byt. [7]

3.2.1 Zigbee vs WiFi v zabezpečovacím systému

Obě technologie mají své výhody i nevýhody pro využití v zabezpečovacím systému. Mezi přednosti WiFi patří možnost přímého připojení zařízení k síti bez nutnosti použití speciálních bridge nebo adaptérů (tedy mezičlánků zajišťujících komunikaci mezi protokoly) a také její vysoká rozšířenost. Díky tomu je nabídka modulů pro WiFi velmi široká a jejich integrace

do systému bývá technicky nenáročná. Nevýhodou však je závislost na funkčnosti lokální sítě a kvalitě pokrytí zabezpečovaného bytu WiFi signálem. V případě poruchy routeru nebo jiného síťového prvku senzory a aktory (např. chytré zásuvky nebo spínače) ztrácí schopnost komunikovat s centrální jednotkou. Mezi další nevýhody WiFi systémů patří vyšší energetická náročnost oproti Zigbee, což u bateriových zařízení znamená kratší výdrž baterie a nutnost její častější výměny. Navíc velká část výrobců využívá své cloudové prostředí, ke kterému se WiFi moduly automaticky připojují. Tím pádem komunikace neprobíhá výhradně v rámci lokální sítě a může být závislá na dostupnosti internetu – což je z pohledu dostupnosti důležitý faktor.

Pro zvýšení zabezpečení komunikace WiFi modulů a Home Assistanta je vhodné vytvořit samostatnou síť WiFi, která bude oddělena v rámci samostatné VLAN. Toto řešení pomáhá omezit možný přístup k citlivým částem domácí sítě například při napadení některého z chytrých zařízení. Implementace VLAN však vyžaduje pokročilejší znalosti nastavení a správy síťových prvků a zároveň zvyšuje nároky na vybavení – je nutné použít síťová zařízení, která tuto funkcionalitu podporují. V popisované domácnosti je toto opatření již zavedeno.

Hlavní výhodou Zigbee oproti WiFi je nižší energetická náročnost, díky které mohou senzory a další bateriově napájené prvky dosahovat výrazně delší výdrže baterie. Tento faktor je zásadní zejména u prvků, které musí být v provozu neustále. Další výhodou Zigbee je schopnost vytvářet mesh síť pomocí prvků připojených k elektrickému napájení, takže není nutná instalace opakovačů signálu nebo dalších přístupových bodů jako u WiFi. Na rozdíl od WiFi se mesh síť v rámci Zigbee vytváří automaticky a nevyžaduje žádnou speciální konfiguraci. Stačí aktivovat párovací režim na Zigbee zařízení i na řídicí jednotce (tzv. Zigbee bridge nebo adaptér) a nové zařízení je následně do sítě připojeno bez dalších zásahů. Po případném výpadku napájení se síť automaticky znovu obnoví, aniž by bylo potřeba provádět manuální nastavení. Pokud je v síti dostatečné množství prvků s podporou mesh, vzniká více redundantních tras, takže i při výpadku jednoho zařízení zůstává celá síť plně funkční.

Nevýhodou Zigbee oproti WiFi je nutnost použití bridge nebo adaptéru. Tento prvek představuje potenciální bod selhání, protože v případě jeho výpadku ztratí Home Assistant schopnost komunikovat se všemi Zigbee moduly v síti. Zigbee zařízení také mají nižší datovou propustnost než WiFi, což znamená, že nejsou vhodná pro přenos objemnějších dat –

například živého video přenosu z kamer. Naopak jsou optimalizovaná pro rychlý a spolehlivý přenos malých datových paketů, což je ideální právě pro senzory, spínače, chytré zásuvky a další prvky domácí automatizace, které odesílají jednoduché a časté signály.

V rámci zabezpečení bytu je vhodnější využít Zigbee pro kritické senzory a bezpečnostní prvky, protože je nezávislé na lokální datové síti, má nižší energetickou náročnost a vytváří mesh síť s možností redundantních tras. WiFi je vhodné pro zařízení s vyššími nároky na přenos dat, jako jsou kamery. Kombinace obou technologií umožňuje vytvoření robustního a spolehlivého zabezpečovacího systému.

3.2.2 Výběr senzorů a dalšího hardwaru

Pro výběr potřebného hardwaru byly zvoleny e-shopy alza.cz a www.chytrevypinace.cz, a to na základě jejich široké nabídky IoT modulů a jejich mnohaletých zkušeností s těmito moduly. E-shop www.chytrevypinace.cz byl preferován zejména díky podrobným popisům produktů, které zahrnují i míru kompatibility s platformou Home Assistant, což usnadňuje výběr vhodných komponent pro daný systém.

Jelikož na většině míst v zabezpečované domácnosti není možné využít síťové napájení, byla možnost napájení pomocí baterií zásadním kritériem pro výběr senzorů. Dalším významným kritériem byla pořizovací cena senzorů a typ využívané baterie. Netypické baterie by mohly zvýšit náklady na provoz, což je nežádoucí. Preferovanými typy baterií byly standardně dostupné formáty jako AA, AAA nebo CR2032, zatímco bylo cílem vyhnout se typům jako CR123A, které jsou nákladnější a hůře dostupné v běžném maloobchodním prodeji.

Zigbee senzor otevření dveří/oken

Pro detekci neoprávněného vniknutí do bytu byl vybrán ZigBee magnetický senzor otevření dveří s bateriovým napájením. V okolí dveří není k dispozici zdroj napájení, proto bylo nutné využít bateriové řešení. Senzor je plně kompatibilní se systémem Home Assistant. Do systému zasílá informace o změně stavu, tedy otevření nebo zavření dveří. [17]

Vzhledem k bateriovému napájení senzor neplní funkci tzv. routeru v Zigbee síti, ale funguje pouze jako tzv. endpoint – tedy koncové zařízení, které je k síti připojeno, ale dále ji nerozšiřuje.

Zigbee detektor kouře

Pro detekci případného požáru byl zvolen Zigbee detektor kouře pracující na principu měření rozptylu světla způsobeného přítomností kouře ve vzduchu. Senzor obsahuje sirénu o hlasitosti 85 dB, takže i v případě selhání systému Home Assistant nebo Zigbee koordinátoru je schopný signalizovat nebezpečí. [16] Senzor pomocí Zigbee zasílá pouze informaci o tom, zda kouř detekuje, či nikoliv, pomocí binární proměnné, míru koncentrace kouře v ovzduší nelze ze senzoru získat.

Napájení senzoru je zajištěno 3V baterií, takže ho nelze použít pro rozšíření Zigbee mesh sítě.

Zigbee senzor methanu

Jelikož se v bytě nachází plynový sporák s přivedeným zemním plynem – methanem –, byl vybrán Zigbee senzor methanu pro detekci jeho případného úniku. Senzor disponuje vestavěnou sirénou o hlasitosti 65 dB a stavovou diodou, díky čemuž dokáže upozornit na nebezpečí i bez připojení k Zigbee síti – například při výpadku centrální jednotky. Senzor je napájen z elektrické sítě, tudíž v Zigbee mesh síti funguje jako router a dokáže tak rozšiřovat její rozsah. [15]

Do systému Home Assistant senzor zasílá pouze binární informaci o přítomnosti plynu, konkrétní koncentraci methanu nelze z jeho výstupu zjistit.

Zigbee senzor vytopení

Pro ochranu domácnosti před únikem vody byl zvolen bateriový Zigbee senzor vytopení, který se skládá ze dvou částí – základny, která obsahuje řídicí elektroniku, a samotné detekční části, která je připojena kabelem a může být umístěna i do hůře přístupných míst. Přestože

je senzor vybaven integrovaným bzučákem, jeho zvukový výstup je velmi slabý. Upozornění na únik vody je proto v praxi plně závislé na bezchybné komunikaci v rámci Zigbee sítě a systému Home Assistant. [18]

Zigbee spínač

Jako další prvek hardwaru byl zvolen Zigbee spínač. Jedná se o zařízení plnící funkce klasického spínače pro osvětlení, jeho ovládání je možné buď fyzicky pomocí tlačítek, nebo prostřednictvím Zigbee sítě. Jelikož je permanentně připojený k síťovému napájení, plní funkci routeru v rámci Zigbee sítě a tím zvyšuje její stabilitu a dosah. V zabezpečovaném bytě jsou staré elektrické rozvody ze 70. let, které neobsahují samostatně přivedený nulový vodič do instalační krabice. Z tohoto důvodu bylo nutné zvolit speciální typ spínače, který dokáže fungovat bez připojení nulového vodiče, a je tak vhodný i pro starší typy elektroinstalace. [14]

Zigbee siréna

Pro akustickou a optickou signalizaci byla zvolena Zigbee siréna o hlasitosti 90 dB. Siréna je vybavena redundantním napájením – primární napájení je zajištěno pomocí USB kabelu, jako záložní napájení slouží baterie. [19]

Server s nainstalovaným systémem Home Assistant je zálohován pomocí UPS (nepřerušitelného napájecího zdroje), takže i v případě výpadku elektrické energie zůstává po určitou dobu v provozu a je tak možné spustit signalizaci prostřednictvím této sirény, a to i bez dostupné lokální sítě. Nevýhodou tohoto řešení je, že v případě poruchy Zigbee adaptéru systém ztrácí schopnost spouštět akustická varování přes tuto sirénu.

WiFi zásuvka

V zabezpečovaném bytě se u zásuvek nenachází standardní elektroinstalační krabice, a proto není možné využít vestavěné zásuvky s připojením k WiFi nebo Zigbee. Z tohoto důvodu byla zvolena alternativa v podobě modulu, „který lze připojit přímo do klasické zásuvky [2]. Byl zvolen model od společnosti Sonoff, protože zařízení Sonoff je možné ovládat pomocí API v rámci lokální sítě – není tedy nutné, aby zásuvky měly po prvotním nastavení přístup k internetu. Ovládání přes API je již plně integrováno do systému Home Assistant, což umožňuje bezproblémové začlenění zásuvek do domácí automatizace.

Po dohodě s obyvateli zabezpečované domácnosti bylo rozhodnuto, že zásuvky budou instalovány pouze v místech, kde jsou trvale připojené spotřebiče – například televize,

mobilní klimatizace nebo server s Home Assistant. Díky tomu v případě, kdy systém Home Assistant přestane reagovat, bude možné jej na dálku restartovat – buď prostřednictvím připojení přes tzv. cloudové rozhraní, nebo pomocí zabezpečeného vzdáleného přístupu (VPN) do domácí sítě. Restart lze provést jednoduše přes mobilní aplikaci eWeLink, která slouží k ovládání chytrých zařízení.

Zigbee detektor přítomnosti

Pro detekci pohybu byl vybrán Zigbee PIR senzor, který rozpoznává změny teploty způsobené pohybem osob (tzv. pasivní infračervená detekce). Zařízení je napájeno 3V baterií, a proto funguje v síti Zigbee pouze jako koncový prvek. Senzor odesílá do systému Home Assistant oznámení o detekci pohybu nebo klidu, která byla využívána pro aktivaci alarmu. Detektor lze zároveň využít i pro automatizaci osvětlení – například pro automatické rozsvícení světel při pohybu v místnosti.

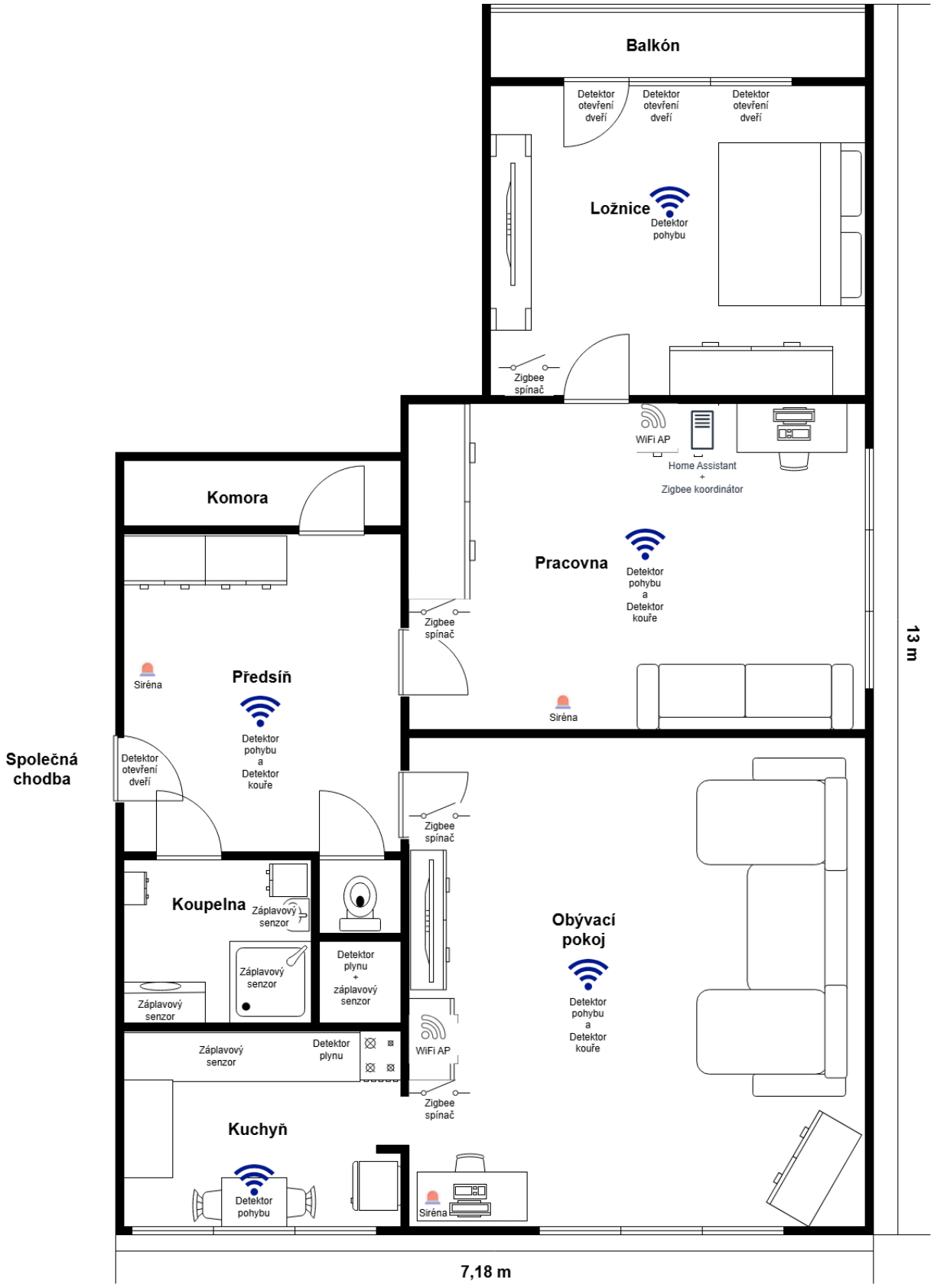
Předpokládaná výdrž senzoru je 254 dní. Zorný úhel detekce pohybu činí 120° a dosah je uváděn 10 metrů, což je vzhledem k velikosti místností v zabezpečovaném bytě dostačující. [1]

3.3 Návrh systému

Návrh systému byl vytvořen s ohledem na konkrétní dispozice zabezpečovaného bytu, technologická omezení i požadavky na jeho zabezpečení. Při návrhu bylo nutné zohlednit absenci kabelových rozvodů pro napájení senzorů. Dále bylo přihlédnuto k charakteristice stavby, kde silné stěny mohou snížit dosah signálu bezdrátových prvků.

3.3.1 Schéma zapojení a rozmístění zařízení

Ve schématu (viz obrázek 2) bylo zakresleno rozmístění senzorů, Zigbee spínačů, WiFi přístupových bodů a sirén. Pro zachování přehlednosti schématu nebyly zakresleny WiFi zásuvky, jejichž umístění není pro přenosové pokrytí zásadní. Rozmístění senzorů bylo stanoveno na základě specifik objektu a jeho rizikových míst. Umístění WiFi přístupových bodů bylo stanoveno podle měření síly signálu tak, aby celý byt byl pokrytý WiFi signálem. Zigbee spínače byly instalovány nejen podle dispozičního uspořádání bytu, ale zároveň plní důležitou síťovou funkci – tím, že jsou trvale napájené, slouží jako opakovače signálu v rámci Zigbee mesh sítě a tvoří jakousi páteř pro pokrytí celého bytu Zigbee signálem.



Obrázek 2: Schéma zabezpečovaného bytu doplněné o instalované prvky zabezpečení, Zdroj: vlastní

3.3.2 Definování automatizací a scénářů chování

Režim nepřítomnost

Všichni obyvatelé mají ve svých mobilních telefonech nainstalovanou aplikaci Home Assistant, která umožňuje sledování polohy zařízení. Pokud se žádné z nich nenachází v zóně „Domov“ (tedy v bytě nebo jeho bezprostředním okolí, s ohledem na případné nepřesnosti GPS) a současně není po dobu alespoň tří minut detekován žádný pohyb, dojde k automatické aktivaci režimu nepřítomnosti. Tento režim lze aktivovat či deaktivovat také manuálně – zadáním číselného kódu v aplikaci, nebo prostřednictvím tabletu umístěného na chodbě bytu.

Po aktivaci tohoto režimu dojde ke spuštění sirén v případě detekce otevření dveří, oken nebo pohybu uvnitř bytu. Spuštění sirén je odloženo o jednu minutu, aby byl obyvatelům ponechán čas na případné manuální vypnutí režimu prostřednictvím tabletu umístěného na chodbě.

Noční režim

Každý den po 23. hodině dojde k automatické aktivaci dveřního senzoru, přičemž jeho deaktivace je možná pouze zadáním číselného kódu. Noční režim se aktivuje pouze v případě, že není současně aktivní režim nepřítomnosti, aby nedošlo ke snížení úrovně zabezpečení.

Režim simulace přítomnosti

Tento režim slouží k simulaci běžného chodu domácnosti v době nepřítomnosti jejích obyvatel – např. během dovolené. Režim může být aktivován pouze manuálně. Režim automaticky napodobuje obvyklé chování členů domácnosti – během dne například zapíná televizi, po setmění rozsvěcí světla a po 22. hodině je opět zhasíná a televizi vypíná. Tím vytváří dojem, že je byt obýván, což může odradit případné neoprávněné vniknutí. Simulace probíhá až do deaktivace režimu po návratu obyvatel.

Detekce nebezpečí

Při detekci úniku plynu nebo kouře dojde k okamžitému spuštění sirén a zaslání notifikací prostřednictvím aplikace Home Assistant všem obyvatelům. Pokud nedojde k reakci do pěti minut, systém opakovaně odesílá notifikace každou další minutu, dokud není situace vyřešena.

4. Realizace řešení

4.1 Instalace systému

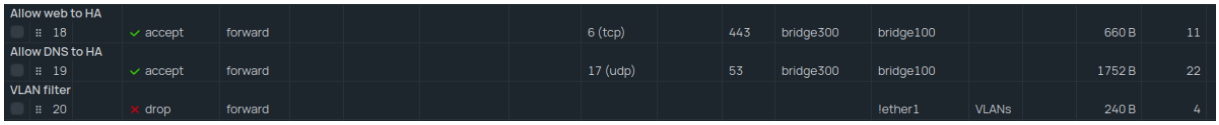
Před začátkem realizace celého řešení bylo zapotřebí vyřešit bezpečnost současného systému a umožnit k němu vzdálený přístup. Pro zvýšení bezpečnosti bylo rozhodnuto převést instalaci systému Home Assistant do tzv. Docker verze – řešení, které umožňuje provoz systému v kontejneru, tedy odděleném prostředí s vlastním nastavením. Výhodou Dockeru je, že klíčová nastavení a data se ukládají trvale na disk, zatímco zbytek systému běží v dočasném prostředí, které lze kdykoli snadno přeinstalovat pomocí tzv. statického image – předem připraveného obrazu systému se všemi potřebnými komponenty a nastaveními.

Protože se na serveru nacházelo pouze minimum automatizací, byl vytvořen jen stručný seznam scénářů, které bude potřeba po nové instalaci znovu nastavit. Jednalo se převážně o jednoduché scénáře, jako jsou ovládání několika světel v závislosti na denní době a spínání klimatizace na základě údajů z teplotního senzoru.

Nová instalace byla provedena na operačním systému Ubuntu Server 24 LTS. Vzhledem k tomu, že systém běží na minipočítači Raspberry Pi 4, byl pro zápis systému na disk využit nástroj BalenaEtcher, sloužící k jednoduchému nahrání systémového obrazu. Kvůli omezené životnosti paměťových karet byl místo SD karty použit 128GB SSD disk připojený přes USB 3.0 – SATA adaptér. Po dokončení instalace byl na serveru nastaven firewall pomocí balíčku *iptables-persistent,* který umožňuje trvalé uložení firewallových pravidel. Pro monitorování provozu serveru byl nainstalován SNMP démon – služba, která poskytuje informace o stavu zařízení (např. vytížení CPU, RAM, připojení). Tyto údaje byly následně integrovány do nástroje The Dude, což je přehledová aplikace pro sledování zařízení v síti, provozovaná v prostředí routerů MikroTik.

Systém byl zařazen do samostatné VLAN, která má povolený přístup pouze do VLAN vyhrazené pro zařízení typu IoT. Přístup do této VLAN, kde se nachází server, je možný pouze ze dvou dalších VLAN – administrátorské a uživatelské. Z uživatelské VLAN je přístup omezen pouze na webové rozhraní systému a DNS servery, čímž se snižuje riziko napadaní systému škodlivým softwarem z uživatelských zařízení. Naproti tomu administrátorská VLAN má plný přístup bez omezení. Všechna tato přístupová pravidla byla nakonfigurována na routeru MikroTik. Na obrázku 3 jsou znázorněna konkrétní filtrovací pravidla – *bridge100* reprezentuje síťový most, ke kterému je připojen server, zatímco

bridge300 slouží pro WiFi síť běžných uživatelů. Veškerý ostatní provoz, který neodpovídá definovaným pravidlům, je automaticky zablokován. Administrátorská VLAN není zahrnuta do seznamu rozhraní, jejichž provoz je filtrován, a má proto plný přístup. Stejná pravidla byla aplikována i na IPv6 firewall, čímž je zajištěna konzistence nastavení.



Obrázek 3: MikroTik Firewall, Zdroj: vlastní

Po instalaci základních balíčků pro správu serveru, jako jsou *htop*, *mc* a *net-tools*, byl do systému nainstalován Docker spolu s nástrojem Docker Compose. Před samotnou instalací Dockeru bylo nejprve nutné instalovat GPG klíče pro ověření důvěryhodnosti zdrojů a poté doplnit adresu oficiálního instalačního balíčku do systému pro správu softwaru (APT), konkrétně do souboru */etc/apt/sources.list.d/docker.list*. Teprve po tomto kroku mohla být instalace Dockeru a souvisejících nástrojů úspěšně dokončena.

Po dokončení instalace byla vytvořena uživatelská skupina *docker*, do které byl přidán uživatel *ubuntu*, jenž byl vytvořen při instalaci operačního systému. Tím bylo zajištěno, že Docker kontejnery neběží pod účtem *root*. Nakonec bylo nutné pomocí *systemctl* povolit automatické spouštění služeb *docker.service* a *containerd.service*, aby byl Docker (a tím i Home Assistant a další související kontejnery) automaticky spuštěn po každém restartu zařízení.

Aby mohl systém Home Assistant komunikovat se Zigbee zařízeními, bylo nejprve nutné nainstalovat tzv. broker, který slouží jako prostředník mezi těmito zařízeními a samotným systémem Home Assistant. Tento broker byl rovněž nasazen ve formě Docker kontejneru.

Instalace jednotlivých Docker kontejnerů probíhala postupně. Jako první byl nasazen kontejner s aplikací Nginx Proxy Manager, která v tomto případě slouží jako reverzní proxy server – tedy služba, která zajišťuje bezpečnou komunikaci přes protokol HTTPS a zároveň přidává vrstvu základního zabezpečení celého systému. Tato aplikace je postavena na webovém serveru Nginx, jenž je běžně konfigurován prostřednictvím textových konfiguračních souborů. Výhodou Nginx Proxy Manageru je však to, že poskytuje uživatelsky přívětivé webové rozhraní, které umožňuje snadnou správu konfigurací bez nutnosti ruční editace souborů.

Výhodou tohoto nástroje je také integrovaná databáze známých bezpečnostních zranitelností (tzv. exploitů), čímž do určité míry plní i funkci Web Application Firewallu – tedy vrstvy, která chrání webové aplikace před známými typy útoků. Součástí aplikace je navíc sada šablon pro vystavování SSL certifikátů prostřednictvím služby Let's Encrypt, V rámci této instalace byla navíc využita i možnost automatizace vystavování certifikátů pomocí API služby Cloudflare, což umožňuje využití striktního ověřování certifikátů mezi serverem a proxy servery Cloudflare.

Pro potřeby tohoto kontejneru byla vytvořena složka */home/ubuntu/nginx*, která obsahuje podadresáře *data* a *letsencrypt*, určené pro ukládání konfiguračních a certifikačních dat. V rámci této složky byl rovněž vytvořen konfigurační soubor *docker-compose.yml*, jehož struktura je zobrazena na obrázku 4.

```yaml
version: "3"
services:
  app:
    image: 'jc21/nginx-proxy-manager:latest'
    restart: unless-stopped
    network_mode: host
    volumes:
      - ./data:/data
      - ./letsencrypt:/etc/letsencrypt
```

Obrázek 4: Nginx docker-compose.yml, Zdroj: vlastní

Tato konfigurace umožňuje kontejneru přímé využití síťového rozhraní hostitelského systému. Zároveň dochází k mapování složek z hostitelského systému do kontejneru – konkrétně složka *data* je připojena do cesty */data* a složka *letsencrypt* do */etc/letsencrypt* uvnitř kontejneru. Kontejner byl následně spuštěn v adresáři */home/ubuntu/nginx* pomocí příkazu *docker-compose up -d*, přičemž parametr *-d* (*detached mode*) zajistí, že kontejner poběží na pozadí.

Pro instalaci systému Home Assistant byla vytvořena složka */home/ubuntu/homeassistant*, která je v rámci kontejneru připojena jako adresář */config*. Díky tomuto nastavení je veškerá konfigurace uložena mimo samotný kontejner, což značně usnadňuje její zálohování a obnovení. V případě neúspěšné aktualizace systému Home Assistant stačí smazat kontejner, vytvořit jej znovu a systém automaticky načte stávající konfigurační soubory – tím se obnoví jeho plná funkčnost. Home Assistant je spouštěn pomocí následujícího příkazu:

```
docker run -d --name homeassistant \
--privileged \
  --restart=unless-stopped \
  -e TZ=Europe/Prague \
  -v /home/ubuntu/homeassitant:/config \
  --network=host \
  ghcr.io/home-assistant/home-assistant:stable
```

Tento příkaz spouští kontejner v tzv. privilegovaném režimu, což znamená, že má rozšířený přístup i k hostitelskému operačnímu systému. Takové nastavení například umožňuje, aby bylo možné v daném prostředí spouštět další Docker kontejnery uvnitř již běžícího kontejneru. Přestože se tento režim doporučuje používat co nejméně kvůli bezpečnostním rizikům, v případě Home Assistantu je jeho použití nezbytné.

Příkaz dále specifikuje přímý přístup k síťovému rozhraní hostitelského systému, nastavuje automatické restartování kontejneru v případě selhání, spouští ho na pozadí a zároveň mu přiřazuje název *homeassistant*. Pomocí přepínače *-e* (environment) je kontejneru předána informace o časové zóně, kterou má Home Assistant používat.

Po dokončení úvodního nastavení (tzv. onboardingu) na IP adrese serveru a portu *8123* byl v adresáři */home/ubuntu/homeassistant* automaticky vytvořen hlavní konfigurační soubor *configuration.yaml*. Tento soubor byl následně upraven tak, aby umožňoval provoz systému za reverzní proxy (server zprostředkovávající zabezpečený přístup zvenčí, byl využit již nainstalovaný Nginx Proxy Manager) a pro základní funkce panelu zabezpečení (alarmu). Tento konfigurační soubor je uveden v příloze A – Konfigurace Home Assistant.

Dalším nainstalovaným kontejnerem byla aplikace Zigbee2MQTT, která zprostředkovává komunikaci mezi Zigbee zařízeními a Home Assistantem. Pro její provoz byl vytvořen

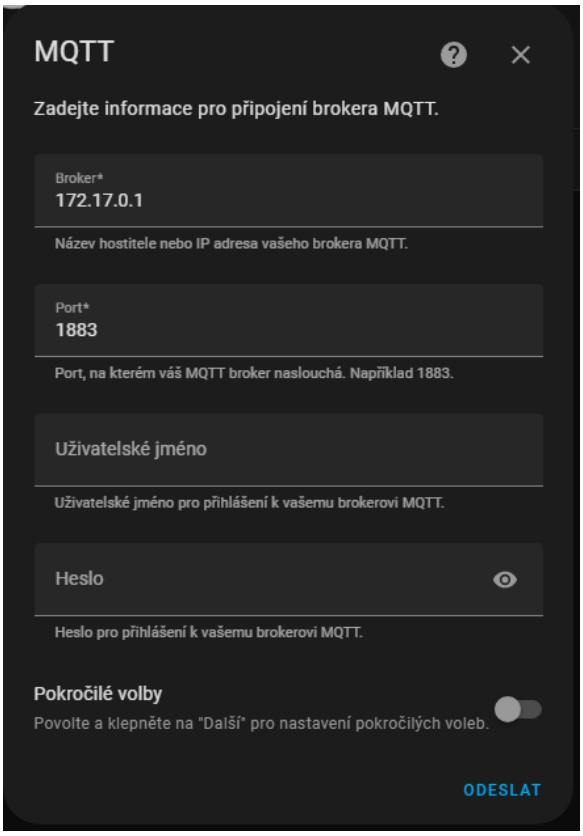
samostatný adresář */home/ubuntu/zigbee2mqtt*, kam se ukládají veškerá nastavení. Konfigurační soubory této aplikace jsou automaticky vygenerovány při jejím prvním spuštění:

```
docker run -d \
  --device=/dev/ttyACM0 \
  --network=host \
  --name=zigbee2mqtt \
  -v /home/ubuntu/zigbee2mqtt/:/app/data \
  -v /run/udev:/run/udev:ro \
  -e TZ=Europe/Prague \
  koenkk/zigbee2mqtt
```

Tento spouštěcí příkaz zároveň zpřístupňuje kontejneru fyzické zařízení připojené přes USB – konkrétně Zigbee dongle, který zajišťuje komunikaci se Zigbee zařízeními. K tomu slouží parametr *--device=/dev/ttyACM0*, jenž definuje komunikační rozhraní pro připojený dongle. Další parametr *-v /run/udev:/run/udev:ro* připojuje do kontejneru adresář */run/udev* díky němuž má kontejner přístup k informacím o USB zařízeních, která jsou právě připojená k systému. Tato složka je připojena v režimu pouze pro čtení (read-only), což stačí k tomu, aby aplikace zařízení rozpoznala. Přepínač *-d* zajišťuje, že kontejner poběží na pozadí.

Po spuštění kontejneru bylo v uživatelském rozhraní Zigbee2MQTT, dostupném prostřednictvím webového prohlížeče na portu *8080*, nutné povolit integraci s Home Assistantem. Následně bylo možné přistoupit k párování jednotlivých Zigbee zařízení, přičemž postup závisel na konkrétním výrobci každého modulu.

V systému Home Assistant pak stačilo v sekci „Integrace“ přidat *MQTT* a zadat IP adresu a port instance Zigbee2MQTT. Na obrázku 5 je znázorněn vyplněný formulář pro tuto integraci.



Obrázek 5: Připojení Zigbee2MQTT, Zdroj: vlastní

Po uložení formuláře se v prostředí Home Assistant zobrazila všechna připojená zařízení, která byla úspěšně spárována přes Zigbee2MQTT.

Vzhledem k tomu, že jeden z obyvatel zabezpečované domácnosti používá pro svou doménu nameservery společnosti Cloudflare, bylo této infrastruktury využito i pro zpřístupnění systému Home Assistant z internetu. Pro zajištění jednoduchého přístupu byla vytvořena subdoména *home.domena.ltd*, která je v prostředí Cloudflare nastavena jako proxy s režimem plného a striktního ověřování SSL certifikátů. Toto nastavení vyžaduje, aby se server vůči proxy serveru Cloudflare identifikoval certifikátem vydaným důvěryhodnou certifikační autoritou.

Aby bylo možné SSL certifikáty generovat a obnovovat automaticky, tedy bez nutnosti jejich ručního vytváření a nahrávání na server, bylo využito API služby kompatibilní s Let's Encrypt a nástrojem Nginx Proxy Manager. Po vložení příslušného API klíče do rozhraní Nginx Proxy Manageru dochází k automatickému vystavení, ověření a nasazení certifikátu pro subdoménu systému Home Assistant.

V nástroji Nginx Proxy Manager byl následně vytvořen nový záznam typu host, který přesměrovává provoz směřující na doménu *home.domena.ltd* na port *8123*, kde je dostupné uživatelské rozhraní systému Home Assistant. Zároveň je provoz kontrolován proti databázi známých webových exploitů. Do sekce Custom configuration byl přidán seznam IP adres proxy serverů Cloudflare, aby bylo možné v logu zaznamenávat skutečné IP adresy klientů. Toho se dosahuje pomocí parametru *set_real_ip_from*.

Následně byl v nástroji Nginx Proxy Manager vytvořen další záznam typu host pro webové rozhraní služby Zigbee2MQTT. Přístup k tomuto rozhraní byl omezen pouze na konkrétní adresní rozsah administrátorské VLAN, čímž se zajistilo, že se k němu dostanou pouze oprávnění uživatelé ze správcovské části sítě. Stejným způsobem byl omezen i přístup do rozhraní samotného Nginx Proxy Manageru. Díky tomuto nastavení je možné přistupovat ke všem důležitým webovým rozhraním jednotlivých kontejnerů prostřednictvím šifrovaného připojení přes standardní port 443, který slouží pro HTTPS komunikaci. Pokud by se uživatel pokusil připojit nezabezpečeně přes protokol HTTP, systém jej automaticky přesměruje na šifrovanou verzi stránky (HTTPS), čímž je zajištěno, že všechna komunikace probíhá bezpečně.

Na serveru byl nastaven firewall s výchozí politikou *DROP* pro řetězec *INPUT*, což znamená, že veškerý nepovolený provoz je automaticky blokován. Výjimku tvoří následující pravidla:

- port *53/UDP* (DNS) je povolen pro příchozí provoz z lokální sítě,
- port *22/TCP* (SSH) je dostupný pouze z administrátorské VLAN,
- porty *80* a *443/TCP* (HTTP a HTTPS) jsou přístupné bez omezení.

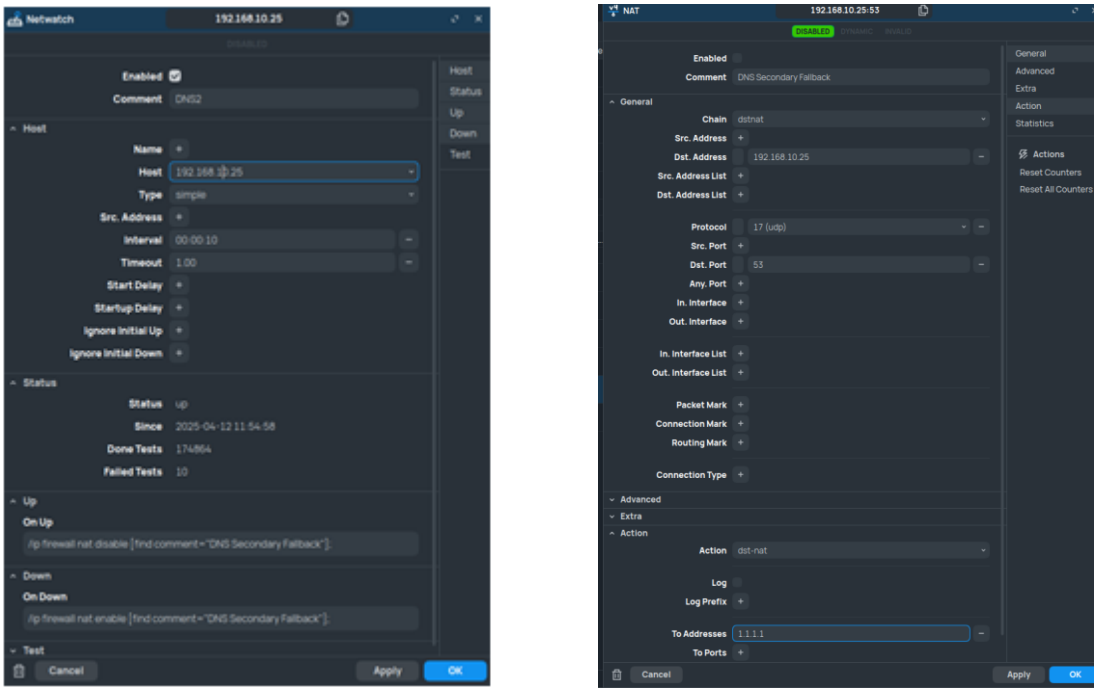
Díky tomuto nastavení je přístup na nezabezpečené porty jednotlivých kontejnerů zablokován a systém je tak chráněn proti neautorizovaným pokusům o připojení.

Aby nebylo nutné veřejně zpřístupňovat kontejnery s Nginx Proxy Managerem a Zigbee2MQTT přes internet, byl na server nainstalován balíček *BIND*, který slouží jako rekurzivní DNS server. Ten zajišťuje, že když zařízení v domácí síti vyhledá adresu mqtt.domena.ltd, nginx.domena.ltd nebo home.domena.ltd, bude je směřovat přímo na lokální IP adresu serveru. Díky tomu zůstává komunikace v rámci domácí sítě a není přesměrována ven na internet.

Aby tato konfigurace fungovala správně, bylo nutné v DHCP serveru (který automaticky přiděluje IP adresy a další síťové nastavení zařízením v síti) na routeru nastavit, aby jako primární DNS server používal právě lokální server s běžící službou *BIND*. Po rozšíření této změny v síti začala klientská zařízení směrovat své DNS dotazy na nový DNS server, který zajišťuje překlad domén na interní IP adresy.

Vzhledem k tomu, že výpadek tohoto DNS serveru by mohl způsobit nedostupnost překladu domén v celé síti, bylo na routeru MikroTik nastaveno sledování dostupnosti serveru pomocí nástroje Netwatch. Tento nástroj pravidelně testuje, zda je server aktivní, a to pomocí jednoduchého síťového dotazu ICMP (ping). Pokud server přestane odpovídat, router automaticky přesměruje veškeré DNS dotazy, které směřují na lokální IP adresu DNS serveru, na veřejný DNS server Cloudflare s adresou *1.1.1.1* Toto přesměrování je realizováno pomocí pravidla typu NAT, které nezmění adresu, na kterou se zařízení ptají – pouze změní to, kdo na tyto dotazy odpovídá. Klientská zařízení díky tomu stále komunikují se stejnou IP adresou, ale odpovědi poskytuje Cloudflare. Po obnovení dostupnosti lokálního DNS serveru se pravidlo *NAT* automaticky zruší a provoz je opět směrován lokálně.

Na obrázku 6 je vlevo znázorněna konfigurace nástroje Netwatch a vpravo příslušné pravidlo v NAT tabulce.

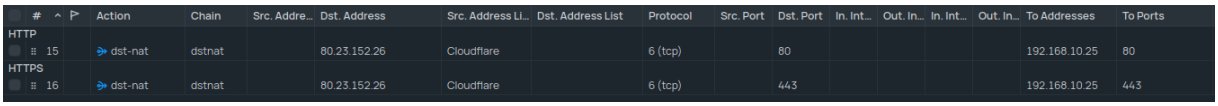


Obrázek 6: Netwatch vlevo a NAT pro DNS vpravo, Zdroj: vlastní

Pro dokončení konfigurace vzdáleného přístupu bylo ještě nutné nastavit přesměrování portů (port forwarding) tedy zajistit, aby se provoz přicházející z internetu na veřejnou IP adresu domácího routeru dostal až na správný server uvnitř domácí sítě. Vzhledem k tomu, že pro veřejný přístup je využívána proxy služba Cloudflare, není třeba zpřístupňovat daný port bez omezení. Místo toho stačí omezit přístup pouze na IP adresy, které Cloudflare používá. Tyto adresy jsou k dispozici ve formě veřejně dostupného textového seznamu.

Tyto IP adresy jsou jednou za 24 hodin automaticky stahovány. O toto stažení se stará Bash skript, který běží na webovém serveru jednoho z obyvatel. Tento skript nejprve stáhne aktuální seznam IP adres Cloudflare a pomocí něj vygeneruje druhý skript, který je spouštěn přímo na routeru MikroTik a aktualizuje příslušná pravidla, která určují, odkud je přístup k portu povolen. Oba skripty jsou uvedeny v příloze B.

Skript je navržen pouze pro práci s IPv4 adresami, protože připojení zabezpečované domácnosti aktuálně neumožňuje veřejný přístup přes protokol IPv6. Na obrázku 7 jsou zobrazena výsledná pravidla pro port forwarding, která umožňují přístup k systému Home Assistant pouze prostřednictvím serverů služby Cloudflare. Z důvodu zachování anonymity byla skutečná veřejná IP adresa nahrazena náhodnou hodnotou.



#	Action	Chain	Src. Addre...	Dst. Address	Src. Address Li...	Dst. Address List	Protocol	Src. Port	Dst. Port	In. Int...	Out. In...	In. Int...	Out. In...	To Addresses	To Ports
HTTP															
15	dst-nat	dstnat		80.23.152.26	Cloudflare		6 (tcp)		80					192.168.10.25	80
HTTPS															
16	dst-nat	dstnat		80.23.152.26	Cloudflare		6 (tcp)		443					192.168.10.25	443

Obrázek 7: Port forward pro HTTP a HTTPS pro Cloudflare servery, Zdroj: vlastní

Tímto byly dokončeny veškeré přípravné kroky nezbytné pro spuštění a bezpečný provoz systému Home Assistant.

4.2 Realizace návrhu

4.2.1 Instalace hardwaru

Instalace hardwarových komponent v zabezpečované domácnosti probíhala ve dvou etapách. V první fázi došlo k osazení Zigbee spínačů, což vyžadovalo odpojení napájení ve světelném okruhu. Pro zajištění bezpečnosti při manipulaci s elektrickým vedením byl před každým zásahem použit multimetr. Pomocí něj bylo ověřeno, že byl vypnut správný jistič a že se v obvodech nenachází žádné indukované napětí.

Fotografie instalovaného Zigbee spínače je uvedena v příloze C. V předsíni byl původně použit klasický schodišťový spínač, který umožňuje ovládání světla ze dvou míst. Zakoupené Zigbee spínače však tuto funkci nepodporují. Z tohoto důvodu byla zvolena alternativa v podobě bezdrátových Zigbee tlačítek, která nejsou přímo napojena na elektrický obvod. Místo toho slouží čistě jako ovládací prvky, které po stisknutí odesílají signál do systému Home Assistant. Napájení lustru bylo v rozvodné krabici nastaveno jako trvale zapnuté a samotné spínání světla je nyní řízeno softwarově – podle přijatého signálu od tlačítka. Pro ovládání napájení lustru bylo do stropní rozety nainstalováno Zigbee relé, které na základě přijatého signálu zajišťuje zapínání a vypínání osvětlení bez nutnosti fyzického zásahu prostřednictvím vypínače.

Ve druhé etapě proběhla instalace samotných senzorů. Některá zařízení, například Zigbee sirény, detektory kouře nebo detektory úniku plynu, byla uchycena pomocí dodaných hmoždinek a vrutů. Naproti tomu detektory úniku vody a senzory otevření dveří a oken byly připevněny pomocí oboustranných lepicích podložek značky 3M. Před jejich nalepením bylo nutné povrchy důkladně očistit technickým lihem, aby byla zajištěna dobrá přilnavost.

Do chodby zabezpečovaného bytu byl dále nainstalován tablet s aplikací Home Assistant, který umožňuje rychlý přístup k ovládání zabezpečovacího systému. Pro jeho uchycení byl

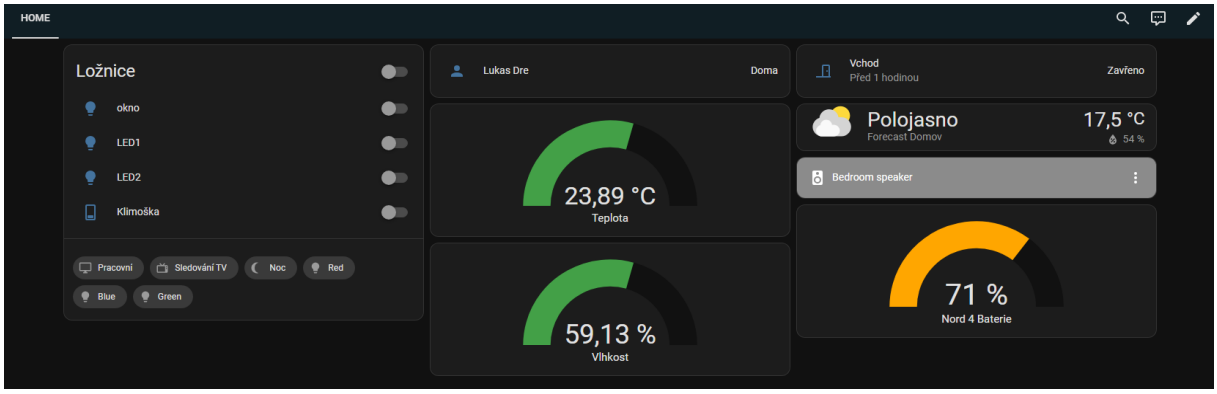
v programu Cinema 4D navržen vlastní držák, který byl následně vytištěn na 3D tiskárně. Tablet se do něj jednoduše zasouvá, což umožňuje snadné vložení i případné vyjmutí zařízení.

Pro zajištění nepřerušeného provozu systému i v případě výpadku elektrické energie byl nainstalován záložní zdroj (UPS). K tomuto zdroji byly připojeny klíčové síťové prvky, jako je router, síťové switche a také server se systémem Home Assistant. Tím je zajištěna kontinuita provozu a dostupnost systému i během krátkodobých výpadků napájení.

Ukázky nainstalovaných zařízení jsou uvedeny v příloze D.

4.2.2 Nastavení Home Assistant

Do systému Home Assistant byli přidáni tři uživatelé: Lukas Dre s administrátorskou rolí a dvě uživatelky Jana a Tereza, obě s rolí *uživatel*. Uživatelé s touto rolí nemají oprávnění měnit systémová nastavení, upravovat dashboardy, automatizace ani přidávat nová zařízení. Dále byl vytvořen speciální účet s názvem *Panel chodba*, který umožňuje přihlášení pouze z lokální sítě. Tento účet slouží pro přístup k aplikaci Home Assistant na tabletu umístěném na chodbě zabezpečovaného bytu. U všech uživatelů, s výjimkou účtu *Panel chodba*, bylo aktivováno dvoufázové ověřování prostřednictvím aplikace Authenticator. Pro každého uživatele byl rovněž vytvořen individuální dashboard přizpůsobený jeho potřebám a preferencím. Na obrázku 8 je zobrazen dashboard uživatele Lukas Dre.



Obrázek 8: Home Assistant dashboard, Zdroj: vlastní

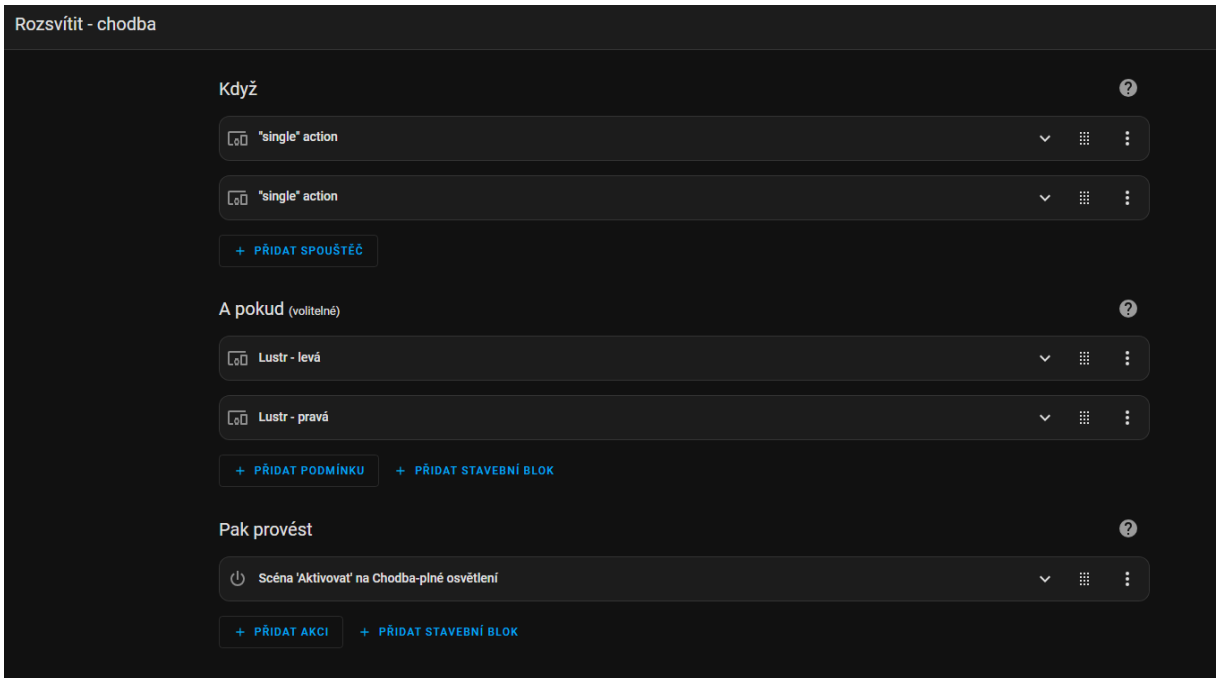
V další fázi byla aplikace Home Assistant nainstalována na mobilní zařízení každého z uživatelů. Následně bylo provedeno spárování jednotlivých zařízení s příslušnými uživatelskými účty v prostředí Home Assistant. Toto propojení umožňuje systému sledovat polohu jednotlivých uživatelů, což slouží jako jeden z klíčových vstupů pro automatické

řízení zabezpečovacích režimů – například automatickou aktivaci nebo deaktivaci alarmu podle toho, zda je někdo doma.

Na základě požadavků obyvatel bytu byly vytvořeny vlastní scény – přednastavené kombinace stavů zařízení (např. světla, teploty). Tyto scény jsou zobrazeny v přehledovém rozhraní (dashboardu) na obrázku 8, konkrétně pod ovládacími prvky v dlaždici „Ložnice“. Scény byly vytvořeny přímo ve webovém rozhraní systému Home Assistant. Jejich tvorba probíhá tak, že uživatel jednoduše vybere zařízení, která mají být součástí scény, a nastaví pro každé z nich jejich požadovaný stav (např. zhasnout lampičku). Změny se okamžitě projeví v chování chytré domácnosti, uživatel tak vidí reálný výsledek, díky čemuž může ladit scénu přímo při jejím vytváření. Jakmile je uživatel s výsledkem spokojen, scénu jednoduše uloží. Ukázka konfigurace scény je uvedena v příloze E.

Následně bylo nutné vytvořit automatizace – tedy pravidla, která zajišťují, že systém Home Assistant bude automaticky reagovat na konkrétní události. Vznikla celá řada jednoduchých automatizací, například pro ovládání světel pomocí Zigbee tlačítek. Tato řešení byla obzvlášť důležitá zejména na chodbě, kde byly původně klasické schodišťové vypínače. Ty byly nahrazeny bezdrátovými tlačítky, přičemž elektrický obvod pod vypínači byl trvale propojen a řízení osvětlení bylo převedeno na systém Home Assistant.

Na obrázku 9 je znázorněna jednoduchá automatizace, která se spustí po stisku tlačítka v předsíni. Pokud jsou obě relé (jedno pro levou a druhé pro pravou polovinu lustru) vypnutá, systém automaticky aktivuje scénu, která lustr rozsvítí. Využití scén v tomto případě výrazně zjednodušuje správu – není nutné v každé automatizaci zvlášť nastavovat zapnutí či vypnutí obou relé, protože požadovaný stav osvětlení je definován přímo ve scéně.



Obrázek 9: Automatizace rozsvícení na chodbě, Zdroj: vlastní

Dále byly vytvořeny rozsáhlejší a složitější automatizace, například podmíněné rozsvěcení světel v závislosti na denní době nebo dalších časových podmínkách. Ukázka takové automatizace je uvedena v příloze F.

Pomocí automatizací byla rovněž realizována logika zabezpečovacího systému, včetně reakce na podněty ze senzorů. Příkladem je situace, kdy dojde k otevření dveří při aktivním alarmu ve stavu „Zabezpečeno doma“ nebo „Zabezpečeno noc“. Tato automatizace zahrnuje několik navazujících kroků:

1. Dveřní senzor detekuje otevření dveří.
2. Pokud je alarm alespoň pět minut aktivní ve stavu „Zabezpečeno doma“ nebo „Zabezpečeno noc“, automatizace pokračuje.
3. Všem uživatelům je odeslána notifikace s upozorněním na otevření dveří při aktivním zabezpečení.
4. Systém čeká po dobu dvou minut, aby uživatelé měli čas na případnou reakci.
5. Pokud během této doby nedojde ke změně stavu alarmu na „Nezabezpečeno“ (tedy není zadán bezpečnostní kód), je odeslána další výstražná notifikace.
6. Po uplynutí další jedné minuty systém znovu ověří stav alarmu. Pokud je stále aktivní, dojde ke spuštění sirény.

7. Siréna zůstává aktivní, dokud není zadán bezpečnostní kód. Během této doby systém každých 10 sekund zasílá uživatelům opakovaná upozornění.

Celá automatizace zadaná do systému Home Assistant je zobrazena v příloze G.

4.3 Testování systému

Částečné testování systému probíhalo již během implementace a tvorby jednotlivých scénářů, kdy bylo nezbytné průběžně ověřovat jejich funkčnost a provádět potřebné úpravy. Testy byly vždy zaměřeny na právě vytvářenou automatizaci, aby bylo možné efektivně sledovat její chování bez rušivých vlivů jiných prvků systému. Scénáře byly spouštěny manuálně přímo z webového rozhraní Home Assistant, tedy bez nutnosti fyzické aktivace senzorů (například otevíráním dveří nebo pohybem v místnosti). Tato možnost urychlila celý proces ladění, neboť bylo díky tomu možné efektivně otestovat logiku daného scénáře, ověřit reakci systému a upravit podmínky nebo akce podle potřeby, aniž by bylo třeba opakovaně prováděl fyzické úkony.

4.3.1 Test funkčnosti jednotlivých komponent

V této fázi proběhlo testování jednotlivých senzorů a dalších komponent systému. K ověření funkčnosti detektorů kouře byl použit cigaretový kouř, který byl nasměrován přímo do štěrbiny, kterou se dostává vzduch do detektoru. Během několika vteřin došlo k aktivaci zvukové signalizace a současně detektor odeslal upozornění do systému Home Assistant, čímž byla potvrzena správná funkčnost zařízení i jeho integrace do systému.

Plynové senzory byly testovány aplikací malého množství plynu ze zapalovače do vstupní štěrbiny detektoru. Detektor okamžitě zareagoval spuštěním akustické signalizace a současně odeslal signál do systému Home Assistant. Vzhledem k intenzitě vestavěných sirén obou typů detektorů bylo při testování nezbytné používat ochranu sluchu.

Senzory detekce vytopení byly testovány jednoduchým způsobem – na jejich detekční plochu bylo aplikováno několik kapek vody. Senzor následně aktivoval akustickou signalizaci prostřednictvím vestavěného bzučáku a současně odeslal do systému Home Assistant signál označující přítomnost vody (stav „mokro“).

Senzory otevření oken a dveří byly testovány běžným způsobem – opakovaným otevřením a zavřením dveří. Při každé změně stavu odeslal senzor do systému Home Assistant odpovídající trigger, tedy „otevřeno“, nebo „zavřeno“. Následně byly ověřeny detektory

pohybu, které začaly téměř okamžitě po instalaci zasílat signál při každém zaznamenaném pohybu.

Na závěr proběhlo testování sirén, během něhož byly zkoušeny různé úrovně hlasitosti a typy zvukových tónů, aby bylo možné zvolit nejvhodnější nastavení pro různé situace.

4.3.2 Simulace hrozeb

Simulace hrozeb byla provedena po dokončení konfigurace všech automatizací a nastavení notifikačního systému. Hrozby požáru a úniku plynu byly otestovány pomocí vestavěných testovacích tlačítek na jednotlivých detektorech. Po jejich stisknutí došlo ke spuštění akustické signalizace přímo na senzoru. Systém Home Assistant následně správně zareagoval – aktivoval sirény a odeslal všem uživatelům notifikaci o detekovaném nebezpečí.

Únik vody byl simulován opětovným aplikováním malého množství vody na detekční plochu záplavového senzoru. I v tomto případě systém zareagoval podle očekávání – Home Assistant aktivoval optickou signalizaci na sirénách a uživatelům odeslal notifikaci s upozorněním na detekovaný únik vody.

Hrozba vloupání byla testována ve dvou scénářích. První test simuloval situaci při aktivním režimu „noc“, kdy jsou střeženy pouze vchodové dveře. Pokud dojde k jejich otevření, systém Home Assistant odešle všem uživatelům notifikaci s upozorněním na možný poplach. Tím je dán prostor pro ověření, zda se nejedná o falešný poplach. Pokud uživatelé do dvou minut nezareagují, systém odešle další upozornění a po uplynutí další jedné minuty automaticky spustí sirény. Tento scénář byl otestován opakovaným aktivováním režimu „noc“ a následným otevřením dveří. Testování proběhlo ve více iteracích, aby byla ověřena také funkčnost rušení poplachu prostřednictvím zadání bezpečnostního kódu. Ve všech případech systém reagoval podle očekávání.

Druhý test zaměřený na hrozbu vloupání se zaměřil na scénář, kdy je alarm aktivován v režimu „nikdo není doma“. V tomto režimu se očekává, že v případě detekce pohybu nebo otevření dveří či oken systém spustí 60sekundový odpočet, během něhož je nutné alarm deaktivovat zadáním bezpečnostního kódu – buď prostřednictvím mobilní aplikace, nebo na ovládacím panelu umístěném v předsíni. Po uplynutí této lhůty systém zkontroluje aktuální stav alarmu. Pokud nebyl změněn na „nezabezpečeno“, dojde ke spuštění akustické signalizace a uživatelům jsou každých 10 sekund rozesílány notifikace s upozorněním na narušení. Tento scénář bylo nutné otestovat opakovaně, a to nejen kvůli ověření správného

spuštění poplachu, ale i jeho následné deaktivace. Nevýhodou tohoto testu bylo, že si vyžadoval skutečné opuštění bytu všemi obyvateli. I přesto však všechny testy proběhly podle očekávání a systém reagoval správně ve všech situacích.

V další fázi byl otestován scénář výpadku elektrického napájení. Simulace byla provedena vypnutím příslušných jističů. Během výpadku byly klíčové prvky systému – router, switche a server s Home Assistantem – napájeny prostřednictvím záložního zdroje (UPS), což zajistilo jejich nepřerušený provoz. Většina senzorů, s výjimkou detektoru úniku plynu, je napájena z baterie, jejich funkčnost tedy zůstala plně zachována. V provozu zůstaly i sirény. Výpadek byl simulován po dobu jedné hodiny. Díky nízkému odběru všech napájených zařízení (včetně Raspberry Pi 4) nedošlo k žádnému přerušení provozu systému.

4.4 Vyhodnocení implementace

4.4.1 Efektivita systému v reálném prostředí

Implementovaný systém byl testován v běžném provozu v bytové jednotce po dobu několika týdnů. V rámci testování byly sledovány tyto klíčové parametry:

- spolehlivost detekce (pohyb, otevření dveří/oken, kouř, plyn, voda),
- rychlost reakce systému (čas mezi detekcí a reakcí – např. zaslání notifikace),
- přesnost a falešné poplachy,
- uživatelská přívětivost ovládání a notifikací,
- stabilita systému při výpadku internetu nebo napájení.

Výsledky ukázaly, že systém poskytuje dostatečně rychlou a přesnou detekci událostí s minimem falešných poplachů. Výhodou je také modulární rozšiřitelnost, která umožňuje snadné doplnění dalších senzorů bez zásahu do stávající instalace.

Omezením zůstává závislost na správné konfiguraci uživatelem, přičemž složitější automatizace mohou být pro laika náročné. Na druhou stranu možnost lokálního provozu bez cloudu výrazně zvyšuje bezpečnost a soukromí uživatele.

4.4.2 Srovnání s komerčními systémy

Při porovnání open-source systému s komerčními byly zohledněny aspekty jako cena, možnost úprav, závislost na cloudu, uživatelská přívětivost, rozšiřitelnost a podpora. V tabulce 3 je provedeno obecné srovnání systémů.

Tabulka 3: Obecné srovnání open-source systému a komerčních systémů

Kritérium	**Open-source systém**	**Komerční systém**
Cena	Nízká (komponenty + vlastní čas)	Vysoká (balíčky + případné služby)
Možnost úprav	Vysoká, otevřená platforma	Omezená, uzavřený ekosystém
Závislost na cloudu	Nepovinná, volitelná	Většinou povinná
Uživatelská přívětivost	Vyšší nároky na nastavení	Intuitivní, připravené řešení
Rozšiřitelnost	Prakticky neomezená	Limitována výrobcem
Podpora a servis	Komunita, vlastní zkušenosti	Profesionální podpora

Zdroj: vlastní

Z porovnání vyplývá, že open-source řešení je vhodné pro technicky zdatnější uživatele, kteří ocení otevřenost, přizpůsobitelnost a nezávislost na výrobci. Naopak pro uživatele preferující jednoduchost a rychlou instalaci může být vhodnější komerční systém, který však přináší vyšší náklady a omezenou flexibilitu.

Závěr

Tato bakalářská práce se zaměřila na návrh a realizaci zabezpečovacího systému pro bytovou jednotku s využitím open-source platformy Home Assistant. Na základě provedené analýzy dostupných senzorů a komunikačních protokolů bylo navrženo a implementováno řešení, které splňuje požadavky na spolehlivost, flexibilitu a nezávislost na cloudových službách třetích stran.

Systém založený na platformě Home Assistant se v reálném provozu osvědčil jako efektivní nástroj pro detekci pohybu, otevření oken a dveří, přítomnosti kouře, úniku vody i plynu. Díky jeho modularitě, otevřenému rozhraní a široké komunitní podpoře je možné systém snadno rozšiřovat o další zařízení a funkce podle aktuálních potřeb uživatele. Velkou výhodou je také možnost provozování systému na běžně dostupném hardwaru, jako je například Raspberry Pi, což výrazně snižuje celkové pořizovací náklady.

Práce prokázala, že open-source řešení na platformě Home Assistant představuje vhodnou alternativu ke komerčním zabezpečovacím systémům, zejména pro technicky zdatné uživatele, kteří požadují vyšší míru kontroly, transparentnosti a nezávislosti.

V průběhu realizace bylo nutné překonat řadu výzev, zejména v oblasti konfigurace Docker kontejnerů, síťového prostředí a integrace různorodých technologií do jednoho funkčního celku. Další výzvu představovalo navržení logiky jednotlivých automatizací tak, aby byly nejen funkční, ale zároveň i intuitivní a snadno spravovatelné.

Do budoucna je možné systém dále rozvíjet například o prvky strojového učení pro predikci chování, pokročilé automatizace založené na historických datech nebo integraci kamerových systémů s funkcí detekce pohybu a rozpoznávání obrazu. Z dlouhodobého hlediska lze také uvažovat o vyšší míře autonomie systému a adaptivním řízení na základě chování uživatelů, což by mohlo výrazně posílit jak úroveň zabezpečení, tak i komfort celé domácnosti.

Použitá literatura

[1] ALZA.CZ A.S. IMMAX NEO Smart PIR senzor 2v1 Zigbee 3.0. ALZA.CZ A.S. *Alza.cz* [online]. c1994-2025 [cit. 2025-03-14]. Dostupné z: https://www.alza.cz/immax-neo-smart-pir-senzor-2v1-zigbee-3-0-d12450230.htm

[2] ALZA.CZ A.S. SONOFF iPlug Wi-Fi Smart Plug (S60 Series). ALZA.CZ A.S. *Alza.cz* [online]. c1994-2025 [cit. 2025-03-12]. Dostupné z: https://www.alza.cz/sonoff-iplug-wi-fi-smart-plug-s60-series-d12316469.htm

[3] ASIF, Omar, et al. Fire-detectors review and design of an automated, quick responsive fire-alarm system based on SMS. *International Journal of Communications, Network and System Sciences*, 2014, 7.9: 386-395.

[4] BURDA, Karel. *Základy elektronických zabezpečovacích systémů*. Brno: Akademické nakladatelství CERM, 2017. ISBN 978-80-7204-967-7.

[5] Český statistický úřad. Kriminalita – trestné činy. In: *ČSÚ Veřejná databáze* [online]. [cit. 2025-03-06]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt&pvo=KRI05&z=T&f=TABULKA&katalog=31008&str=v35&evo=v104_!_KRI05-H-6068_1&u=v35__VUZEMI__100__3018

[6] Český statistický úřad. Požáry. In: *ČSÚ Veřejná databáze* [online]. [cit. 2025-03-06]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt&pvo=KRI09&z=T&f=TABULKA&katalog=31008&str=v27&u=v27__VUZEMI__100__3018

[7] CHOU, Timothy Chen Kuang. *Precision: principles, practices and solutions for the internet of things*. Edition 1.4. [Spojené státy americké]: CrowdStory Publishing, [2016]. ISBN 978-1-329-84356-1.

[8] Installation. *Home Assistant* [online]. [cit. 2025-02-05]. Dostupné z: https://www.home-assistant.io/installation/

[9] LOXONE ELECTRONICS GMBH. Chytrá domácnost od Loxone. *LOXONE* [online]. c2025 [cit. 2025-02-01]. Dostupné z: https://www.loxone.com/cscz/chytry-dum/

[10] LOXONE ELECTRONICS GMBH. Loxone technologie. *LOXONE* [online]. c2025 [cit. 2025-02-01]. Dostupné z: https://www.loxone.com/cscz/produkty/technologie/

[11] OPENHAB COMMUNITY AND THE OPENHAB FOUNDATION E.V. Add-on Reference. *OpenHab.org* [online]. c2025 [cit. 2025-02-02]. Dostupné z: https://www.openhab.org/addons/

[12] OPENHAB COMMUNITY AND THE OPENHAB FOUNDATION E.V. Download openHab. *OpenHab.org* [online]. c2025 [cit. 2025-02-02]. Dostupné z: https://www.openhab.org/download/

[13] OPENHAB COMMUNITY AND THE OPENHAB FOUNDATION E.V. openHAB empowering the smart home. *OpenHab.org* [online]. c2025 [cit. 2025-02-02]. Dostupné z: https://www.openhab.org/

[14] [SMARTICA AUTOMATION S.R.O.]. Tlačítkový ZigBee vypínač bez "nuly" - 2CH. *Chytré vypínače* [online]. [cit. 2025-03-10]. Dostupné z https://www.chytrevypinace.cz/Tlacitkovy-ZigBee-vypinac-bez-nuly-2CH-d309.htm

[15] [SMARTICA AUTOMATION S.R.O.]. ZigBee Sensor CNG (Zemní plyn). *Chytré vypínače* [online]. [cit. 2025-03-10]. Dostupné z: https://www.chytrevypinace.cz/ZigBee-Sensor-CNG-Zemni-plyn-d256.htm

[16] [SMARTICA AUTOMATION S.R.O.]. ZigBee Sensor Kouře. Chytré vypínače [online]. [cit. 2025-03-10]. Dostupné z: https://www.chytrevypinace.cz/ZigBee-Sensor-Koure-d258.htm

[17] [SMARTICA AUTOMATION S.R.O.]. ZigBee Sensor Okna/Dveře USB. *Chytré vypínače* [online]. [cit. 2025-03-25]. Dostupné z: https://www.chytrevypinace.cz/ZigBee-Sensor-Okna-Dvere-USB-d176.htm

[18] [SMARTICA AUTOMATION S.R.O.]. ZigBee Sensor Vytopení. *Chytré vypínače* [online]. [cit. 2025-03-10]. Dostupné z https://www.chytrevypinace.cz/ZigBee-Sensor-Vytopeni-d174.htm

[19] [SMARTICA AUTOMATION S.R.O.]. ZigBee Siréna. *Chytré vypínače* [online]. [cit. 2025-03-10]. Dostupné z https://www.chytrevypinace.cz/zigbee-sirena

[20] TUYA INC. About Tuya. *Tuya Smart - Global AI Cloud Platform Service Provider* [online]. c2025 [cit. 2025-02-01]. Dostupné z: https://www.tuya.com/about

[21] VALEŠ, Miroslav. *Inteligentní dům*. Brno: ERA, 2006. ISBN 80-7366-062-8.

Seznam příloh

PŘÍLOHA A: Konfigurace Home Assistant

Konfigurační soubor systému Home Assistant obsahuje definici zabezpečovacího systému (alarmu) a nastavení potřebná pro provoz prostřednictvím reverzního proxy serveru. V úvodu souboru je zahrnuta také funkce Wake-on-LAN, která byla doplněna dodatečně za účelem vzdáleného zapínání síťového úložiště (NAS). Zdroj: vlastní.

```yaml
# Loads default set of integrations. Do not remove.
default_config:
wake_on_lan:
switch:
  - platform: wake_on_lan
    mac: "00:00:00:00:00:00"

# Text to speech
tts:
  - platform: google_translate

automation: !include automations.yaml
script: !include scripts.yaml
scene: !include scenes.yaml

alarm_control_panel:
  - platform: manual
    name: Home Alarm
    code: "0000"
    arming_time: 30
    delay_time: 20
    trigger_time: 4
    disarmed:
      trigger_time: 0
    armed_home:
      arming_time: 0
      delay_time: 0

http:
  cors_allowed_origins:
    - https://google.com
    - https://www.home-assistant.io
  use_x_forwarded_for: true
  trusted_proxies:
    - 172.19.0.0/24
    - 192.168.10.25
    - fe80::e65f:1ff:fea8:554f
    - 2001:470:5a3c:0:e65f:1ff:fea8:554f

```

PŘÍLOHA B: Skripty pro dynamickou aktualizaci firewallu na routeru MikroTik

Na webovém serveru je pomocí *crontab* spouštěn jednou za 24 h následující bash script:

```bash
#!/bin/bash

OUTPUT="/var/www/html/lukasgraphic/cloudflare-address-list.rsc"
LIST_NAME="Cloudflare"

# Stažení IP rozsahů
URL="https://www.cloudflare.com/ips-v4"
TMP_FILE=/tmp/ipsv-4

if ! curl -s "$URL" -o "$TMP_FILE"; then
    echo "Chyba: Nepodařilo se stáhnout seznam z $URL"
    rm -f "$TMP_FILE"
    exit 1
fi

# Kontrola, zda soubor není prázdný
if [ ! -s "$TMP_FILE" ]; then
    echo "Chyba: Stažený soubor je prázdný"
    rm -f "$TMP_FILE"
    exit 1
fi

#Začátek RSC skriptu
echo "# Cloudflare Address List" > "$OUTPUT"
echo "# Generated on $(date)" >> "$OUTPUT"
echo "" >> "$OUTPUT"

# Generování address-list položek
while read -r ip; do
    # Přeskakuj prázdné řádky
    [[ -z "$ip" ]] && continue
    echo "/ip firewall address-list add list=$LIST_NAME address=$ip comment=\"Automatically generated\"" >> "$OUTPUT"
done < "$TMP_FILE"

rm "$TMP_FILE"

chown www-data:www-data "$OUTPUT"

#echo "RSC skript byl uložen jako: $OUTPUT"
```

Skript slouží ke stažení aktuálního seznamu IP rozsahů používaných servery společnosti Cloudflare z jejich oficiálního webu. Po stažení ověří, zda soubor není prázdný. Pokud je obsah v pořádku, přepíše skript data do souboru ve formátu .rsc, který je následně zpřístupněn prostřednictvím webového serveru. Výsledný generovaný skript má následující podobu:

```
# Cloudflare Address List
# Generated on Thu Apr 17 23:20:02 CEST 2025

/ip firewall address-list add list=Cloudflare address=173.245.48.0/20 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=103.21.244.0/22 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=103.22.200.0/22 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=103.31.4.0/22 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=141.101.64.0/18 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=108.162.192.0/18 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=190.93.240.0/20 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=188.114.96.0/20 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=197.234.240.0/22 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=198.41.128.0/17 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=162.158.0.0/15 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=104.16.0.0/13 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=104.24.0.0/14 comment="Automatically generated"
/ip firewall address-list add list=Cloudflare address=172.64.0.0/13 comment="Automatically generated"

```

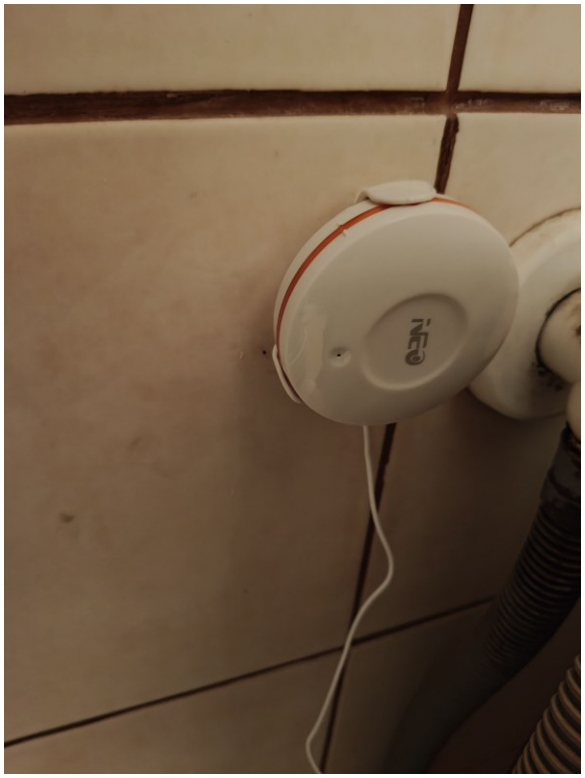
Vygenerovaný RSC skript je automaticky stahován a spouštěn na routeru pomocí plánovače úloh. Zdroj: vlastní.

PŘÍLOHA C: Instalovaný ZigBee spínač

Zdroj: vlastní.

PŘÍLOHA D: Ukázky instalovaných prvků

Na levém obrázku je zobrazen nainstalovaný detektor kouře, zatímco pravý obrázek zachycuje detektor úniku plynu. Ten byl, v souladu s doporučením výrobce, umístěn ve výšce 2 metry v místnosti s instalovaným plynovým spotřebičem. Zdroj: vlastní.



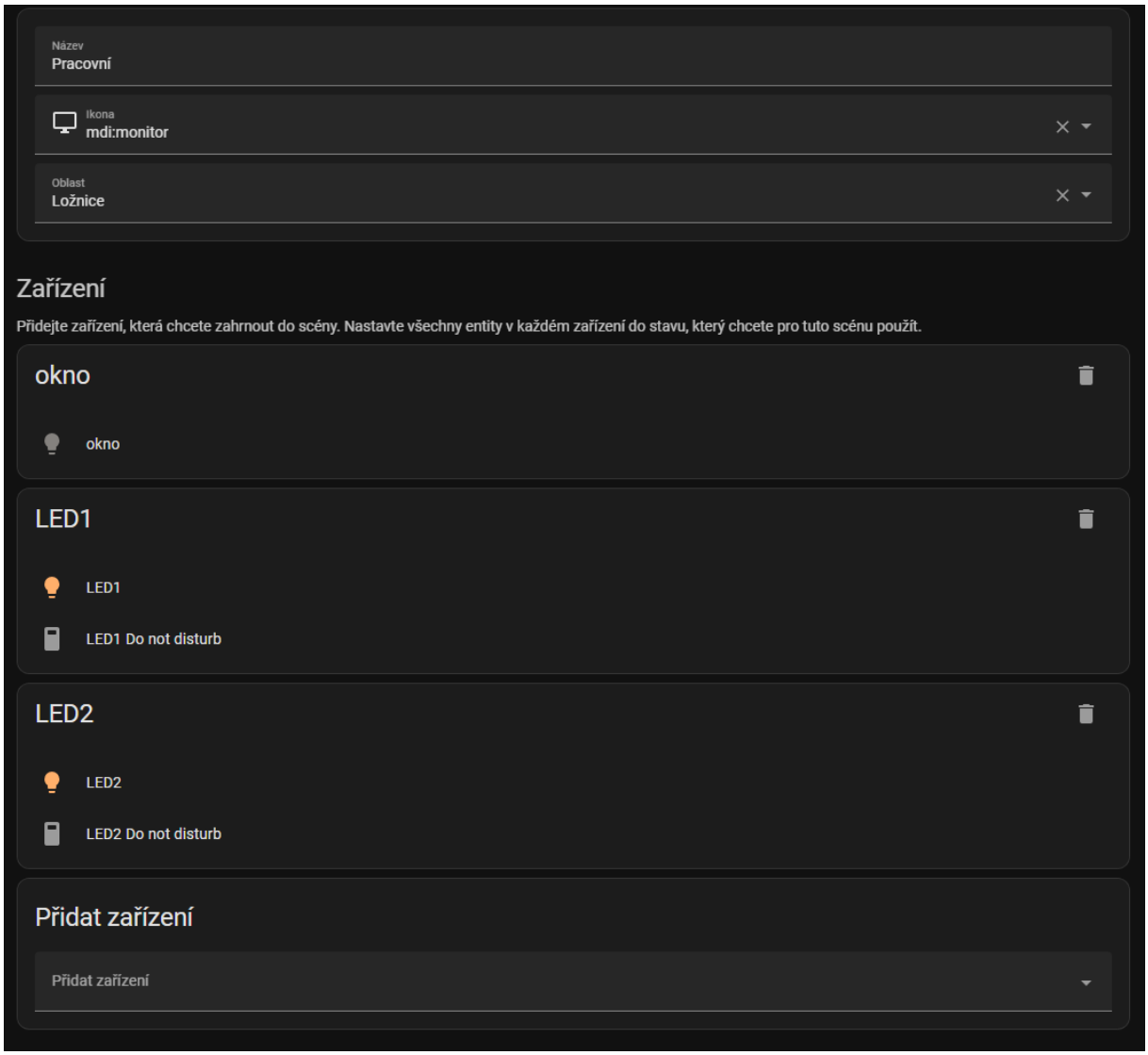
Na levém obrázku je zobrazen záplavový senzor umístěný za pračkou. Viditelný je řídicí modul, ze kterého vede kabel k detekčnímu modulu umístěnému pod pračkou. Zdroj: vlastní.

Na pravém obrázku je zachycen detektor otevření dveří nainstalovaný na hlavních vstupních dveřích bytu. Zdroj: vlastní.

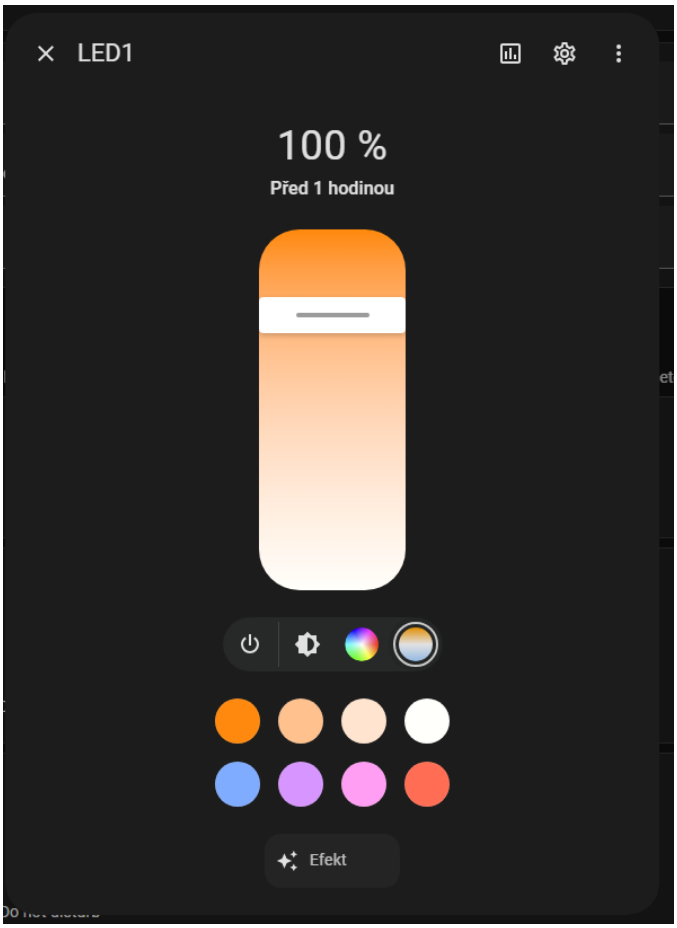
Na obrázku je zobrazen ovládací panel nainstalovaný na chodbě bytu. Panel je uchycen pomocí jednoduchých držáků vytištěných na 3D tiskárně. Zdroj: vlastní.

Na obrázku je ovládací panel s aktivní obrazovkou pro ovládání alarmu. Tlačítko pro vstup do rozhraní alarmu je záměrně skryto, aby se předešlo neautorizovanému přístupu. Zdroj: vlastní.

PŘÍLOHA E: Nastavení a tvorba scén v Home Assistant

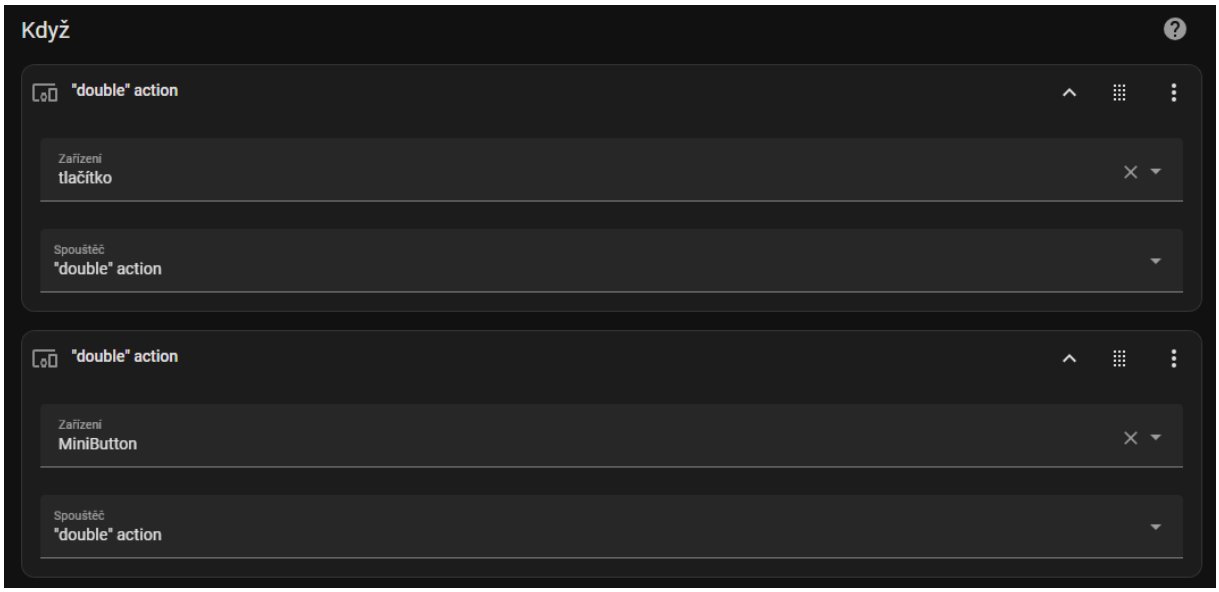


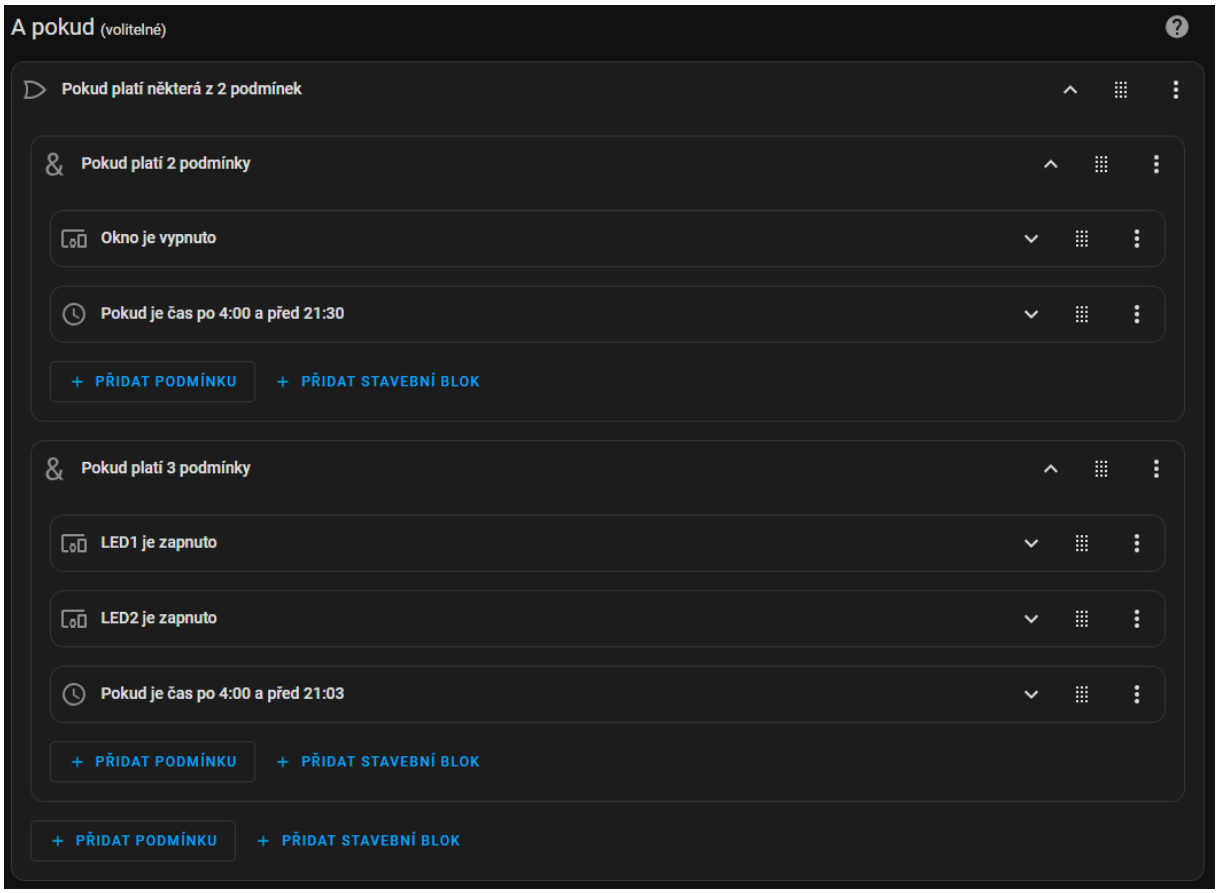
Na obrázku je zobrazena základní obrazovka rozhraní Home Assistant pro přidání zařízení do scény. Uživatel zde vybírá, která zařízení chce do scény zahrnout, a nastavuje jejich požadované stavy. Zdroj: vlastní.

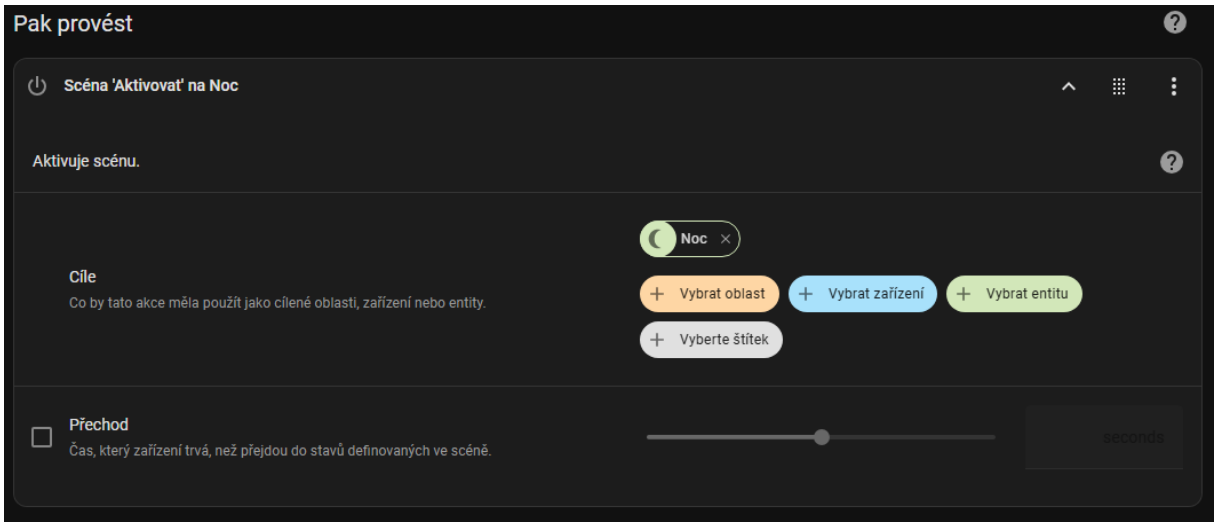


Nastavení konkrétního zařízení ve scéně. V případě světla je možné upravit jeho jas, barevnou teplotu nebo barvu. Dostupné možnosti se liší podle schopností daného zařízení. Zdroj: vlastní.

PŘÍLOHA F: Automatizace s použitím časových podmínek

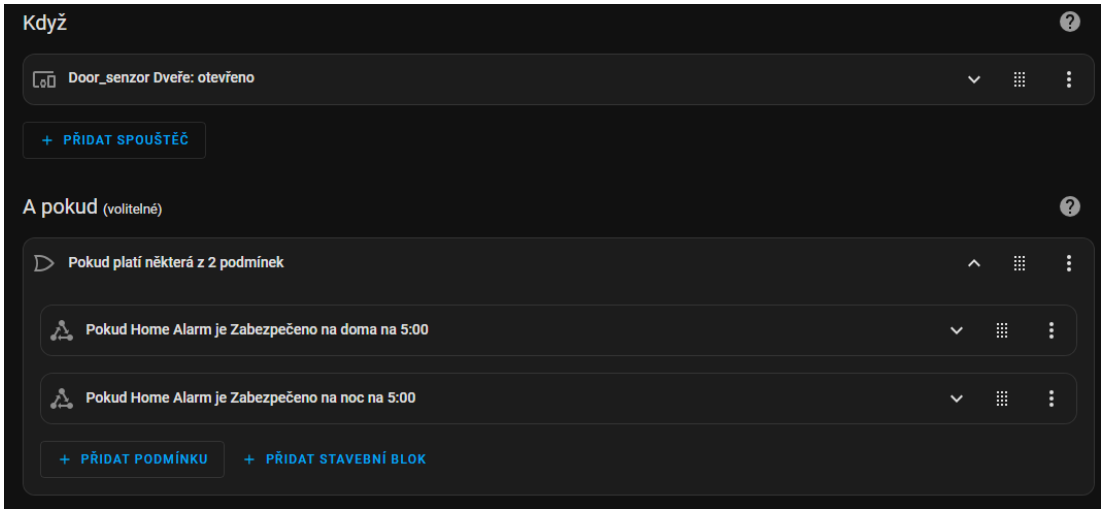


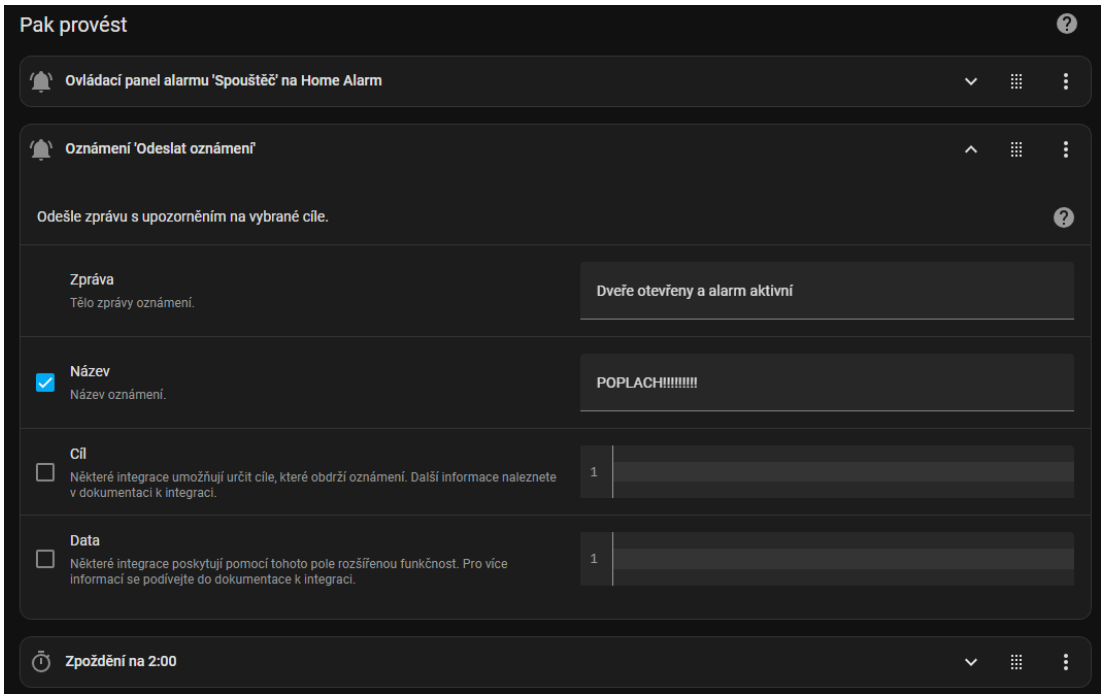


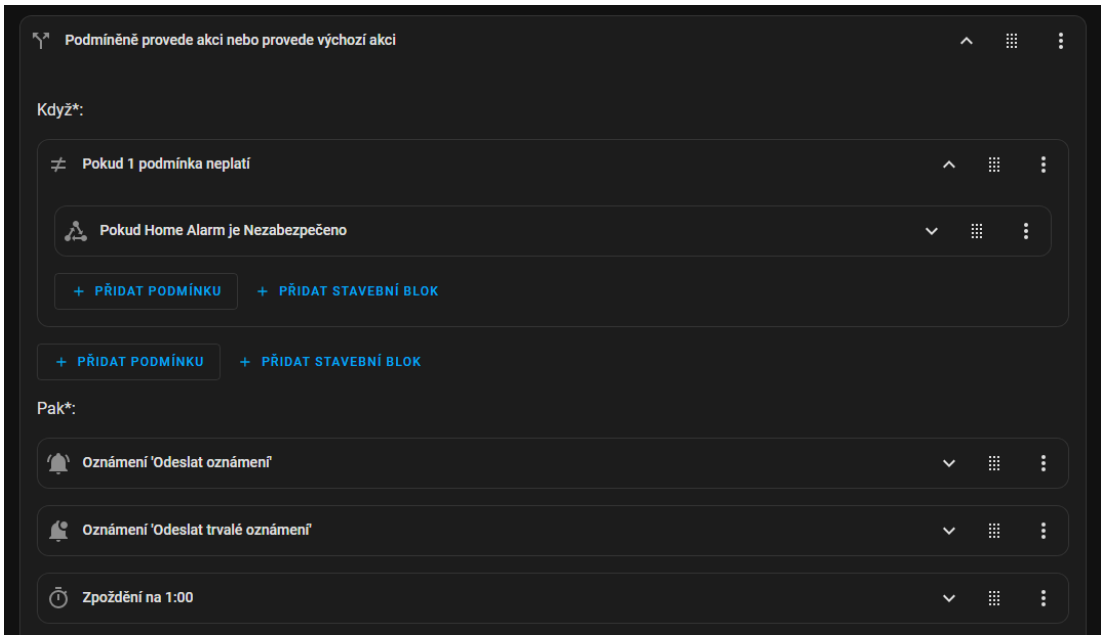


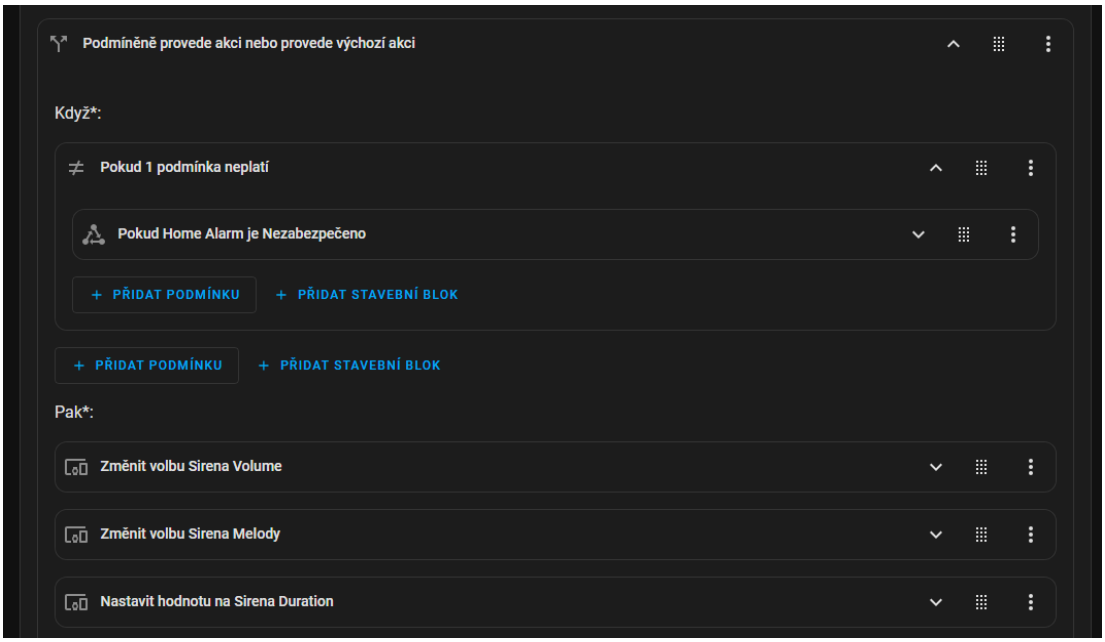
Tato automatizace slouží k ovládání osvětlení v ložnici. Aktivuje se při detekci dvojkliku na nástěnném Zigbee spínači nebo bezdrátovém mini tlačítku. Po aktivaci se ověří, zda je světlo pod oknem zhasnuté a současně zda je aktuální čas mezi 4:00 a 21:30, případně zda jsou zapnutá světla LED1 a LED2 a zároveň je splněna časová podmínka. Pokud jsou podmínky splněny, aktivuje se scéna „noc“. Automatizace je navržena tak, aby umožnila plynulý přechod ze scény „pracovní“, kdy jsou aktivní LED1, LED2 a světlo pod oknem. Bez druhé části podmínky by první dvojklik pouze zhasl světlo pod oknem (což zajišťuje jiná automatizace) a až opakovaný dvojklik by aktivoval noční scénu. Tímto řešením se přechod mezi scénami zjednodušuje a zvyšuje se komfort ovládání. Zdroj: vlastní.

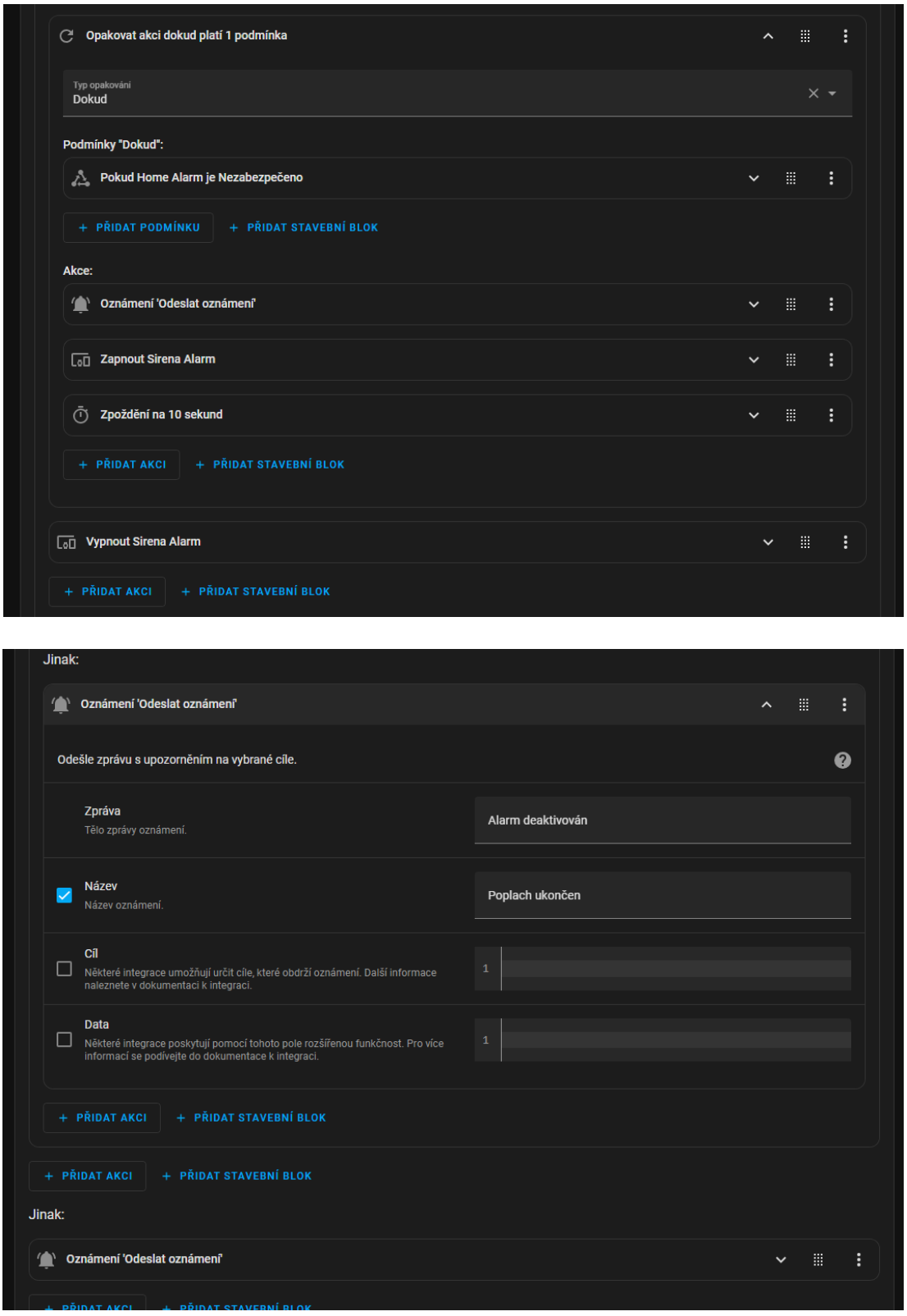
PŘÍLOHA G: Automatizace pro poplach při stavu Zabezpečeno doma/Zabezpečeno noc






Podmíněně provede akci nebo provede výchozí akci
Když*:
Pokud 1 podmínka neplatí
Pokud Home Alarm je Nezabezpečeno
+ PŘIDAT PODMÍNKU
+ PŘIDAT STAVEBNÍ BLOK
+ PŘIDAT PODMÍNKU
+ PŘIDAT STAVEBNÍ BLOK
Pak*:
Oznámení 'Odeslat oznámení'
Oznámení 'Odeslat trvalé oznámení'
Zpoždění na 1:00


Podmíněně provede akci nebo provede výchozí akci
Když*:
Pokud 1 podmínka neplatí
Pokud Home Alarm je Nezabezpečeno
+ PŘIDAT PODMÍNKU
+ PŘIDAT STAVEBNÍ BLOK
+ PŘIDAT PODMÍNKU
+ PŘIDAT STAVEBNÍ BLOK
Pak*:
Změnit volbu Sirena Volume
Změnit volbu Sirena Melody
Nastavit hodnotu na Sirena Duration



Na obrázku je znázorněno kompletní zadání jedné z automatizací souvisejících s ovládáním alarmu. Vzhledem k jejich rozsahu a složitosti je pro ilustraci přiložena pouze jedna ukázka. Zdroj: vlastní