Lås- och Larm System

En implementation av ett larmsystem med rörelse-, vibrations- och dörrsensorer på mikrodatorn MD407

Rachel* Samuelsson, Jonatan Gunnarsson, Mohammad Mourad, Olof Forsberg, Samuel Runmark Thunell

Handledare: Johannes Holmgren

27 oktober 2022

Institutionen för data-och informationsteknik
Datateknologiska programmet

Chalmers Tekniska Högskola
Göteborg, Sverige

*Folkbokförd som "David"

Ordlista

Nedan följer en lista av ämnesspecifika termer respektive dess beskrivningar.

ARM *Advanced RISC Machines*, är en processorarkitektur.

CAN *Controller Area Network*, ett protokoll ämnat åt busskommunikation. Vanligt i bilar.

GPIO *General-Purpose Input/Output*, stift på en mikrodator som godtyckligt kan läsas av samt skrivas till via mjukvara.

Imitationsattack En typ av cyberattack där en förbrytare skickar meddelanden in i ett system för att främja ett eget syfte. Dessa meddelanden påstås skickats från en enhet i systemet.

Knappsats Ett fysiskt tangentbord för att mata in numeriska värden till ett datorsystem.

Kopplingsplatta En platta för att möjliggöra snabb koppling och frånkoppling av tekniska komponenter.

MD407 En mikrodator baserad på STM32407 processorn. [1]

STM biblioteket *STM32F4xx Standard Peripheral Library*, ett mjukvarubibliotek för att underlätta utveckling av C kod till STM32F4xx processorer.

USART *Universal Synchronous/Asynchronous Receiver/Transmitter*, ett gränssnitt för seriekommunikation som bland annat möjliggör kommunikation mellan en mikrodator och en PC.

Innehåll

1 Inledning

Det finns i dagsläget ett mycket stort behov av verkningsfulla säkerhetssystem. Detta på grund av att den tekniska utvecklingen i sin tur förbättrar inbrottsverktyg. Behovet av larmsystem syns tydligt i statistiken, året 2021 anmäldes totalt 72 884 inbrottsstölder. [2]

1.1 Syfte

Baserat på den tidigare nämnda inbrottsstatistiken är projektets syfte att konstruera ett larmsystem säkrat mot moderna intrångsmetoder. Detta grundas i systemets kommunikationssystem. Dessutom kommer systemet att kontrolleras kontinuerligt så att systemet inte kan avaktiveras av en icke-befogad individ.

1.2 Mål

Det övergripande målet med projektet är att konstruera ett säkert larmsystem. Produkten kommer att kunna känna av rörelse i en larmad miljö samt fånga vibrationer. Det kommer att vara möjligt att justera känsligheten så att produkten inte larmar när området är tomt. Produkten kommer också att kontrollera om en enskild dörr är olåst eller har lämnats öppen en viss tid, där tiden kan konfigureras i en centralenhet. När larmet aktiveras ska det vara möjligt för produkten att inaktivera det genom att en fyrsiffrig kod matas in i centralenheten. Produkten kommer också att kunna aktivera och inaktivera larmet för varje enskild dörr. Flera dörrar kommer att kunna larmas samtidigt och produkten visar med grönt ljus ifall en dörr inte är larmad.

En ytterligare ambition med projektet är att utöka säkerhetsdetaljer i produkten. Till detta syfte skall en störenhet utvecklas, för att kunna testa hur systemet beter sig när CAN-kommunikationen överbelastas. Larmet kommer att utlösas ifall en periferienhet går sönder eller kopplas från systemet. Om en periferienhet tar emot ett meddelande som hävdats vara skickat från den själv kommer den slå larm. Detta för att förebygga eventuella imitationsattacker. Angripare med god kunskap kring systemets implementation ska likaså förhindras från att komma åt systemet.

2 Teknisk beskrivning

I detta kapitel ges en teknisk beskrivning av systemet, samt de ämnespecifika kunskaper som krävs för att följa rapporten.

2.1 Teknisk bakgrund

I dagens samhälle är larmsystem ett sätt att hålla viktiga objekt säkra utan vakter närvarande. Det är i led med den modernisering och digitalisering som sker i samhället. [3] Ett stabilt system ökar säkerheten genom att den mänskliga faktorn avlägsnas. Detta förutsätter att systemet saknar direkta svagheter och kommer att larma varje gång ett fel sker.

Digitala larmsystem bygger på att sensorer övervakar ett specifikt föremål, en plats, eller en process. När en sensor observerar en eftertraktad händelse skickas en larmsignal till en enhet som aktiverar en lampa, ljud, eller båda. [4]

Ett vanligt kommunikationsmedium mellan flertalet kopplade enheter är CAN-bussar. Meddelanden skickade över CAN-bussen har ett 11 bitars ID fält, samt upp till 64 bitar av data. [5] Då två CAN-meddelanden skickas samtidigt får meddelandet med lägre ID prioritet.

USART är ett vanligt kommunikationsmedel för seriell kommunikation mellan två enheter. USART används ofta för att tillåta kontinuerlig kommunikation mellan en mikrodator och en PC. [6]

I ett larmsystem är säkerhet en av de viktigaste faktorerna, det är därför viktigt att förebygga olika cyberattacker. Återuppspelningsbaserade attacker är en variant av imitationsattack som ej kräver någon förkunskap om systemet. I en återuppspelningsattack spelas systemets meddelanden in under en period då larmet stängs av. Meddelandena återspelas sedan för att larma av systemet. [7]

2.2 Tekniska förutsättningar

Projektet är grundat kring mikrodatorn MD407 och dess implementation av CAN, USART, samt andra periferienheter. MD407-kontrollern är baserad på ARM Cortex M4 processorn STM32407 som innehar 1MB flash-minne samt en klockfrekvens på 168MHz. [1]

För att känna av vibrationer används sensorn SW-18010 och för rörelser används avståndsmätaren HCSR04. STM32 mjukvarubiblioteket användes under utvecklingen för att abstrahera hårdvarunära kod. Baserat på detta har ett CAN-kommunikationsprotokoll utvecklats, vilket samtliga MD407 använder för kommunikation. Huvudlogiken för samtliga enheter och funktioner för sensoravläsning har implementerats från grunden.

2.3 Enheter

Larmsystemet består av tre komponenter, två periferienheter och en centralenhet. Utöver dessa komponenter skapades tre enheter i testningssyfte.

2.3.1 Dörrperiferienhet

Första periferienheten är ett dörrlarm som larmar när en dörr stått öppen för länge. Enheten är kapabel till att övervaka flera dörrar vars tidsgränser är individuellt konfigurerbara samt kan avlarmas individuellt. Då en tidsgräns överskrides larmas först lokalt, följt av att centralenheten larmas.

2.3.2 Rörelseperiferienhet

Andra periferienheten är ett rörelselarm som larmar om rörelse eller vibration avläses. Gränserna för dessa sensorer är konfigurerbara och denna enhet larmar direkt till centralenheten.

2.3.3 Centralenhet

Centralenheten är ansvarig för att larma av via en knappsats. Likaså ansvarar centralenheten för konfiguration av periferienheter och kommunikation med en PC. Den ansvarar även för att larma då någon periferienhet frånkopplas eller av annan anledning blir otillgänglig. Flera periferienheter kan kopplas till centralenheten och samspela.

2.3.4 Störenhet

Störenheten är en enhet kapabel till att generera slumpmässig data samt skicka denna data till en slumpmässig enhet över en CAN-buss. Mängden och tiden mellan skickade meddelanden kan konfigureras via en PC.

2.3.5 Återuppspelning- och avlyssningsenhet

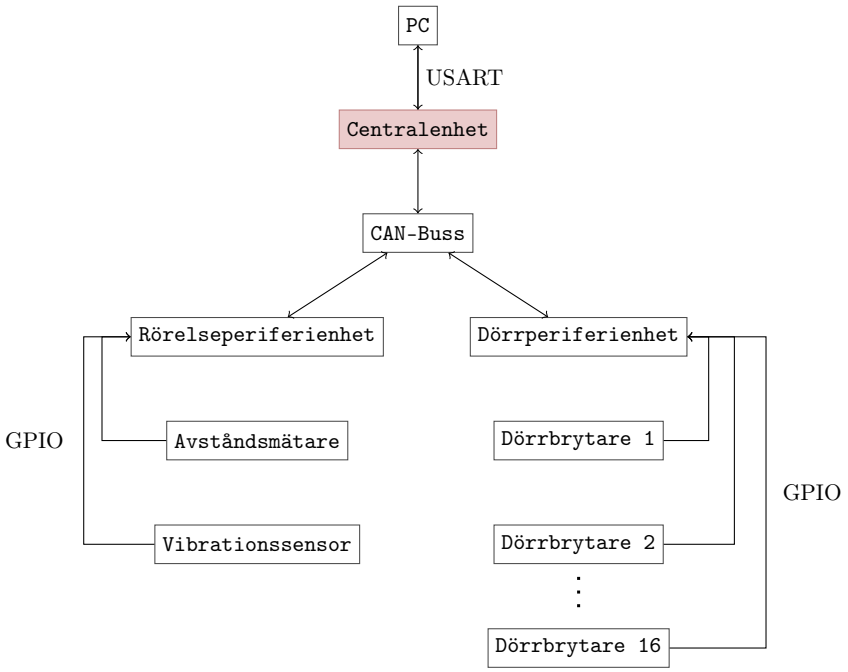
Återuppspelning- och avlyssningsenheten är en enhet som konstant tar emot meddelanden på CAN-bussen. Det senaste 256 mottagna meddelanden sparas i en buffert. Dessa meddelanden kan skrivas ut till en konsol via USART, eller skickas tillbaka ut på CAN-bussen.

2.3.6 Testenhet

Beroende på användarens inmatning antar testenheten rollen av centralenhet eller periferienhet. Enheten låter sedan en användare skicka meddelanden över CAN-bussen.

2.4 Kommunikationsmodell

De olika enheterna kommunicerar med varandra över en CAN-buss. Periferienheterna kopplas direkt till brytare och sensorer, PC kopplas till centralenheten via USART. En överskådlig bild av dataflödet i systemet ges av Figur 1.



Figur 1: Diagram över dataflödet i systemet. Pilriktning antyder kommunikationsriktning.

På CAN-bussen sker kommunikation mellan systemets olika enheter, exempelvis omkonfigurering av en periferienhet eller larmande. USART-kommunikationen sker mellan PC och centralenheten och används för att konfigurera systemet.

2.4.1 Kommunikationsprotokoll

Kommunikationen sker över CAN och protokollets meddelandeinformation placeras i ID fältet av CAN-meddelandet. Varje meddelande har en nödlägesflagga som nollställs i brådskande meddelanden, en kommunikationsriktning som ettställs då meddelandet kommer från styrenheten, meddelandetyp som beskriver datainnehållet och avsändare respektive mottagares ID, beroende på kommunikationsriktning. En överblick av meddelandeinformationen ges i Tabell 1 och en preliminär bild av meddelandetyper ges i Tabell 2 och 3.

Tabell 1: Protokollöverblick

Bit	B_{10}	B_9	B_8	B_7	B_6	B_5	B_4	B_3	B_2	B_1	B_0
Fält	Nödläge	Riktning	Meddelandetyp				Mottagare/Sändare				

Tabell 2: Utgående meddelandetyper

Bitmönster	Meddelandetyp	Data innehåll
0000	Dörr timeout	Dörr ID, Timeout i sekunder
0001	Inaktivera dörrlarm	Dörr ID
0010	Aktivera dörrlarm	Dörr ID
0011	Vibrationskänslighet	Känslighet värde
0100	Vibrationskalibrering	Tomt
0101	*RESERVERAD*	*RESERVERAD*
⋮	⋮	⋮
1111	*RESERVERAD*	*RESERVERAD*

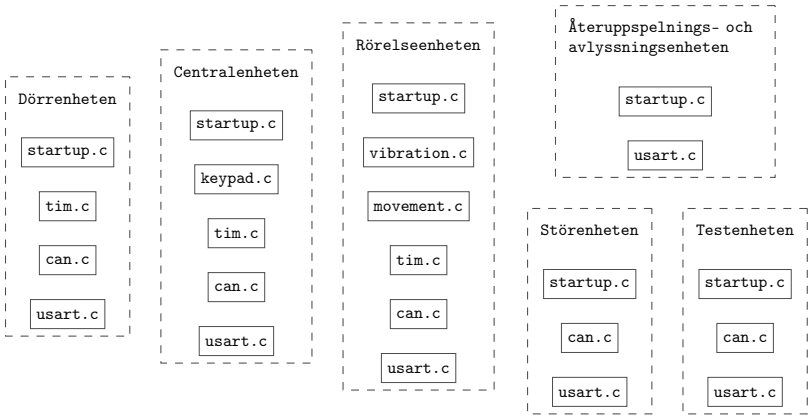
Tabell 3: Ingående meddelandetyper

Bitmönster	Meddelandetyp	Data innehåll
0000	Livstecken	TOMT
0001	Dörrlarm	Dörr ID
0010	Rörelselarm	RESERVERAD
0011	Vibrationslarm	RESERVERAD
0100	Imitationslarm	Meddelandetyp av imiterat meddelande
0101	*RESERVERAD*	*RESERVERAD*
⋮	⋮	⋮
1111	*RESERVERAD*	*RESERVERAD*

Innehållet av fält markerade som "RESERVERADE" är inte användbart för systemet, dock kan dessa användas vid framtida implementeringar. Dessa fält antar alltså inget användbart värde.

2.5 Delsystem

Mjukvaran utvecklad för systemet har delats in i olika delsystem. Delsystemen överskrider enhetsgränserna då samma funktion krävs i olika enheter. En överblick av delsystemen ges i Figur 2.



Figur 2: Överblick av delsystem
[1]

CAN-delsystemet används genomgående i systemet då samtliga enheter kommunicerar över CAN. Systemet abstraherar processen av att initiera CAN-kommunikationen, samt att skapa och skicka meddelanden enligt protokollet definierat i avsnitt 3.4.1. Snarlikt inkluderas USART i alla enheter då seriekommunikation används för felsökning. Delsystemet för timers genererar kontinuerligt avbrott, vilket används för att skicka livstecken och mäta tid sedan förgående livstecken. Rörelseenheten använder sig av separata delsystem som abstraherar avläsning av båda sensorer. Likaså använder sig centralenheten av ett delsystem som abstraherar knappsatsen. Varje enhet har även ett specifikt uppstartssystem som implementerar enhetens huvudlogik.

[1] "startup.c" är unik för varje enhet

2.6 Användarhandledning

Användningen och installationen av larmsystemet bildar en enhetshierarki. Centralenheten är kärnan för hela systemet med diverse periferienheter kopplade till denna. I dagsläget så har två slags periferienheter utvecklats till systemet, en för dörrlarm och en för rörelse- och vibrationslarm. Centralenheten kommunicerar med periferienheterna genom CAN-protokollet som skickas över RJ11-telefonkablar, se Bilaga 1. Dessa kablar skall kopplas till portarna markerade CAN1 på respektive MD407-kort. Utöver detta skall respektive enhetsmjukvara laddas till sammanhörande MD407-kort. Det är dessutom viktigt att erhålla en USB-koppling till centralenheten via USART-kommunikation. Detta för att kunna ange vilka och hur många periferienheter som är kopplade till centralenheten. Dessutom krävs det för att konfigurera och kalibrera utrustning och sensorer som kopplas till periferienheterna genom GPIO.

Att larma av och på sker genom en knappsats där enhets-ID först specificeras följande vilket en lämplig knapp trycks ner; 'A' för att larma på och 'B' för att larma av. USART-kommunikationen mellan PC och centralenheten kan användas för att konfigurera enheter. För att kalibrera rörelseenheten placeras denna på en stationär plats. Därefter skickas ett USART-meddelande som startar kalibreringen. Denna kalibrering mäter avståndet framför sensorn och larmar om annat avstånd upptäcks. Tillåten avvikelse för avståndet kan även konfigureras genom USART.

3 Metod

Metoden bygger på två huvuddelar, den teoretiska delen samt den praktiska delen. Den teoretiska delen innehåller främst genomförd bakgrundsforskning och undersökningar. Dessa är nödvändiga för att kunna gå vidare till den praktiska delen. I praktiska delen beskrivs hur implementation och testning genomfördes. Utvecklingsmiljön CodeLite användes för programutveckling med hjälp av STM-biblioteket. Hårdvarutestning av koden utfördes parallellt med programutvecklingen. Nedan följer en detaljerad beskrivning av metoderna i samtliga delsystem.

3.1 Enhetskommunikation genom CAN och USART

För att möjliggöra kommunikation mellan systemets olika delar utvecklades ett CAN-protokoll. En nödlägesflagga sattes på högsta biten av CAN-meddelandets ID-fält för att angelägna meddelanden skulle få lägre ID, vilket prioriteras på CAN-bussen. För att avgöra riktningen på meddelandet ettställdes den nionde biten om avsändaren var centralenheten. Detta valdes då samtliga meddelanden antingen skickades eller mottogs av centralenheten. Följaktligen krävdes endast ett fält för mottagar- och avsändar-ID.

För att användaren ska kunna interagera med och konfigurera systemet krävdes ännu ett kommunikationssätt. För detta användes USART-gränssnittet. Användarens inmatning på PC skickades således genom en USB-kabel till centralenheten. USART valdes då MD407 har inbyggt hårdvarustöd för gränssnittet vilket redan nyttjades för att ladda över mjukvaran.

3.2 Periferienheterna

De två periferienheterna som användes i larmsystemet var ett dörrlarm och ett rörelselarm.

3.2.1 Rörelseeenheten

Rörelselarmet kopplades till två sensorer, en ultraljudsbaserad avståndsmätare och en vibrationssensor. Dessa kopplades till en kopplingsplatta som i sin tur kopplades till 5V och jord från MD407. För att verifiera funktionaliteten och kvaliteten på avståndsmätaren placerades olika objekt på varierande avstånd framför mätaren. På så vis säkerställdes det att avståndsmätaren gav korrekta värden. Vibrationssensorn kopplades även till kopplingsplattan och testades med variabla vibrationsnivåer. Detta för att endast registrera relevanta vibrationer.

3.2.2 Dörrenheten

Det valdes att dörrenheten skulle stödja upp till 16 dörrar samtidigt. 16 dörrar valdes då 32 stift var lättillgängliga på MD407 och varje dörr behövde två stift var. Dessa 16 dörrar representerades av 16 stift som individuellt kunde anta värde 1 om dörren var öppen eller 0 om dörren var stängd. Kvarstående 16 stift kopplades till lysdioder för att indikera ett lokalt larm på respektive dörr. Vid testning av dörrenheten ansågs det att kortsluta stift var ett lämpligt tillvägagångssätt. Detta då alternativet att ansluta till en dörr var märkbart svårare att implementera.

3.3 Centralenheten

För att binda ihop de tidigare nämnda periferienheterna krävdes en enhet som såg till att dessa kunde konfigureras och skicka larm. Därmed utvecklades en centralenhet kopplad till PC genom USART samt periferienheterna genom CAN-bussen.

Utvecklingen av centralenheten grundades främst på periferienheternas specifikationer, exempelvis larmmeddelanden, konfigurationsinställningar och livstecken. Det grundades också i hur användarens interaktion skulle implementeras. Centralenheten mottog även textmeddelanden över USART för att styra systemet.

3.4 Testning och verifiering

För att kvaliteten av slutprodukten skulle kunna säkerställas har testning använts under arbetets gång. Testerna säkerställde att både hård- och mjukvara fungerade korrekt. Genom verifiering av att delsystemen fungerade korrekt har längre felsökningsuppdrag undvikits.

Tester utvecklades genom att en testprocedur specificerades. Testproceduren ämnades att efterlikna ett delsystems bruksförhållanden för att notera dess beteende. Utöver detta har procedurer utvecklats som simulerade felaktiga bruksförhållanden samt möjliga cyberattacker, exempelvis återspelningsattacker. Testproceduren antecknades i en testmall som fylldes i vid utförande av tester.

Genomförande av tester har skett vid närvarande av minst två projektmedlemmar, varav minst en ej medverkat i utvecklingen av systemet som testades. Efter att medverkande medlemmar utförde en testprocedur, fyllde dessa i resultaten i den tillhörande testmallen. Därefter tolkades resultaten i analyssektionen av testmallen.

Beroende på testresultatet vidtogs olika åtgärder. Vid test där förväntat beteende noterades tillämpades ingen direkt åtgärd, men systemet fortsatte att återmkommande testas. Då systemet ej fungerade som förväntat har en felkälla sökts. Felen bestod oftast av felaktig programkod eller inkorrekt förståelse av hårdvaran. Efter att ett fel åtgärdades upprepades testet där felet uppstod.

Tre enheter utvecklades även i testningssyfte. En störenhet skapades med syfte att testa systemets bruk då det skedde störningar på CAN-bussen. Under implementationen av denna enhet valdes det att nyttja slumpgeneratorn på MD407 för att generera slumpmässiga meddelanden. Detta valdes då störningar i system beter sig slumpmässigt. En återuppspelning- och avlyssningsenhet utvecklades i syfte att testa systemets försvar mot återuppspelningsbaserade attacker, samt underlätta felsökande av CAN-kommunikation. Enheten använde ej samma bibliotek för CAN-kommunikation som resterande enheter då den var ämnad till att kunna attackera ett godtyckligt system. En testenhet utvecklades för att utföra test som krävde enheter som ej hade implementerats eller verifierats vid testtillfällena.

4 Resultat och diskussion

Projektet hade i syfte att konstruera ett larmsystem, säkrat mot moderna intrångsmetoder grundade i systemets kommunikation. Samtliga enheter uppfyllde detta syfte. Centralenheten konstruerades med alla periferienheternas specifikationer implementerade. Kommunikationssystemen fungerade som förväntat under vanliga förhållanden. Dörrenheten larmade lokalt följt av att ett larmmeddelande skickades till centralenheten. Rörelseenheten visade klart att både avstånds- och vibrationssensorn fungerade korrekt. Testerna underlättade och minimerade felsökningen av programutvecklingen avsevärt. En detaljerad bild av resultaten ges och diskuteras nedan.

4.1 Enhetskommunikation genom CAN och USART

Meddelanden skickade över CAN-bussen mottogs korrekt, både innehåll och meddelandetyp var intakta. Likaså skickades och mottogs data korrekt över USART. Initialt framträdde problem inom USART-systemet då icke-blockerande meddelanden ej mottogs. Detta problem upphörde efter en kodrevison.

Testresultat (se Bilaga 2) verifierar att CAN- och USART-systemen fungerade korrekt. Kodrevisionen bedöms ha löst felet i USART-systemet. En möjlig förbättring hade varit att möjliggöra emulering av CAN-kommunikation över USART i felsökningssyfte. Ett sådant simuleringsläge skulle effektiviserat testprocessen genom att minska antalet MD407 som krävdes per test.

Under imitationstestet (se Bilaga 3) avlästes imitationsattacker korrekt och larm slogs. I fallet då periferienheter imiterades skickade enheterna ett larmmeddelande till centralenheten som mottogs korrekt. Om centralenheten imiterades upptäcktes detta av centralenheten.

Systemet identifierar bevisligen imitationsattacker och larmar korrekt då de sker. Följaktligen är det inte möjligt att stänga av larm genom att imitera centralenheten. Däremot är systemet mottagligt för andra typer av attacker som skulle kunna motverkas i kommunikationsystemet. Exempelvis skulle en periferienhet kunna frånkopplas från bussen samtidigt som en enhet som imiterar dess livstecken kopplas in på bussen. En sådan attack skulle kunna motverkas genom att bifoga oförutsägbar data i livstecknen som verifieras av CAN-systemet.

Systemets funktion testades även under icke-förväntade förhållanden då CAN-bussen var överbelastad (se Bilaga 13). I dessa förhållanden tog meddelanden markant längre tid på sig att mottas. Meddelanden där nödlägesflaggan var nollställd anlände hastigare. Emellanåt aktiverades imiteringslarmet då höga nivåer av brus befann sig på bussen. Utifall brusnivån blev tillräckligt hög aktiverades även frånkopplingslarmet.

Under tunga förhållanden fungerade systemet måttligt, eller inte alls. Detta är ej optimalt, men ej förödande för larmets säkerhet. De meddelanden som drabbas kraftigast är icke-brådskande meddelanden, olikt larmmeddelanden som kommer igenom under tyngre brus. En viktig detalj är att under tungt brus kan larm aktiveras då någon enhet ej nås, eller då bruset efterliknar ett imiterat meddelande. Detta bedöms vara acceptabelt då brus kan orsakas av en förbrytare med ändamål att förhindra aktivering av larm. I detta scenario är det föredragna beteendet att slå larm, även om falsklarm riskeras på en buss med mycket störningar.

Sammanfattningsvis bedöms systemet uppfylla de mål som ställts utan problem. Däremot finns fortfarande möjliga förbättringar inom felsökning, säkerhet, samt under tunga förhållanden.

4.2 Periferienheterna

Tack vare en grundlig implementation av CAN-protokollet, var det möjligt för periferienheterna att korrekt kommunicera med centralenheten. Nedan följer en presentation av de enskilda periferienheternas resultat.

4.2.1 Rörelseenheten

Avståndsmätaren mätte avståndet till olika objekt och bedömde om avståndet var tillåtet eller ej. Om avståndet ej var tillåtet skickades ett larmmeddelande via CAN-bussen till centralenheten. Kalibreringsfunktionen ändrade korrekt det tillåtna avståndet till andra objekt.

Resultatet av avståndsmätaren blev som förväntat. Rörelseenheten skulle skicka ett larmmeddelande när en rörelse inträffade, vilket visades regelbundet i testresultaten (se Bilaga 10 och 11). När ett larmmeddelande skickades innebar det att ett objekt befann sig utanför det tillåtna intervallet. Detta antydde att en rörelse befann sig i rummet. Utan kalibreringsfunktionen hade det varit omöjligt att använda avståndsmätaren effektivt eftersom den möjliggjorde användning i godtyckliga omgivningar. Rörelsesensorn hade kunnat ge ett exaktare värde genom fler tester i olika omständigheter.

Vibrationssensorn visade i de flesta fall om det avlästes vibrationer i en larmad miljö. I vissa fall fångades vibrationer utanför den larmade miljön och tolkades som relevanta vibrationer. När vibrationssensorn upptäckte vibrationer skickades ett larmmeddelande via CAN-bussen till centralenheten. Känslighetsfunktionen gjorde det möjligt att i de flesta fall justera känsligheten för att undvika larm vid irrelevanta vibrationer.

Vibrationssensorn har haft problem med att ställas in till lämplig känslighetsnivå. Antingen avlästes för svaga eller för få vibrationer. Möjligtvis hade systemet förbättrats genom att byta ut vibrationssensorn mot en som kan finjusteras.

4.2.2 Dörrenheten

De periodiska signaler som skickades för att testa om anslutningen till centralenheten fungerade och systemet larmade om de inte kom fram under ett bestämt tidsintervall. Dörrenheten kunde baserat på om en dörr var larmad eller ej starta larmet eller ignorera dörren. Varje dörr kunde hanteras individuellt, till exempel hade varje dörr en egen larmstatus och tid den varit öppen.

Dörrenhetens implementation var lyckad. Förväntningen var att systemet skulle ha förmågan att hantera kontakten med samtliga dörrar, hantera status likt om dörrarna är larmade samt larma både lokalt och sedan globalt. Alla dessa uppdrag förmår dörrenheten att utföra. Testen som utfördes (se Bilaga 8 och 11) bekräftade att enheten larmade i samtliga tilltänkta fall. Möjligen skulle ett bredare mål specificerats. Systemet blev nu enklare att skapa men med mindre säkerhet. I dörrenhetens mening skulle detta betyda att använda fler dörrar i systemet eller extra kontroller för att undvika attacker. Exempelvis skulle

ytterligare meddelanden från centralenheten kunna låsa och låsa upp dörrar samt om ett larm aktiveras.

4.3 Centralenheten

Enheten ansvarar för all trafik från USART i dess huvudlogik där meddelandena tolkas och delas upp utefter dess meddelandetyp. Uppdelningen bestämmer sedan vilken funktion som ska exekveras med meddelandet. Till exempel om en enhet konfigureras så skickas användarens inställningar vidare till rätt enhet.

Samma sak gäller åt det motsatta hållet. Om ett meddelande kommer från periferienheterna genom CAN-bussen så tolkas även dessa och en lämplig funktion tillämpas. Exempelvis säkerställde man genom tester (se Bilaga 11) att centralenheten skilde mellan ett meddelande som skulle larmas och ett vanligt livstecken genom nödlägesflaggan i CAN-meddelandet. Livstecken från periferienheterna samlades hos centralenheten separat och om någon enhet inte skickade något tecken under 300 millisekunder larmade centralenheten, detta säkerställdes genom ett stort systemtest (se Bilaga 7). Centralenheten innehöll ett fält av 32 bitars heltal som visade hur mycket tid det var kvar tills ett frånkopplingslarm utlöstes. I slutet av huvudlogiken gick centralenheten igenom detta fält och fyllde på tid till de enheter som skickade livstecken.

Utvecklingen av centralenheten grundades huvudsakligen på de minimikrav som föreslogs i projektets syfte. Detta innebar två kriterier: Att förse periferienheterna med alla definierade funktionskrav och att förse användaren med ett gränssnitt för att konfigurera systemet. Det finns fortfarande en stor katalog av nya säkerhetsfunktioner som kan implementeras i systemet, detta kommer förslagsvis innebära stora förändringar i centralenheten. Dessa revisioner kommer inte påverka andra delar av systemet då implementeringar i centralenheten endast ses som tillägg till sin huvudlogik. Ett förslag på detta kan vara ett bättre utbyggt användargränssnitt som i nuläget endast består av en terminal kopplad genom USART till centralenheten. För att implementera ett bättre användargränssnitt, exempelvis ett grafiskt, krävs det endast en ombyggnad av hur huvudlogiken tar emot användarens inmatning. Resten av huvudlogiken kommer därmed inte påverkas av denna vidareutveckling.

4.4 Testning och verifiering

Förståelsen för hur larmsystemet och dess delenheter fungerade breddades i samband med att testerna utfördes.

Störenheten som användes för att störa systemet implementerades framgångsrikt. Testerna som utfördes med enheten (se Bilaga 13) försäkrade att larmsystemet fungerar trots kommunikationstörningar. Testerna med återuppspelnings- och avlyssningsenheten (se Bilaga 3) bidrog kraftigt till systemets utveckling. Detta då dess positiva resultat lade grunden för att förhindra en attack på systemets säkerhet. Testenheten har använts för att skicka livstecken och andra CAN-meddelanden (se Bilaga 7). Enheten möjliggjorde tester som krävde icke-implementerade enheter vilket effektiviserade testnings- och utvecklingsprocessen.

Ett säkrare och mer komplext larmsystem kunde utvecklats då flertalet implementationer var möjliga, framförallt gällande periferienheterna. Exempelvis skulle man kunnat utveckla en annan rörelsesensor som kunde detektera rörelser

runt sin axel och inte endast rakt framför sig. I samband med denna utvecklingen hade mer avancerade och djupgående tester behövts genomföras. Detta hade även gällt för ytterligare implementationer. Som följd hade kvaliteten på larmsystemet med största sannolikhet ökat och därmed hade möjligheten för en förbrytare att kringgå systemet minskat avsevärt.

5 Slutsatser

Projektets syfte, att säkra mot moderna intrångsmetoder, är till stor del uppnått. Systemet är säkrat mot de intrångsmetoder som förebyggts mot, dock är det möjligt att en förbrytare med god kunskap om systemet skulle kunna kringgå larmsystemet. Samtliga mål har uppnåtts, det finns dock ytterligare funktioner som skulle kunna implementeras. Exempelvis användarvänlighet då det saknas grafiskt gränsnitt.

6 Referenser

[1] F. Östman, "Md407 - en arm-baserad laborationsdator för utbildning," Institutionen för data -och informationsteknik Chalmers tekniska högskola, Tech. Rep., 2014.

[2] B. Rådet. (2022) Statistik för bostadsinbrott. [Online]. Available: https://bra.se/statistik/statistik-utifran-brottstyper/bostadsinbrott

[3] S. offentliga utredningar. (2016) Digitaliserings effekt på individ och samhälle. [Online]. Available: https://www.regeringen.se/contentassets/bf87c5fce6fc4f9a889d57ea2e46a27d/sou-2016_85_webb-pdf-med-framsida.pdf

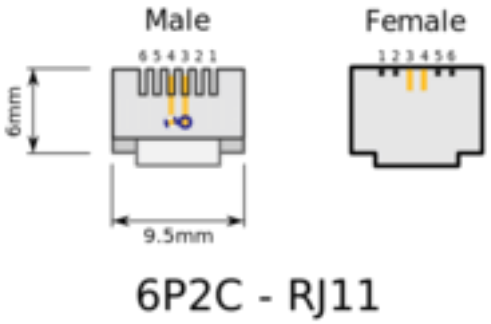
[4] T. Harris. (2022) How burglar alarms work. [Online]. Available: https://home.howstuffworks.com/home-improvement/household-safety/burglar-alarm.htm

[5] C. P. Szydlowski, *CAN Specification 2.0: Protocol and Implementations*, SAE International, 1992.

[6] M. G. L. Eric Peňa. (2020) Uart: A hardware communication protocol understanding universal asynchronous receiver/transmitter. [Online]. Available: https://www.analog.com/en/analog-dialogue/articles/uart-a-hardware-communication-protocol.html

[7] K. Lab. (2022) What is a replay attack? [Online]. Available: https://www.kaspersky.com/resource-center/definitions/replay-attack

7 Bilagor



Bilaga 1: Specifikation över en RJ11-kabel och -port

CAN funktion test

Grupp 13
Datum: 22 September 2022 **Tid:** 14:08

Testfall-id: 000
Testobjekt: CAN bussen
Testares namn: Rachel Samuelsson och Samuel Runmark Thunell

Beskrivning

Testar att CAN kommunikation fungerar under normala förhållanden. Kräver 3 MD407 kort, 2 RJ11 kablar samt 1 RJ11 förgrening.

1. En av de tre MD407 utses till centralenhet.
2. RJ11 förgreningen ansluts till CAN1 på centralenheten.
3. RJ11 kablar ansults från förgreningen till CAN1 på resterande MD407.
4. CAN testmjukvara laddas upp till varje MD407.
5. Centralenhet utses till centralenhet i testmjukvaran.
6. ID delas till resterande enheter i testmjukvaran.
7. Mjukvaruanvisningarna följs för att skicka en av varje meddelandetyp från varje enhet. För varje meddelande noteras följande.
    - Når meddelandet den korrekte mottagaren, och ingen annan?
    - Har mottaget meddelande korrekt meddelandetyp och data?

Resultat

Samtliga meddelanden skickades till korrekt mottagare och ingen annan, med rätt meddelandetyp och data.

Analys

CAN kommunikation fungerar som förväntat under normala förhållanden.

1

Bilaga 2: Test angående CAN-protokollet

CAN enhets imitation test

Grupp 13
Datum: 22 September 2022 **tid:** 16:07

Testfall-id: 001
Testobjekt: CAN bussen
Testares namn: Rachel Samuelsson och Samuel Runmark Thunell

Beskrivning

Testar om imitering av anslutna enheter (som kan komma ske genom återspelningsattacker) upptäcks och larmas. Kräver 3 MD407 kort, 2 RJ11 kablar samt 1 RJ11 förgrening.

Deltest 1

1. En av de tre MD407 utses till centralenhet.
2. RJ11 förgreningen ansluts till CAN1 på centralenheten.
3. RJ11 kablar ansults från förgreningen till CAN1 på resterande MD407.
4. CAN testmjukvara laddas upp till varje MD407.
5. Centralenhet utses till centralenhet i testmjukvaran.
6. Samma id delas till resterande enheter i testmjukvaran.
7. En av periferienheterna skickar ett godtyckligt meddelande.
8. Inkommande meddelanden på centralenheten avläses.

Deltest 2

1. RJ11 kablar ansults direkt mellan två MD407.
2. CAN testmjukvara laddas upp till varje MD407.
3. Båda enheter utses till centralenhet i testmjukvaran.
4. En av enheterna skickar ett godtyckligt meddelande.
5. USART konsolen av andra enheten avläses.

Resultat

Deltest 1

På centralenheten avläses en konstant ström av inkommande imiteringslarm.

Deltest 2

På enheten skrivs det ut ett meddelande om att enheten blivit imiterad.

1

Bilaga 3: Test angående CAN-immitering (utan analys)

Analys

I periferienhetens fall då meddelande mottags som hävdas komma från den enhet som mottar meddelandet larmar denne enheten centralenheten. I centralenhetens fall kallas återanropsfunktionen korrekt. Därav verifieras att systemet är skyddat mot återuppspelningsattacker.

Anledningen till strömmen av imiteringslarm är alldeles säkert att de två enheterna med samma id läser varandras larmmeddelanden och därav fortsätter skicka larm. Detta bekräftas av att meddelandströmmen stoppas då en av enheterna frånkopplas.

2

Bilaga 4: Analys av test angående CAN-immitering

Centralenhet In/Utmatning

Grupp 13
Datum: 11 Oktober 2022 **tid:** 15:43

Testfall-id: 002
Testobjekt: Centralenheten
Testares namn: Samuel Runmark Thunell och Rachel Samuelsson

Beskrivning

Testar om inmatning genom USART, samt konfigurations meddelanden fungerar korrekt. Kräver 2 MD407 kort samt 1 RJ11 kabel.

1. En av de tre MD407 utses till centralenhet.
2. RJ11 förgreningen ansluts till CAN1 på centralenheten.
3. RJ11 kablar ansults från förgreningen till CAN1 på resterande MD407.
4. Centralenhetens mjukvara laddas upp via USART.
5. Återuppspelning- och avläsningsmjukvaran laddas upp till andra enheten via USART.
6. Användarhänvisningarna på centralenheten följs för att skicka flertalet meddelanden med olika typ och data.
7. Användarhänvisningarna återuppspelning- och avläsningsenheten följs för att läsa av innehållet av mottagna meddelanden.
8. Meddelandeinnehållet jämförs mot det som förväntats skickas.

Resultat

Då andra bokstaven matades in över USART skickade centralenhet ett oväntat meddelande.

Analys

Centralenheten hanterar ej användarinmatning korrekt. Troligen beror detta på fel i kod. Efter en analys och kodrevis förväntas felet upphöra, se test 003.

1

Bilaga 5: Första test av centralenhets in- och utmatning

Centralenhet In/Utmatning

Grupp 13
Datum: 11 Oktober 2022 **tid:** 16:22

Testfall-id: 003
Testobjekt: Centralenheten
Testares namn: Samuel Runmark Thunell och Rachel Samuelsson

Beskrivning

Testar om inmatning genom USART, samt konfigurations meddelanden fungerar korrekt. Kräver 2 MD407 kort samt 1 RJ11 kabel.

1. En av de tre MD407 utses till centralenhet.
2. RJ11 förgreningen ansluts till CAN1 på centralenheten.
3. RJ11 kablar ansults från förgreningen till CAN1 på resterande MD407.
4. Centralenhetens mjukvara laddas upp via USART.
5. Uppspelning och avläsnings mjukvaran laddas upp till andra enheten via USART.
6. Användarhänvisningarna på centralenheten följs för att skicka flertalet meddelanden med olika typ och data.
7. Användarhänvisningarna återuppspelning- och avläsningsenheten följs för att läsa av innehållet av mottagna meddelanden.
8. Meddelandeinnehållet jämförs mot det som förväntats skickas.

Resultat

De meddelanden som angavs till centralenheten via USART mottogs av återuppspelning- och avläsningsenheten.

Analys

Inmatningen av data, samt dess tolkning i centralenheten fungerar korrekt. Dessutom överförs data korrekt på CAN-bussen.

Bilaga 6: Andra test av centralenhets in- och utmatning

Centralenhet Livstecken

Grupp 13
Datum: 11 Oktober 2022 **tid:** 16:53

Testfall-id: 004
Testobjekt: Centralenheten
Testares namn: Samuel Runmark Thunell och Rachel Samuelsson

Beskrivning

Testar om inmatning genom USART, samt konfigurations meddelanden fungerar korrekt. Kräver 2 MD407 kort samt 1 RJ11 kabel.

1. En av de tre MD407 utses till centralenhet.
2. RJ11 förgreningen ansluts till CAN1 på centralenheten.
3. RJ11 kablar ansults från förgreningen till CAN1 på resterande MD407.
4. Centralenhetens mjukvara laddas upp via USART.
5. Testmjukvaran laddas upp till andra enheten via USART.
6. Användarhänvisningarna testmjukvaran följs för att anta ID 0.
7. Användarhänvisningarna testmjukvaran följs för att börja kontinuerligt skicka livstecken.
8. Användarhänvisningarna på centralenheten följs för att ange antalet anslutna enheter. Antalet sätts till 1.
9. Notera om larm utlöses.
10. Koppla från andra enheten.
11. Notera om larm utlöses.
12. Koppla tillbaka andra enheten.
13. Notera om larm utlöses.

Resultat

Då antalet enheter konfigurerades till ett skedde inget larm. Efter att testenheten frånkopplats skedde kontinuerligt larm. Då testenheten kopplades tillbaks upphörde larmen.

Analys

Livsteckens funktionen fungerar som förväntat.

1

Bilaga 7: Test av centralenhets frånkopplingslarm

Dörrenhettest

Grupp 13
Datum: 17 Oktober 2022 **tid:** 11:01

Testfall-id: 005
Testobjekt: Dörrenheten
Testares namn: Olof Forsberg , Rachel Samuelsson, Samuel Runmark Thunell

Beskrivning

Testar dörrenhetens förmåga att slå lokala alarm.

1. Dörrenhetens mjukvara laddas in i MD407-enhet.
2. En annan MD407-enhet laddas in med centralenhetens kod.
3. Dessa två ansluts med en RJ11-kabel.
4. Anslut lampor till GPIOD.
5. Starta mjukvaran på centralenheten
6. Aktivera larmet för en dörr samt öppna den.
7. Vänta och se om en lokal larmsignal slås.
8. Vänta och se om en global larmsignal slås.

Resultat

Både lokalt samt globalt larm aktiverades.

Analys

Dörrenheten kan korrekt läsa av om dörr är öppen, larmad samt aktivera larm.

1

Bilaga 8: Test av dörrenhetens huvudfunktionalitet

Timeouttest

Grupp 13
Datum: 17 Oktober 2022 **tid:** 11:15

Testfall-id: 006
Testobjekt: Dörrenheten
Testares namn: Olof Forsberg, Rachel Samuelsson, Samuel Runmark Thunell

Beskrivning

Testar för timeout på två dörrar samtidigt

1. Ladda in dörrenhetens mjukvara på en MD407-enhet
2. Ladda in centralenhetens mjukvara på en annan MD407-enhet
3. Anslut lampor till GPIOD
4. Starta mjukvaran på centralenheten
5. Ställ timeout på en dörr till 10 sekunder
6. Ställ timeout på en annan dörr till 15 sekunder
7. Aktivera båda dörrarna
8. Vänta och se om timout sker med 5 sekunders mellanrum

Resultat

Larmen aktiverades med 5 sekunders mellanrum. Detta 10 respektive 15 sekunder efter timout ställdes in för dörrarna.

Analys

Systemet fungerar som tänkt med timouts som sker efter tänkt tid.

1

Bilaga 9: Test av dörrenhetens olika timeouts

Rörelseenhetens test

Grupp 13
Datum: 13 oktober 2022 **Tid:** 15:07

Testfall-id: 007

Testobjekt: rörelsesensorn och vibrationssensor

Testares namn: Mohammad Mourad, Rachel Samuelsson och Samuel Runmark Thunell

Beskrivning

Testar om rörelsesensorn och vibrationssensor fungerar tillsammans, kräver 3 MD407 kort, 3 RJ11 kablar, samt 1 RJ11 förgrening, rörelsesensorn, vibrationssensor och kopplingsplattan.

1. En av de tre MD407 utses till centralenhet.
2. En av de tre MD407 utses som rörelseenheten.
3. En av de tre MD407 utses som återuppspelning- och avläsningsenheten.
4. RJ11 förgreningen ansluts till centralenheten och återuppspelning- och avläsningsenheten.
5. RJ11 kablar ansults från förgreningen till rörelseenheten på resterande MD407.
6. Rörelseenhetens programvara laddas till en MD407 kort.
7. Centraleneheten programvara laddas till ett annat MD407 kort.
8. Rörelsesensorn och vibrationssensor ansluts till kopplingsplattan.
9. Ett papper placerades framför rörelsesensorn.
10. Olika objekt resulterade vibrationer.
    - Känner vibrationssensor vibrationer?
    - Mäter rörelsesensorn avstånd till papper?
    - Funkar kaliberingsfunktionen?

Resultat

Samtliga tester visade korrekt avstånd med hjälp av avståndsmätare och vibrationssensor regerade med vibrationer

Analys

Rörelseenheten funkar som förväntat under normala förhållanden.

Bilaga 10: Test av rörelseenheten huvudfunktionalitet

Systemtest

Grupp 13
Datum: 19 Oktober 2022 **tid:** 13:31

Testfall-id: 008
Testobjekt: Centralenheten, Röreleseenheten och Dörrenheten
Testares namn: Samtliga medlemmar

Beskrivning

Testar systemet i sin helhet. Kräver 3 MD407, 2 RJ11 kablar samt 1 RJ11 förgrening.

1. Samtliga MD407 tilldelas en roll.
2. Motsvarande mjukvara laddas upp till varje MD407.
3. Avståndssensor och vibrationsensorn kopplas på kopplingsplatta och ansluts till röreleseenheten.
4. Sladdar kopplas löst till 5V på dörrenheten.
5. Lampor (eller 7 segmentsdisplay) kopplas till GPIOD 0-7 på dörrenheten.
6. Röreleseenheten ges ID 0.
7. Dörrenheten ges ID 1.
8. Centralenheten loggas in på genom knappsatsen.
9. Antal anslutna enheter konfigurerar till två på centralenheten.
10. Notera om livsteckenslarm uppstår.
11. Konfigurera timeout för dörr 0 och 1 via centralenheten.
12. Aktivera dörr 0 och 1 via centralenheten.
13. Avvakta och notera om larm uppstår.
14. Kortslut E0 och E1 med 5V kablarna på dörrenheten.
15. Avvakta och notera om larm uppstår.
16. Avaktivera dörr 0 och 1 via centralenheten.
17. Placera ett solitt objekt framför avståndssensorn.
18. Sätt avståndssensorns avvikelse till 2cm via centralenheten.
19. Notera om larm uppstår.
20. För godtyckligt objekt mellan avståndssensorn och pappret.
21. Notera om larm uppstår.
22. Skaka kopplingsplatta.
23. Notera om larm uppstår.

Bilaga 11: Systemtest (utan analys)

Resultat

- Inga larm efter antal enheter sätts till 2.
- Inga larm efter dörr timeouts.
- Larm efter rätt tid efter dörrar öppnats, lokalt och till central.
- Inga larm efter dörrar avaktiveras, lokalt eller central.
- Larm uppstår vid rörelse framför avståndssensorn.
- Larm uppstår vid vibration.

Analys

Systemet fungerar som förväntat.

2

Bilaga 12: Analys systemtest

Testning av en störenhets påverkan på larmsystemet

Grupp 13
Datum: 2022-10-19 **tid:** 15:31

Testfall-id: 009

Testobjekt: Störenheten

Testares namn: Jonatan Gunnarsson, Samuel Runmark Thunell, Mohammad Mourad, Rachel Samuelsson

Beskrivning

Testar om störenheten lyckas skicka en konfigurerbar mängd randomiserade meddelanden till en randomiserad enhet med ett konfigurerbart intervall. Dessutom testas dessa meddelandens påverkan på larmsystemets kommunikation, dvs. om systemet lyckas larma trots flertalet meddelanden på CAN-bussen. Störenhetens funktion är att försöka "störa" CAN-bussen i larmsystemet.

1. Kopplade ett komplett larmsystem enligt systemtest, men bytte ut rörelseenheten mot en störenhet.
2. Kopplade upp systemet med två st PC, störenhet till den ena och dörr- och centralenhet till den andra.
3. Initierade systemet och började skicka meddelanden från störenheten på CAN-bussen.
4. Triggar ett alarm på dörrenheten och observerar om systemet slår larm.

Resultat

Då störenheten skickade meddelanden kunde fortfarande larmsystemet slå larm som vanligt, samt att systemet märkte av att ytterligare en enhet skickade meddelanden, vilket även det slogs larm om.

Analys

Störenheten kan anses fungera som förväntat samt att dess påverkan på systemet är korrekt. Randomiserade meddelanden skickas och mottags och systemet larmar om att en annan enhet skickar meddelanden. Systemet larmar även om ett annat larm aktiveras.

Bilaga 13: Testning av en störenhets påverkan på larmsystemet