Relazione Embedded Systems: Modellazione di un Sistema di Allarme con SysML

Giovanni Burbi

16 febbraio 2023

Sommario

In questo progetto è stato modellato un sistema di sicurezza per abitazioni private. Per la realizzazione dell'elaborato è stato utilizzato il linguaggio di modellazione SysML, il quale estende UML in ottica di progettazione, sia hardware che software, di sistemi. Il processo di modellazione comprende sia aspetti strutturali del sistema che aspetti funzionali, come per esempio la reazione della compagnia di sicurezza quando viene rilevata un'intrusione in un'abitazione. Inoltre sono stati inseriti alcuni vincoli non-funzionali arbitrari. L'obiettivo di questo lavoro è quello di esplorare le varie tipologie di diagrammi che mette a disposizione SysML, così da creare diverse prospettive dalle quali si può progettare e studiare un sistema complesso. Questo processo di sviluppo si inserisce nel contesto del Model-Driven Engineering, il quale comprende anche l'uso di metodi formali, come le reti di petri tempificate, per modellare e analizzare i vincoli non-funzionali del sistema. I tools grafici per la realizzazione dei diagrammi SysML che sono stati utilizzati sono Papyrus e Visual Paradigm Online. Mentre per la realizzazione della rete di petri è stato utilizzato Oris 1.

1 Diagramma dei Requisiti

Il primo passo della modellazione consiste nel definire i requisiti del sistema di allarme, i quali servono a formalizzare i bisogni degli utilizzatori in termini di funzionalità, struttura e vincoli che il sistema dovrà soddisfare. Per la formalizzazione di questi è stato usato il diagramma dei requisiti di SysML, il quale fornisce una rappresentazione grafica dei requisiti in forma testuale, delle loro associazioni e dei vincoli che devono rispettare.

I requisiti possono essere distinti in 3 tipologie:

- Requisiti strutturali
- Requisiti comportamentali o funzionali
- Requisiti non-funzionali

In figura 1 viene mostrato come le tipologie sono state suddivise.

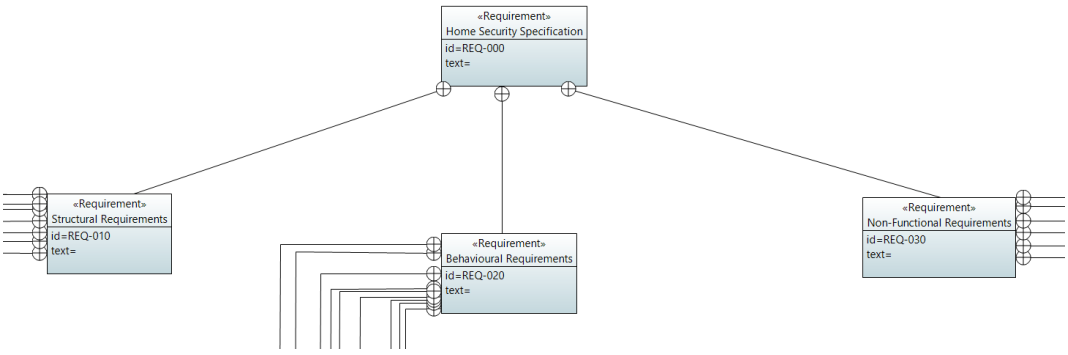

Figura 1: Diagramma dei requisiti: Suddivisione delle tipologie con Papyrus

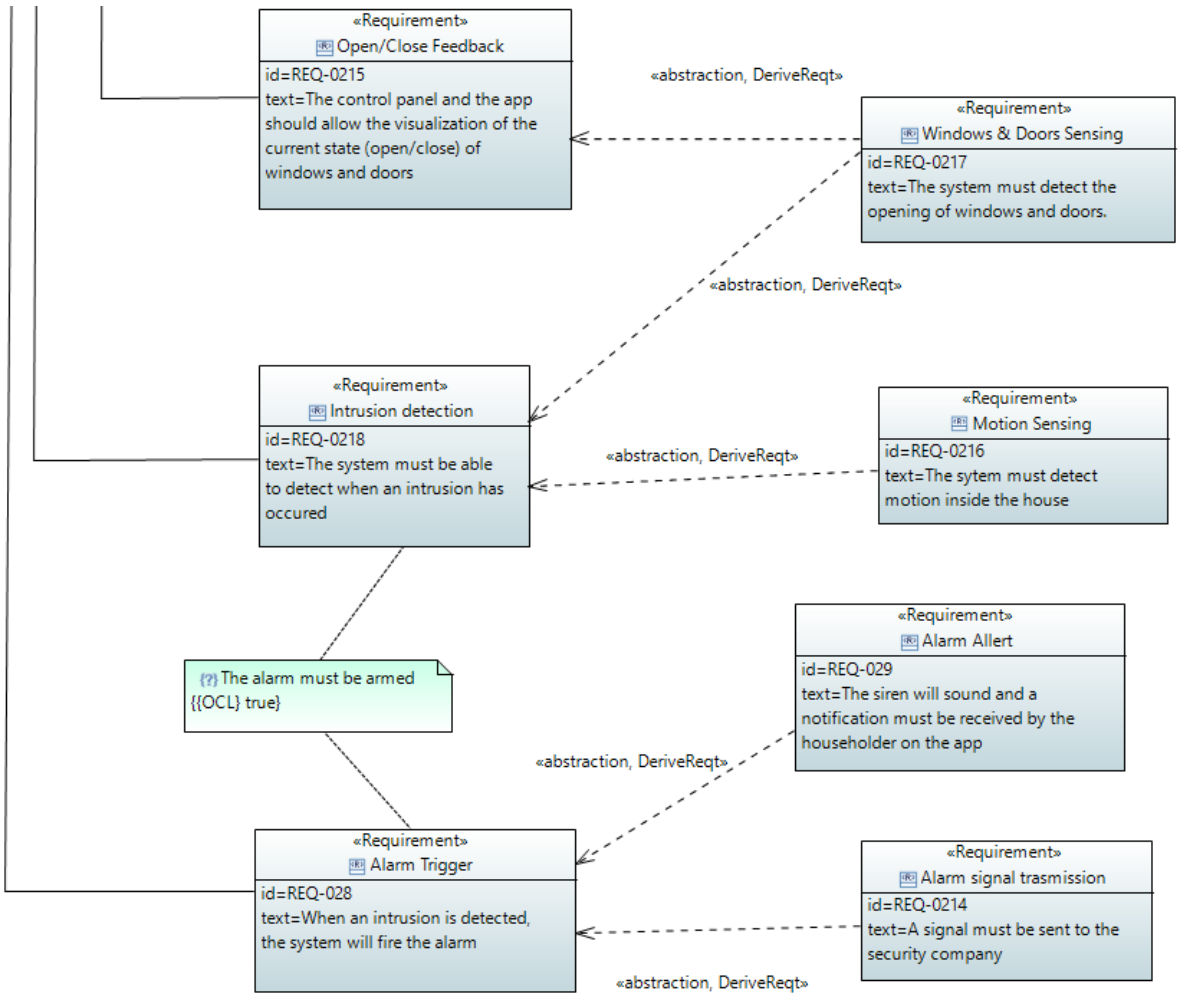

Figura 2: Esempio di alcuni requisiti comportamentali del sistema e le relazioni fra loro

Per motivi di spazio, in figura 2 vengono mostrati solo alcuni requisiti comportamentali. Questi requisiti impongono che il sistema deve permettere la visualizzazione dello stato delle finestre e delle porte (aperte o chiuse) sia dall'applicazione che dal pannello di controllo installato nell'abitazione. Per fare questo il sistema deve essere in grado di rilevare l'apertura di porte e finestre. Quest'ultimo requisito, insieme alla capacità di identificare movimento all'interno dell'abitazione, contribuisce anche al requisito richiesto dal sistema di essere in grado di rilevare eventuali intrusioni.

Il requisito di rilevazione delle intrusioni ha come vincolo, rappresentato dal blocco in verde, il fatto che il sistema di allarme sia stato armato in precedenza. Questo stesso vincolo è presente anche nel requisito di fare scattare l'allarme una volta che una possibile intrusione sia stata rilevata. Come si può vedere, l'attivazione dell'allarme deve comprendere il suono della sirena, la ricezione di una notifica sull'applicazione del sistema di allarme installata sul telefono del proprietario di casa e l'invio di un segnale di allarme alla compagnia di sicurezza responsabile.

Per l'intero diagramma dei requisiti che comprende i restanti requisiti funzionali, quelli strutturali e non-funzionali, si rimanda al progetto su GitHub.

2 Diagramma dei Casi d'Uso

La modellazione del comportamento (componente funzionale) del sistema è supportata da diversi diagrammi che offrono diverse prospettive del sistema e degli attori intorno ad esso.

In particolare, uno di questi è il diagramma dei casi d'uso che è utile per identificare chi sono gli attori e come essi interagiscono con il sistema, dal punto di vista della usabilità.

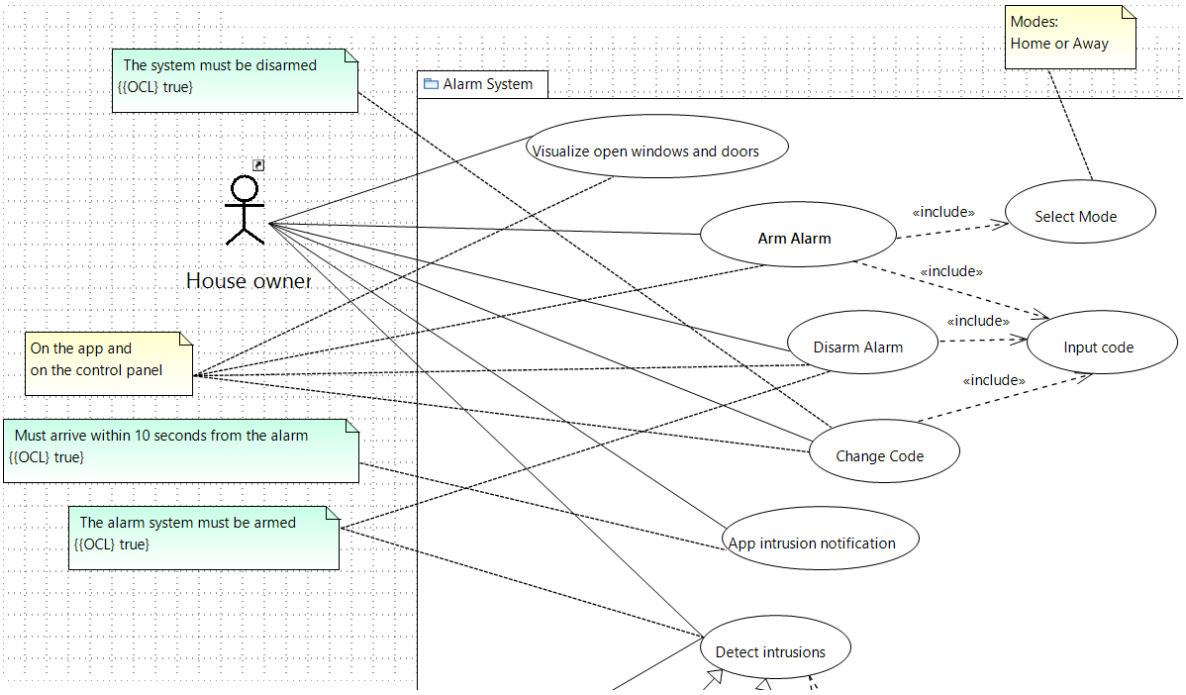

Figura 3: Casi d'uso riguardanti il proprietario della casa in cui è installato il sistema di allarme

In figura 3 sono mostrati graficamente i casi d'uso e alcuni vincoli che riguardano l'interazione fra il proprietario dell'abitazione e il sistema estratti dai requisiti definiti precedentemente nel diagramma dei requisiti. Possiamo vedere che è stato modellato il fatto che il sistema d'allarme permette al proprietario di visualizzare quali porte e finestre sono aperte e di poter armare o disarmare l'allarme inserendo il corretto codice. In particolare il proprietario può selezionare una modalità, fra "home" e "away", quando arma il sistema. Il proprietario può anche cambiare il codice quando il sistema è disarmato immettendo il vecchio codice e poi specificando quello nuovo. Tutti i casi d'uso descritti in precedenza possono essere fatti dal proprietario interfacciandosi sia dall'applicazione che dal pannello di controllo del sistema di allarme. Inoltre, il sistema, quando è armato, permette al proprietario di casa di identificare intrusioni e di ricevere una notifica sull'applicazione entro 10 secondi dal rilevamento.

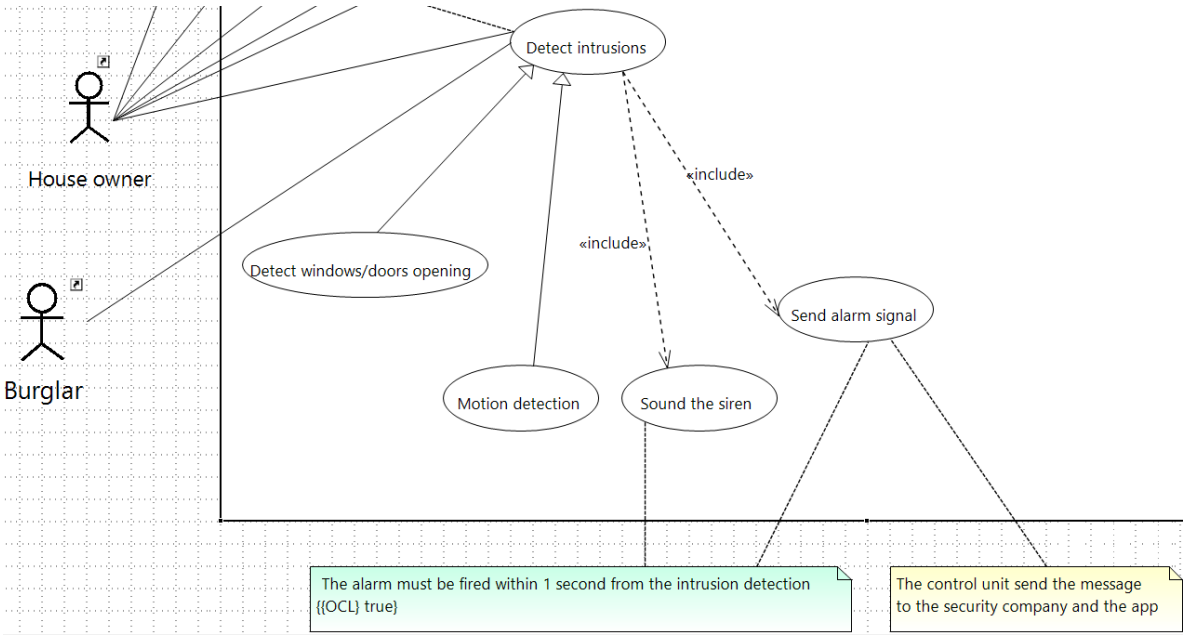

Figura 4: Caso d'uso riguardante la rilevazione dell'intrusione nell'abitazione del proprietario

Il caso d'uso relativo al rilevamento di un'intrusione viene mostrato più nel dettaglio in figura 4. Questo caso d'uso indica che il sistema permette al proprietario di individuare intrusioni da parte di ladri nella sua abitazione e che la rilevazione viene concretizzata dal sistema attraverso il riconoscimento di movimenti all'interno della casa e dal rilevamento dell'apertura di porte e finestre. In aggiunta, il rilevamento delle intrusioni da parte del sistema include l'azionamento della sirena e l'invio del segnale di allarme alla compagnia di sicurezza e all'app tramite la centralina, che devono essere effettuati entro 1 secondo dal rilevamento dell'intrusione.

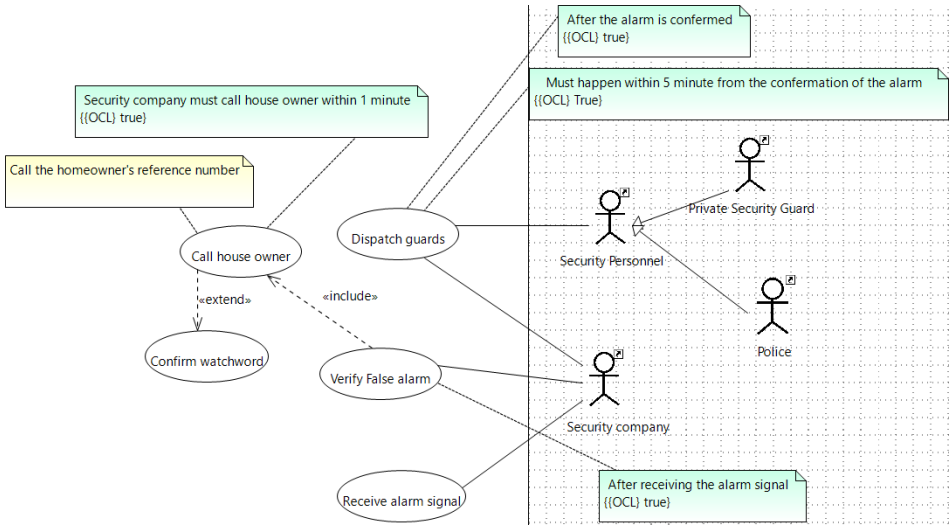

Figura 5: Casi d'uso relativi alla compagnia di sicurezza

Infine, in figura 5 vengono mostrati i casi d'uso relativi alla compagnia di sicurezza, la quale riceve i segnali di allarme per poi procedere a verificare se è un falso allarme attraverso una telefonata al numero di riferimento fornito dal proprietario della casa entro 1 minuto. Se il proprietario risponde alla chiamata, la compagnia di sicurezza chiederà la parola d'ordine. Infine, nel caso in cui l'allarme sia confermato, la compagnia di sicurezza manderà il personale all'abitazione entro 5 minuti.

3 Diagramma della Definizione dei Blocchi e del interno

Prima di vedere altri diagrammi che descrivono il comportamento del sistema, vengono mostrati i blocchi che caratterizzano il sistema di allarme dal punto di vista strutturale. I blocchi possono rappresentare vari aspetti del sistema e le associazioni specificano relazioni fra loro che possono anche non tradursi in una connessione fisica nella sua effettiva realizzazione.

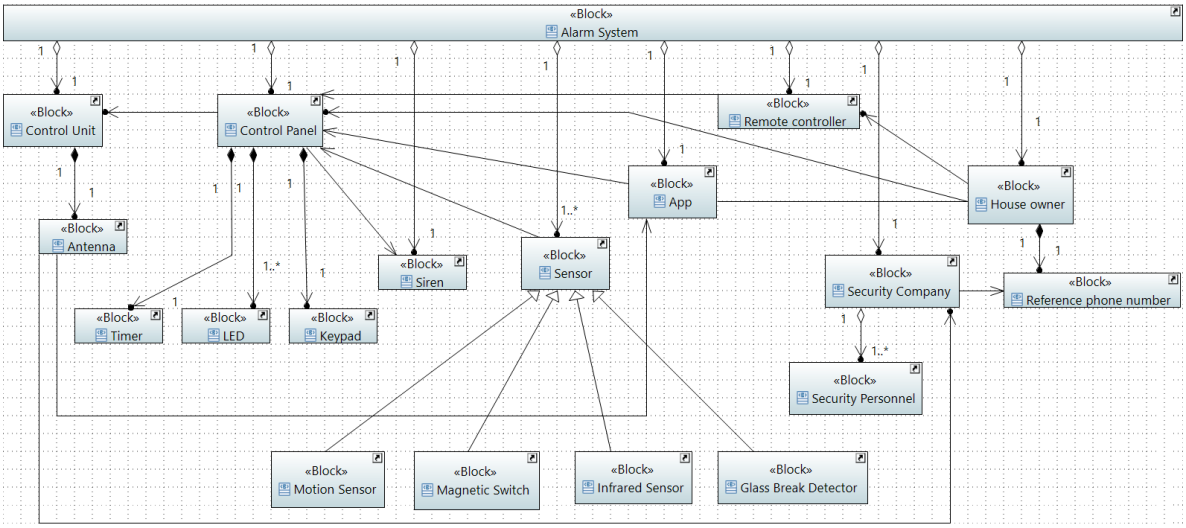

Figura 6: Diagramma di definizione dei blocchi del sistema di allarme

In figura 6 vengono rappresentati tutti i blocchi che andranno a far parte del sistema di allarme. Il sistema è composto da una moltitudine di sensori, una centralina, un pannello di controllo e una sirena. Inoltre, mette a disposizione un'applicazione da associare alla propria installazione e un telecomando remoto con il quale controllare il pannello di controllo. Il sistema di allarme è gestito da una compagnia di sicurezza ed è utilizzato dal proprietario dell'abitazione nel quale il sistema è installato.

Nella figura 6 sono mostrate anche associazioni di composizione. La centralina è composta da un'antenna per trasmettere informazioni alla compagnia di sicurezza e all'applicazione. Il pannello di controllo è composto da un tastierino per immettere il codice di armamento e disarmo dell'allarme, una moltitudine di led che indicano l'apertura o chiusura delle porte e finestre, e un timer che serve per implementare il delay specificato nel diagramma dei requisiti che serve quando il sistema di allarme viene armato per far uscire il proprietario dall'abitazione e, quando la porta viene aperta, per dare il tempo di inserire il codice per il disarmo dell'allarme.

Si può vedere anche che il blocco che rappresenta il proprietario di casa contiene un recapito rappresentato da un numero di telefono di riferimento che la compagnia di sicurezza utilizzerà per contattare il proprietario in caso di allarme.

La compagnia di sicurezza contiene il personale addetto alla gestione del sistema e al intervento in caso di emergenza. I sensori sono specializzati in 4 tipologie e comunicano con il pannello di controllo, il quale a sua volta è connesso con una sirena che viene attivata dal pannello di controllo in caso di necessità. Sono anche riportate delle associazioni in termini di comunicazione/utilizzo tra blocchi. Il proprietario di casa può interagire direttamente con il pannello di controllo o usare come tramite l'applicazione e il telecomando remoto. L'applicazione fornisce anche notifiche al proprietario di casa in caso di intrusioni.

Questo diagramma fornisce una prospettiva strutturale che descrive gli elementi che vanno a comporre il sistema di sicurezza e che interagiscono con esso, insieme alle associazioni fra i blocchi.

3.1 Diagramma di Blocco Interno

Se vogliamo avere una vista più dettagliata dei blocchi strettamente in relazione fra loro possiamo utilizzare un altro tipo di diagramma in prospettiva strutturale, cioè il diagramma di blocco interno, che si concentra sulla struttura interna dei blocchi e come le informazioni fluiscono al loro interno.

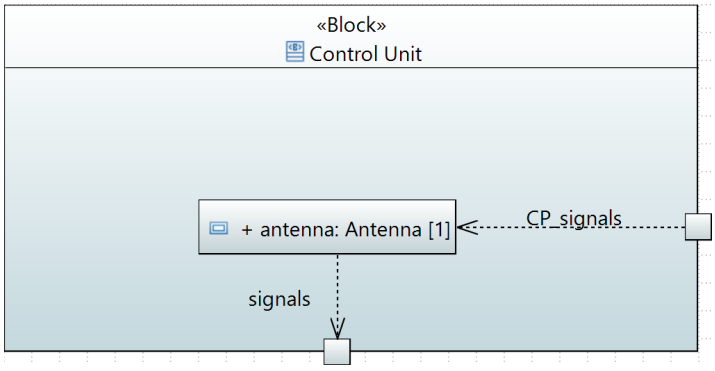

Figura 7: Diagramma di blocco interno della centralina

In figura 7 viene mostrato il diagramma interno del blocco che rappresenta la centralina, la quale riceve in ingresso segnali dal pannello di controllo e attraverso l'antenna trasmette in uscita il segnale verso la compagnia di sicurezza e verso l'applicazione.

In figura 8 invece, viene mostrata la struttura interna del pannello di controllo che è composto da un tastierino, un timer e una certa quantità di led. Il pannello di controllo riceve in ingresso i valori immessi nel tastierino e in base al tasto premuto agirà in un certo modo. In particolare quando il sistema viene armato in modalità "away" dal tastierino o da un apparato remoto (applicazione o telecomando) viene fatto partire il timer per dare il tempo al proprietario di uscire dall'abitazione. Il timer fornirà in uscita un segnale di allarme nel momento in cui il contatore raggiungerà lo zero e un sensore rileva l'apertura di una porta o finestra. Il timer viene anche azionato quando viene ricevuto un segnale di apertura della porta della casa mentre l'allarme è armato, implementando così il requisito di dare al proprietario di casa il tempo di immettere il codice per il disarmo prima che l'allarme scatti. Il pannello di controllo riceve degli input dai sensori che vengono usati per cambiare lo stato dei led e spediti alla centralina (WindowsDoors_OpenSignal) per far si che anche dall'applicazione sia visualizzabile lo stato aggiornato dell'apertura di porte e finestre. Inoltre, se il sistema è armato, i segnali dei sensori delle finestre diventano un segnale d'allarme per la centralina che dovrà inoltrarlo alla compagnia di sicurezza.

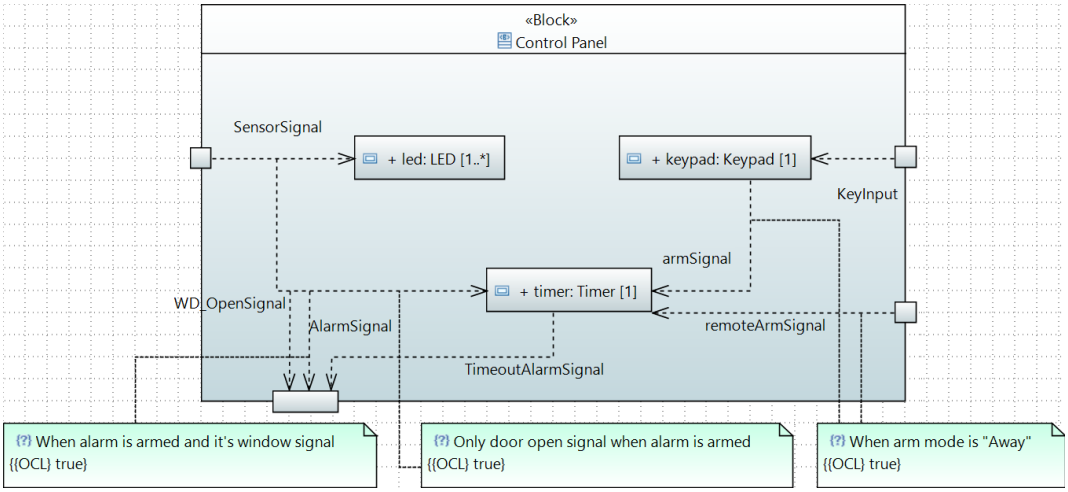

Figura 8: Diagramma di blocco interno del pannello di controllo

4 Diagramma d'Attività

Dopo aver visto i componenti che partecipano al sistema di allarme come blocchi, la struttura interna di alcuni di essi, e le loro associazioni usando i diagrammi in prospettiva strutturale, utilizziamo dei diagrammi in prospettiva comportamentale per descrivere come questi blocchi interagiscono fra loro e l'ordine delle azioni che sono necessarie a soddisfare alcuni dei casi d'uso formalizzati in precedenza.

In particolare, il diagramma d'attività viene utilizzato per descrivere il flusso di operazioni necessarie dal sistema per svolgere una certa attività, inteso come sequenza di comportamenti funzionali.

Per la realizzazione di questo diagramma è stato utilizzato un altro tool grafico che, a differenza dell'attuale versione di Papyrus, mette a disposizione la possibilità di inserire le swimlanes.

Le swimlanes verticali servono ad allocare determinate azioni agli attori corrispondenti, mentre quelle orizzontali generalizzano un insieme di azioni svolte da uno o più attori in un comportamento complessivo a più alto livello.

Figura 9 mostra il diagramma per l'attività di individuazione e risposta ad un'intrusione. Gli attori che agiscono in questo contesto sono il proprietario di casa, il ladro, il sistema di allarme, la compagnia di sicurezza ed il personale di sicurezza. L'attività inizia con il proprietario che arma il sistema di allarme immettendo il codice di sicurezza e selezionando la modalità di allarme. Successivamente, quando un ladro prova ad accedere all'interno dell'abitazione, i sensori del sistema di sicurezza lo rileveranno e verrà attivato l'allarme attraverso il suono della sirena e l'invio del segnale di allarme, il tutto entro 1 secondo dal rilevamento. A questo punto il flusso si divide in due: il segnale d'allarme viene ricevuto dalla compagnia di sicurezza e viene anche visualizzato dal proprietario tramite notifica dell'applicazione associata al sistema di sicurezza entro 10 secondi. Il flusso di azioni della compagnia di sicurezza prosegue con la verifica del segnale d'allarme che consiste nella chiamata al numero di telefono di riferimento del proprietario entro 1 minuto dall'allarme. Se il proprietario risponde, la compagnia di sicurezza gli chiederà la parola d'ordine concordata e, se corretta, concluderà che l'avvenimento sia stato un falso allarme, concludendo così l'attività descritta dal diagramma. Se invece il proprietario non risponde o fornisce una parola d'ordine sbagliata, la compagnia di sicurezza considererà l'allarme come vero e provvederà ad inviare, entro 5 minuti, la richiesta di supporto al personale di sicurezza, il quale deve recarsi all'abitazione del proprietario per fornire assistenza.

Questo diagramma formalizza una situazione che il sistema deve poter gestire e che include alcuni dei casi d'uso visti precedentemente, con una prospettiva adatta ad analizzare ad alto livello l'ordine del flusso delle azioni da compiere dai vari attori e come essi devono interagire tra loro per portare a compimento le proprie responsabilità.

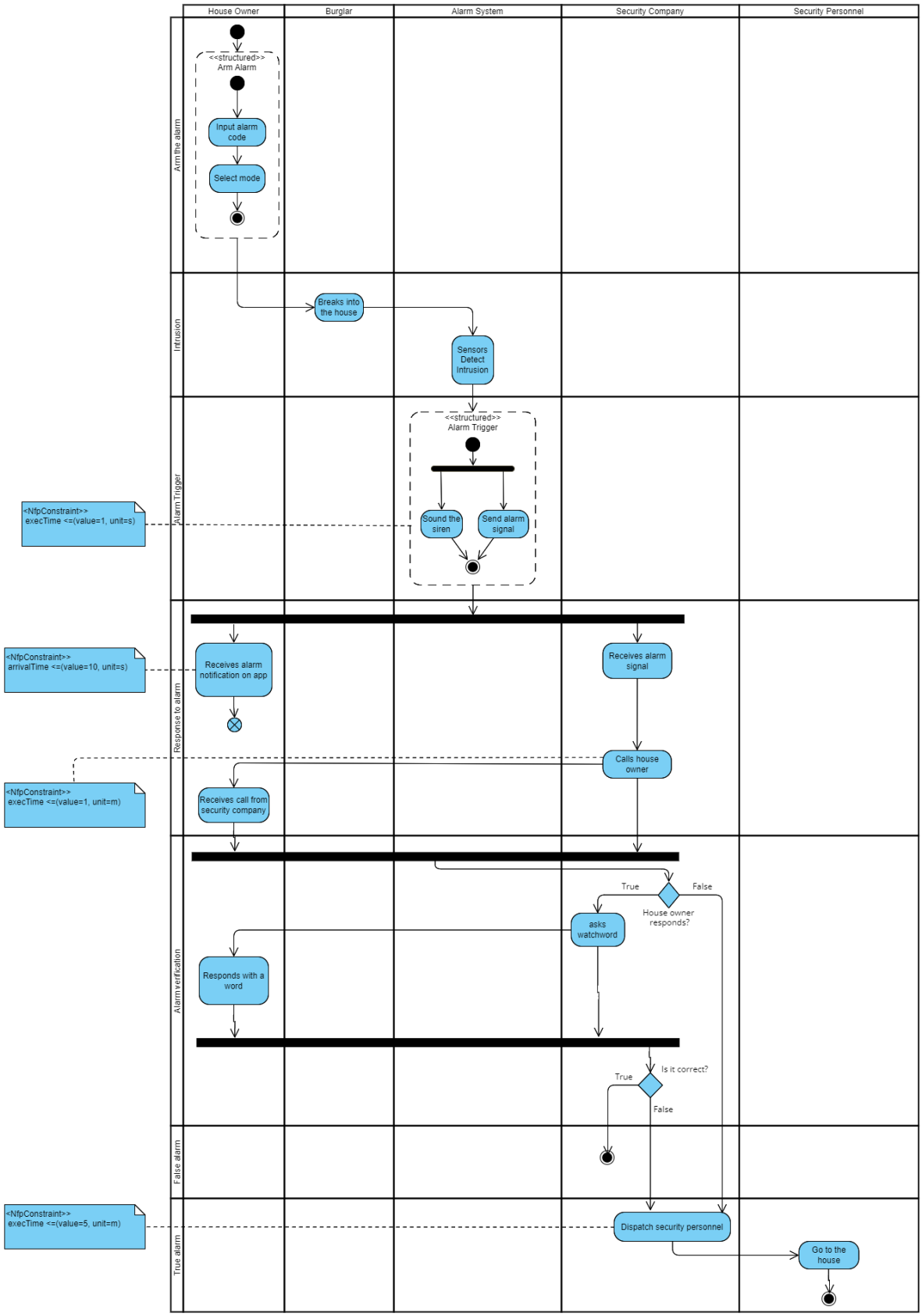

Figura 9: Diagramma d'attività: risposta del sistema di allarme a seguito di una rilevazione di intrusione

5 TPN

Come si può vedere da figura 9, l'attività appena descritta include anche dei vincoli non-funzionali riferiti al tempo con cui certe azioni devono essere compiute. Queste componenti non-funzionali possono essere modellate utilizzando una rete di petri tempificata.

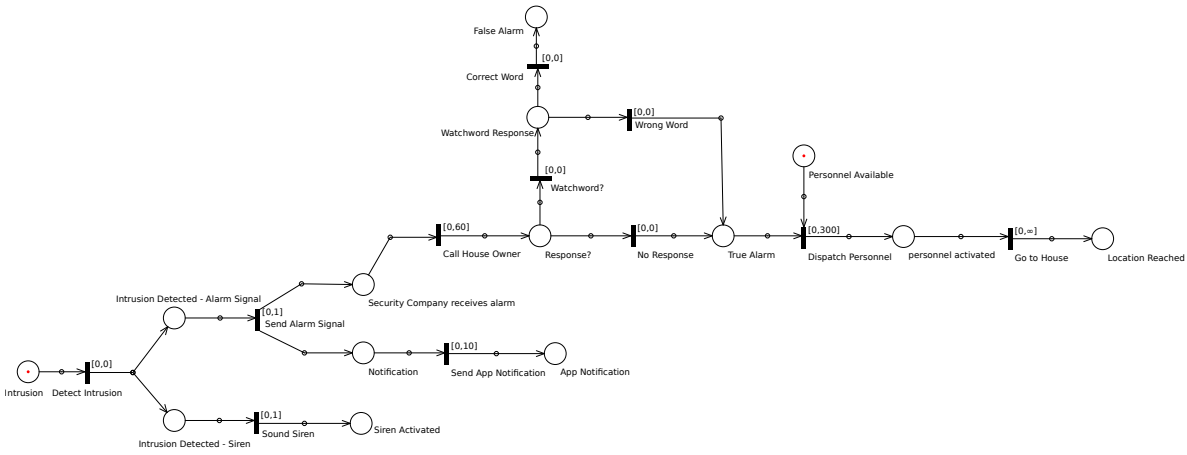

Figura 10: Modello TPN relativo all'attività di risposta ad una possibile intrusione

Figura 10 mostra il modello TPN del sistema per l'attività di rilevamento e risposta ad intrusioni in cui sono specificati i vincoli sulle transizioni in termini del tempo massimo con cui devono essere compiute. La realizzazione di questa TPN ha solo l'intento di sperimentare con il tool messo a disposizione, Oris 1, e con la modellazione di requisiti non-funzionali di un possibile sistema complesso con le reti di petri. L'implementazione su un RTOS e la relativa analisi del comportamento tempificato vanno al di là degli obiettivi di questo progetto. La modellazione TPN che è stata fatta, assume che il sistema si trovi in uno stato in cui l'intrusione stia avvenendo, per questo viene messo un gettone sul posto "intrusion". L'intrusione viene rilevata nel momento in cui avviene e successivamente vengono modellate le sequenze di azioni viste per il diagramma d'attività con i loro requisiti non-funzionali. Sono state assunte come istantanee le transizioni che rappresentano la comunicazione della parola d'ordine e la verifica della sua correttezza.

6 Diagramma di Sequenza

Come ultimo passo della modellazione del sistema d'allarme, è interessante vedere da un altro punto di vista la risposta ad una possibile intrusione. I diagrammi di sequenza sono diagrammi comportamentali incentrati sulle interazioni tramite scambio di messaggi in ordine cronologico. Con il diagramma di attività è stato possibile descrivere il flusso di azioni dei vari attori e come essi interagiscono fra loro ad alto livello. Con il diagramma di sequenza, invece, osserviamo più nel dettaglio gli elementi responsabili delle varie azioni e come le informazioni, in termini di messaggi, vengono scambiate fra loro nel tempo.

Gli elementi principali in un diagramma di sequenza sono rappresentati da "lifelines" e corrispondono ai blocchi del modello definiti nel diagramma della definizione dei blocchi.

Anche per questo diagramma non è stato usato Papyrus in quanto non permette di inserire graficamente i vincoli temporali in modo intuitivo, diversamente da Visual Paradigm.

Figura 11 mostra lo stesso scenario descritto dal diagramma di attività precedentemente visto con un maggior grado di dettaglio in termini di elementi del sistema di sicurezza che partecipano al corretto svolgimento dello scenario e al loro scambio di messaggi.

In questo caso è stata rappresentata la situazione in cui il proprietario di casa risponde alla chiamata della compagnia di sicurezza a seguito di un segnale di allarme (la chiamata può essere automatizzata e non richiedere un operatore umano) e comunica una parola d'ordine errata, la quale fa scattare l'invio di guardie di sicurezza all'abitazione.

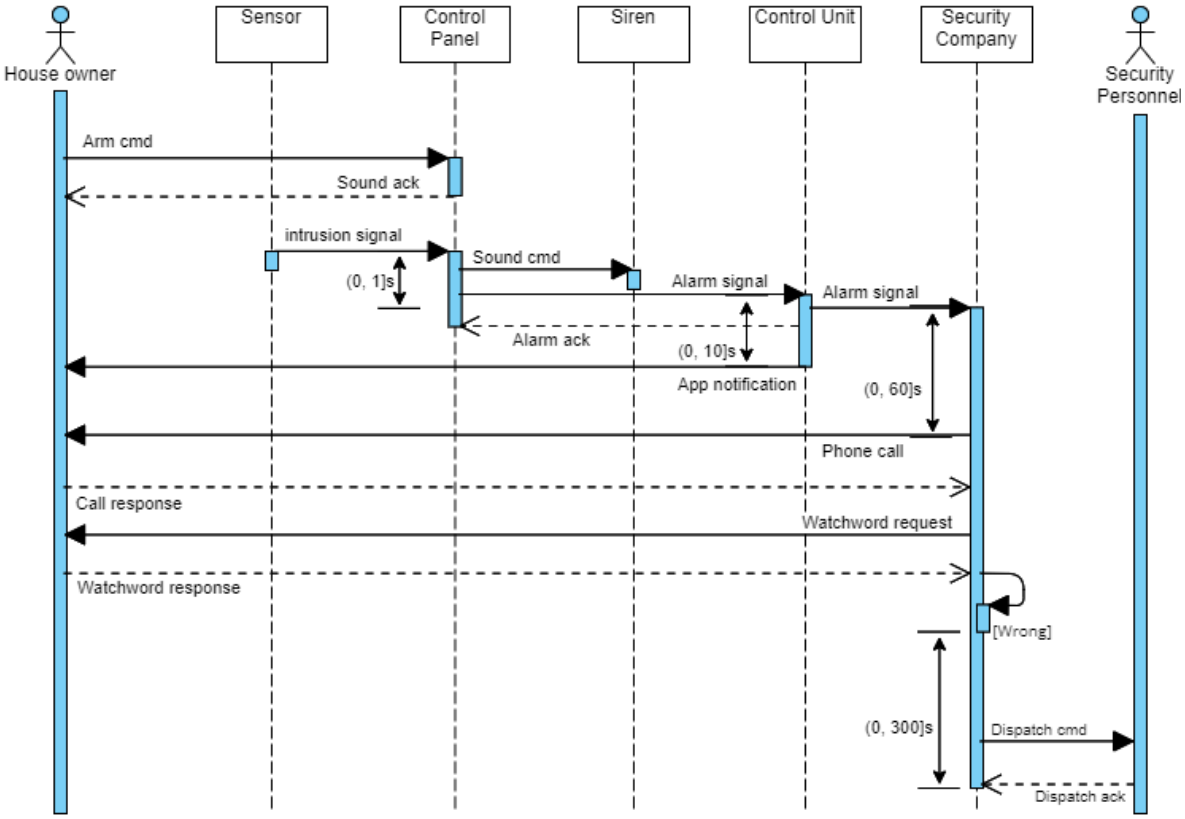

Figura 11: Diagramma di sequenza: risposta del sistema di allarme a seguito di una rilevazione di intrusione

7 Conclusione

Questo progetto ha avuto come obiettivo l'approfondimento della modellazione di sistemi complessi tramite il linguaggio SysML. Il sistema modellato è un esempio giocattolo, con requisiti strutturali, comportamentali e non-funzionali scelti in maniera arbitraria basati su una ricerca riguardo il dominio del problema che non voleva essere esaustiva, ma sufficiente per procedere alla creazione dei diversi diagrammi definiti da SysML. Questo tipo di modellazione si inserisce in una metodologia più ampia, quella del Model-Driven Engineering, che si basa sui modelli per portare avanti lo sviluppo del sistema. La modellazione dei vincoli non-funzionali attraverso la TPN vista durante questa trattazione si inserisce proprio all'interno di una delle fasi della metodologia MDE e supporta la modellazione effettuata tramite SysML. Il procedimento seguito in questo lavoro è partito dalla definizione dei requisiti del sistema, suddivisi in comportamentali, strutturali e non-funzionali. Poi sono stati utilizzati i vari tipi di diagrammi SysML per modellare i requisiti definiti e fornire diverse prospettive del sistema complessivo. I requisiti funzionali, o comportamentali, di alto livello sono stati rappresentati attraverso casi d'uso per formalizzare chi sono gli attori e cosa essi possono fare nel contesto del sistema di allarme. Poi sono stati definiti i blocchi costituenti del sistema dal punto di vista strutturale attraverso i diagrammi di definizione di blocco e di blocco interno. Sono state mostrate sia associazioni di composizione che associazioni di utilizzo e comunicazione fra blocchi. Successivamente sono state definite le responsabilità degli attori in un contesto che racchiude più casi d'uso definiti in precedenza. Questo viene fatto con il diagramma di attività che mostra la sequenza delle azioni che gli attori devono compiere durante una certa attività insieme ai vincoli non-funzionali che devono essere rispettati. A supporto dell'attività presa in considerazione è stato creato un modello di petri tempificato che permette di analizzare il soddisfacimento dei vincoli non-funzionali presenti nell'attività.

Anche se fuori dalla finalità di questo progetto, la realizzazione di un modello formale come quello di una TPN è particolarmente utile per creare, anche automaticamente, il codice che implementa i requisiti non-funzionali del sistema e, dove aver instrumentato il codice così generato, per analizzare lo spazio degli stati al fine di verificare che i vincoli temporali di certi percorsi all'interno di questo spazio siano sempre rispettati dall'implementazione reale del sistema.

Infine, è stato realizzato un diagramma di sequenza per vedere in maggior dettaglio come l'attività presa in considerazione può essere svolta dagli elementi del sistema attraverso uno scambio di messaggi che deve rispettare uno specifico ordinamento e dei specifici vincoli temporali.