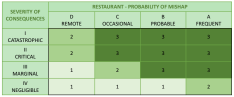
Restaurant alarm system

System Hazard Analysis

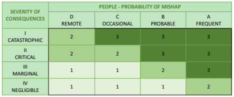
Alex Delbono

alex.delbono@mail.polimi.it
Politecnico di Milano

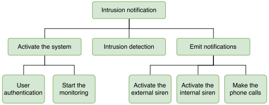
December 4 2016



SEVERITY OF CONSEQUENCES	RESTAURANT - PROBABILITY OF MISHAP			
	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC	2	3	3	3
II CRITICAL	2	3	3	3
III MARGINAL	1	2	3	3
IV NEGLIGIBLE	1	1	1	2



SEVERITY OF CONSEQUENCES	PEOPLE - PROBABILITY OF MISHAP			
	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC	2	3	3	3
II CRITICAL	2	2	3	3
III MARGINAL	1	1	2	3
IV NEGLIGIBLE	1	1	1	2



Intrusion notification

Activate the system

Intrusion detection

Emit notifications

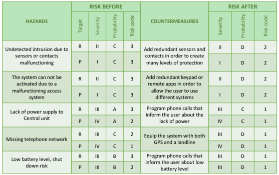
User authentication

Start the monitoring

Activate the external siren

Activate the internal siren

Make the phone calls



HAZARDS	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	Target	Severity	Probability	Risk code		Severity	Probability	Risk code
Undetected intrusion due to sensors or contacts malfunctioning	R	II	C	3	Add redundant sensors and contacts in order to create many levels of protection	II	D	2
	P	I	C	3		I	D	2
The system can not be activated due to a malfunctioning access system	R	II	C	3	Add redundant keypad or remote apps in order to allow the user to use different systems	II	D	2
	P	I	C	3		I	D	2
Lack of power supply to Central unit	R	III	A	3	Program phone calls that inform the user about the lack of power	III	C	1
	P	IV	A	2		IV	C	1
Missing telephone network	R	III	C	2	Equip the system with both GPS and a landline	III	D	1
	P	IV	C	1		IV	D	1
Low battery level, shut down risk	R	III	B	3	Program phone calls that inform the user about low battery level	III	D	1
	P	III	B	2		III	D	1

Overview

1. System description
2. Functional analysis
3. Architectural analysis
4. Qualitative analysis (PHA)
5. Quantitative analysis
    - FMEA
    - FTA
    - TTM
    - ET

Table of Contents

1. System description

2. Functional analysis

3. Architectural analysis

4. Qualitative analysis (PHA)

5. Quantitative analysis
   - FMEA
   - FTA
   - TTM
   - ET

System description

The system we are going to analyze is a simplified example of a **surveillance system** for a restaurant.

The system must notify to the owner and to the people nearby when someone tries to break in and enter in the restaurant in order to steal goods or damage the equipment.

Figure 1: Source: Alarm.org

Main functions

1) The main function of the system, when active, is to signal eventual intruders with phone calls and acoustic signals from the sirens.

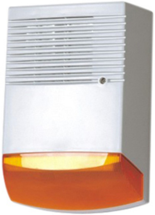


Figure 2: Source: bizspia.org

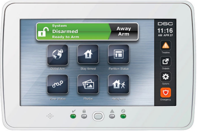


Figure 3: Source: dsc.com

2) It must be possible for authorized people to disable the system, either locally or using a remote procedure.

Focus of the analysis

The objective of the analysis is to provide a description of the system hazards from an **high level point of view**, considering the main components as atomic.

In this way we avoid the complexity of the analysis of the subcomponents, but we can focus only on the functionalities offered to the users.

Figure 4: Source: DHgate.com

General system overview

The **main** hardware and software **components** of the system are presented in the following list:

- Central unit
- Infrared sensors
- Magnetic contacts
- Internal and external sirens
- Telephone module
- Alarm module
- Output modules
- User access points

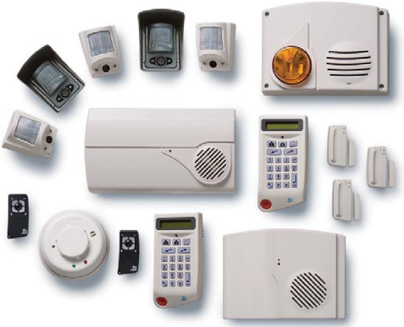


Figure 5: Source: coreportal.org

Components

The **Central unit** controls all the system and offers the power supply to all the components.

The **infrared sensors and the magnetic contacts** protect the openings and the rooms of the building.

The **two sirens**, one internal and one external, signal a perceived intrusion through acoustic advices.

The **telephone module** is in charge to make phone calls whenever an alarm is detected.

The **alarm module** receives the perceptions of the sensors and decides whether there is an intrusion or not. It also communicates with the sirens and the telephone module.

The **output module** informs the user about the state of the system, using leds.

The **user access points** allow the user to login and change the state of the system.

Table of Contents

POLITECNICO
MILANO 1863

1. System description
2. Functional analysis
3. Architectural analysis
4. Qualitative analysis (PHA)
5. Quantitative analysis
   - FMEA
   - FTA
   - TTM
   - ET

Functional analysis

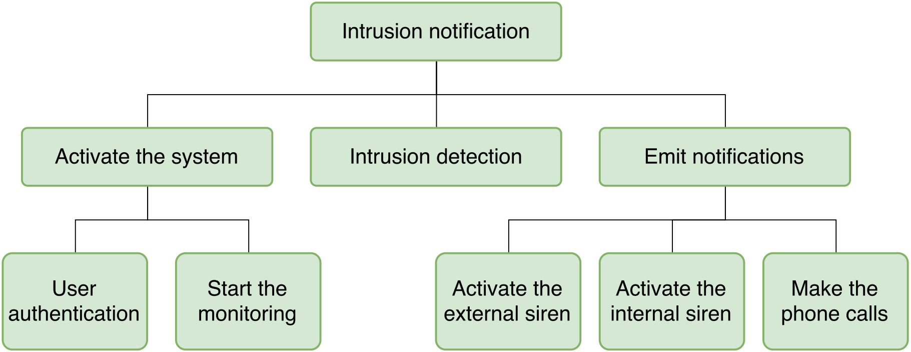


Table of Contents

1. System description
2. Functional analysis
3. Architectural analysis
4. Qualitative analysis (PHA)
5. Quantitative analysis
   - FMEA
   - FTA
   - TTM
   - ET

Architectural analysis

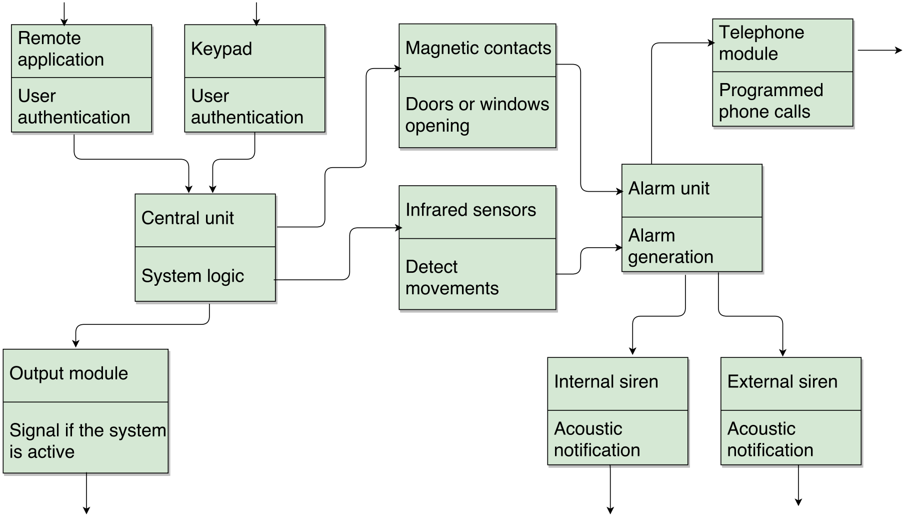


Table of Contents

POLITECNICO
MILANO 1863

1. System description
2. Functional analysis
3. Architectural analysis
4. Qualitative analysis (PHA)
5. Quantitative analysis
   - FMEA
   - FTA
   - TTM
   - ET

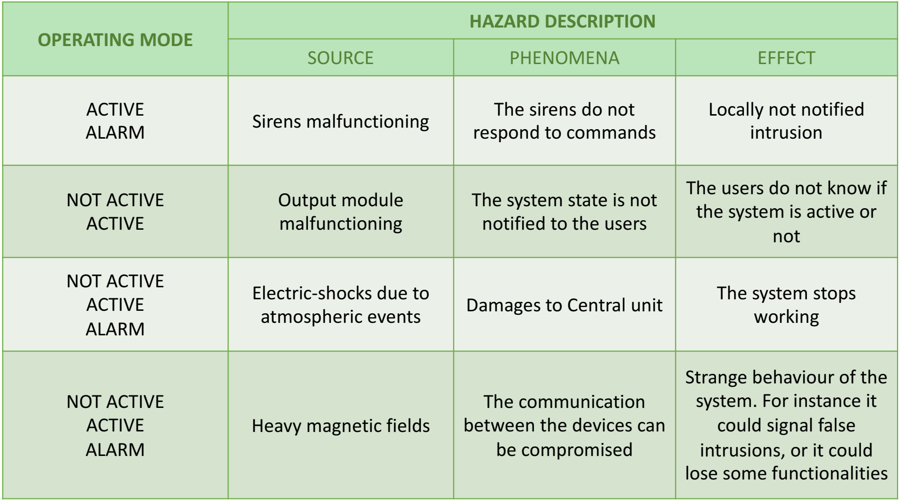
PHA - Operating modes

OPERATING MODE	DESCRIPTION	INVOLVED COMPONENTS
NOT ACTIVE	Waiting for the user to authenticate and activate the monitoring	Central unit, Remote application, Keypad, Output module
ACTIVE	Monitoring the environment searching for intrusion	Central unit, Remote application, Keypad, Output module, Sensors
ALARM	Intrusion detected, notifying the alarm	Central unit, Remote application, Keypad, Output module, Sensors, Alarm unit, Telephone module, Sirens

PHA - Hazard description (1)

OPERATING MODE	HAZARD DESCRIPTION		
	SOURCE	PHENOMENA	EFFECT
ACTIVE	Sensors or contacts malfunctioning	No signal of possible intrusion sent to the Alarm unit	Undetected intrusion
NOT ACTIVE ACTIVE	Access points (keypads and remote apps) malfunctioning	Authentication of the users unavailable	The system can not be activated or deactivated
NOT ACTIVE ACTIVE ALARM	Missing power supply to Central unit	Limited autonomy of the system due to the battery level	The battery supplies energy for a maximum of 12 to 24 hours
ACTIVE ALARM	Missing telephone network	The telephone module can not reach the network	No possibility of making phone calls when an intrusion is detected
NOT ACTIVE ACTIVE ALARM	Low battery level	All the system can not rely on the battery if the power supply lacks	No effect on the system if the power supply is still present

PHA - Hazard description (2)



OPERATING MODE	HAZARD DESCRIPTION		
	SOURCE	PHENOMENA	EFFECT
ACTIVE ALARM	Sirens malfunctioning	The sirens do not respond to commands	Locally not notified intrusion
NOT ACTIVE ACTIVE	Output module malfunctioning	The system state is not notified to the users	The users do not know if the system is active or not
NOT ACTIVE ACTIVE ALARM	Electric-shocks due to atmospheric events	Damages to Central unit	The system stops working
NOT ACTIVE ACTIVE ALARM	Heavy magnetic fields	The communication between the devices can be compromised	Strange behaviour of the system. For instance it could signal false intrusions, or it could lose some functionalities

PHA - Targets

POLITECNICO
MILANO 1863

RESTAURANT	
SEVERITY OF CONSEQUENCES	
CATASTROPHIC	Damages to the structure and equipment
CRITICAL	Huge damages or risks for the equipment
MARGINAL	Minor damages or risks for the equipment
NEGLIGIBLE	No risk

PEOPLE	
SEVERITY OF CONSEQUENCES	
CATASTROPHIC	Risks for life or safety, huge economical damages
CRITICAL	Huge economical damages
MARGINAL	Limited economical damages
NEGLIGIBLE	No damage

Time interval for computing the hazard probabilities	**10 YEARS**

PHA - Risk assessment matrixes

SEVERITY OF CONSEQUENCES	RESTAURANT - PROBABILITY OF MISHAP			
	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC	2	3	3	3
II CRITICAL	2	3	3	3
III MARGINAL	1	2	3	3
IV NEGLIGIBLE	1	1	1	2

SEVERITY OF CONSEQUENCES	PEOPLE - PROBABILITY OF MISHAP			
	D REMOTE	C OCCASIONAL	B PROBABLE	A FREQUENT
I CATASTROPHIC	2	3	3	3
II CRITICAL	2	2	3	3
III MARGINAL	1	1	2	3
IV NEGLIGIBLE	1	1	1	2

PHA (1)

HAZARDS	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	Target	Severity	Probability	Risk code		Severity	Probability	Risk code
Undetected intrusion due to sensors or contacts malfunctioning	R	II	C	3	Add redundant sensors and contacts in order to create many levels of protection	II	D	2
	P	I	C	3		I	D	2
The system can not be activated due to a malfunctioning access system	R	II	C	3	Add redundant keypad or remote apps in order to allow the user to use different systems	II	D	2
	P	I	C	3		I	D	2
Lack of power supply to Central unit	R	III	A	3	Program phone calls that inform the user about the lack of power	III	C	1
	P	IV	A	2		IV	C	1
Missing telephone network	R	III	C	2	Equip the system with both GPS and a landline	III	D	1
	P	IV	C	1		IV	D	1
Low battery level, shut down risk	R	III	B	3	Program phone calls that inform the user about low battery level	III	D	1
	P	III	B	2		III	D	1

PHA (2)

HAZARDS	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	Target	Severity	Probability	Risk code		Severity	Probability	Risk code
Intrusion detected but not notified locally due to sirens malfunctioning	R	III	C	2	Placement of two or more sirens, at least one internal and one external	III	D	1
	P	I	C	3		III	D	1
System state not notified due to Output module malfunctioning	R	III	C	2	Insert acoustic or view signals from the sirens in order to communicate the state of the alarm	IV	D	1
	P	II	C	2		IV	D	1
Electric-shocks due to atmospheric events	R	I	C	3	Add smoke detectors (if not already present) in the restaurant in order to signal the presence of fire	II	C	2
	P	I	C	3		II	C	2
Strange behaviour due to heavy magnetic fields	R	III	B	3	Add redundancy in the sensors and contacts and protect the other modules with sensors and contacts	III	D	1
	P	III	B	2		III	D	1

Table of Contents

POLITECNICO
MILANO 1863

1 System description

2 Functional analysis

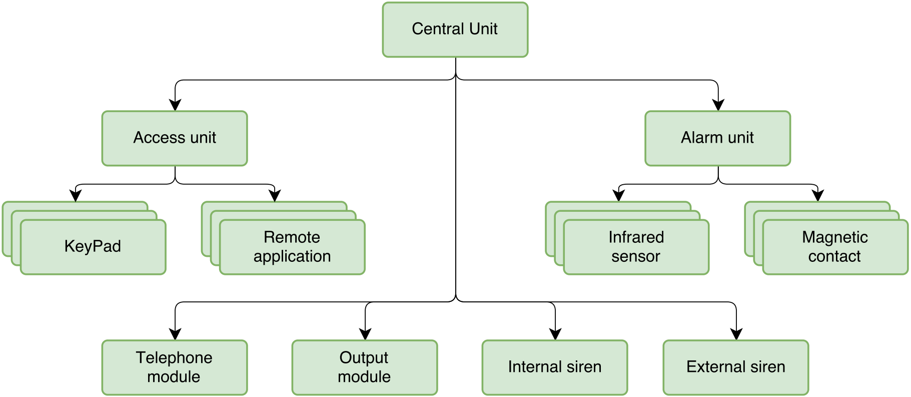
3 Architectural analysis

4 Qualitative analysis (PHA)

5 Quantitative analysis

- FMEA
- FTA
- TTM
- ET

FMEA - Structure definition



FMEA - Change system state

Object	Failure mode	Causes	Effects	Severity	Frequency	Detection	RPN	Recommended action	Severity	Frequency	Detection	RPN
Keypad or remote app	Malfunctioning	Electronic or software failure	No possible authentication	3	2	2	12	Redundant access points	1	2	2	4
Connection to central unit	No connection	Electronic or physical failure	No possible authentication	3	2	4	24	Periodic maintenance, accurate installation procedure	3	1	4	12
Output module	No information about the state of the system	Electronic or software failure	The user can not know the state of the system	5	2	1	10	Redundant way of knowing the state of the system	2	2	1	4
Central unit	Malfunctioning	Electronic or software failure	No operation possible	9	2	3	54	Periodic maintenance, accurate installation procedure, safe power supply line	9	1	3	27

FMEA - Intrusion detection

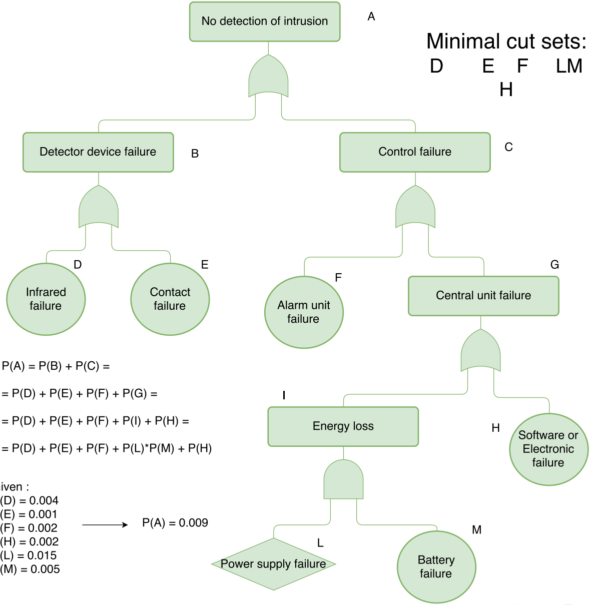
Object	Failure mode	Causes	Effects	Severity	Frequency	Detection	RPN	Recommended action	Severity	Frequency	Detection	RPN
Alarm unit	Malfunctioning	Electronic or software failure	No generation of the alarm	9	2	4	72	Periodic maintenance, accurate installation procedure, safe power supply line	9	1	2	18
Sirens	Malfunctioning	Electronic or physical failure	No acoustic signal	5	3	4	60	Periodic maintenance, accurate installation procedure, multiple sirens	1	2	4	8
Telephone module	No line for calling	Provider malfunctioning, intentional cut of the line	No possible calls to users	5	3	2	30	Redundant methods: GPS and landline. Trusty provider and inaccessible cables	2	1	1	2
Central unit	Malfunctioning	Electronic or software failure	No detection	9	2	3	54	Periodic maintenance, accurate installation procedure, safe power supply line	9	1	3	27
Infrared sensor or contact	Malfunctioning	Electronic or physical failure	No detection of the intrusion	6	4	3	72	Periodic maintenance, accurate installation procedure, redundant sensors or contacts	3	2	2	12

FMEA - System not active

Object	Failure mode	Causes	Effects	Severity	Frequency	Detection	RPN	Recommended action	Severity	Frequency	Detection	RPN
Sirens	Malfunctioning	Electronic or physical failure	Acoustic signal without real alarm	4	3	2	24	Periodic maintenance, accurate installation procedure	4	1	2	8
Central unit	Malfunctioning	Electronic or software failure	Strange behaviour of the system	9	2	3	54	Periodic maintenance, accurate installation procedure, safe power supply line	9	1	3	27
Telephone module	Unpredictable use of the line	Electronic or software failure	Useless calls	5	3	2	30	Periodic maintenance, accurate installation procedure	5	1	2	10
Infrared sensor or contact	Fake manumission alarm	Electronic or physical failure	Loss of activity	7	4	2	56	Periodic maintenance, accurate installation procedure	7	2	1	14

FTA - Undetected intrusion

Minimal cut sets:
D E F LM
H



No detection of intrusion A

Detector device failure B

Control failure C

Infrared failure D

Contact failure E

Alarm unit failure F

Central unit failure G

Energy loss I

Software or Electronic failure H

Power supply failure L

Battery failure M

P(A) = P(B) + P(C) =

= P(D) + P(E) + P(F) + P(G) =

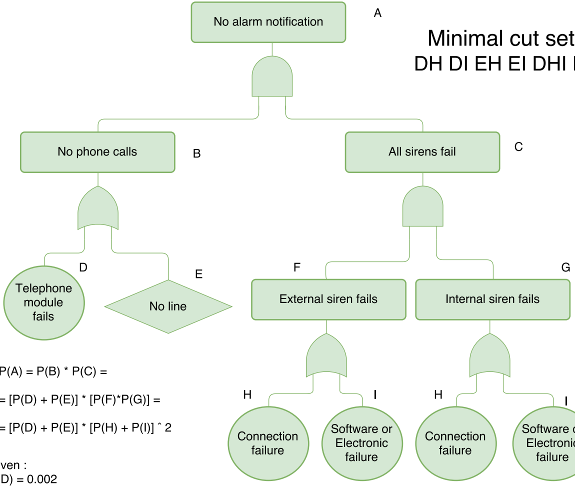
= P(D) + P(E) + P(F) + P(I) + P(H) =

= P(D) + P(E) + P(F) + P(L)*P(M) + P(H)

Given :
P(D) = 0.004
P(E) = 0.001
P(F) = 0.002
P(H) = 0.002
P(L) = 0.015
P(M) = 0.005

→ P(A) = 0.009

FTA - No alarm notification



Minimal cut sets:
DH DI EH EI DHI EHI

P(A) = P(B) * P(C) =

= [P(D) + P(E)] * [P(F)*P(G)] =

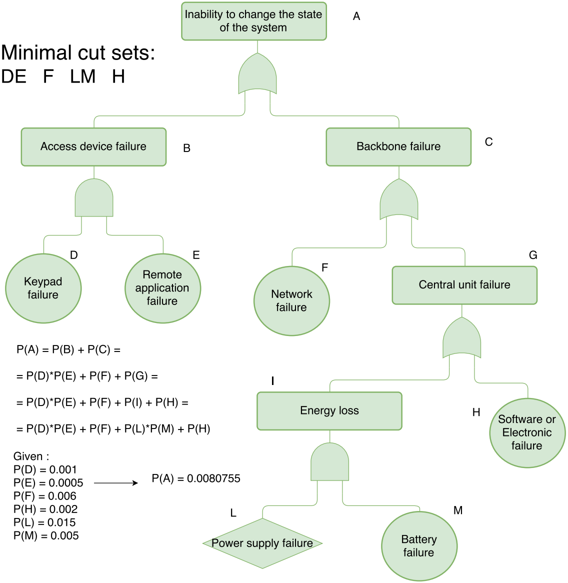
= [P(D) + P(E)] * [P(H) + P(I)] ˆ 2

Given :
P(D) = 0.002
P(E) = 0.025
P(H) = 0.001
P(I) = 0.004

→ P(A) = 0.000000675

FTA - No change of the system state

Minimal cut sets:
DE F LM H



$P(A) = P(B) + P(C) =$

$= P(D)*P(E) + P(F) + P(G) =$

$= P(D)*P(E) + P(F) + P(I) + P(H) =$

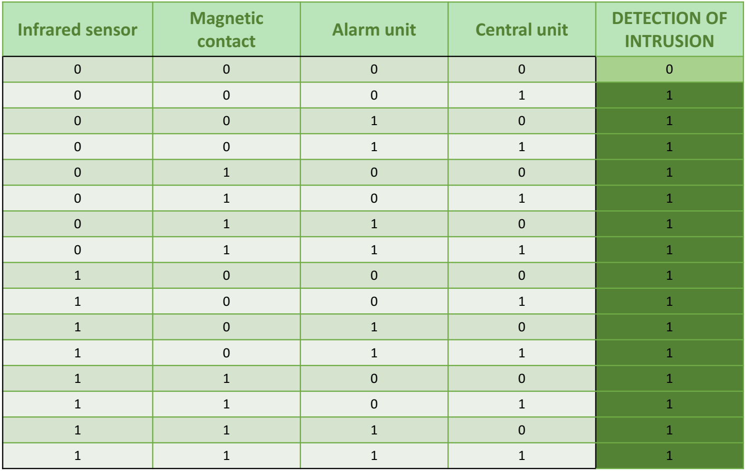
$= P(D)*P(E) + P(F) + P(L)*P(M) + P(H)$

Given :
$P(D) = 0.001$
$P(E) = 0.0005$
$P(F) = 0.006$
$P(H) = 0.002$
$P(L) = 0.015$
$P(M) = 0.005$

→ $P(A) = 0.0080755$

TTM - Undetected intrusion

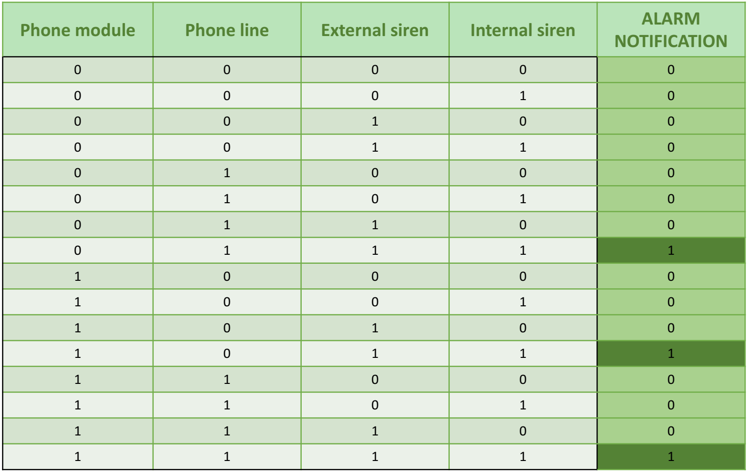
The following table refers to FTA - Undetected intrusion.
1 indicates failure of the component.



Infrared sensor	Magnetic contact	Alarm unit	Central unit	DETECTION OF INTRUSION
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	1
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

TTM - No alarm notification

The following table refers to FTA - No alarm notification.
1 indicates failure of the component.



Phone module	Phone line	External siren	Internal siren	ALARM NOTIFICATION
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

TTM - No change of the system state

The following table refers to FTA - No change of the system state. 1 indicates failure of the component.

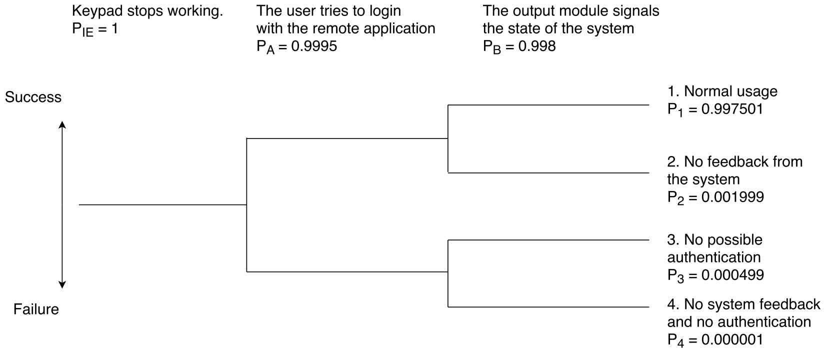
Keypad	Remote application	Network	Central unit	CHANGE SYSTEM STATE
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	1
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

ET - User interaction

Initiating event: keypad stops working

The user has to access with the remote application.

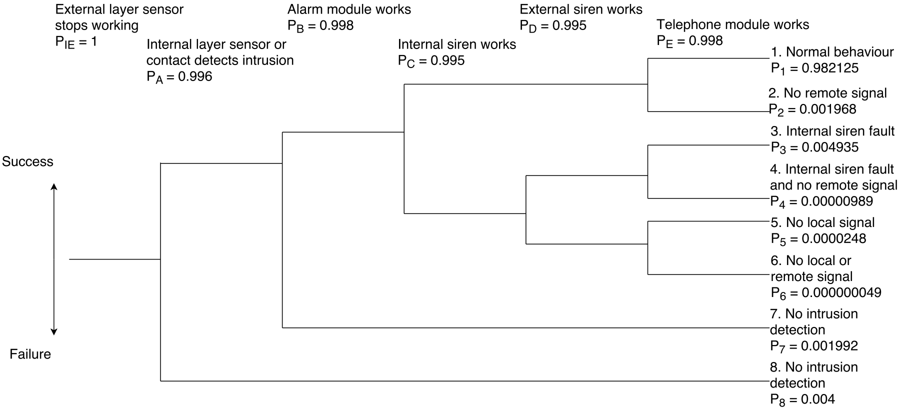
The user also needs the feedback from the output module in order to know if the operation was successful or not.


Keypad stops working.
$P_{IE} = 1$
The user tries to login with the remote application
$P_A = 0.9995$
The output module signals the state of the system
$P_B = 0.998$
Success
Failure
1. Normal usage
$P_1 = 0.997501$
2. No feedback from the system
$P_2 = 0.001999$
3. No possible authentication
$P_3 = 0.000499$
4. No system feedback and no authentication
$P_4 = 0.000001$

ET - Intrusion notification

Initiating event: sensor stops working

The system needs to detect the intrusion and notify it locally or remotly.


External layer sensor stops working $P_{IE} = 1$
Internal layer sensor or contact detects intrusion $P_A = 0.996$
Alarm module works $P_B = 0.998$
Internal siren works $P_C = 0.995$
External siren works $P_D = 0.995$
Telephone module works $P_E = 0.998$
1. Normal behaviour $P_1 = 0.982125$
2. No remote signal $P_2 = 0.001968$
3. Internal siren fault $P_3 = 0.004935$
4. Internal siren fault and no remote signal $P_4 = 0.00000989$
5. No local signal $P_5 = 0.0000248$
6. No local or remote signal $P_6 = 0.000000049$
7. No intrusion detection $P_7 = 0.001992$
8. No intrusion detection $P_8 = 0.004$
Success
Failure

References

- **Beep - [2016-2017] - SAFETY IN AUTOMATION SYSTEMS** - Riccardo Scattolini - https://beep.metid.polimi.it/
- **Tecnoalarm systems** - Design of the system http://www.tecnoalarm.com/en-uk/installatore/
- **Latex** - Document preparation system https://www.latex-project.org