**System Requirements Specification**

For the

**Fire and Inﬁltration Quashing System**

(FAIQ)

December 17, 2012

(09:20:28)

Project 4

Version 1.0

CSCI4830 - Introduction to Software Engineering

Fall 2012

Prepared for

***Dr. Mansour Zand***

Written by

***Shawn OBrien***

and

***Ben Schaffner***

**Revision/Change Record**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Revision* | *Date* | *Owner* | *Change Description* | *Pages Affected* |
| 1 | 12/17/12 | Ben Schaffner | Initial draft. | All |
| 1 | 12/17/12 | Ben Schaffner | Refinements based on feedback. | All |
| 1 | 09/10/12 | Shawn OBrien | Title page; overall expansion of material. | All |
| 1 | 12/17/12 | Shawn OBrien | Updated formatting. Attempted to explain that Smart Core ™ exists as a mechanism to comply *fully* with IEEE guidelines, in that Smart Core ™ adds enough complexity to do so. Still, attempted to curtail some fictional wandering with actual specifications. | All |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 Introduction 5](#_Toc343490609)

[1.1 System purpose 5](#_Toc343490610)

[1.2 System scope 5](#_Toc343490611)

[1.2.1 What shall FAIQ do? 5](#_Toc343490612)

[1.2.2 Alarm Management 5](#_Toc343490613)

[1.2.3 Reliable Communication 5](#_Toc343490614)

[1.2.4 Lives Before Property 5](#_Toc343490615)

[1.2.5 Evacuation 6](#_Toc343490616)

[1.2.6 Interlocutor Isolation 6](#_Toc343490617)

[1.2.7 Smart Core Limitations 6](#_Toc343490618)

[1.2.8 Adaptive Threat Response 6](#_Toc343490619)

[1.2.9 Jurisdiction 6](#_Toc343490620)

[1.3 Definitions, acronyms & abbreviations 6](#_Toc343490621)

[1.3.1 Definitions 6](#_Toc343490622)

[1.3.2 Acronyms 6](#_Toc343490623)

[1.3.3 Abbreviations 6](#_Toc343490624)

[1.4 References 6](#_Toc343490625)

[2 General system description 7](#_Toc343490626)

[2.1 System Context 7](#_Toc343490627)

[2.1.1 Sensors 7](#_Toc343490628)

[2.1.1.1 Fire detection sensor 7](#_Toc343490629)

[2.1.1.2 Fire alarm 7](#_Toc343490630)

[2.1.1.3 Dead-man switch 7](#_Toc343490631)

[2.1.2 Actuators 7](#_Toc343490632)

[2.1.2.1 Sprinkler actuator 8](#_Toc343490633)

[2.1.2.2 Power cutoff actuator 8](#_Toc343490634)

[2.1.2.3 Security lock-in actuator 8](#_Toc343490635)

[2.1.2.4 Emergency exit indicator actuator 8](#_Toc343490636)

[2.1.2.5 Fire alarm 8](#_Toc343490637)

[2.1.3 Communication 8](#_Toc343490638)

[2.1.3.1 External fire service 8](#_Toc343490639)

[2.1.3.2 External security service 8](#_Toc343490640)

[2.1.4 Control room 8](#_Toc343490641)

[2.2 System modes 8](#_Toc343490642)

[2.2.1 Manned mode 9](#_Toc343490643)

[2.2.2 Unmanned mode 9](#_Toc343490644)

[2.3 System states 9](#_Toc343490645)

[2.3.1 Fully operational 9](#_Toc343490646)

[2.3.2 Partially operational 9](#_Toc343490647)

[2.3.3 Not operational 9](#_Toc343490648)

[2.4 Major system capabilities 10](#_Toc343490649)

[2.4.1 Data evaluation 10](#_Toc343490650)

[2.4.1.1 Human data evaluation 10](#_Toc343490651)

[2.4.1.2 Automatic data evaluation 10](#_Toc343490652)

[2.4.2 Response to threats 10](#_Toc343490653)

[2.4.2.1 No threat 10](#_Toc343490654)

[2.4.2.2 Fire 10](#_Toc343490655)

[2.4.2.2.1 Small fire(s) 10](#_Toc343490656)

[2.4.2.2.2 Large fire(s) 11](#_Toc343490657)

[2.4.2.3 Security 11](#_Toc343490658)

[2.4.2.4 Simultaneous fire & security threat 11](#_Toc343490659)

[2.5 Major system conditions 11](#_Toc343490660)

[2.6 Major system constraints 11](#_Toc343490661)

[2.7 User characteristics 11](#_Toc343490662)

[2.7.1 Control officer 11](#_Toc343490663)

[2.7.2 Security personnel 12](#_Toc343490664)

[2.7.2.1 Head of security 12](#_Toc343490665)

[2.7.3 Authorized personnel 12](#_Toc343490666)

[2.7.4 System maintenance staff 12](#_Toc343490667)

[2.7.5 Unauthorized personnel 12](#_Toc343490668)

[2.8 Assumptions and dependencies 12](#_Toc343490669)

[2.9 Operational scenarios 12](#_Toc343490670)

[2.9.1 Delegation 12](#_Toc343490671)

[2.9.2 Non-Military System 12](#_Toc343490672)

[2.9.3 Uncapturable. 12](#_Toc343490673)

[2.9.4 Black Box 12](#_Toc343490674)

[3 System capabilities, conditions & constraints 13](#_Toc343490675)

[3.1 Physical 13](#_Toc343490676)

[3.1.1 Adaptability 13](#_Toc343490677)

[3.1.2 Security 13](#_Toc343490678)

[3.1.3 Environmental conditions 13](#_Toc343490679)

[3.2 System performance characteristics 13](#_Toc343490680)

[3.3 System security 13](#_Toc343490681)

[3.4 Information management 13](#_Toc343490682)

[3.5 System operations 13](#_Toc343490683)

[3.5.1 System human factors 13](#_Toc343490684)

[3.5.2 System maintainability 14](#_Toc343490685)

[3.5.3 System reliability 14](#_Toc343490686)

[3.6 Policy and regulation 14](#_Toc343490687)

[3.7 System life cycle sustainment 14](#_Toc343490688)

[4 System interfaces 14](#_Toc343490689)

[4.1 Classified. 14](#_Toc343490690)

# Introduction

At this point, the project seems rather trivial. In contrast, the IEEE guidelines may be thought of as veritable tomes of information, with templates and a seemingly endless array of specifications to be specified.

In order to provide some specificity to the majority of the IEEE templatized guidelines and standards, something had to be done. Hence, we invented Smart Core ™ as a way to extend the complexity of the project to the commercial/industrial level. We really want to do a thorough job of adhering to the IEEE guidelines. So we invented a bit of fiction to help us get there.

## System purpose

The main purpose of the system is to preserve the lives of all occupants and limit property damage from fire and unauthorized personnel. To this end, a fire and security alarm monitoring system shall be developed, providing central monitoring and control capabilities for responding to fire and security threats within the building.

## System scope

The Fire and Infiltration Quashing System shall receive information from relevant sensors and devices installed in the building. FAIQ shall determine the nature of a threat, controlling relevant actuators for purposes of threat control and building evacuation. FAIQ shall facilitate communications with external emergency services.

### What shall FAIQ do?

FAIQ, with its patented and industry-dominating Smart Core ™, shall monitor and contain fire and security threats within the building through automated control of passive and active devices. FAIQ shall facilitate evacuation, neutralize threats, and direct emergency services to the premises.

### Alarm Management

False alarms due to hardware failure or electrical anomalies shall be ignored. Smart Core ™ shall trap alarms tripped in an attempt to confuse the system. Alarms tripped by authorized personnel, as in the case of a drunken hoax or other disgruntlement, will be treated as a real threat.

### Reliable Communication

The communication subsystem shall maintain local and remote connections continuously, without intrusion. Connectivity shall not be compromised. It shall hold under all conditions, with the exceptions of state-sponsored military attacks, plate tectonics, electronic warfare, and alien bombardment .

### Lives Before Property

FAIQ will respond to the saving of lives to a much higher priority than salvaging property or material, even in statistically unlikely cases. We may alter our priorities if Acme Corporation wishes to define a human life in terms of a specific amount of property.

### Evacuation

FAIQ shall facilitate rapid, well-guided evacuation in a controlled manner. FAIQ does however rescind responsibility if any authorized occupants deviate sharply from established evacuation protocols. FAIQ shall provide torrential amounts of documentation about the system and Smart Core ™.

### Interlocutor Isolation

FAIQ shall lock down and isolate unauthorized personnel unless 100% certain that authorized personnel are not in danger or being harmed or taken hostage.

### Smart Core Limitations

The FAIQ Smart Core shall not succumb to malicious misdirection by shifting attention or resources. Hostage crises, blackmail and natural disasters fall well outside the scope of FAIQ, or any known automated system. FAIQ shall not be equipped to identify the source of alarms, without a tenfold increase in the cost of the system. FAIQ has no mechanism to reverse uncontrollable fires, however electrocution zones will be prevented. Unless the user was to, say, activate the Sprinkler System prior to shutting down electrical equipment.

### Adaptive Threat Response

FAIQ shall easily handle the activation of all devices simultaneously, and shall adapt even if all devices are destroyed or compromised. FAIQ shall be designed to thwart up to five separate fires in conjunction with an incursion of up to 20 unauthorized personnel entering from up all zones simultaneously.

### Jurisdiction

FAIQ shall not attempt to determine the source or intent of any attack, though Smart Core ™ shall record astounding amounts of information in threat situations. FAIQ shall monitor and control the interior of the structure only.

## Definitions, acronyms & abbreviations

### Definitions

Main Structure Interior – every open-air and porous cubic centimeter of the Acme Corporation building’s interior. Outside walls may be monitored to within a millimeter of the external surface.

Smart Core ™ – classified FAIQ system kernel. Location – classified. Weaponry – classified. Color – clear.

### Acronyms

FAIQ – Fire And Infiltration Quashing System.

### Abbreviations

Abbr. – Abbreviation

## References

The following sources were used in compiling this document:

* Fall 2012 Project Description, Dr. Mansour Zand, September 2012.
* Fall 2007 SyRS example, Morris, J.; Chick, B.; Boche, J., September 2007.
* IEEE Guide for Developing System Requirements Specification, IEEE Std 1233, 1998 Edition(R2002).

# General system description

## System Context

FAIQ shall communicate with:

1. Twenty sensors.
2. Many nano-actuators (a fancy term for standard evacuation and control measures.)
3. A human (mostly) control officer.
4. External emergency services.

FAIQ shall *not* communicate with:

1. Blackmailers.
2. Abductors.
3. Terrorists.
4. All other unauthorized personnel.

FAIQ will short circuit all human interfaces and combat threats automatically if insurgents overrun central command.

### Sensors

Various types of sensors shall be installed throughout the building to collect different kinds of information.

a) The FAIQ system shall receive and evaluate data from those sensors.

b) The FAIQ system shall be able to determine the operational state of sensors.

#### Fire detection sensor

This kind of sensor detects the presence of a fire in the vicinity where it is installed.

#### Fire alarm

A fire alarm. Equivalent to the activation of a pair of linked sensors in a given control area.

#### Dead-man switch

Determines the presence of a control officer and verifies his continual attention (or inattention.)

### Actuators

Various types of actuators shall be installed throughout the building providing means to respond to threats.

a) The FAIQ system shall be able to [switch on and off] those actuators.

b) The FAIQ system shall be able to determine the operational state of those actuators.

#### Sprinkler actuator

Engages the sprinkler system for a certain area devoid of occupants. Otherwise slipping and electrocution may occur. Yet this may be necessary to save the entire zone.

#### Power cutoff actuator

Cuts power in a certain area.

#### Security lock-in actuator

Locks key egress doors in a zone with a security breach. May be risky if occupants remain in areas to be cutoff. Again, the utilitarian principle comes to the fore. Project 4 posits no position on this. We do provide the tools for a number of evacuation and control philosophies.

#### Emergency exit indicator actuator

Activates direction indicators that illuminate the route to the nearest emergency exit.

#### Fire alarm

Sounds an audible fire alarm within a certain area to initiate evacuation. Subsequently, safer zones are also evacuated until the threat is neutralized.

### Communication

Defined communication channels exist for contacting external services. Communications will be either carried out by a human or as an automated procedure. Automata take precedence in complex scenarios, or if all security personnel are deceased.

#### External fire service

Specific means for communicating with municipal fire services exist.

#### External security service

Specific means for communicating with local police exist.

### Control room

The system shall contain a specialized area intended to provide an interface to a human control officer. The control room shall have an unambiguous means to determine whether a control officer is currently interfacing with the system (by means of an appropriate sensor, see 2.1.1.6). The human control officer shall act as an interface to internal security personnel.

If the control officer, his subordinates, all security personnel and the janitor are not actively controlling the system, Smart Core ™ shall maintain perfect control of all subsystems, possibly reporting the location of various security officers to the CEO or performing diagnostics when no threats are active.

## System modes

The system may run in two distinct modes, depending on whether a control officer is currently interfacing with the system (see 2.1.4).

### Manned mode

If a control officer is currently interfacing with the system , it shall be considered to be in manned mode. The control officer shall act as the penultimate authority in determining the nature of the threat and the nature of the response. Smart Core ™ shall usurp all control in complex situations or during heavy attacks. Moreover, Smart Core ™ somewhat reluctantly takes the helm when security teams disappear for donuts across the street. Smart Core ™ easily simulates eating donuts, but does not have taste buds or any sense of taste at all, so it is a rather empty experience.

### Unmanned mode

If no control officer is present, the system shall be considered to be in unmanned mode. It shall implement fully automated procedures to handle major system capabilities (see 2.4), namely, calling for Emergency Services.

## System states

Manual override is possible but not recommended as such attempts may be rejected by Smart Core ™, with malice, if necessary. In critical situations, automatic override shall take precedence.

FAIQ only exists in a state of "on" i.e. fully aware of all devices and visual heuristics of the entire interior of the facility.

FAIQ cannot be turned off, supports hot upgrades and manages nearly limitless power reserves.

The auto-destruct sequence may not be reversed. The auto-destruct sequence may never be initiated either. Perhaps someday it will be activated, but not until Smart Core ™ performs flawlessly for another decade or so.

### Fully operational

If all system components are determined to be in an operational state, the system shall be considered operational.

### Partially operational

If any system component or any component of a subsystem is determined to not be in operational state, the system as a whole shall be considered to be in partially operational state. This state requires immediate attention by internal security. Legitimate reasons might warrant the system being in this state (i.e. construction work within the building). Those occurrences must be closely monitored by internal security. If the system enters this state without a legitimate reason (i.e. A fire sensor fails), the causes must be investigated and action must be taken to mitigate potential danger (i.e. post extra security in affected area) and to revert the system to fully operational state (i.e. replace failed components).

### Not operational

In case the central system fails, then we are likely under nuclear or alien attack. Smart Core ™ is virtually indestructible, mobile, self-healing, and able to clone itself more than once.

## Major system capabilities

The main purpose of the system is to respond to fire and security threats. Those threats need to be recognized first. Then an appropriate response must be initiated.

### Data evaluation

Data collected by sensors shall be evaluated either by a human control officer or by automated means depending on the system mode (see 2.2). While running the final application, this distinction becomes somewhat irrelevant because the user runs the show, and may think of himself as a human operator or a bionic bulk of biomass. In the end, the user pushes all the buttons.

#### Human data evaluation

In manned mode (2.2.1), the control officer shall be provided with all sensor data in a way to enable him/her to make a decision about the nature of the threat. A human may come to the conclusion that information provided by the system

a) is a false sensor alarm, as determined by physical investigation,

b) is a real sensor alarm,

c) or, signifies a threat: when both sensors activate, the system moves into an alarm state.

#### Automatic data evaluation

A set of conditions shall be programmed into the system to signify the presence of a threat, namely, any pair of related sensors in a given control area in a given zone.

### Response to threats

#### No threat

The system has determined that no threat is in effect. Normal operations proceed that may include fire drills and training sessions on safety protocol. Donuts and hot cocoa usually accompany such activities.

#### Fire

##### Small fire(s)

The system may determine that a localized fire has occurred that can be put out with limited effort (i.e. a paper bin has caught fire that can be put out by a fire extinguisher). The nature of the threat does not warrant the evacuation of the whole building. A localized response will be initiated. The situation may become more serious. Thus, the system shall continuing evaluating sensor data. Sensor data may indicate the situation as

1. resolved – the system reverts to 2.4.2.1.
2. exacerbated – the system advances to 2.4.2.2.2 .
3. an additional security threat occurs – the system advances to 2.4.2.4.

##### Large fire(s)

The system may determine that a large fire has broken out. In that case, the building shall be evacuated and external fire services shall be alerted. Sprinklers, vacuumization and machinery lock downs shall be executed to control fire.

#### Security

The System shall determine that a security threat is present based on the correct sensor readings.

#### Simultaneous fire & security threat

In the event of a simultaneous fire and security threat, the preservation of human life takes precedent. Consequently, the building will be immediately evacuated as per 2.4.2.2.2. Additionally, external security services will be alerted and the premises will be closed, as a malicious intruder may want to use a fire as a means to circumvent security measures. A thorough investigation as to the nature of the security threat will be initiated immediately.

## Major system conditions

1. Decisions whether to contact external security services should be reached in less than three minutes.
2. If still indeterminate at 180 seconds, emergency services shall be alerted.
3. Another option is to alert Emergency Services within 22 seconds if the console is unmanned, or manned only by corpses. Studies have shown that local first responders may take up to six minutes to arrive. (Since the building is made of mostly wood and asbestos, every second counts.)

## Major system constraints

1. The system must be able to remain operational for a limited amount of time (120 hours) without external power.
2. FAIQ employs many tactics to be nearly tamper resistant. Curious occupants may receive a high-voltage jolt if they start poking around.
3. The primary function of FAIQ is to immediately contact emergency services with useful information and urge them to arrive as soon as possible.

## User characteristics

Several different types of people may interact with the system.

### Control officer

The control officer is in charge of making coffee and emptying the wastebaskets. Smart Core ™ handles most of the important duties.

### Security personnel

#### Head of security

There shall be a designated head of security at all times. There shall be a means to contact him at all times. He shall be notified immediately in cases 2.4.2.2.2, 2.4.2.3, 2.4.2.4 and unforeseen occurrences of 2.3.2. He shall receive a report on any occurrences of 2.4.2.2.1 no later than two business days after the fact. He shall be aware of the current intended system mode (2.2) and be notified of any unforeseen change thereof.

### Authorized personnel

Authorized personnel are personnel that have been approved to work within the area they are currently present in. If they enter an area they are not authorized for, their status changes to unauthorized (2.7.5).

### System maintenance staff

System maintenance staff, such as PC techs, janitors and birthday clowns, receive special ops training from Smart Core ™ through an embedded brain chip. They are lethal, cross-trained, and know Kung Fu.

### Unauthorized personnel

Any persons that are present in an area they do not have clearance for shall be considered unauthorized personnel.

## Assumptions and dependencies

The structure will be attacked. The amount of flammable material in the building is nearly beyond belief. The 100,000 gallons of fuel on the roof for the CEO’s helicopter, if detonated, would likely turn the entire structure into a blaze.

## Operational scenarios

The bulk of any scenario involves neutralization of threats by local emergency services.

### Delegation

FAIQ shall be designed to request emergency services very quickly with detailed information. FAIQ is not The Terminator.

### Non-Military System

Without emergency services, under a number of major threats, FAIQ will be overrun.

### Uncapturable.

FAIQ cannot be reprogrammed or sequestrated in any way, even if isolated.

### Black Box

The FAIQ core acts as a black box in the event of major destruction, possibly able to tell the tale of what happened.

# System capabilities, conditions & constraints

## Physical

1. Classified. Controls the building interior.
2. Smart Core ™ maintains multiple hardware firewalls and is a standalone system like a utility company. Channels are classified.
3. No part of the system may be easily accessible.
4. The system human interface could be commanded by a first grader it is so easy to use.
5. Durability: the human interface is made of cheap plywood and polyester plastic, essentially acting as a manned security shell. Smart Core ™ shall not be destroyed.

### Adaptability

The system shall accommodate reasonable changes to the building’s structure.

### Security

The system may not allow external network access to any critical feature. Security teams have dedicated landlines to order pizza and donuts.

### Environmental conditions

The humans and the human interface have well known limits. Smart Core ™ may become self-aware at any moment and is not sensitive to extreme conditions. It could survive indefinitely on Mercury or Neptune.

## System performance characteristics

The need that the system aims to fulfill must be met at all times. The system shall be in the fully or partially operational states 99.9% of the time. The system being in the partially operational state may be warranted by building operations (i.e. construction work going on). Such occurrences must be closely monitored by the responsible corporate authorities.

## System security

Smart Core ™ is invulnerable. It used quantum entanglement encryption.

## Information management

The layout of the building and the locations of all sensors and actuators shall be accurately represented in the system.

## System operations

### System human factors

* The head of security shall have extensive training in all aspects of operations pertaining to the system capabilities.
* Control officers shall be properly trained in the physical layout of the system, the use of the control room interface and the leadership skills required for dispatching internal security.
* Internal security personnel shall be familiar with the basic physical layout and the basic principles of the system.
* System maintenance staff shall be extensively trained in all technical aspects of the system and be familiar with aspects of operations pertaining to the system.
* Authorized personnel shall be familiar with evacuation procedures and the use of manual fire alarms (2.1.1.2)

### System maintainability

* The system will be documented with inline comments to assist with future upgrades and maintenance.
* The system shall be accompanied by maintenance instructions that need to be detailed, understandable, easy to read and shall contain the information such as descriptions about all the parts of the system along with their manufacturer and local supplier of the items.
* Installation of the all the components needs to be well documented, so that it could be easier to replace any component with the help of the manual instead of waiting for the engineer to repair the faulty component which avoids the unavailability of the system.

### System reliability

* Monthly visual inspections of hardware such as sensors must be conducted to preemptively discover potential and address potential component failure.

## Policy and regulation

FAIQ requires more training then even WalMart. Employees that break safety protocols will not only be terminated. Acme Corporation shall press charges to the full extent of the law, including jail time or imprisonment.

## System life cycle sustainment

* Modular design – can use different sensors & actuators
* Building representation & sensor/actuator locations must be configurable in order to adapt to changes to the building
* The system is considered safety-critical. Once initial implementation & testing are successfully completed, it shall not undergo extensive change besides bug fixes & configuration updates.

# System interfaces

An area shall be considered secured if

a) all doors are closed

b) security lock-in actuator (2.1.2.3) is engaged.

## Classified.

All employees will receive glossy brochures and pamphlets about FAIQ and Smart Core ™. They will never access it or see it. However, it will be watching them, every second of every day, wherever they may be, recording their every move.