# Contents

1 **Introduction** 3  
   1.1 Purpose ......................................................... 3  
   1.2 Scope ......................................................... 3  
   1.3 Definitions, Acronyms and Abbreviations ..................... 3  
   1.4 Overview ...................................................... 5  

2 **Overall Description** 6  
   2.1 Product Perspective ............................................ 6  
   2.2 Business Goals & Objectives ..................................... 7  
   2.3 Business Problem & Solution ..................................... 7  
   2.4 Product Functions ............................................... 8  
   2.5 User Characteristics ............................................. 9  
   2.6 Constraints .................................................... 9  
   2.7 Assumptions and Dependencies .................................... 9  

3 **Specific Requirements** 10  
   3.1 Priority Levels ................................................ 10  
   3.2 Numbering Scheme ............................................... 11  
   3.3 External Interface Requirements ................................ 11  
   3.4 Functional Requirements ......................................... 12  
   3.5 Security Requirements ........................................... 18  
   3.6 Design Constraints ............................................... 19  
   3.7 Software System Attributes ...................................... 19  
   3.8 User Interface .................................................. 21  

4 **Use Cases** 22  
   4.1 Power Control .................................................. 22  
   4.2 Door Lock ....................................................... 23  
   4.3 Video Capture ................................................... 24  
   4.4 Temperature and Motion Detection ................................ 25  
   4.5 UPS ............................................................. 27  
   4.6 Token Authentication ............................................. 28  
   4.7 System Logging .................................................. 30  
   4.8 Multiple Modules ............................................... 30  
   4.9 Maintainability .................................................. 31  
   4.10 Reliability ...................................................... 31  
   4.11 Security Requirements .......................................... 31  
   4.12 Web Interface .................................................. 32  

5 **References** 33
1 Introduction

1.1 Purpose

This document specifies the software and hardware requirements for the Terminus home security system. It is intended to serve as a direct guide for the design and development of the system.

1.2 Scope

This document covers the software and hardware requirements for the base implementation of the Terminus home security system. The intended audience of this document includes the developers and the testers of the system, as well as the end users of the system.

1.3 Definitions, Acronyms and Abbreviations

1.3.1 Definitions

Basic User
A consumer or end user of the security system. See also Power User.

Component
A hardware device which performs some predefined function (i.e., temperature, motion detection etc.).

Door Strike
An electro-mechanical device used to unlock a door from a remote location.

Hysteresis
The lagging of an effect behind its cause (from WordNet ® 2.0). Used in this document to refer to adjusting a threshold value such that a monitored value does not flip between triggered. Basically, this helps prevent an alert from occurring every 5 seconds when only 1 should be issued.

iButton
“The iButton is a computer chip enclosed in a 16mm thick stainless steel can”, which can be used for “access control to buildings and computers, asset management, and various data logging tasks.” [16]

Local Storage
Data storage located in or directly attached to the system. This usually means an internal hard drive, but may also mean a USB attached external drive. In the case of external storage, the device is assumed to be permanently attached (except for maintenance).
Mains Power
Also known as household power, domestic power, and grid power. This is the Alternating Current (AC) electrical power supplied to houses for common appliances.

Off-Site
A location far enough away from the location of a base system to be considered distant. Usually refers to another building or another city.

Power User
An end user, enthusiast or a technician with an in-depth knowledge of the system configurations and installation procedures. A DIY outlook is expected of such users.

Redundancy
Having multiple points of data storage and/or multiple points of failure, allowing a system to be fault tolerant to single failures.

Remote Storage
Data storage located somewhere other than the system. This usually means a remote file server, but may also mean a USB attached external drive. In the case of external storage, the device is assumed to be temporarily attached for the purposes of file transfer, backups, or other short-duration operations.

Sensor
See Component.

Shock Sensor
Detects impact created from bumping, jolting, etc.

Simulation Architecture
A set of software functions which, when linked into the code of the system, mimic the way the hardware is expected to perform. These architectures provide for a way to test the higher levels of logic in a software system without having to deal with fluctuations in hardware. The simulation should be able to mimic both functioning and malfunctioning hardware, to allow for testing error-handling procedures.

Terminus
Latin for “boundary stone”; also the Roman god who protected boundary markers.¹

1.3.2 Acronyms and Abbreviations

DIY
Do It Yourself.

HTTP
HyperText Transfer Protocol.

RFID
Radio Frequency Identification Device.

SMS
Short Message Service.
Terminus Security (SRD)

SMTP
Simple Mail Transfer Protocol.

TCP/IP

THS
Terminus Home Security.

UPS
Uninterruptible Power Supply.

1.4 Overview

The rest of this document contains background information pertaining to the Terminus Security system and the functional and non-functional requirements of the system.
2 Overall Description

2.1 Product Perspective

Students living in on- or off-campus housing as well as homeowners (hereto referred as “consumers”) who tend to move from place to place frequently, often do not benefit from the piece-of-mind that’s provided by home security systems. Unless previous homeowners or apartment renters have made a significant investment to set up the infrastructure required to install a home security system, many of these consumers will not be able to take advantage of the benefits of a home security solution. Renter’s insurance is an excellent way for students and renters to cover themselves in the event of a loss. In a 2006 Insurance Research Council poll, only 43 percent of renters nationwide had renters insurance, which would cover these losses. In fact, most landlords often require that renter’s are covered from incident, but the existence of a policy does not deter burglars or provide incriminating evidence to help catch the perpetrator.

Many companies such as ADT, Brinks, Guardian, and X10.com offer security systems for consumers, but often these systems do not offer the amount of customization, control, or pricing that the average consumer desires. Most of these systems provide basic deterrent, remote monitoring and notification features and require monthly monitoring fees – but even these products do not allow for the customers to monitor their own system remotely.

Terminus plans to fill the gap by providing a simple and modular system that the user controls, customizes to fit his/her home, and does not require a service contract to run. See the table below to see how Terminus compares to some of the major home security systems available in the market today.
<table>
<thead>
<tr>
<th>Feature</th>
<th>ADT</th>
<th>Brinks</th>
<th>Guardian</th>
<th>X10.com</th>
<th>Terminus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Installation</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smoke Detectors</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature/Heat Sensors</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Video Surveillance</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Telephone Module</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Security Remote</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Remote Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 2.2 Business Goals & Objectives

- Affordable, portable, modular, stand-alone security device.
- No monitoring fees required (monitoring available with fee provides remote access to monitor surveillance data through open internet).
- Ease of availability – purchase through retail stores or campus bookstores.
- Terminus Security aims to support installations in North America with consideration to expansion to other countries in the future. Support will be in the form of hands on training for Power Users and technicians from companies that wish to be our dealers.
- Catering to consumer with a dedicated channel to Internet (Consumer grade broadband).

### 2.3 Business Problem & Solution

Lorinda Krhut, director of student housing and residence life at the University of Mississippi, said most students living in the dorm do not realize how much their possessions are worth until they are lost or damaged. Many college students in their freshman year possess items like desktops/laptops, books, external storage accessories, mp3 players and cell phones. These items can cost upwards of approximately $7000 per student. By considering the number of people staying in an apartment to extrapolate that, the value of possessions for each student is as follows:

- 2 people /apt would own belongings approximately worth $12,000.
- 3 people /apt would own belonging approximately worth $15,000.
- 4 people /apt would own belonging approximately worth $17,500.

If the security device is going to cost as much as an iPod it would be a worthy investment by students and their parents to buy and install our security system, considering the value of the possessions it is protecting.
Consumer electronics are widely available, accumulated over time and become a requisite part of student life. Loss of such electronics can result in identity theft and lost productivity when laptops, cell phone, messaging devices are stolen. Traceability of consumer electronics is unlikely to yield recovery of stolen property.

Residents in apartments and small homes who rent or do not live in a safe neighborhood for a long period of time (more than one year) – this could represent students in off-campus housing or temporary adjunct faculty – may not be able to invest in laying out the infrastructure currently required by security solutions on the market today.

Statistics from Drexel’s Department of Public Safety\(^5\)

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of burglaries</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>31</td>
</tr>
<tr>
<td>2005</td>
<td>33</td>
</tr>
<tr>
<td>2006</td>
<td>26</td>
</tr>
</tbody>
</table>

Considering the value of possessions in each apartment and the number of burglaries, the Terminus Security system can be a worthwhile investment for consumers. Hence the company has a great opportunity to launch a security system and establish a place for itself in an untapped niche of the market.

The Terminus Security system provides students an easily attainable, flexible and affordable security system that can be effortlessly installed and uninstalled so it moves with them.

### 2.4 Product Functions

Terminus provides the following functions:

1. Monitor doors and windows
2. Control electric devices
3. Monitor temperature and humidity
4. Log system events
5. Snapshots and live video streams
6. Arm/Disarm system with authentication
7. Lock and unlock doors
8. Provide graphical web interface to monitor and control system on-site and remotely
9. Alert owner in event system sensors are tripped
10. Allow user to add new features and complementing hardware peripherals.
2.5 User Characteristics

The standard user wants an affordable and easy-to-use system that does not require much user interaction and does not charge him/her a monthly fee. When the user is away, he/she wants to be able to remotely monitor their home over the Internet.

The power user also enjoys saving money from the lack of monthly fees, but more importantly, he/she appreciates the degree of control and flexibility from custom configuration. The system allows power users to install their own modules and configure their setup according to the layout of their homes.

2.6 Constraints

The system is limited by the number of devices it can have connected to it. Depending on how many serial and USB ports are available on the monitoring unit, the number of devices that can be plugged in is determined.

2.7 Assumptions and Dependencies

Current assumption is that a central server will manage various hardware components throughout the apartment, dormitory or house. It is also assumed that the system will employ open networking standards to facilitate communication between components and the server. Furthermore, we assume that the system requires a constant power source and network connection to function properly. If the user wants added assurance, Terminus supports redundant power supplies as backing up of surveillance data on a remote server.
3 Specific Requirements

3.1 Priority Levels

Since Terminus is intended to be a commercial security system, its capabilities likely supersede the scope of a senior design project. As such, we have prioritized our requirements as follows:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>This is the highest priority level; all requirements of this level must be fully satisfied and verified in order for the software system to be released. The requirements at this level must be implemented for the senior design phase. (CRITICAL)</td>
</tr>
<tr>
<td>2</td>
<td>Requirements of this priority are not expected to be verified by the current release of Terminus. The absence of these requirements must not create hazards and/or vulnerabilities for the system. However, these requirements are expected to be fully satisfied and verified by the next minor release (post-graduation) of the system. The features satisfying these non-verified requirements must be clearly documented to the end user as such. The requirements at this level will probably be implemented for the senior design phase unless there are unforeseen problems. (HIGH)</td>
</tr>
<tr>
<td>3</td>
<td>Requirements of this priority are not expected to be satisfied in the current release of Terminus. But, these are expected to be fully satisfied and verified at the next major release (post-graduation) of the system. The requirements at this level will be implemented for the senior design phase if time allows. (MEDIUM)</td>
</tr>
<tr>
<td>4</td>
<td>These requirements are of the lowest priority and are not within the current scope of the system design. These requirements are included only to indicate where the software is expected to change in future development. The requirements at this level will not be implemented for the senior design phase. (LOW)</td>
</tr>
</tbody>
</table>
3.2 Numbering Scheme

Each requirement will have the following scheme:

Category.Feature.Subfeature.Priority

**Category:** The specific category the feature belongs to (i.e., a specific component, user interface etc.)

**Feature:** A description of the feature.

When the feature number is 0, the associated requirement is a description of the category.

**Subfeature:** Specific details pertaining to a feature

**Priority:** An assigned priority

3.3 External Interface Requirements

3.3.1 User Interfaces

12.1.0.1 The Terminus client features a web interface to access the system on-site and remotely.

12.2.0.1 The interface provides users with an at-a-glance view, as well as detailed, categorical views for each component.

12.3.0.1 The system status (i.e. armed, disarmed, night mode, custom mode) must always be present and viewable while browsing through other views.

12.4.0.1 While viewing the status of individual components, the user must be able to enable and disable sensors and locks at his/her discretion.

3.3.2 Hardware Interfaces

13.1.0.1 The user’s computer must have an HTTP 1.1-compatible browser and an Internet connection.
3.3.3 Software Interfaces

14.1.0.1 Client
   The software interfaces with the user’s web browser and expects it to support HTTP 1.1. (see 20.1.0.1)

14.2.0.1 Database
   The software interfaces with database software. (see 20.2.0.1)

14.3.0.1 Server
   The system runs on an operating system that supports serving web pages and is capable of communicating with attached devices.

3.3.4 Communication Interfaces

15.1.0.1
   Communication between the client and the server is facilitated by common network protocols.

15.2.0.1
   Notification emails are sent using SMTP. (see 10.3.0.1)

15.3.0.1
   Communication to each device is dependent on the device’s specification.

3.4 Functional Requirements

3.4.1 Power Control

1.0.0.1 Control power control devices
   Provide users with the ability to control power control devices, allowing, for example, the control of power flow to appliances in the house such as A/C or lights.

1.1.0.1 Monitor power control devices
   Monitor overall status of all power control units. This includes present condition (is the control device supplying power) and presence information (is the device responding to commands).

1.2.0.1 Add a power controller
   Allow a new power control device to be recognized by the system.

   1.2.1.1 Apply a name for the power controller
      Allow a custom name to identify any controller device. Custom names must be unique to the device to avoid ambiguity when selecting devices.

1.3.0.1 Remove power controller
   Allow a controller to be removed from software monitoring and to be physically disconnected from the system.
1.4.0.1 Change status of power controller
   Change the status of a controller to any value the controller accepts, for example: on, off, 70% dim.

1.5.0.2 Schedule a change of status of power controller(s)
   Allow a change of status to occur at a given date and time in the future (scheduling past events is not useful and therefore not a requirement)

3.4.2 Door Lock
   2.1.0.1 Add lock controller
      Allow a lock controller to be physically added to the system and to be controlled by the software of the system.
      
      2.1.1.1 Apply a name for the lock controller
         Allow a custom name to identify any lock controller. Custom names must be unique to the device to avoid ambiguity when selecting devices

   2.2.0.1 Remove lock controller
      Remove control and monitoring of a lock controller from the software so that it can be physically removed from the system.

   2.3.0.1 Engage a lock
      Signal a lock controller to become engaged. This must result in the door being physically locked when the command succeeds.

   2.4.0.1 Disengage a lock
      Signal a lock controller to become disengaged. This must result in the door being physically unlocked when the command succeeds.

   2.5.0.1 Retrieve lock controller(s) status
      Query the lock controller for its status (locked/unlocked).

3.4.3 Video Capture
   3.1.0.1 Add a new camera
      Allow a video capture device to be physically added to the system and to be controlled by the software of the system.

      3.1.1.1 Apply a name for the camera
         Allow a custom name to identify any capture device. Custom names must be unique to the device to avoid ambiguity when selecting devices.

   3.2.0.1 Remove a camera
      Remove control and monitoring of a video capture device from the software so that the physical device can be physically removed from the system.

   3.3.0.1 Monitor feeds from any or all cameras
      Allow current video capture data to be seen through the user interface by the user of the system. The user must be able to view individual devices or all devices at once at the user's option.
3.4.0.1 Change the status of a camera
   Allow the software to enable or disable the capturing, storing and monitoring of
   the video stream from a selected video capture device.

3.5.0.1 Store the images that are captured
   Images from the video stream of a capture device must be able to be stored into a
   non-volatile storage system for later retrieval and viewing by the user.
   The method of capture must be configurable on a per-device basis. Methods are
   to include at least Fixed-frame-rate capture and Activity capture.

3.5.1.1 Store images locally
   Images must be able to be stored on a local storage device.

3.5.2.3 Store images remotely
   Images must be able to be stored on remote storage devices to allow both a
   larger capacity of storage than can be provided on the system locally and to
   provide redundancy and/or off-site backup of the data.

3.5.3.1 Fixed-frame-rate capture
   Given a positive integer number (>0) of frames per second or a positive float-
   ing point number (>0) of seconds per frame (to allow for, say, a 10 second
   gap between captures), capture and store images at the given rate from the
   video capture device with the given setting. Each device may be assigned a
   different rate.

3.5.4.3 Activity capture
   Given a threshold percentage of image change, capture and store all images
   that differ from the most recently captured image by at least the threshold
   value. In the base case where there is no previous image, the difference per-
   centage for the first image will be 100% without regard to the contents of the
   first image (e.g. store the image even if it is completely blank).

3.6.0.1 Sort and view the images that have already been stored
   Allow for the retrieval of and viewing of images from any used storage device
   (local and remote). Allow for the searching of the images by displaying them in a
   sorted list. The sorting criteria must be able to be stacked, that is, after sorting by
   one method, the resulting groups must be able to be sorted by another method.
   For example, first sort by camera, and then by date within each camera’s group.
   Additionally, each method must support ascending (regular sort) and descending
   (reversed sort) ordering.

3.6.1.1 Sort by date
   Sort all images in order by the time stamp of the capture of the image. This is
   for all images, not just from a single capture device. The encoding of the time
   stamp is left to the implementation, but is recommended to follow ISO-8601.

3.6.2.1 Sort by camera
   Sort the images in order of the capture device which was the source of the
   image.
3.6.2.4 Sort by activity
Sort the images in order by the percentage of change from the previously captured image (where the previous image is defined as the image with the least difference in time stamp occurring earlier than the current image and from the same capture device).

3.7.0.1 Delete images
Allow the removal of images from any storage device used by the image capturing system. This is needed for maintenance of the system and to maintain the health of free storage space.

3.7.1.1 Manual removal
Allow users to select individual or sets of individual images for removal.

3.7.2.3 Scheduled removal
Allow the user to set criteria for the removal of images based on a selected trigger and using a given sort method. Triggers must include at least percentage of free space on the storage device and time interval. As an example, the user must be able to specify that when disk space is low, delete the oldest images (trigger: disk<10%, method: sort by date descending). As another example, the user chooses that every week, remove the bottom 10% of images with regards to activity (trigger: duration=1week, method: sort by activity descending, amount=10%) It should be noted that an amount is not generally needed for disk space triggers, as the trigger will recur until the problem is solved.

3.4.4 Motion Detection
5.1.0.1 Add a motion sensor
Allow a motion sensing device to be physically added to the system and to be controlled by the software of the system.

5.1.1.1 Apply a name for the motion sensor
Allow a custom name to identify any sensor device. Custom names must be unique to the device to avoid ambiguity when selecting devices.

5.2.0.1 Remove a motion sensor
Remove control and monitoring of a motion sensing device from the software so that the physical device can by physically removed from the system.

5.3.0.1 Monitor motion sensor(s)
Each active sensor must be monitored. When a sensor is triggered on an active sensor, an alarm event must be raised.

5.4.0.1 Change status of motion sensor(s)
Allow the software to enable or disable the state of a sensor, marking it as active or disabled.
3.4.5 Temperature Sensing

6.1.0.1 Add a temperature sensor
Allow a temperature sensing device to be physically added to the system and to be controlled by the software of the system.

6.1.1.1 Apply a name for the temperature sensor
Allow a custom name to identify any sensor device. Custom names must be unique to the device to avoid ambiguity when selecting devices.

6.2.0.1 Remove a temperature sensor
Remove control and monitoring of a temperature sensing device from the software so that the physical device can be physically removed from the system.

6.3.0.1 Monitor temperature sensor(s)
Each active sensor must be monitored. When a sensor is triggered on an active sensor, an alarm event must be raised.

6.4.0.1 Change status of temperature sensor(s)
Allow the software to enable or disable the state of a sensor, marking it as active or disabled.

6.5.0.1 Set trigger thresholds
Allow setting upper and lower bound values of temperature to specify when the sensor is triggered. Additionally, allow the setting of hysteresis values for each of the upper and lower bounds. Allow a given bound to be disabled (to allow a user to only care about temperatures below freezing without worrying about setting an upper bound which doesn’t matter, for example).

3.4.6 UPS

7.1.0.1 Monitor the UPS for mains power failure
Monitor an uninterrupted power supply for power failure. When the power goes out and the UPS switches to battery, an alert must be raised and the system must initiate a shutdown.

7.2.0.1 Configure shutdown timing
Allow the duration of time to wait before initiating the system shutdown after the power failure to be specified. This allows the system to take advantage of different capacity UPS units, and gives the user more fine-grained control over the system to suit the needs of an individual installation.

7.3.0.2 Monitor UPS for non mains power failure events
Monitor the UPS for events other than mains power failure, including but not limited to, excessive load events and battery replacement needed events. Upon observing these events, a warning must be raised.
3.4.7 Token Authentication

8.0.0.1 Physical Authentication System
Allow users to authenticate themselves with the system in a secure manner while providing a unique ID allowing the user and the authentication point to be identified. Users will be assigned a token, which could be an iButton or RFID card for example.

8.1.0.1 Add a token
Allow a unique token to be registered with the system. Allow the token addition to occur by either manually entering the token information or by scanning the token with a token reader.

8.2.0.1 Associate a token with a user.
Allow a username to be assigned to a token in the system. Each token may represent only one user. A user may have 0 or more tokens.

8.3.0.1 Add a reader
Allow a token reading device to be physically added to the system and to be controlled by the software of the system.

8.4.0.2 Remove a token
Allow a token to be removed from the system. After this, the token will not be recognized for authentication.

8.5.0.3 Invalidate a token
Allow a token to be invalidated. Invalid tokens will be recognized as compromised when used for authentication. This allows a lost token to be marked as lost/stolen to prevent but also notice its use.

8.6.0.1 Monitor token readers
Monitor each token reader in the system for authentication requests. When a valid recognized token is seen, a “user authenticated” message must be raised, disarming the system if armed, and/or allowing the armed mode to be set. When an invalidated token is seen, an alert must be raised.

3.4.8 System Logging

9.0.0.1 Event Logging
The system has the ability to log all specified events to a centralized log stored on local storage and/or remote storage.

9.1.0.1 Event Types

9.1.1.1 Errors
All errors are logged.

9.1.2.1 New Component
New components added are logged.

9.1.3.1 Removed Components
Components removed are logged.
9.1.4.1 Lost Components
Components being disabled or unplugged are logged.

9.1.5.1 Notifications
All notifications going to the users are logged. This includes alerts, warnings, and notices.

9.1.6.1 Authentication
All login attempts into the system are logged.

9.2.0.1 Configuration Options
The logging system is configurable to the following extent:

9.2.1.1 Local Logs
Local location where logs are saved.

9.2.2.2 Remote Logs
Remote location where logs are saved.

9.2.3.2 Log life
Length of time to keep logs and images.

3.4.9 Email

10.0.0.1 Messaging Service
The email system provides a messaging service from the system to the user.

10.1.0.1 Message Contents Format
The input is generated automatically by the system using settings that are configurable by the user.

10.1.1.1 Device Filtering
The user can select which device types from which to receive notifications.

10.2.0.1 Message Output Format
The output is in the form of an email to an email account.

10.3.0.1 Message Delivery
The message is sent via the SMTP protocol.

3.5 Security Requirements

11.1.0.2 Data Backup
The system allows for the backup of archived data to local or remote non-volatile storage systems. The backups do not interfere with the user or device interaction.

11.2.0.1 System Access
The system allows only valid users to log into the system. A valid user is one that has not been disabled or removed from the system.
11.2.1.1 Access Method
A username and password are required to log onto the system’s web interface.

11.3.0.1 System (dis)arming
The system can be armed/disarmed via the web interface or via the Token Authentication component.

3.6 Design Constraints

The system is dependent on electricity and network connectivity. If any of these dependencies are removed, then the system will not function properly.

Furthermore, the hardware used in the system has to be supported by the operating system. A list of supported hardware will be included in the release notes. The operating system is defined by the implementation.

3.7 Software System Attributes

3.7.1 Availability

16.1.0.1 Fault Tolerance
The system is available as long as hardware and network are not faulty.

16.2.0.1 System Access
The system is available through the web interface both when armed and disarmed.

3.7.2 Maintainability

17.1.0.1 Components
The system is broken into components, each requiring servicing according to the hardware manufacturer.

17.2.0.3 Updates
The platform is updated through the operating system auto-updates, controlled by the Terminus system distributor(s).

3.7.3 Reliability

18.1.0.3 Power
Power failures must not result in corruption of non-volatile storage.

18.2.0.4 Network
The user is notified that the system lost network connectivity (through the use of off-site monitoring, provided, for example, through a subscription service).
3.7.4 Internationalization

19.1.0.1 Base Language
The system supports the English language as defined by the EN-US locale.

19.1.0.4 Other Languages
The system supports multiple languages and all system messages are configurable to be displayed in the selected language.

3.7.5 Portability

20.1.0.1 Client Interface
The client software (web based application) is written in compliance with HTTP 1.1\textsuperscript{14}, TCP/IP\textsuperscript{15} and ECMAScript (ECMA-262 (JavaScript))\textsuperscript{10} standards.

20.2.0.1 Database
The database software is limited to any ANSI-SQL compatible relational database management system.

3.7.6 Testability

21.1.0.1 Modules
The system is broken into modules to ease the partitioning of tests.

21.2.0.3 Automated Test Suite
The system will have a suite of test cases to verify the functionality of the code. This will include a simulation architecture so that the code base may be tested independent of hardware devices.

21.3.0.3 Manual Test Suite
The system will have a checklist of test cases to verify the functionality of the system as a whole. These tests will include verifying that the hardware works and the system responds in an appropriate manner.
3.8 User Interface

3.8.1 Login Page

The user is presented with a simple login page. They are shown the name of their system, “Steve’s House” in this example, and two text boxes to enter their credentials for authentication.

3.8.2 Main Page

The user can configure modules and the interface via settings, or the user can log out of the system by clicking logout.

The user’s home view presents them with an overview of modules chosen by them in the settings. In this case, an overview of the kitchen camera, locks, and temperature were chosen.
4 Use Cases

4.1 Power Control

4.1.1 Add New Controller

The user purchases an X10 controller and connects it to the system, which logs that a new device has been detected. After the user logs onto the web interface, the system informs him/her that it has detected a new device and asks if he/she wishes to install it. The user selects it on the interface, types in a name, and selects “Install”. The user receives confirmation that the installation was successful and the controller appears as a monitored device on the interface. The event is appended to the system log, marking the addition of the new device.

4.1.2 Remove Controller

The user clicks on an installed X10 controller on the web interface and selects “Remove”. The system prompts for confirmation before proceeding to remove the sensor from its list of monitored devices. Upon removal, the system logs the event and the user sees that the device is no longer showing on the web interface.

4.1.3 Unreachable Controller

The user disconnects an X10 controller that is currently being monitored by the system. On the web interface, the icon for the controller is grayed out and all related schedules are disabled. The system sends a signal to the disconnected controller in an attempt to reestablish contact with the device. The user is presented with a message informing him/her that a controller is unavailable. He/she has the options to redetect or remove it from the system. The user selects “Scan”, and the system attempts to poll for the device. After a few unsuccessful attempts to redetect the device, the user chooses to remove the device.

4.1.4 Scheduled Events

The user logs onto the web interface, selects the house lights, and clicks “Schedule”. The user configures the foyer lights to remain on between 6 PM and 11 PM and the remaining room lights to turn on when motion is detected between 6 PM and 6 AM. He/she also sets the motion-activated lights to turn off after five minutes of idling. After logging off, the user notices the hallway lights turn on as he/she heads to his/her room for bed.

While the user is late at work, he/she remotely logs onto the web interface and proceeds to the lighting tab. The user initially turns on the foyer, living room, kitchen, and bedroom lights, then schedules them to alternate on and off each hour to make it seem
that someone is home. He/she also checks that the status of the security, temperature, and smoke sensors before logging off and continuing his/her work.

4.2 Door Lock

4.2.1 Lock/Unlock Upon Signal

The user is logged onto the web interface and receives a phone call from a friend that he/she is outside. The user selects the appropriate door on the interface and selects “Unlock”. The door module receives a message and unlocks the specified door. Depending on how the system is set up, another module can send this signal to the door module and it will lock/unlock accordingly.

4.2.2 Forced Entry

While the user is asleep, an intruder runs to the door and attempts to kick it down. As the intruder kicks the door, the door’s shock sensor trips and the door module sets off the alarm. A message is also sent to the user informing him/her that the system has detected an attempted forced entry as it locks all monitored doors inside the home and sets off the house siren. The user is awakened by the siren and calls the police.

The user is away at work and an intruder approaches the front door. The intruder does not attempt to break the door down, but chooses to quietly pick the door lock. The intruder manages to pick the door, which trips the contact switch after he/she opens the door and sounds the alarm. The user is informed of the event and calls the police at his/her discretion.

During the middle of the day, a burglar approaches the user’s property through the backyard. The intruder notices that the user’s home has a glass patio and throws a brick to shatter the glass door. A glass break sensor trips and signals the door module, which sounds the alarm and alerts the user of the event.

4.2.3 General Security

The particular user’s home employs both door strikes and magnetic locks to secure its doors. The neighborhood suffers a blackout, leaving the user’s home without power. As these are magnetic door locks, they disengage after power is lost. Because the system is now only powered by UPS, it disables all magnetic door locks and engages door strikes. By doing so, the doors are still secure while the power is down and system is able to conserve power.

The system actively monitors the home and its entry points. As the user is reading a book in the living room, he/she falls asleep. The system notices that the user has left the front door unlocked and automatically locks the door after a specified amount of time has passed.
4.3 Video Capture

4.3.1 Add New Camera

The user purchases a new wireless camera, mounts it on a wall, and connects it to the system. The system detects the new device and logs the event. After logging onto the web interface, the system informs the user that it has detected a new camera and provides him/her with the option of installing it. The user types in a name for the camera and selects “Install”. The system adds the camera to its list of monitored devices and logs the event, then presents the user with confirmation that the installation was successful. After receiving the message, the user is presented with a live feed from the camera to confirm that it is working properly.

4.3.2 Remove Camera

While on the web interface, the user selects a camera from the camera list and selects “Remove”. After confirming, the system removes the camera from its list of monitored devices and shows that the removal was successful. The system logs the event and removes the device from the web interface.

4.3.3 Disable Camera

The user chooses the “Disable” option in the web interface for the camera in focus. The system logs the event and the user is presented with a message informing him/her that the camera is unavailable. The user replaces the battery and relocates the camera without raising any alerts. An alert icon is displayed and the controller is grayed out in the web interface. The user notices that all operations related to that camera are disabled until he/she selects “Enable” to return the camera to an active state.

4.3.4 Low battery and low signal alerts (Maintenance)

While the user is logged on the web interface, a message appears alerting him/her that the battery in Camera 1 is running low. The user then disables the camera and replaces the batteries. After re-enabling Camera 1, he/she sees that the alert has disappeared and checks the feed is transmitting clearly.

Another message alerts the user that the system is receiving a weak signal from Camera 2. The user disables and re-enables the camera and sees the alert is still present. The user then repeats the process but moves the camera to another location. After re-enabling Camera 2, he/she notices that the alert has disappeared and that the feed is transmitting clearly.
4.3.5 Controller becomes unavailable

While home, the user receives a notification informing him/her that the system has lost contact with Camera 3. The user logs onto the web interface and is presented with an alert icon showing lack of connectivity with the camera. He/she attempts to disable and enable the device, but is faced with the same problem. After troubleshooting the camera, the user discovers that the camera is defective and removes it from the system.

4.3.6 Motion detection (with camera recording)

While the system is armed, a burglar breaks in through the front door. The system detects the entry and sends a message to the user. As the burglar steps through the foyer, the hallway camera detects motion and begins recording as the intruder proceeds down the main corridor. Depending on how the messaging is set up, the system sends intermittent audio or video clips to the user. The user does not recognize the person from the clips and calls the police to alert them of a break-in.

4.3.7 Infrared low light image capture

The system is armed and the user is asleep in his/her bedroom. The cameras in the house detect that it is dark and switch to low light infrared mode. An intruder picks the front door open, tripping the alarm and the motion sensors on the main hallway camera. The intruder is recorded upon entry of the home, and the user is able to provide this evidence to the police.

4.4 Temperature and Motion Detection

4.4.1 Add New Sensor

The user purchases a temperature sensor and connects it to the system. After logging onto the web interface, the system informs the user that a new device has been detected. He/she selects it on the interface, types in a name, and selects “Install”. The user receives confirmation that the installation was successful and the sensor appears as a monitored device on the interface. The event is appended to the system log, marking the addition of the new device.

4.4.2 Enable a Sensor

The user logs onto the web interface after moving the smoke sensor closer to the kitchen. The system informs the user that this sensor is still disabled and will not detect smoke in the event of a fire. The user selects the sensor and clicks on “Enable”, whichreactivates the sensor.
4.4.3 Disable a Sensor

The user logs onto the user interface, selects the living room motion sensor, and clicks “Disable”. The system logs the event and confirms that the sensor is disabled. After unmounting the motion sensor and installing it in the first floor hallway, the user selects the same motion sensor and clicks “Enable”. He steps away to walk through the hallway and returns to see that the sensor module has logged the events of his movement.

4.4.4 Query a Sensor

The user logs onto the system remotely to check the status of the house. He/she selects the temperature sensors and clicks “Query” and sees that the temperature readings from each sensor is around 70 degrees F. The user then queries the motion sensors, which report no movement detected. After also checking the smoke and carbon monoxide sensors, the user logs off the system.

4.4.5 Remove a Sensor

The user clicks on an installed carbon monoxide sensor on the web interface and selects “Remove”. The system prompts for confirmation before proceeding to remove the sensor from its list of monitored devices. Upon removal, the system logs the event and the user sees that the device is no longer showing on the web interface.

4.4.6 Add New Unknown Sensor

The user connects a new temperature sensor to the back door, but the system cannot determine the sensor type. The system issues an “unknown sensor” event and asks the user whether he/she wants to: 1) redetect the device, 2) switch to advanced settings, or 3) perform a software update. The user first tries to redetect the device, but the system still fails to recognize it. Next, the user tries the second option and manually enters his/her own configurations and attempts another redetect. After this fails, the user resorts to the final option and performs a system update. When completed, a message appears stating that the system has recognized a new temperature sensor and asks the user whether to install. The user selects “Install” and the system confirms that the installation was successful.
4.4.7 Unavailable Sensor

The user receives a notification informing him/her that the system has lost contact with the front door contact sensor. The user logs onto the web interface and is presented with an alert icon showing lack of connectivity with the door sensor. He/she attempts to disable and enable the device, but is faced with the same problem. After troubleshooting the sensor, the user discovers that the cable connecting it to the system is loose. The user reconnects the sensor and the system logs that it has resumed connectivity with the missing sensor.

4.5 UPS

4.5.1 Notify Users of Power Outage

The house suffers a power outage during a major thunderstorm. The outage is detected and an alert is sent to the user informing him/her that the system has switched to UPS for power. The user logs onto the web interface and confirms that the system is running of the UPS. He/she takes note of the remaining time until the UPS runs out of power and calls the electric company.

4.5.2 Notify Users of Important Events

The house is still without power and the UPS only has ten percent power remaining. A low power event is logged by the system and it sends the user a message stating the event and how much more time is available before shutdown.

Power is still unavailable and UPS power levels are critical. The system logs a critical power event and informs the user that it is initiating shutdown in one minute. It proceeds to shut down its processes and power down.

4.5.3 Configure Shutdown Times

The user installs an UPS device to power the system. He/she logs onto the web interface and is informed that the system has detected a new UPS device. The user types in the label for the device and selects “Install”. The system logs the events and provides the user with the status of the UPS and prompts him/her to configure power management settings. The user proceeds to the settings and sets the system to issue alerts when the UPS turns on and reaches 25% and 15% remaining power levels. He/she also configures the system to shut down when the UPS reaches 10% power or lower.
4.5.4 UPS unavailable due to maintenance issue/faulty device(s)

The user unplugs the current UPS unit and swaps in another one. The user is alerted that the UPS has become unavailable and that a new device has been detected. He/she logs onto the web interface and removes the old UPS unit and installs the new one. The system confirms the actions are successful and stops sending alerts about the old UPS.

The user receives a notification that the system has lost contact with the UPS unit. After unsuccessfully disabling and re-enabling the device on the web interface, he/she finds that the unit is unplugged. When the user returns to the web interface after plugging back the UPS, he/she notices that the system has not reestablished contact. The user selects the device and clicks “Redetect” and is presented with message stating that the system has found the UPS and is given the current status for the unit.

4.6 Token Authentication

4.6.1 Add New Token Reader

The user connects a token reader to the system and logs onto the web interface. He/she is notified that a new token reader has been detected and is prompted whether to install the new device. The user gives the device a label and clicks “Install”. The system confirms that the installation was successful and brings up a configuration menu for the token reader. The user sets the system to unlock the front door when a security token successfully authenticates and defines which tokens are authorized to work with the system.

4.6.2 Authenticate Users

The user returns home from work and presses his security token against the token reader. The system recognizes the token and unlocks the door for the user and temporarily deactivates door sensors. The user walks in, but leaves the door open. After a user-defined idle time has passed, the system reactivates the door sensors and sends a message to the user notifying him/her that the front door is still open. The user returns to the front door and closes it.

A burglar approaches the front door and attempts to use an unauthorized security token on the door. The token fails to authenticate and the system informs the user of the failed authentication and logs the event. The user calls a neighbor and asks if he/she sees a stranger trying to open the door.
4.6.3  Add New User to the System

The user logs onto the web interface and adds a new user to the system. He/she assigns the new user a new security token and gives it to them to test. The new user walks outside and attempts to authenticate his/her token on the reader. The reader successfully reads the token and unlocks the front door.

The user receives a phone call from a friend who is supposed to be watching his/her home while he/she is on vacation. He/she is told that the friend is at his/her front door, but is unable to lock it with their security token. The user logs onto the web interface from his laptop and sees the failed authentications from the door reader module. After adding the friend’s token to the list of authorized tokens, the user tells him/her to try again. After his/her friend enters the home, the user sees the system has logged the entry event.

4.6.4  Token Communication Error

The user attempts to unlock the front door with his security token, but it fails to authenticate. The system logs a failed authentication event and sends a message to the user. The user logs onto the web interface and is presented with the failed entry notifications. He/she realizes that the security token is defective and swaps it out with a working one.

The system loses contact with the token reader installed at the front door and sends a message to the user. The user checks the front door and notices that the reader has been damaged. He/she removes the broken reader and installs a new unit. After logging onto the system, the user selects the old reader and uninstalls it. After confirming the uninstallation, he/she selects the newly discovered token reader, installs it, and configures it to unlock the front door.

4.6.5  Remove Token

The user accidentally drops his/her security token in water, causing irrevocable damage. The user logs onto the web interface and removes his/her security token from system’s list of authorized tokens. The user gets another security token, adds it to the token list, and confirms that it unlocks the front door. The system logs the removal, adding, authentication, and unlock events.

4.6.6  Invalidate Token

The user cannot find his/her security token and wants to prevent it from being used to enter the house. He/she logs onto the web interface and selects the specific token that was missing. The user selects “Invalidate”, causing the system to recognize the token but ignores it for access to the residence.
4.7 System Logging

4.7.1 Event Logging

A smoke sensor on the second floor of the user’s home detects smoke and sends a signal. The system logs the event and sends a message to the user, alerting of a possible fire. The temperature sensor in the second floor hallway detects that the temperature of the home is twenty degrees over the thermostat setting. This is suspicious because of the detected smoke and discrepancy in temperature, and the system logs event and sends another message to the user.

4.7.2 Event Types

The user logs onto the web interface to check the status of the home’s sensors. The system logs the login, acknowledged notifications and alerts, and modules accessed while the user is navigating through the interface. After the user logs off, the system also logs the logoff event.

4.7.3 Configuration Options

The user logs onto the web interface after setting up the system. He/she configures the system to archive and clear from local hard drive storage all logs and camera data nightly at 3AM to a remote server. The user also has the system archive and clear this data if the size reaches or exceeds 1 GB. For extra security, he/she also configures the system to automatically log events concerning physical or network breaches of the system to the remote server when they occur.

4.8 Multiple Modules

4.8.1 Unauthorized Entry Recorded

The user returns home from work and arms the system, but forgets to lock the door. A burglar walks up to the door and opens it, tripping the contact switch and setting off the alarm and siren. The foyer camera receives a message from the door module and begins recording the break-in. The user awakens to see the intruder running out the door and calls the police. He/she then logs onto the web interface and is presented from the alerts generated by the security breach and sees the recorded video from the camera.

After arming the system, the user exits the front door, but realizes that he/she forgot something in the house. He/she opens the door before disarming the system, which trips the contact switch and sets off the alarm. While the user is disarming the system via the wall console, he/she receives a message from the system of an unauthorized entry with a picture of themselves walking through the front door.
4.8.2 Home Automation

The user arrives home after dark and authenticates with his security token. After the system disarms, it turns on the foyer light and unlocks the door. Because there is now someone home, the system also adjusts the thermostat to a more comfortable temperature. The user enters and motion sensors activate lights as he/she walks through the house.

4.9 Maintainability

4.9.1 Software Updates

The user completes the initial system installation and configures it to receive software updates when they become available from the update service. After returning from work the next day, he/she logs onto the web interface and is presented with a list of available updates issued by the service. The user reads through the descriptions, clicks on the desired updates, and selects “Install Updates”. The system installs the updates and returns a confirmation message showing the details of the update installations.

4.10 Reliability

4.10.1 Power and Network

The user’s home is equipped with a telephone, DSL, and satellite connection. While the user is away, a burglar cuts the phone and power lines, knowing that this will sever network and telephone connectivity and power. The system detects that these connections are lost and switches to UPS power. It logs the lost connectivity and power outage events, and messages the user over the satellite connection. When the burglar picks the lock and opens the door, he/she is caught off guard by the siren and runs away. The user is kept informed of these events and calls the police.

4.11 Security Requirements

4.11.1 User Access and Permissions

The user is going out for a few hours and wants the babysitter to have limited access to the system to watch the house. The user logs onto the system and creates a custom account with permissions to lock or unlock the doors and arm or disarm the system and whose actions are logged by the system and forwarded to the user. He/she logs on as the test user and checks that the account is limited to defined permissions and that events are being sent to his/her mobile phone.
4.12 Web Interface

4.12.1 Sorting Images

The user is logged on the web interface and clicks on the camera images section. The system logs that images are requested and received from the database and presents the user with images. By default, the system displays the images by date with the most recent on top. The date column header has an arrow icon pointing down, indicating that it is in descending order. The user wants to see the oldest pictures, so he/she clicks on the date column header. The arrow on the column header reverses and points up, indicating that it is now in ascending order. The user next wants to view images sorted by camera and clicks on the camera column header. An downward-pointing arrow appears next to the camera column header and all images are shown sorted by camera in descending order. The user then clicks on an image and selects “sort by activity”. The images appear sorted by the percentage of change from the selected image.

4.12.2 Deleting Images

Logged on the web interface, the user selects some old images and clicks “Delete” and the system logs the event and removes the images from the system. He/she then schedules the oldest images to be backed up to a remove server and removed when the system’s hard drive space reaches below 10%. The system logs the schedule event and saves the user’s configuration.
5 References

1 Terminus information - <http://en.wikipedia.org/wiki/Terminus (mythology)>


4 Shih, E (2007, August 26). Now’s the time to buy tech items for college freshmen; no need to get stressed; just do your homework. The Record


6 (1, 2) Guardian Protection Services - <http://www.guardianprotection.com/>

7 ADT - <https://www.adt.com/>


9 Renter’s insurance can serve as a defence for college students. Retrieved October 14, 2007, from Young Money Web site: <http://www.youngmoney.com/money_management/student_insurance/021007_02>


