**(ADDED TO PAPER)**

**Standards**

When building a fire alarm system there are many standards and regulations that have to be taken into account. Power supply standards need to be taken into account when considering batteries, electrical circuits and AC/DC wall outlet power. Wireless standards have to be considering because out hub will be using WiFi wireless communication and the alarms will be designed to use zigbee wireless communication. Network security standards will also need to be considered. Lastly, there are standards for printed circuit boards that control the PCB layout process.

**Standards for Power Consumption**

CUI inc. provides power consumption standards in their publication of Power Supply Safety Standards. This document includes every aspect of a system and sets voltage limits for all components and sets limitations on what types of components can be used within a circuit. The Power Supply Safety Standards also provides recommendations for insulation and shock prevention. Below is a table detailing the four different types of circuits and their requirements.

|  |  |
| --- | --- |
| **Circuit** | **Definition** |
| Hazardous Voltage | Any voltage exceeding 42.2 Vac peak or 60 Vdc without a limited current circuit |
| Extra-Low Voltage (ELV) | A voltage in a secondary circuit not exceeding 42.4 Vac peak of 60 Vdc, the circuit being separated from hazardous voltage by at least basic insulation. |
| Safety Extra-Low Voltage (SELV) Circuit | A secondary circuit that cannot reach a hazardous voltage between any two accessible parts or an accessible part and protective earth under normal operation or while experiencing a single fault. In the event of a single fault condition (insulation or component failure) the voltage in accessible parts of SELV circuits shall not exceed 42.4 Vac peak or 60 Vdc for longer than 200 ms. An absolute limit of 71 Vac peak or 120 Vdc must not be exceeded. SELV circuits must be separated from hazardous voltages, e.g. primary circuits, by two levels of protection, which may be double insulation, or basic insulation combined with an earthed conductive barrier. SELV secondaries are considered safe for operator access. Circuits fed by SELV power supply outputs do not require extensive safety testing or creepage and clearance evaluations |
| Limited Current Circuit | These circuits may be accessible even though voltages are in excess of SELV requirements. A limited current circuit is designed to ensure that under a fault condition, the current that can be drawn is not hazardous. Limits are detailed as follows:  For frequencies < 1 kHz the steady state current drawn shall not exceed 0.7 mA peak ac or 2 mA dc. For frequencies above 1 kHz the limit of 0.7 mA is multiplied by the frequency in kHz but shall not exceed 70 mA.  For accessible parts not exceeding 450 Vac peak or 450 Vdc, the maximum circuit capacitance allowed is 0.1 μF.  For accessible parts not exceeding 1500 Vac peak or 1500 Vdc the maximum stored charge allowed is 45 μC and the available energy shall not be above 350 mJ.  To qualify for limited current status the circuit must also have the same segregation rules as SELV circuits. |

The circuit design for our Smart Fire Alarm System can be considered as part of the Extra-Low Voltage (ELV) circuit. If designers can find a way to double insulate the system than it can be considered Safety ELV. The Smart Fire Alarm System will pull 5.1 volts from the AC/DC adapter. A maximum of 9 volts will be between the battery terminals and therefor will be the maximum total voltage flowing through out the circuit in battery backup mode. Insulation will be included in the AC/DC adapter as well as the plastic casing that will go around the alarm. The plastic casing will prevent short circuits caused from collisions with the outside environment.

**IEEE Wireless Standards**

The Institute of Electrical and Electronics Engineers, also known as IEEE, is an association that sets many different standards in many different categories. One of the important wireless standards that they maintain is the IEEE 802.11 standards. Products that implement these standards must pass tests and then are referred to as “Wi-Fi certified.” There are two types of Wi-Fi Standards that are to be considered. The one that our project will be using is the 2.4 GHz wireless spectrum. This is the default Wi-Fi Broadcom module that is included with the Raspberry Pi.

The other standard that has to be considered is that of the ZigBee wireless spectrum. The fire alarms themselves will be using Xbee modules that output under what is known as the 802.15.4 spectrum. IEEE also provides standards for this level of spectrum. 802.15.4 is a standard that defines the operation of low-rate wireless personal area networks. IEEE designed the standard way back in 2003 and has been used by ZigBee, WirelessHART, SNAP and others. IEE has defined three frequencies under the 802.15.4 standard. The North American region is defined as between 902 and 928 MHz running on 10 channels. It has a bandwidth of 2 MHz and a data rate of 40 kb/s. Europe also has its own standard defined as 868-868.6 MHz running on only 1 channel. It has a bandwidth of 0.6 MHz and a data rate of 20 kb/s. The last standard for 802.15.4 wireless communication is the global region. This is a frequency between 2.4GHz and 4.483.5 GHz running on 16 channels. This standard has a bandwidth of 5 MHz and a data rate of 250 kb/s. We have chosen to use the North American standard for our project as it provides enough of a data rate while allowing as much energy consumption as possible. (http://www.ieee802.org/15/pub/TG4.html)

**Security Standards**

The last type of standard that needs to be considered is that of network security. IEE specifies that implementing this type of standard is completely optional. The IEEE network security standard defines that a product implements network security if it has “a mechanism to perform a cryptographic transformation on incoming and outgoing frames.” Because our fire alarms will be connected to the building network, it will need to implement network security to keep the integrity of the commercial company and owns the building intact. Thankfully, the Xbee modules that will be used for our project allow for an encryption setting that encrypts all incoming and outgoing messages. There are three variables that need to be set inside of the Xbee module in order to be defined as a secure network. These variables can be set during configuration of the wireless modules. This allows for all devices to talk to each other with only the devices of our system being able to decrypt those messages. Our system will enable this setting so that intruders are unable to get into the company network by intercepting one of the heartbeats sent out by the system and allowing intruders to intercept network data and passwords.