# The Comprehensive Handling of Safety in an Autonomous Robot Capstone Project

*Dr. John G. Ciezki, U.S. Air Force Academy*
*Dr. Steve E. Watkins, Missouri University of Science and Technology*

## Abstract

A systematic approach to safety issues is described in the context of an autonomous robot capstone project. The treatment of safety should not be an ad hoc or after-thought aspect of design projects. Engineering students need to consider safety as an integral component of the design process and to identify and address hazards systematically in each stage of project work. Appropriate actions include researching professional standards and regulations, incorporating safety best practices, developing safety checklists and operating protocols, and providing significant safety documentation. Formal safety components were added to a capstone design project for electrical and computer engineering undergraduates in which an R2D2-like robot was designed and built. The work provides project examples, lessons learned, and student feedback related to the safety treatment.

## Introduction

Fundamental aspects of engineering design include realistic safety constraints and protocols and the professional responsibility to make decisions consistent with the safety of engineers, operators, and the public. An accreditation outcome in engineering education is design in which safety is an important consideration [1]. Professional codes of ethics emphasize the responsibility of engineers to consider the "safety, health, and welfare of the public" [2,3]. Regulations, standards, laboratory practices, etc. reflect the importance of safety in engineering work. Also, the negative consequences associated with safety-related failures such as accidents and product defects make such issues a priority for industry. Creating a safety culture is difficult. It involves the performance of proper actions and the avoidance of improper actions. Any definition of safety must specify what is considered proper, what is considered improper, and what is an acceptable degree of risk.

In engineering education, practical safety concerns are necessarily part of laboratory courses and safety concepts are often included in lecture discussions. However, these concepts must compete with full curricula that address the many technical aspects of engineering practice. Also, the incorporation of safety considerations into the design process is a high level challenge. A natural opportunity to treat safety as a design component is in the capstone design experience. If safety instruction is an educational objective of the capstone experience, the pedagogy must be intentional. For instance, students may come away with the impression that safety considerations have secondary importance or that such considerations are an end-of-project exercise, if the project definition, the design documentation, and project evaluation do not include significant safety requirements. Without specific expectations, students are prone to focus on immediate concerns of technical specifications, scheduling pressures, and budgetary constraints and they may handle safety issues in an ad hoc fashion relying mainly on common sense and protocols practiced in the typical undergraduate laboratory environment. There is clear educational value to integrating safety considerations and processes in a comprehensive fashion.

This work proposes a comprehensive treatment of safety issues within a capstone design project. The intention is to integrate safety considerations into all stages of design activity, while avoiding exercises that may be seen as contrived or superficial. The systematic approach to safety and risk includes formal engineering standards and practice. It starts at initial design definitions and is part of each subsequent stage. Design documentation should address hazards and remediation for the design team during the development process, for operators and bystanders during normal usage, and for maintainers during the product life cycle. The context for initial implementation was a capstone design project for electrical and computer engineering undergraduates with an R2D2-like autonomous robot. Project examples, lessons learned, and student feedback as related to the safety treatment are discussed.

## Engineering Education and Safety

### *Safety Overview*

The study and practice of engineering safety is certainly nothing new. Books have been written on the subject [4]. Accident prevention techniques and best practices have been documented in handbooks [5]. Groups like the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), the Institute of Electrical and Electronic Engineers (IEEE) and the U.S. military routinely create requirements documents or "standards" to ensure materials, products, processes and services meet certain safety guidelines [6-9]. The Occupational Safety and Health Administration (OSHA) sets and enforces protective workplace safety and health standards [10], while independent not-for-profit testing laboratories, like Underwriters Laboratories (UL), certify the safety and quality of a broad range of products. Specific technology may also have safety rules and standards such as those for laser eye safety [11, 12]. In Europe, the "CE" marking (European Conformity) is either a manufacturer's declaration or certification by a "notified body" that a product meets applicable directives, including those on safety. This focus and emphasis on safety and reliability within industry and government contracting is understandable because accidents directly affect the bottom line due to (1) employee injuries, (2) broken equipment or lost material, (3) fines and penalties, (4) lawsuits, and (5) negative impacts on reputation. But the question becomes, how well are engineering programs doing readying students to function in this safety-oriented environment and, more specifically, how are they instilling safety considerations within the capstone design experience?

As an academic community, we acknowledge the importance of considering safety by prominently instantiating it as a "realistic constraint" in the ABET student outcome on design:

> **ABET Criterion 3, Student Outcome (c)**: an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic,

> environmental, social, political, ethical, health and safety, manufacturability, and sustainability [1].

We also see this emphasis reflected in the ethical obligation of an engineer to society as listed in the IEEE code of ethics:

> **IEEE Code of Ethics, Item 1**: to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment [2].

But telling students to "be safe" is entirely different than educating them in "how to be safe" and understanding the value of a safety culture. In light of regularly occurring safety challenges in our own senior design capstone projects, the authors were then interested in understanding how colleagues across engineering disciplines were addressing safety in the capstone experience. Is there a growing consensus on the pedagogy or, due to the nature of senior design, is it more ad hoc?

So, the starting point of our investigation was to review the literature using keywords like *safety*, *design*, *capstone*, and *education*. To our surprise, there were not many articles that focused specifically upon how the safety element of student outcome (c) was being assessed and not one article that proposed any sort of comprehensive safety framework for capstone projects. We are not insinuating that senior design projects are being supervised unsafely or that valuable safety exercises aren't being done, just that there is an apparent hole in the discussion and reporting on safety in the academic literature.

There are several outstanding articles that discuss the need for engineering safety education and how specialized courses can address that need. For instance in [13], the authors describe a 3-credit course on electrical safety offered during the summer months between junior and senior year at the Colorado School of Mines. The primary goal of the course is to equip students with the necessary skill set to recognize and avoid or control hazards posed by electrical work. The course does this by exposing student misconceptions about working with electricity, using incident case studies to personalize electrical accidents, team activities are emphasized over traditional lecturing, and modeling the correct attitudes about safety through invited expert guest lecturers such as electricians from regional plant facilities. Interestingly, this paper draws out an important perceived deficiency in academia: "A common criticism from industry representatives is that their new hires have very little understanding of how to conduct themselves safely in the work environment." [13]

In [14], authors at the Georgia Institute of Technology make the case for why accident causation and system safety should be taught to engineering students, how such a course can be organized, and how it specifically maps to ABET Criterion 3 Student Outcomes. Here are some important observations about teaching about accidents: (1) helps to ensure that they won't be repeated, (2) provides a multidisciplinary perspective on accidents and what is required by stakeholders to prevent them, (3) inculcates concern with failure promoting better problem solving, and (4) establishes an emotional connection through case studies that produce positive and enduring effects. The authors emphasize "learning loops" that provide both backward-looking and forwarding-looking perspectives on an accident investigation, and the notion of a "safety value chain" which emphasizes identifying all of the stakeholders who contribute to accident prevention. The course stresses concepts of "defense-in-depth" and "safety barriers" to prevent incidents from occurring, preventing escalation, and mitigating consequences. Finally, the course introduces risk analysis theory and tools. Students write analyses of case studies and a major term paper. [14]

In [15], the authors at Washington State University describe teaching safety in bioengineering design. Specifically, the paper advocates for the concept of "prevention through design", addressing safety needs in the design process to prevent or minimize hazards and risks found through the life cycle of facilities, materials, and equipment. The severity of safety issues is highlighted, tools are provided to assess risk, and then applied to existing projects. MIL-STD-1629A is used to assess reliability and then risk reduction strategies are formally identified, using design and then barriers, personal protective equipment, and warning signs. Students perform a risk analysis using ANSI B11.0 and learn that risk reduction is enhanced by a more robust design. [15]

Reference [16] documents the design of a graduate-level course in electrical safety. It too emphasizes the need to address safety at the design stage, identifying the presence of electrical hazards, and implementing measures to minimize risk. The course supplements lecture with videos, in-class activities, industry guests, and group project reports. [16]

Finally, in [17], some useful terms are defined and emphasized by the UK Health and Safety Executive (HSE) to the UK education community. It defines **safety** as the absence of danger. **Dangers** arise from hazards being realized through the failure of risk control. A **hazard** means anything that can cause harm.  Whereas **risk** is the chance, high to low, that someone can be harmed by the hazard. A **risk assessment** evaluates risks and whether controls are adequate. **Risk controls** involve the steps needed to reduce the chance or mitigate the consequences of a hazard causing harm. [17]

A 2016 report [18] analyzes attitudes, procedures, and administrative structures needed to reduce calamities in university labs.  It provides 20 specific recommendations drawn from multiple National Research Council (NRC) reports. Importantly, it describes why sometimes the academic environment is vulnerable to accidents that may not otherwise happen in industry. Lack of (1) independent lab facility and practices review, (2) incentives, (3) a safety culture, (4) training and (5) formalized best practices are areas that were exposed for attention. This is all complicated by students rushing to produce results or finish their work and known safety rules not being followed.

### *Capstone Design and Safety*

We want to re-emphasize that many programs across engineering disciplines are integrating considerations of safety into senior design through risk assessment templates and checklists [19], guidelines, and training [20]. And as mentioned previously, some programs have courses dedicated to safety that may precede and prepare a capstone experience. Our goal is to explore how to integrate some of these safety best practices into the framework of a senior design project. The challenge here is that capstone experiences can be structured quite differently going from one institution to another. Design courses may be one, two, or three semesters. They me be individual projects, partnered, small teams, or large interdisciplinary efforts. The project may be assigned, independently proposed by the students, or may arise from an external competition or corporate sponsor. It is easy to hypothesize that this variety in duration, complexity, focus, and project definition may significantly contribute toward more individualized approaches to the safety topic. It is obvious that some projects will not have many safety concerns and will not benefit from a comprehensive framework that will undoubtedly come across as "make work" for the student. In addition, senior design course directors and project mentors may have very different backgrounds and professional experiences with regards to safety that might complicate establishing a uniform framework. Another challenge is that safety issues in interdisciplinary projects may easily fall into expertise cracks that may not get exposed in a timely manner. In academia, we are generally more risk-adverse when it comes to undergraduate activities, and we will err on the side of avoiding any safety uncertainty because of the ethical responsibility to protect the student from harm.

A final challenge to implementing a safety framework is that we are dealing with engineering students and not practicing engineers. Students by definition are inexperienced and may disregard safety procedures or considerations out of haste, ignorance, or distraction. Students are still trying to master technical detail and have limited exposure to what can go wrong, what can break, and how to assess the reliability of a design. Industry addresses the issue of new engineers by assigning senior engineer mentors, having careful design reviews, and developing an unambiguous culture of safety where all stakeholders are on the lookout for unsafe practices.

Before we delve into a specific senior design case study, we want to outline a general framework for incorporating safety into such a project:

a. Define specific safety-related technical requirements for the project definition presented to the students;
b. Guide students to adopt clear safety metric(s) for use in subsystem/component trade studies;
c. Perform a top-down assessment of safety hazards; encourage students to consult with multiple technical experts to avoid gaps in hazard identification;
d. Complete a risk assessment, determining the likelihood of a hazard occurring, the severity of its impact, the ability to avoid the hazard or to detect its onset;
e. Identify relevant standards/best practices;
f. Consider design choices that might prevent hazards or minimize their impact;
g. Formulate barriers to isolate unavoidable hazards and mandate the use of appropriate personal protective devices to minimize the potential for injury;

h. Schedule appropriate lab/equipment training;
i. Institute well-defined rules governing lab use, including after-hour sign-in/out sheets and rules governing when, for instance, main battery power can be applied to any robot;
j. Schedule periodic safety reviews/inspections by someone external to the project. The goal here is to clearly show an institutional commitment to safe practices;
k. Perform a bottom-up failure analysis and risk reconsideration; establish how system components can fail and what combinations of failure can create project hazards;
l. Develop an operational checklist to instantiate a proven and tested means of operating the system;
m. Arrange for the capstone team to receive emergency training so they understand what needs to be done and who needs to be contacted if there is an accident or injury;
n. Label systems to make future users aware of areas that may pose shock, pinching, cutting, or piercing hazards;
o. Require clear and complete documentation of mechanical layout and electrical circuitry to ensure accurate information for users to trouble-shoot or decommission the system.

Where possible, the above list should be incorporated into existing capstone technical deliverables to avoid both project over-load and the perception by students that safety considerations are somehow separate and distinct of the design process. Mentors should be ready to assist students in areas where students historically struggle due to inexperience or ignorance. As always, the results of exercises should be tangible to avoid students complaining about “make work” and reducing the educational value.

## Robot Case Example

### *R2D2 Project*

A comprehensive safety treatment was incorporated into a capstone design project. The project was supported by the Department of Electrical and Computer Engineering and satisfied a two-semester senior requirement. The team consisted of five Air Force Academy cadets: two electrical engineering seniors, two computer engineering seniors, and a systems engineering senior.

The technical objective of the project was to design, build, and test a full-sized replica of the R2D2 Astromech droid from the Star Wars franchise. The basic frame as shown in Figure 1 was provided. The desired functions included remote-controlled and autonomous movement.

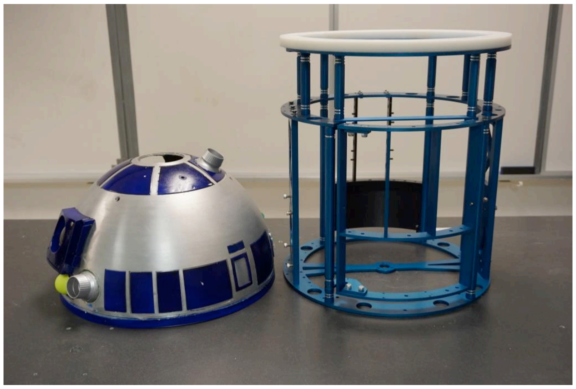


Figure 1. Frame for the R2D2 Robot.

The scope of the project was specified per the following requirements.

- The robot should be an accurate physical depiction of the character (within reasonable constraint of the other requirements).
- The vehicle should be Radio-Control (RC) drivable with a maximum speed of ~1m/s.
- The unit should demonstrate a limited autonomous operation, implementing some sort of rudimentary routine to follow walls and/or people.
- The dome of R2D2 should rotate in either direction under computer control and be accurately resettable to its nominal forward position.
- The robot should detect sound and speech via microphone.
- R2D2 should be able to generate sounds consistent with the character.
- The robot should be capable of mapping a space for obstacles and use sensors to dynamically identify path obstacles.
- The navigation system should employ motor encoders to aid in odometry and vehicle localization.
- The vehicle should accommodate computer-controlled video projection onto a wall.
- The vehicle should facilitate computer-controlled on-board camera recording for later playback.
- The robot navigation software should allow camera-assisted color vest tracking.
- The R2D2 unit should have convenient on-board battery charging.
- *The robot electrical system should be protected by fuses, should employ emergency shutdown via a "kill switch," and should relay error messages to an external status screen.*
- *The vehicle should have an external LED status indicator to show the mode of operation.*
- *The robot mechanical and electrical layout should have no sharp edges or exposed terminals.*
- *Robot operation should lead to no unwanted collisions or destruction of property.*

The final four items (shown in italics) represent how safety factors were included into the project definition. The kill switch was to be augmented by a computer-generated "kill" command that could also disable all robot motion. It was also emphasized via item 16 that loss of communication or control power should lead to a safe robot operating condition. Metrics used during the design trade studies included: reliability, potential hazard, validation complexity, and maintainability.

### *Approach to Safety Issues*

Students were prepared for general laboratory work through on-site resources. This low-level safety training reinforced prior laboratory safety activities. They were trained in the safe use of hand tools in the department machine shop and were instructed on how to use a 3D-printer to produce some of their required parts. The department technician also made sure they were clear on safely best practices for soldering, crimping, or any work with paints and adhesives. The students were also prepared to take a formal safety class for using some of the larger cutting tools available in the Mechanical Engineering Lab, but this became unnecessary as the students were able to leverage full-time personnel to assist in larger activities like milling out the aluminum legs and welding the structure for the feet. Prior to final integration and testing, students were made aware of emergency contacts if an accident occurred where someone was hurt or significant damage to equipment occurred.

Higher-level safety preparation came through a review of standards related to the project. Many robot safety standards have been developed, some quite recent [21-25]. However, most of these standards primarily apply to industrial robots, e.g. robots with manipulator arms. This is understandable with the significant number of commercial robots that are involved with assembly, welding, and painting. Where mobile robots are addressed, the main applications include warehouse navigation via reflective tape or beacon, where the paths and function are repeated and predictable. The autonomous or RC-controlled operation of R2D2 does not fall into this discussion as nicely. However, there are basic considerations that can be drawn out from the standards that seem reasonable to also apply to R2D2: (1) identify the maximum allowable speed (safe slow speed is identified as 0.25-1.0m/s), (2) determine the minimum distance of separation with a human, (3) confirm reliable detection of obstacles close to the ground, hanging on a wall, and comprised of material that may not reliably reflect, (4) monitor the force that the robot is pressing upon something because it could be a human, and (5) consider the use of pendants to enable operation, barricades to secure areas, kill switches for power and control, warning labels for moving parts and voltage terminals, and flashing lights for signaling operation.

The next level of safety treatment was a top-down student analysis of possible failures, hazards, and risk. A failure event is hypothesized, the probability of it happening is assessed, and the seriousness of the failure weighed [26]. The most significant failure events then result in specifications being pushed down into various subsystems to help reduce the probability and seriousness, or make failure detection and mitigation easier. Appendix I lists some risk assessment tools/procedures found in reference [21]. These tools were incorporated in a formal safety and risk discussion at each major stage of the project. The stages were: (1) project initiation, (2) development stage, (3) integration stage, (4) software, and (5) operations stage.

## Implementation Details

### *Project Initiation*

Using the project scope statement, the standards background, and the risk assessment tools, students began a fault tree analysis in which the most likely hazards were identified. The following hazards were in this initial list:

- Robot collision with human, equipment, or wall
    - Sensor failure or inadequate sensor placement
    - Software logic failure
    - Loss of control connectivity
    - Unplanned obstacle
    - Kill-switch failure
- Mechanical failure that leads to R2D2 toppling over
    - Weight too large for bolts
    - Bad weld
    - Material strength failure
- Shock from exposed wiring or poor layout
    - Bad choice in connector
    - Bad solder joint
    - Bad crimp
- Battery initiating a fire or battery rupture
    - Overload
    - Mechanical shock due to collision
- Thermal overload
    - Propulsion or dome motor get stuck
    - Internal short
    - Relay or fuse failure

### *Development Stage*

First, the students analyzed what voltage should be selected for the propulsion system. The value was in part driven by the availability of a motor controller that had the ability to be computer or RC controlled. The students attempted to minimize the size and weight of the battery solution while being able to satisfy the specified operating time of the robot. The choice of 12V also was influenced by the desire to maintain a low voltage for reasons of safety. Obviously though, this would imply a system that had higher average currents. Students developed a dynamic model of the robot so they could anticipate current draw requirements and then size any protective devices and identify the required conductor gauge. Here, the students had to estimate the overall robot weight using estimates of previous designs and available parts.

In order to account for the safety hazard of a collision, the team emphasized minimizing the overall weight of the robot where possible to minimize the kinetic energy. Next, the team decided to go with a “foot design” that included two wheels per foot to enhance the stability of the robot. A non-powered castor wheel completed how the robot would contact the ground. Milled out aluminum was used for the legs; an aluminum frame was used for the body, and wood shelves were fitted inside the body to place electronics. Components in the body were planned to be secured to the shelves using velcro$^{TM}$ and cable tie wraps to enable ease of installation and removal.

Upon testing and evaluating options, the students decided to include both ultrasonic and laser-range-finder (LRF) sensors on the robot for path planning and obstacle avoidance. The goal was to achieve some level of redundancy and complement the field of view offered by each technology. The safety requirements on the LRF were investigated to ensure that its operation would not cause any concerns for those operating or observing the robot [27, 28]. The brain of R2D2 would consist of a collection of Raspberry Pi 3’s and associated shields, with some lower-level functionality implemented with Arduino Mega boards and available hats. Communication would occur wirelessly between a laptop and the Raspberry Pi’s, with a joystick used for RC-mode and Python scripts for autonomous operation. The students carefully investigated what would happen if the wireless connection was interrupted and found that the software would default to a stopped robot. Connectors, relays, and in-line fuses were selected for reliability of connection and operation in a mobile platform where there would be some vibration and limited air flow.

*Integration Stage*

Once subsystem designs had gone from detailed design to testing, the team was now aware of all of the prospective components that would be in the system and were next considering how subsystems would interface or connect. This was a good opportunity to consider safety now from the bottom up. In the literature, this is called Failure Mode Effect and Criticality Analysis (FMECA) [26]. Here, the engineers consider the failure modes of each component, the effects of failure, the probability of failure, the seriousness of failure, and the difficulty of detecting the onset of failure. With limited experience, students are not very good at identifying potential failure modes. One suggestion from mentors was to look at internet discussion sites for various components and see what problems other designers have had with specific components. The layout of the major components of the electrical system is shown below in Figure 2 and was used to consider potential electrical failures.

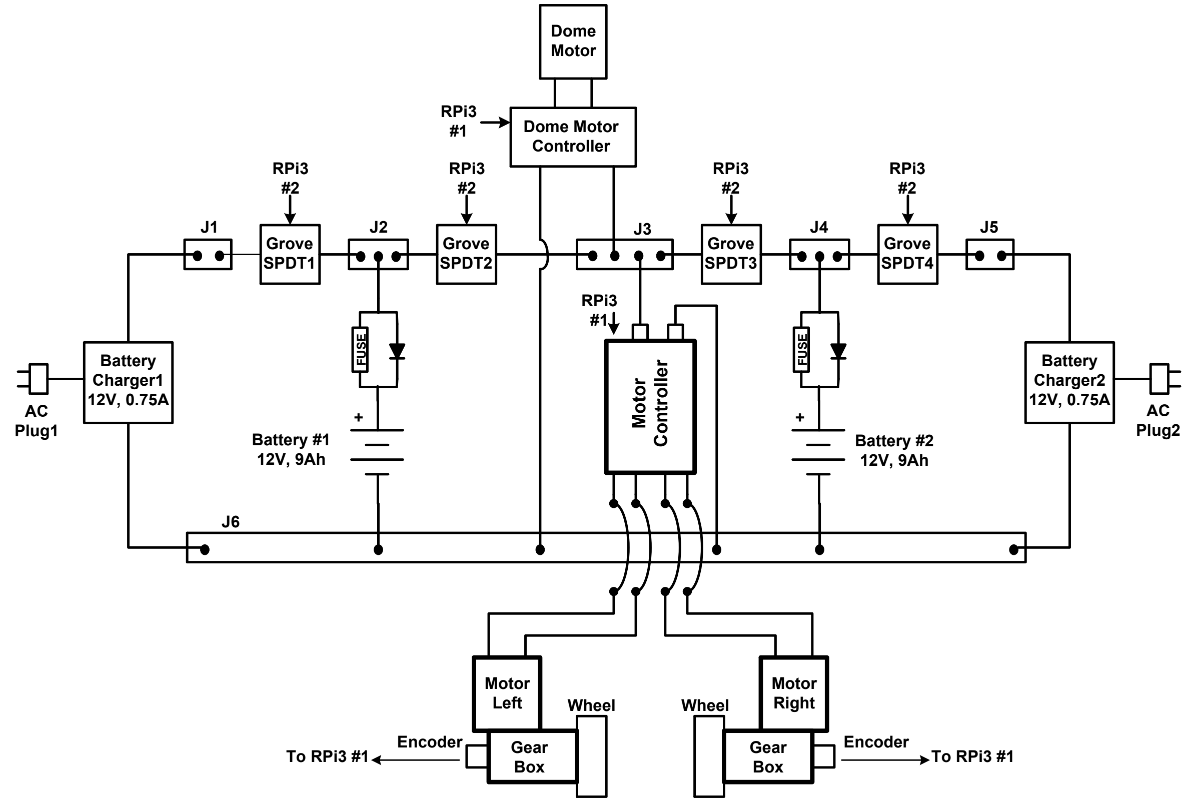


Figure 2. Electrical Functional Diagram.

*Software*

Software safety poses a different challenge than encountered with electrical and mechanical components or subsystems. Software does not wear out, break, or have increasing tolerances that result in failure. Software errors generally manifest because of the failure to account for certain logical conditions, an external component providing bad data input to the software, or an algorithm being improperly coded. It is also possible for software errors to lead to system hazards due to coding that exceeds the hardware capabilities of the computing system. [29-34]

So the starting point in assessing the safety of R2D2's software was to determine which software functions are "safety critical" or can lead directly to a failure or a hazardous condition. The team initially identified the following three items as "safety critical":

- Control of the propulsion motor controller;
- Control of the dome motor controller;
- Logging of laser range finder data and video data (that can be used for navigation).

The software was developed in modules, with "safety critical" modules partitioned from "non-safety critical" software. A goal was to minimize the number and complexity of the "safety critical" modules. These modules were then tested more thoroughly. Test cases assessed both normal and abnormal conditions, ensuring that all software requirements were being met, and ensuring that all pieces of code were being executed (white-box testing). Testing exercised all inputs at or near the limits of their range. Timing is also a key aspect of code that must be carefully tested, especially if "safety-critical" and "non-safety critical" interrupts are used. Code was developed using best practices. Some of these include but are not limited to [34]:

- Ensure that all variables are properly defined, data typed, and initialized
- Ensure that all comments are accurate
- Ensure that version control is in place
- Ensure all process loops have correct starting and stopping criteria
- Ensure that array subscripts do not go out of bounds
- Check the correct order, number, and type of variables in function calls
- Ensure there is no self-modifying code
- Ensure there is no extraneous code that does not operate
- Ensure no jumps to middle of loops
- Minimize the length and complexity of subroutines or functions
- Re-check logical expressions and equations
- Check that logical exceptions are processed correctly
- Ensure that memory storage is not exceeded
- Ensure a safe power-up state
- Ensure a safe shut-down state under power failure conditions
- Create software modules to detect and log all errors, faults, or timing problems

The computer hardware block diagram is shown in Figure 3. The layout contains two Raspberry Pi 3's (RPi3) and one Arduino Mega.  The Arduino was selected as the controller for the peripherals because of its ease of interface with the dome motor controller. The second RPi3 was used to accommodate the Grove Relay Control board (hat) that was used to interface to the four control relays in the circuit (shown in Fig. 2). The memory cards on the RPi3 were sufficiently large to handle any expected video or sound recordings.

Even with carefully crafted code and good sensor data, it is still possible for autonomous operation to lead to hazards and unsafe operation. The consideration of safe navigation by an autonomous robot is a subject of much research [35]. For instance, authors have considered how to optimize the speed of an autonomous robot to not just avoid detected obstacles, but to minimize the probability of colliding with dynamic obstacles occluded from the sensors' fields of view. Optimal path-planning becomes another piece of the safety puzzle. The R2D2 team was only able to make preliminary progress into implementing autonomous behaviors, focusing on a rudimentary wall-following algorithm, a person-following algorithm using color detection, and a generic obstacle avoidance routine using the combination of sonar and laser-range-finder data. Issues with integration limited the testing of these algorithms and exploring the safety implications. Fortunately, the capstone project will get extended for a second year to focus more specifically on autonomy.

The layout of the computer hardware and interfaces for R2D2 is documented in Figure 3. This figure was used to identify conflicts and challenges for the integration stage.

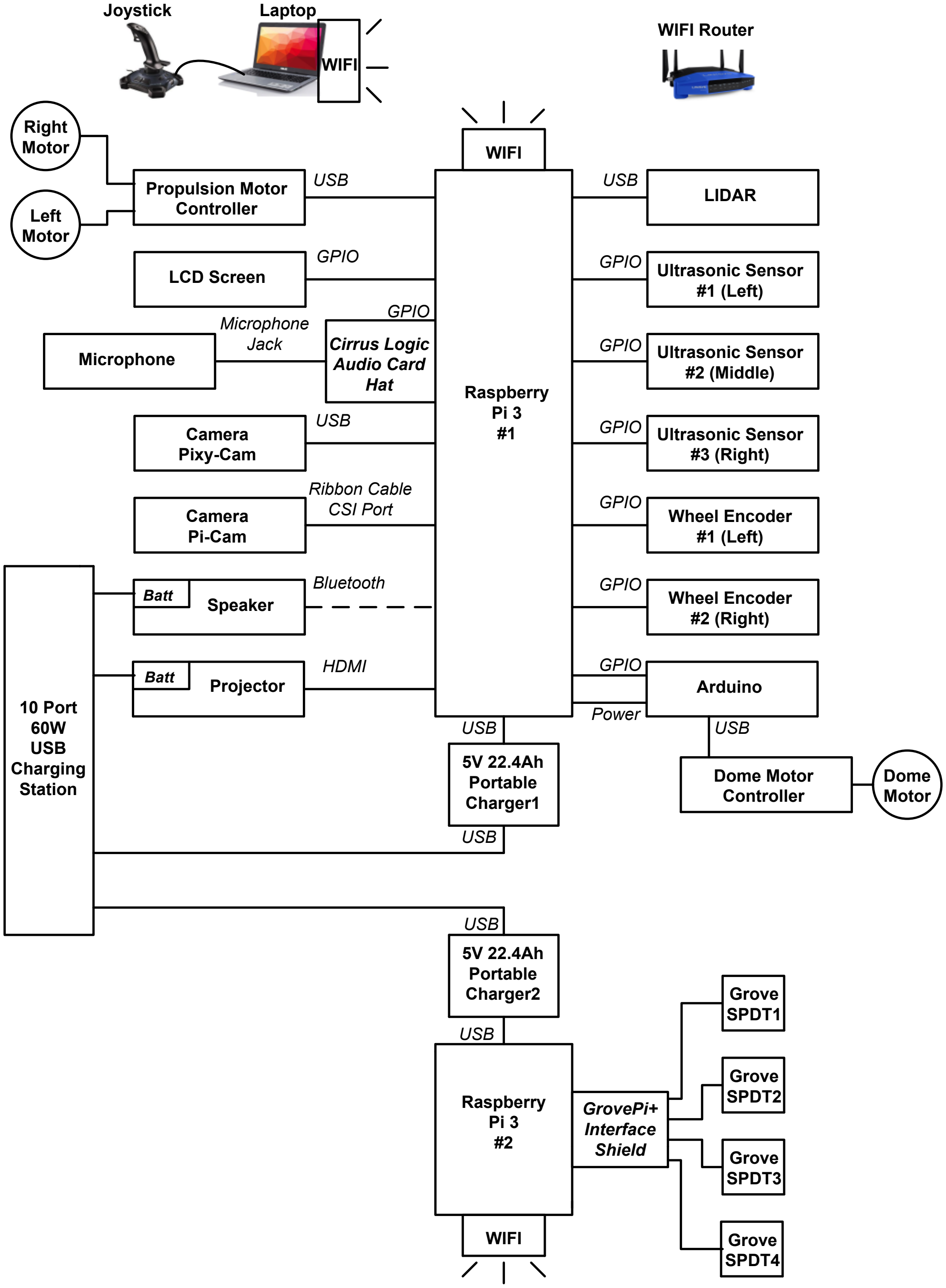


Figure 3. Functional Layout of Computer Hardware Solution.

*Operation Stage and Technical Review*

As R2D2 was being readied for final testing, the team instituted a safety checklist to ensure that a consistent and tried process was used to start up, operate the robot, and then deactivate it. An operating checklist is included in Appendix II. Testing was primarily done in a laboratory space that could be closed off to any intruders. When operation was moved out to the hallways, barricades were used to ensure that no one could inadvertently come upon R2D2 and cause a collision. The safety button was tested several times to ensure that it was a reliable last defense against rogue robot motion.

As the robot was being readied for delivery to the department for use in future capstones and directed studies, the team made sure to deliver a detailed user manual that would include the safety checklist and the various circuit schematics and layout drawings to facilitate troubleshooting and future modification. Finally, the team included warning stickers on the robot to alert any future operator of dangers that might result from an accidentally opened door on the vehicle.

At the conclusion of the project, the following items were identified as potential safety improvements during the technical review:

- Measurement and logging of battery currents to identify any faults or aberrant conditions;
- Status LEDs need to be included to show that propulsion power is connected; autonomous mode is engaged, and control power is available;
- The vision system could also be leveraged to help with obstacle detection and autonomous navigation;
- Sensors can be placed in the robot testing area to detect any unauthorized entry while also backing up the obstacle detection sensors on-board the R2D2;
- More test points should be included to aid in troubleshooting and localizing bad connections;
- Bumpers or rubberized guards could be mounted on the robot during testing and development to lessen the problem with inadvertent impacts.

## Summary and Recommendations

An undergraduate capstone design project was structured to provide engineering undergraduates with greater awareness of safety issues. The R2D2 autonomous robot project offered many non-contrived opportunities for the students to use high-level safety concepts and to address relevant safety issues. The safety issues related to mechanical, electrical, software, and operational aspects of the project. Features of the systematic approach include awareness of formal engineering standards, progressive attention to safety, checklist development, an external safety review, and operational/maintenance documentation. The emphasis on safety in this initial implementation seemed to advance the students' understanding of engineering safety and to produce a better overall robot design.

Overall the R2D2 robot project was a technical success and safety considerations were formally considered at each stage of the design process. The final R2D2 robot is shown in Figure 4.

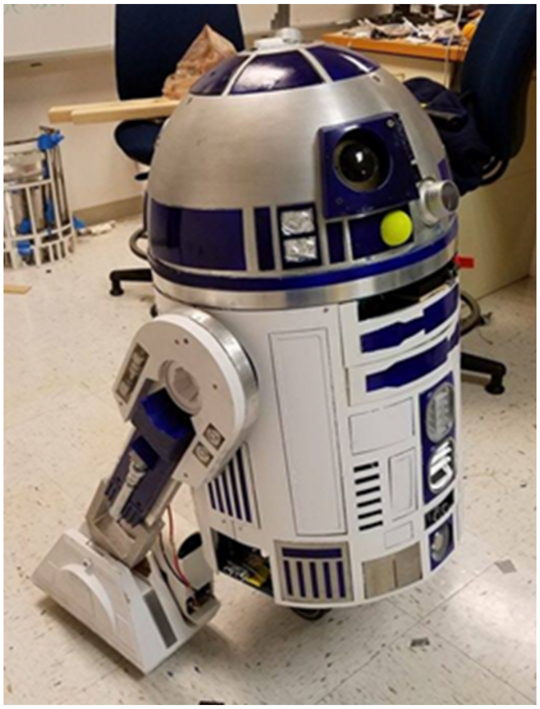


Figure 4. The final R2D2 Robot.

Not all design requirements were accomplished; the project scope was quite ambitious. In particular, not all desired safety features and documentation were incorporated due to time constraints and integration challenges. The final project review specified areas where improvements could be made in the next iteration of the project. The following recommendations were made.

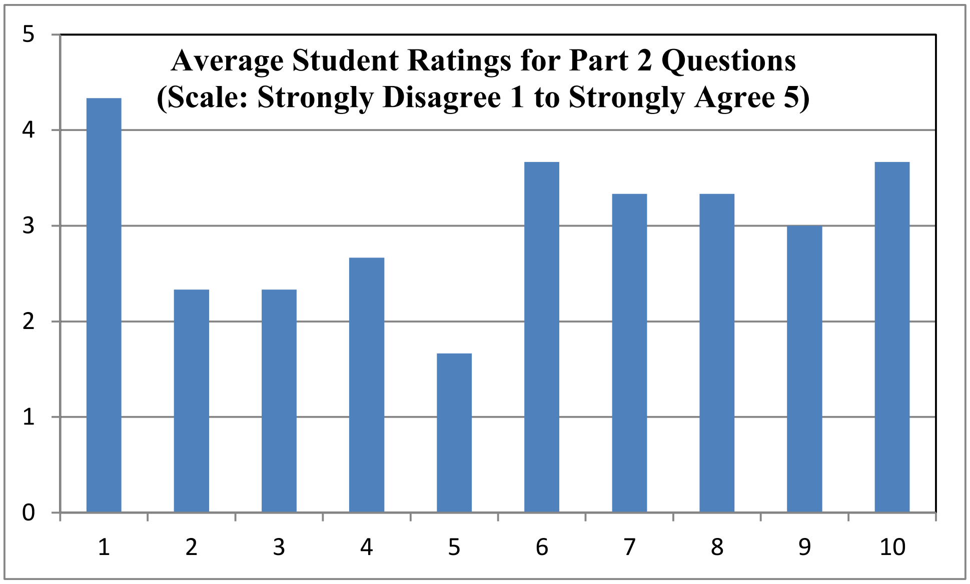
- The project scope should be reduced to allow more time for integration and testing.
- Students have little experience at predicting how complex systems break and at estimating the time required for system integration. Mentors need to guide the failure analysis activities for specific systems, so that students gain understanding in a less adversarial venue than formal reviews.
- Software reliability was a problem. More detailed software reviews are recommended to ensure that best practices are being followed, especially practices related to documenting driver installation processes and other configuration settings.
- Additional instruction on electrical safety is recommended, but the instruction should target the specific project requirements.
- The work area was sometimes cluttered and electrical power was sometimes left applied for extended periods. A periodic graded safety inspection is needed to eliminate these

general safety hazards, to reduce opportunities for component overheating and failure, and to emphasize a safety culture.

- The project documentation was updated irregularly and was rushed at the project end. No specific safety problems resulted, but timey documentation would improve the overall project activity, including the handling of safety.
- The general safety standards such as MIL-STD-882 [29] were useful for creating a safety mindset. Other specific standards, such as those addressing industrial robots, had limited application due to the commercial focus of the standard. A standard and/or best practices related to autonomous mobile robots would be useful.
- Further incorporation of LCD status panels, LED indicators, kill switches, and engineering test points would enhance the safety features for the robot.
- An external safety review by an expert from the National Renewable Energy Laboratory (NREL) was performed. Additional reviews may be helpful to address specific safety aspects and to create an environment in which reviews are an expected part of the design experience.

Two electrical engineering majors and one computer engineering major in this project returned the safety evaluation survey given in Appendix III. Their project roles were in the mechanical, electronics, and programming areas. All students indicated that they were somewhat familiar with safety standards and risk assessment and that the safety documentation could use further improvement. They differed on the stage that most emphasized safety and on the most difficult safety-related problems. Their average responses to the questions in Part 2 are shown in Table 1. The extreme averages related to their familiarity with general laboratory safety rules and to their perceived value of the external review. They tended to feel that safety was emphasized in all but the operation stage of the project and they generally considered the robot to be ”safe.”

Table 1. Evaluation Survey Results for Part 2 Questions (see survey questions in Appendix III).



The authors plan to use this approach in future capstone projects. In particular, the R2D2 robot will continue as a capstone project in which the autonomous capabilities will be further developed. Such further implementations will address the recommendations as given above and will give more student feedback. Based on the student survey, the external safety review seemed to be ineffective and this feature of the approach needs to be modified. The benefits of the safety framework need to be quantified in these future implementations through surveys and other data analyses. Experience in applying the approach to other types of capstone projects may enhance the pedagogical value.

## References

1. Accreditation Board for Engineering and Technology (ABET), "Criteria for Accrediting Engineering Programs," (Accessed 2017). Available WWW: http://www.abet.org.
2. IEEE, *IEEE Code of Ethics*, (Accessed 2017). Available WWW: http://www.ieee.org/about/corporate/governance/p7-8.html.
3. Watkins, S. E., "Teaching Engineering Ethics," *Proceedings of the 2015 ASEE Zone III Conference*, ASEE, Missouri, USA, 2015.
4. Dhillon, B. S., *Engineering Safety: Fundamentals, Techniques, Applications*, World Scientific Publishing Company, 2003.
5. Cadick, J. and Capelli-Schellpfeffer, M., *Electrical Safety Handbook*, 4th Edition, McGraw-Hill, 2012.
6. *Road Vehicles – Functional Safety*, ISO 26262-1:2011.
7. *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, IEC 61508:2010.
8. *Department of Defense Standard Practice: System Safety*, DOD MIL-STD 882E, 11 May 2012.
9. *2017 National Electrical Safety Code (NESC)*, IEEE, 2017.
10. *Occupational Safety and Health Standards*, 29 CFR Part 1910, 1994.
11. *ANSI Z136.1-2014 American National Standard for Safe Use of Lasers*, American National Standards Institute, (2014).
12. *ANSI Z136.5-2009 American National Standard for Safe Use of Lasers in Educational Institutions*, American National Standards Institute, (2009).
13. Ammerman, R. F., Sen, P. K., and Stewart, M., "The Importance of Electrical Safety Training in Undergraduate Power Engineering Education," *Proceedings of the 2006 ASEE Annual Conference*, Kansas, USA, 13-15 Sep 2006.
14. Pendley, C. C. and Saleh, J. H., "System Safety Literacy and Multidisciplinary Engineering Education: Teaching Accident Causation and Prevention," *Proceedings of the 2011 ASEE Annual Conference*, Vancouver, BC., 2011.
15. Davis, D. C. and Davis, H. P., "Teaching Responsibility for Safety in Bioengineering Design," *Proceedings of the 2013 ASEE Annual Conference*, Atlanta, Georgia, 2013.
16. Ravishankar, J. and King, S., "Electrical Safety in Engineering Education: Teaching Strategies for Postgraduates," *2013 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, 26-29 August 2013, pp 196-200.
17. Pitt, M. J., "Teaching Safety in Engineering", *4th International Symposium for Engineering Education*, Univ. of Sheffield, UK, July 2012.
18. APLU Council on Research: Task Force on Laboratory Safety (2016), "A Guide to Implementing a safety Culture in Our Universities", CoR Paper 1. Washington, DC, Association of Public and Land-grant Universities.
19. Florida Institute of Technology, "Senior Design Project Safety Templates," (Accessed 2017). Available: http://coe.fit.edu/srproject.php.
20. University of Illinois, "ECE 445 Safety Guidelines," (accessed 2017). Available: https://courses.engr.illinois.edu/ece445/guidelines/safety.asp.

21. *Robot and Robot System Safety* , ANSI/RIA R15.06-2012.
22. *Robots and robotic devices – Safety requirements for industrial robots* , ISO 10218-1 & -2: 2011.
23. *Robots and robotic devices – Safety requirements for personal care robots* , ISO 13482: 2014.
24. *Robots and robotic devices – Collaborative robots* , ISO/TS 15066: 2016.
25. *Industrial Robots and Robot System Safety*, OSHA Section IV: Chapter 4.
26. Deward, D. W., Bradley, D. A., and Margrave, F. W., "Hazard Analysis Techniques for Mobile Construction Robots," *Automation and Robotics in Construction XI*, 1994, pp 35-42.
27. K. L. Barat, "Cultural Change to Prevent Laser Eye Injuries in R&D Labs," *2010 IEEE International Conference on Management of Innovation & Technology*, pp. 1103-1105.
28. Mihran, R. T., "Interaction of Laser Radiation with Structures of the Eye," *IEEE Trans. on Education*, Vol. 34, No. 3, Aug 1991, pp. 250-259.
29. *System safety Program Requirements*, MIL-STD-882D, 2012.
30. *Software Safety Standard*, NSS 1740.13, 2013.
31. *Software Safety Plans*, IEEE 1228-1994.
32. *Software in Programmable Components*, UL 1998.
33. Keene, S. L., "Assuring software safety," *Proceedings of the Annual Reliability and Maintainability Symposium*, 1992, pp. 274-279.
34. Joint Software Systems safety Engineering Workgroup, *Joint Software Systems Safety Engineering Handbook*, Version 1.0, August 27, 2010.
35. Chung, W., Kim, S., M. Choi, M., Choi, J., Kim, H., Moon, C., and Song, J., "Safe Navigation of a Mobile Robot Considering Visibility of Environment," *IEEE Trans. on Ind. Electron.*, Vol. 56, No. 10, Oct. 2009, pp. 3941-3950.

## Biographies

**DR. JOHN G. CIEZKI** is an Assistant Professor in the Electrical and Computer Engineering Department at the U.S. Air Force Academy. He received his B.S.E.E., M.S.E.E., and Ph.D. from Purdue University, West Lafayette in 1988, 1990, and 1993, respectively. Dr. Ciezki taught at the Naval Postgraduate School in Monterey, CA from 1994 to 2002. In 2002, he joined the staff of the U.S. Naval Academy where he served as an Associate Professor until 2011. He then worked as an Advisory Power Electronics Engineer for Northrop Grumman Corporation in Sykesville, MD until returning to academia at the Air Force Academy in 2013. Professor Ciezki has conducted research in power system simulation, the development of power electronics-based distribution systems, the control of finite-inertia power systems, the mitigation of power quality issues in large motor drives, and is currently exploring topics related to micro-grids. He has taught courses in power systems, power electronics, electric machines, control systems, and circuit analysis. He has supervised over 30 Master's theses, co-advised two dissertations, mentored three Trident Scholar Projects, received the AY2006-2007 Raouf-Ali-Raouf Award for Excellence in Engineering Teaching at the U.S. Naval Academy, and the 2015 Outstanding Academy Educator Award for the Department of Electrical & Computer Engineering at the U.S. Air Force Academy. Dr. Ciezki is a member of the IEEE and ASEE. Contact: John.Ciezki@usafa.edu

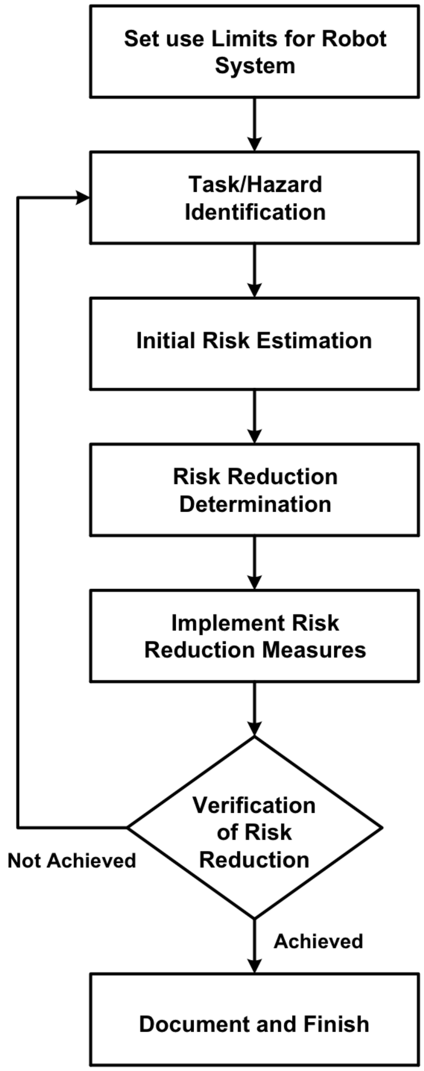
**DR. STEVE E. WATKINS** is Professor of Electrical and Computer Engineering at Missouri University of Science and Technology, formerly the University of Missouri-Rolla. His technical interests include smart sensor systems, optics, and engineering education. He was a 2016-17

Distinguished Visiting Professor at the United States Air Force Academy. He is active in IEEE, IEEE-HKN, SPIE, and ASEE including service as the IEEE Region 5 Ethics Competition Chair, the 2017 IEEE-HKN President-Elect, the 2015-2017 ASEE Zone III Chair, and the 2009 ASEE Midwest Section Chair. His Ph.D. is from the University of Texas at Austin (1989). Contact: steve.e.watkins@ieee.org

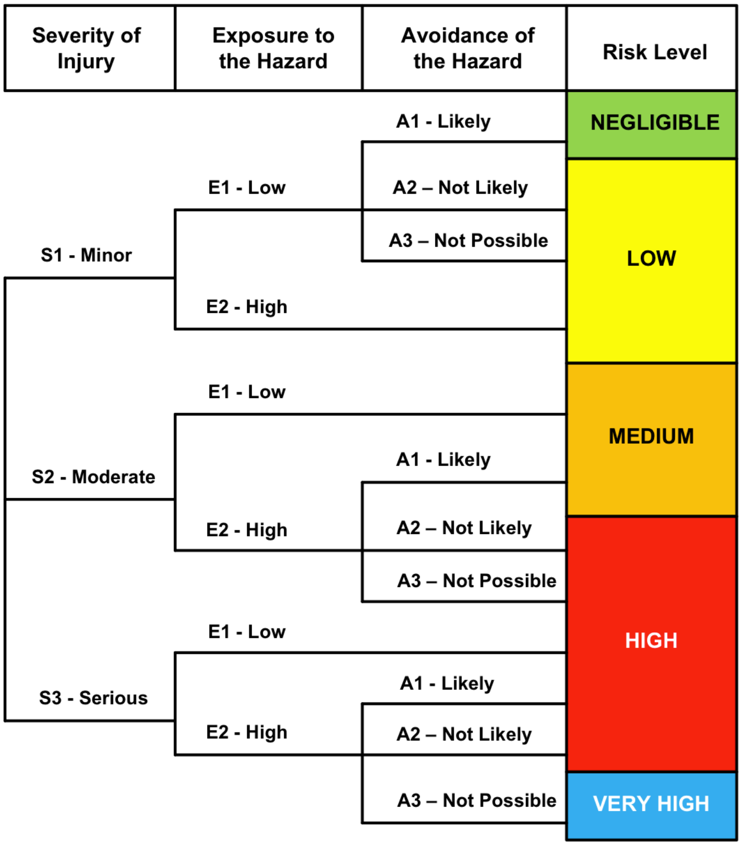
## Appendix I – Risk Assessment Tools

The following tools guided the safety considerations for the various stages of the project. These tools are taken from *Robot and Robot System Safety* by ANSI/RIS [21].

**Tools for Risk Assessment and Mitigation from Ref. [21]**



Set use Limits for Robot System
Task/Hazard Identification
Initial Risk Estimation
Risk Reduction Determination
Implement Risk Reduction Measures
Verification of Risk Reduction
Not Achieved
Achieved
Document and Finish



## Appendix II – R2D2 Project Safety Checklist

The following safety checklist was developed for operation of the R2D2 robot.

### R2D2 Project Safety Checklist

□ 1. Clear room or hallway of any unwanted obstacles; make sure no equipment can be knocked off a table due to an inadvertent collision

□ 2. Set cones in area to block unwanted intrusion into the area

□ 3. Activate wireless router

□ 4. Verify all robot doors secured

□ 5. Position team members to address runaway robot

□ 6. Activate power switch on R2D2

□ 7. Establish connection between laptop and R2D2

□ 8. Establish link between on-board camera and laptop

□ 9. Toggle relay settings on RPi3 #2 to apply battery power to propulsion motor controller

□ 10. Announce robot test

□ 11. Initiate RC control mode

□ 12. Perform planned dome movement

□ 13. Initiate audio test

□ 14. Perform planned trajectory traversal

□ 15. Toggle relay settings on RPi3 #2 to disconnect battery power from propulsion motor controller

□ 16. De-activate power switch on R2D2

□ 17. Disconnect laptop from router

□ 18. Power down RPi3's

## Appendix III – Capstone Safety Survey

This evaluation survey was completed by three of the five students. Responses for Part 1 and 2 are shown with an "X" or the rating 1-5, respectively.

### Evaluation of Capstone Safety

**Part 0: General Information:**

***Academic Major?*** ***What was your primary role in the project?***
______________ Mechanical Electronics Programming Integration (circle one)

***What prior courses were most helpful in completing this capstone project?*** (Select all that apply.)
_____ Robotics _____ Embedded Systems _____ Computer Architecture
_____ Other (specify) _________________________

**Part 1:** Pick the best choice for each statement.

***Formal safety standards and risk assessment …***
______ were new concepts.
_X_X_ were not new, but I better understand how to use the concepts after the capstone project.
_X____ were familiar concepts.

***As a help for future capstone teams, the safety content in the robot documentation (user's manual) …***
_X____ is minimal and it needs general improvement.
_X_X_ is adequate, but it could be improved in some areas.
______ is comprehensive.

***Safety and risk assessment were emphasized the most during ...***
_X_X_ the design/development stage of the project.
_X____ the integration stage of the project.
______ the troubleshooting stage of the project.
______ the operation and documentation stage of the project.

***The most difficult safety-related problems that occurred during the project involved ...***
_X____ anticipating component failure.
______ managing safety-critical software modules.
_X____ developing a safety checklist and protocols for robot operation.
_X____ working safely in the laboratory.

**Part 2:** Please use the following scale to respond to each of the statements in Part 2:

**Strongly Disagree** 1 ... 2 ... 3 ... 4 ... 5 **Strongly Agree**

_5_3_5__ 1. I was very familiar with general laboratory safety rules before the capstone project.
_3_2_2__ 2. I had little experience in my prior college courses to formal risk assessment procedures.
_1_3_3__ 3. I was aware of formal robot safety standards, e.g. ANSI, ISO, and OSHA, before the project.
_3_2_3__ 4. The final capstone report section on safety was significant.
_1_2_2__ 5. The NREL safety review was a valuable part of the design process.

_3_4_4__ 6. Risk assessment was emphasized by the student team during the design/development stage.
_4_4_2__ 7. Risk assessment was emphasized by the student team during the integration stage.
_3_2_5__ 8. Risk assessment was emphasized by the student team during the troubleshooting stage.
_3_3_3__ 9. Risk assessment was emphasized by the student team during the operation stage.
_3_4_4__ 10. I consider the final robot "safe."

**Part 3:** Open Ended Evaluation –

What are the most important safety features that were incorporated into the robot? How could the project process (design, integration, …) be improved related to safety and risk assessment? (Write on back)