Contingency Plans – A Key Element of Successful Engineering Designs

Kirsten Nicolaisen, Gerald Brown, Timothy Dewhurst

Department of Engineering and Computer Science, Cedarville University, Cedarville, Ohio USA

Email: kirstnic@gmail.com, gbrown@cedarville.edu, dewhurst@cedarville.edu

Abstract

Undergraduate engineering programs provide students a great deal of theoretical knowledge but the constraints of the academic environment make it difficult to comprehend certain problems and challenges faced in industry. One key challenge is the possibility of a design failure. Since the probability of failure increases with a system's complexity, engineers must purposefully incorporate contingency plans. However, it is difficult for inexperienced students to accept the need for back-up systems. Only by designing, building, and testing real-world systems do they truly grasp that a well-designed system includes contingency designs that will allow it to continue operation even when a subsystem fails.

Through my senior capstone design project with the Cedarville University Solar Boat Team I learned the necessity of contingency plans. I developed an Energy Management System (EMS) for a solar-powered boat entered in the DONG Energy Solar Challenge (DSC). My task was to integrate all the electronics – Maximum Power Point Trackers (MPPTs), lithium-ion battery system, GPS, and data acquisition circuitry – in order to race the boat competitively. The main function of the EMS was to monitor energy usage and determine and control the boat at an optimum speed. Throughout the design, I considered all possible modes of failure and introduced back-up systems to ensure the boat could still operate if individual components failed.

After spending a year working on the project, we competed in the DSC in July 2012. During the race, we had various failures in the MPPT system, the commercial battery system, and our software code, yet we still finished the race – and won 3rd place in the Top Class – using our contingency plans. This paper addresses how contingency plans were a fundamental part of the design project, teaching an important lesson that will benefit me in my career as an engineer.

Keywords: contingency plan; back-up plan; solar powered boat; energy management system.

1 Introduction

While an undergraduate engineering program provides students the theoretical knowledge needed to pursue a career in engineering, the constraints of the academic environment present a challenge in presenting real-life problems encountered in industry. One key problem faced in industry is the probability of a design failure, which increases with the complexity of a system. Only by designing, building, and testing real-world systems do students truly grasp that a well-designed system includes contingency designs that will allow it to continue operation even when a subsystem fails.

This paper is written from a student perspective. The first author, Nicolaisen is writing from her point of view. The two secondary authors are the faculty advisors.

Through my senior capstone design project with the Cedarville University Solar Boat Team I learned the necessity of contingency plans by developing an Energy Management System (EMS) for a solar-powered boat. My task was to integrate all the electronics in order to race the boat in the DONG Energy Solar Challenge (DSC). The EMS monitors energy usage and determines the optimum speed at which the boat should operate. Throughout the design process we needed to consider all possible modes of failure and introduce the necessary contingency plans.

After a year of working on the project, we competed in the DSC in July 2012. During the race we experienced various failures in our designs, including the EMS. However, despite these failures we finished the race—and won 3rd place in the Top Class—using our contingency plans. This section provides a background on the DSC competition, gives a brief overview of the boat as a whole, and explains the EMS design.

1.1 DONG Energy Solar Challenge

The DONG Energy Solar Challenge (DSC) is a solar boat race that takes place in the Netherlands. The race consists of two broad categories: the Challenge Class and the Top Class. The Challenge Class is divided further into Class A (single

crew member) and Class B (two crew members). Solar cells are provided to teams that compete in the A and B Classes. The Top Class has broader design constraints and the competitors must supply their own cells, providing a more competitive and challenging event. The race follows the route of the *Elfstedentocht*, the eleven cities ice skating race held in the Friesland province, and covers 220 km (136.7 mi.) over five days of racing. It includes such challenges as low bridges, shallow canals, and stretches of open water. Boats are powered by on-board solar panels and batteries which are allowed to be fully charged at the beginning of the race.

1.2 Cedarville University's Top Class Solar Boat

Cedarville competed in the 2006 Frisian Nuon Solar Challenge (an earlier version of the DSC) and won second place in the Class A category. In 2012, we entered at the higher, more challenging level as a Top Class entry. This required us to design and build a new hull, electronics system, solar panels, maximum power point trackers (MPPT), and EMS.

Our design work was governed by a power budget (Figure 1) developed to track energy flow and losses through the system. With limited power coming into the system from the solar cells and batteries, the system needed to operate as efficiently as possible to finish the race in the shortest time. The power budget shows the cumulative effect of component losses and the diminishing amount of power available to propel the boat. It allowed us to estimate the power available at the propeller to balance the hull drag and thereby determine the maximum speed we could travel. For example, with 4.9 kW of power incident on the solar cells, their 18% efficiency leaves only 875 W for the MPPTs. Dewhurst and Brown (2013) give a more detailed description of the power budget.

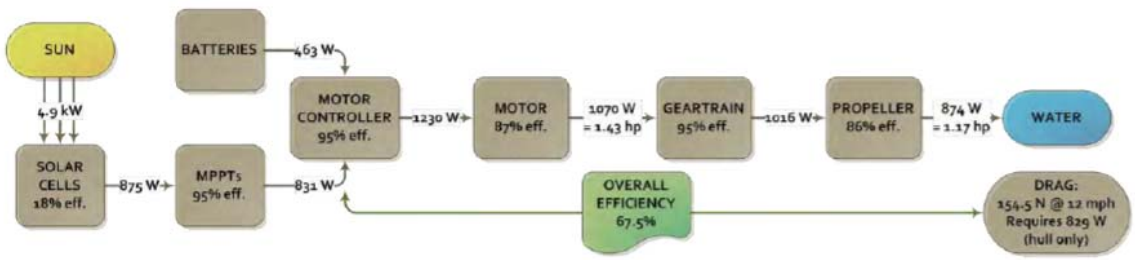

Figure 1: The Power Budget Developed for the Top Class Solar Boat Tracks Losses and Available Power

The energy required to complete each leg of the race increases with boat speed but the time available to harvest solar energy during the race decreases. A mandatory pause and scheduled restart time two thirds of the way through each day's racing allows for faster boats to spend more time recharging before the day's route is finished. However, the available solar energy varies with cloud cover and is not known in advance. Finishing each day as fast as possible also required finishing each day with fully depleted batteries, assuming the weather would permit complete recharging by the beginning of the next day's race. The complex interactions between boat speed, solar energy input, wind and wave effects on drag, drive system efficiency, battery characteristics and the overarching goal of finishing each leg as quickly as possible required a sophisticated energy management system. We needed to develop an EMS that could monitor energy use throughout the system and determine the optimal boat speed throughout the day.

1.3 Background of the EMS

The energy management system is comprised of hardware and software. The major hardware components and system layout are shown in Figure 2. The EMS software runs on a chipKit Max32 microcontroller that reads the incoming signals, runs an optimization algorithm and outputs the desired speed or energy usage requirement. There are two incoming signals (from the lithium-ion batteries and solar panels) and two output signals. The Li-ion battery packs are managed by commercial charge controllers, which supervise battery performance, charge the batteries if power is available, and ensure safe operation. Each charge controller has a dedicated LCD display. Two chipKit Uno32 microcontrollers are devoted solely to serial communication between the EMS and the charge controllers. Dedicated Uno32 microcontrollers on each MPPT send solar power information to the EMS and convey run/charge commands back to the MPPT. The EMS also receives analog signals from a signal conditioning card (SCC) which monitors information such as current and voltage at various locations throughout the boat. A small GPS unit is connected to the EMS microcontroller to provide speed and location. The EMS displays data on a third LCD screen and records data on an SD card for post-race analysis.

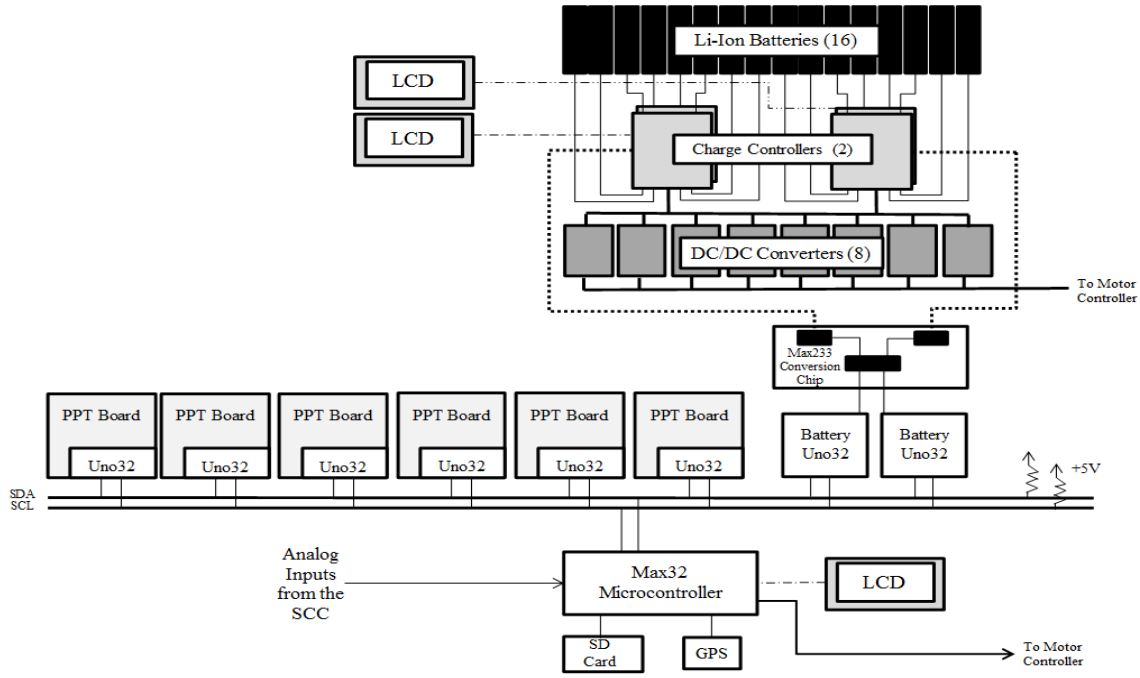

Figure 2: Overview of the EMS showing individual systems and components

The main function of the EMS microcontroller is to process the data and determine the optimum boat speed to complete the current leg of the course in the shortest time. The algorithm inputs are the amount of power remaining in the batteries, the power currently coming from the solar panels, the power the boat is using to maintain the current speed, and the GPS speed and location data. The program determines the distance remaining in the race, estimates the energy that is available, and determines the speed that will use all the energy just as the boat reaches the destination. This will be the shortest possible time and thus the fastest possible speed for our system. Figure 3 shows a basic flowchart of the EMS logic.

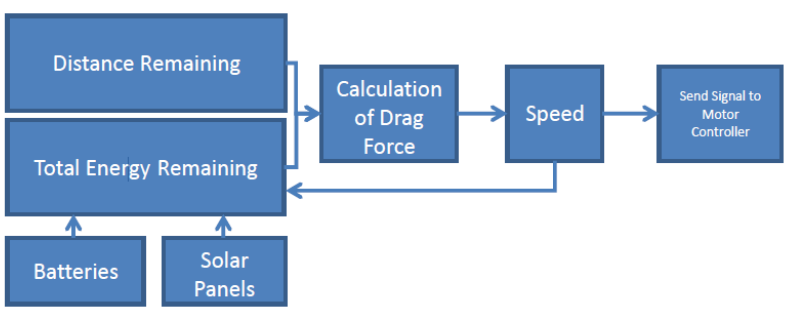

Figure 3: Basic Logic for the Designed EMS Algorithm

The code was developed because this type of real-time calculation is beyond the ability of the driver who must focus on navigating the boat. While much of the data generated by the MPPTs and the charge controllers is useful for tracking battery and system performance, it is not needed for the real-time energy calculations. The EMS code running on the microcontroller analyzes the data in real-time and only displays information crucial to the driver. The remaining data is stored or discarded. The most difficult part of the algorithm was establishing communication with all of the devices and providing seamless integration with the rest of the system.

2 Incorporation of Contingency Plans

There were numerous problems as we designed and developed the electronic system, but the two most serious problems were communication issues between systems and recurring malfunctioning of several components. We could not determine whether the malfunctions were due to errors in our circuit or due to manufacturing defects. It

became evident, however, that the scope and complexity of the required EMS was monumental and our ongoing difficulties made clear the necessity of incorporating contingency plans into the design. We focused on the EMS and each component that interfaces with it and came up with plans so that, in the event of any component failure, we could still send or receive the data necessary to operate the boat successfully.

2.1 Examples of Contingency Plans

Contingency plans are a fundamental part of engineering design. Business Week published an article regarding Boeing's incorporation of contingency plans in the design and manufacturing of the 787 Dreamliner. During initial manufacturing in 2007, Boeing's suppliers didn't install many of the electronic and hydraulic systems into their respective fuselage sections as had previously been planned. Boeing was forced to shift workers from other programs, such as the 777 Jetliner, to make up for the unfinished work. Other production challenges included a global shortage of fasteners requiring the initial 787s to be held together with temporary fasteners (Holmes, 2007).

Unmanned Aerial Systems (UAS) are also a highly complex emerging market that requires a robust design. In a study performed by Lockheed Martin on "Holistic Contingency Management for Autonomous Unmanned Systems", uncontrollable circumstances were examined for their effects on the UAS. Weather, teammate failures, unexpected battlespace developments, failure of external assets, and changes in priorities could all contribute to vehicle system failure. The authors state that "while significant research is being performed in the planning and execution aspects of contingency management, we have specifically addressed the contingency detection and assessment functions required to complete the overall decision cycle" (Franke, Hughes, Jameson, Clark, & Szezerba). The Defense Industry also uses contingency planning with Global Hawk mission planning, allowing for "the safe, predictable operation of the UAV in the event of equipment failure or loss of communications with the ground control station." Mission planners consider capabilities and limitations of the aircraft as well as factors relating to the operational environment (Hopcroft, Burchat, & Vince, 2006).

Within the context of solar racing (cars, boats, etc.) there are numerous examples of the implementation of contingency plans. In a Masters thesis written by R.L. Feldbrugge, the author outlines his research in the area of reinforcement learning in an energy management algorithm to be used specifically in the DSC 2010 competition. When discussing the race and the actual application of his algorithm, he highlights each of the measurements that need to be entered into his code. He alludes to contingency plans that are in place in order to insure that the value will be measured, regardless the method. For instance, velocity is a critical value needed in the code. His suggestion is to use a standard boat-speedometer, though he also outlines an alternate plan for using the winch as a means to gain the necessary value (Feldbrugge, 2010).

We can also see how our competition used contingency plans in their designs. Technical reports from the Solar Splash competition (a US competition we also entered with a separate boat) by both The College of New Jersey (The College of New Jersey, 2012) and Carnegie Mellon discussed contingency plans, or back-up systems, they had in place, specifically in the electronics area. Carnegie Mellon used two separate systems to acquire voltage and current data, and also purchased equipment that included error checking with individual monitoring of each circuit board so that boards could be conveniently added or removed from the system (Carnegie Mellon, 2012).

2.2 Identifying Potential Problems

We needed to design contingency plans for each component that was sending or receiving signals to or from the EMS. This included the batteries, MPPTs, SCC, GPS, LCD, and SD Card. We reviewed the system design and systematically considered what would happen if we lost each of these components. For instance, if we lost communication with the battery system we would have no idea how much energy was left in the batteries and we would run the risk of either draining the batteries before the finish or having unused energy at the end of the race. If we lost communication with the GPS we would not know the boat speed or the distance remaining—two crucial elements of the EMS algorithm. We assessed the consequences and severity that each loss would have on the overall operation in order to create suitable contingency plans.

2.3 Preparing a Contingency Solution

The process of considering all possible failure modes has the natural consequence of recognizing criticality of certain information and functions. From there, it's often a short step to find a contingency, an alternative way to achieve the same result. For example, we purchased two preprogrammed commercial LCDs that connected directly to the battery charge controllers. They provided redundant information during normal operation, but in the event we lost communication with the battery management system they would still provide vital battery information such as energy remaining and important error messages. We also decided to install a small handheld GPS on the control panel to

provide the driver speed data in case we lost our normal GPS signal or could no longer communicate with the GPS card. It's straightforward to locate the boat on the charts of the waterways if we knew its current GPS position coordinates. That and the driver's ability to recognize features and land marks meant we could navigate without the EMS. These plans certainly weren't optimal, but they would work in case of a system failure.

2.4 Building the Plan

Apart from lack of experience, one of the most significant challenges we faced in designing, building and testing the EMS system in the span of ten months was lack of time. This also included developing and testing our contingency plans. The first six months of the project were predominantly spent learning about past research done on the EMS, as well as how EMSs were employed in other systems such as solar-powered cars, by other competitors in the DSC race, and in various other applications. We also had to submit several design reviews and revisions before we began the actual work of building and testing our designs. After identifying problem areas and developing contingency plans, it still remained that there wasn't enough time to thoroughly build and test each scenario and contingency in the plan. So the question became a matter of priorities: Strive to work out the bugs and build a solid design in the remaining time, one that would have a lower risk of failure and less likelihood of needing a contingency plan, or stop revising and improving the incomplete design and focus on developing a robust series of contingency plans, because we were absolutely going to need them.

We never made an official decision on which course to choose, but over time we gravitated away from working on the reliability of the EMS system and focused instead on establishing our contingency plans. Our ultimate goal was not to have a perfect EMS that met all of our design goals, but rather it was the much broader goal of winning the competition. Certainly we needed to implement the functions of the EMS to compete successfully, but it wasn't necessary for us to have the most sophisticated system.

2.5 In Hindsight – Failure was Imminent

There are two types of contingency plans: External and internal. External contingency plans account for malfunctions outside of the specific system. Looking at the EMS for instance, all the contingency plans we had in place were focused on external problems such as lost communication with other systems. Our plans in this regards were fairly sound. Without realizing it, though, we neglected to develop contingency plans for problems internal to the actual EMS algorithm. Such internal contingency plans would take into consideration internal failures in how the software implements the EMS functions. The code was developed in blocks, or subroutines. If one subroutine failed, we had not designed a way for the algorithm to continue running. We checked for certain errors, especially with respect to subroutines associated with data input, but the overall design was very unlikely to run without months of debugging. As things progressed, it became apparent that we did not have proper plans in place to deal with internal errors.

In hindsight we can see that while the energy management logic had been well developed, it's implementation in the microcontroller left a lot to be desired. The primary reason for this was that the team had minimal programming experience and insufficient expertise to create a complex code that would be robust. Secondly, we lacked time and manpower to finish and test the primary EMS code, to build and test contingency plans within the software, and to test all the subsystems.

3 The Race

This section describes the team's experience as the competition got underway and how our contingency plans played a critical role keeping the boat in the race.

3.1 A Fatal Flaw

The DSC competition was held in the Friesland Province of The Netherlands in July 2012. We arrived in Europe five days before the start of competition in order to install the drive system, electronics, EMS, steering system and solar panels on the hull for the first time. Needless to say, the EMS was not fully tested. Individual components worked, but the entire system had never run in the race configuration. The first time we ran the EMS integrated with the boat was on the day of the technical inspections. We passed the inspections but discovered our EMS system didn't work.

With limited resources, limited access to the boat, and less than 24 hours until the start of the race we found a fatal flaw in the EMS algorithm. The problem was in the subroutine which read the current latitude and longitude from the GPS and compared it with a pre-loaded table of coordinates and then calculated the distance remaining on the course. While we were able to pinpoint the problem, the complexity of the code precluded disabling the faulty portion of code without interfering with the rest of the software. Our contingency plan in the event we lost the distance

remaining algorithm was strictly limited to losing the GPS signal. Due to lack of experience and lack of time there was no plan in place that would allow the rest of the code to operate smoothly without distance data.

Loss of the GPS signal, or more specifically, the inability to process our current location, was a fatal flaw for the Energy Management algorithm on the microcontroller to determine and maintain the proper speed for the boat. It forced us to abandon our original plan and resort to our back-up design.

3.2 Our Solution

An important aspect of our design process over the course of the year was a recurring team discussion as to what was critical information versus what would just "be nice." In particular, we had hoped to develop an autopilot function so that the driver could flip a switch into automatic mode and not have to touch the throttle. This certainly would have been a nice function to have, and it may have helped us win the race, but it was clearly not necessary to compete. The essential information we really needed were:

- Position of the boat (latitude and longitude)
- Boat speed
- Power being supplied by the batteries and solar array through the MPPT
- Remaining battery capacity
- A means to implement our EMS algorithm

With the onboard microcontroller unable to perform the EMS functions, we resorted to our most basic plan: manual energy management and speed determination. Implementation began by erasing the entire algorithm from the EMS microcontroller, creating a new file, and building the code portion-by-portion throughout the night until our back up plan was fully operational.

The new algorithm was very minimalistic: it read the raw values we needed from each critical sub-system, sent them to the LCD and stored them on the SD card. We created an Excel spreadsheet that would calculate everything the microcontroller was designed to do in order to give us a single value (battery current) for the driver to control. We had already put so much work into the logic of the EMS algorithm that it was a quick and easy process to translate this to another application, Excel in this case.

We had made provisions for the driver to communicate with other team members via a hands-free Bluetooth mobile phone headset, so we built on that and established an energy management team that would receive status updates on critical information at regular intervals via cell phone, run calculations with a laptop computer in the chase van, and communicate back to the driver the optimal current draw for the motor for that point in the race. The driver would not even use boat speed, he would simply strive to maintain a particular level of battery current and the boat speed would fluctuate with sun and wind conditions.

3.3 Contingency Plan Tested

As the race started, we relied on the untested backup system, unsure of how it would perform. In comparison to the sophisticated EMS systems found on other boats in our class we were in a category of our own. But we fully understood the boat's power budget and knew how to arrive at an optimum boat speed to minimize our travel time over each leg of the race. The race was spread out over the course of a week, giving us time to identify and fix flaws in the new system. The biggest problem we ran into on the first day, for example, was difficulty communicating with the driver. The waterways were often exposed to a great deal of wind which made it very difficult to be understood over the phone. It was also unrealistic for the driver to concentrate on navigation, steer, operate the drive system (with its quirks and nuances), and also relay GPS and other boat status information at the same time. Operator overload, after all, had been a key incentive to develop an automated EMS in the first place. However, by limiting our communication to brief updates every 10-15 minutes—certainly not as optimal as our designed system would have been—we were able to provide the driver sufficient information to drive at the optimum speed and also provide navigation information. This, too, was critical, since he was driving without a map, or GPS map screen, and was not usually following any other boats.

Overall, the system seemed to be working. A great benefit of reverting to such a simplistic approach was that it allowed the EMS team who designed and programmed the algorithm, to understand what would have been going on behind the scenes during a racing scenario. By mentally and tactically being in the loop as part of the EMS process, we were able to see areas where the algorithm could be greatly simplified. We only had to match the remaining battery capacity percentage with the percentage distance of the course remaining. The percent battery capacity was, providentially, already displayed on the commercial LCD displays we had installed as one of our contingencies. Since

minimum race time came down to draining the batteries uniformly until we reached the finish line on "empty", we could achieve our goal by focusing on those two values.

We operated the contingency plan for the remainder of the race with a great deal of success. Despite the crudeness of our new EMS system, we effectively drained our batteries on all but the shortest legs of the race. In fact, our boat excelled the best on long cold, days with head winds and minimal sun because the hull and prop were excellent and we could reliably manage the available battery energy. We had been concerned about other teams with intricate EMS systems, developed by electronic specialists that incorporated CAN buses for data acquisition, Wi-Fi network connections, and much more detailed code structures that could handle large amounts of data. But they weren't without problems. One of our top competitors lost connection with their boat during the race and without an on board back-up system the driver had great difficulty completing that leg of the race. Our team ended up taking 3rd place in the Top Class overall, and finishing as the top university team in the competition.

4 Conclusion

While we had spent nearly a year designing and building our Energy Management System, it proved greatly beneficial that the team understood the physics of the energy management problem and had spent as much time as we did considering how our system could fail and developing contingency plans. Some might argue that if we had focused more attention on making the system work instead of diverting time to our contingency plans, we wouldn't have needed those plans. Yet, we correctly reasoned that the probability of running into some sort of failure was too high to ignore. This was especially true when you consider what was at stake if a failure occurred. By working on the EMS and spending time developing contingency plans—and ultimately relying upon them—we learned valuable lessons in engineering design and how to keep the system running despite failures that will inevitably occur. This was a lesson that could not merely be taught in the classroom, but was one that could only be learned through a design project such as our experience working on the Cedarville University Solar Boat Team.

References

Carnegie Mellon. (2012). *Carnegie Mellon Solar Splash.* Retrieved April 15, 2013, from Solar Splash Technical Reports: Retrieved from http://www.solarsplash.com/documents/2012_Carnegie_Mellon_TechReport.pdf

Cedarville University Solar Boat Team. (2012). *2011-2012 Solar Boat Final Report.* Cedarville, OH.

Dewhurst, T., & Brown, G. (accepted for publication). *The Preliminary Design Phase – The Key to Achieving Project Objectives*. In N. van Hattum-Janssen, R.M. Lima and D. Carvalho (Eds.), *Proceedings of the Fifth International Symposium on Project Approaches in Engineering Education PAEE 2013*, Eindhoven, the Netherlands.

Feldbrugge, R. (2010). *Using Reinforcement Learning to Make Optimal Use of Available Power and Improving Overall Speed of a Solar-Powered Boat.* University of Groningen.

Franke, J. L., Hughes, A., Jameson, S. M., Clark, J. G., & Szezerba, R. J. (n.d.). *Holistic Contingency Management for Autonomous Unmanned Systems.* Retrieved May 18, 2013, from Lockheed Martin Advanced Technology Laboratories. Retrieved from http://www.atl.external.lmco.com/papers/1344.pdf

Holmes, S. (2007, May 22). *Crunch Time for Boeing.* Retrieved May 18, 2013, from Business Week: http://www.businessweek.com/stories/2007-05-22/crunch-time-for-boeingbusinessweek-business-news-stock-market-and-financial-advice

Hopcroft, R., Burchat, E., & Vince, J. (2006). *Unmanned Aerial Vehicles for Maritime Patrol: Human Factors Issues.* Fishermans Bend, Victoria, Australia: DSTO Defence Science and Technology Organisation.

The College of New Jersey. (2012, May 21). *Solar Splash 2012 Technical Report.* Retrieved April 15, 2013, from Solar Splash Technical Reports. http://www.solarsplash.com/documents/2012_TCNJ_TechReport.pdf