Seven Axioms of Good Engineering:
Development of A Case Study-Based Course for NASA

Roger C. Forsgren NASA Academy of Program/Project & Engineering Leadership (APPEL) NASA Headquarters, Office of the Chief Engineer, Washington, D.C. Roger.C.Forsgren@nasa.gov

Anthony Luscher Associate Professor Department of Mechanical & Aerospace Engineering Ohio State University, Columbus OH luscher.3@osu.ed

Abstract

This paper describes the development of a custom course tailored to the mission and program needs of the National Aeronautics and Space Administration (NASA). NASA's Academy of Program/Project & Engineering Leadership (APPEL) was looking for a novel way of educating its engineering and management workforce about engineering design by investigating design successes and failures both internal and external to NASA. Instead of focusing training on a specific tool or methodology for engineering design a broader, higher level, and more conceptual approach was taken. Proximate causes of engineering design failures are often due to technical flaws, but their root causes are often found in human fallibility and lack of understanding about certain fundamental truisms in the design process. Case studies were selected to illustrate the basic rules—or axioms—of good engineering design. The authors developed these axioms. Their application to select case studies were the basis for the course called Seven Axioms of Good Engineering or SAGE. The description of these seven axioms, the rational for their existence, and the case studies used are covered in this paper. Covering landmark cases internal to NASA such as the Columbia accident and external cases such as the Tacoma Narrows Bridge and Three-Mile Island, SAGE leverages lessons from these examples to illuminate seven core principles that are broadly applicable to all engineers, regardless of technical discipline. It has been well received by more than 500 course participants, and serves as a model for future engineering training and education programs.

Introduction

In the 1970s, NASA initiated the design and development of a new space transportation system that would carry humans and payloads into low-Earth orbit and later support the construction of the International Space Station. Called the Space Shuttle Program, it required drawing upon the engineering skills and expertise distributed across NASA's ten centers. Decades later, with the shuttle program preparing to retire in 2011, NASA faced the challenge of developing its next human spaceflight program: Constellation. Announced by President George W. Bush in 2004, Constellation was the first large-scale human space flight program NASA had endeavored to construct since the shuttle, requiring a design effort the agency had not seen in nearly thirty years.[1]

As the Constellation Program ramped up in 2006, NASA's Academy of Program/Project & Engineering Leadership (APPEL) identified a need to provide NASA engineers with a unique learning experience to supplement their existing engineering skill sets as they progressed with

the extraordinary design endeavor before them. APPEL, an organization that supports NASA's missions by promoting individual, team, and organizational excellence in program/project management and engineering, sought to develop a course dedicated to engineering design to provide the NASA workforce with the knowledge and skills they needed on as Constellation progressed. APPEL's Roger Forsgren and Ohio State University faculty member Anthony Luscher initiated the development of a course intended to help its engineers take a step back from specific, tactical engineering design tools such as Six Sigma or failure mode and effects analysis (FMEA), and think about design challenges at a higher level, offering a conceptual approach to designing and reviewing space-faring products.

Engineering design is defined by Dym, et al. as the "systematic, intelligent process in which designers generate, evaluate, and specify concepts for devices, systems, or processes whose form and function achieve clients' objectives or users' needs while satisfying a specified set of constraints."[2] In essence, to design is to solve a problem. It is an inherently creative process that is carried out every day, whether it's for building a rocket ship or planning a date for Friday night. With the rise of technology and globalization, the engineering design environment has a variety of challenges including: increased complexity, shorter lifecycles, constrained budgets, an increased demand for partnerships, in addition to other considerations such as environmental impacts, performance, regulations, and legal ramifications.

The ways in which to approach the design process are varied. For instance, gate-based design (sometimes referred to as algorithmic design) is used on well-defined design processes like those seen in the pharmaceutical industry. It consists of steps to follow, specific decision-making procedures, and the documentation required to achieve the end objective is well known. The inspection, reconditioning, and certification of a space shuttle between flights are examples of well-defined, gate-based processes.

The design effort required for a program such as Constellation, in which little is well defined and systematic, the gate-based design approach is not appropriate. Instead, an axiomatic design approach achieves a quality end product through reasoned experience, knowledge, and practicality. In this context, axioms—or generally accepted truths—are considered the most general rules for design, invariant of the technology used or discipline.

Originally pioneered in the 1970s, the study of axiomatic design typically references two axioms developed by Dr. Nam P. Suh, engineer and professor at the Massachusetts Institute of Technology.[3] In *The Principles of Design*, Suh applies a mathematically rigorous approach to detailing axiomatic design.

The authors opted to take a different approach in order to better emphasize the more human element involved in engineering design. As a result, seven truths of good engineering were identified and developed to serve as the foundation for the course:

1) Avoid Selective Use of Existing Data
2) Extrapolate Existing Data into Unknown Regions with Extreme Caution
3) Understand the Design's Sensitivity
4) When Possible, Always Test in the Physical World

5) Guard Against Unanticipated Loads and/or Failure Modes
6) Avoid Highly Coupled Systems Unless a Strong Benefit is Shown
7) Ensure a Human Understanding of How the System Works

In light of the design effort occurring at NASA, the authors' recognized a need to engage the agency's workforce in a meaningful discussion around these seven design axioms. Derived from years of the authors' individual engineering experiences and principles posited through the writings of engineers such as Henry Petroski, Eugene Ferguson, Edward Tenner, and Charles Perrow,[4-8] the seven axioms serve as the foundation of APPEL's course *Seven Axioms of Good Engineering* (SAGE).

Case Study Learning

Equally important to the development the seven axioms was the approach APPEL employed to teach them. There are many ways to convey learning, and the method selected is dependent upon the desired learning objective. Some methodologies direct learners through a well-characterized scenario or problem and call for a specific solution or response. Others employ a more flexible, exploratory learning approach to achieve a desired learning outcome. Whatever the approach, developing meaningful design competency in the engineering workforce goes beyond simply teaching technical knowledge and includes developing the capability of engineers to engage in a constructive discourse about complex design and engineering concepts. As Atman, et al. said, "The language to which student designers are introduced plays an important role in not only what they know about engineering design but also how they know it."[9]

One approach well suited to promote this type of learning and competency is the case study method, which was pioneered by Harvard Law School in 1870 and later expanded to other disciplines such as business and medicine.[10] Only more recently has case study learning been applied to the sciences and engineering. For example, the National Academy of Engineering has put together an extensive collection of case studies many of which discuss societal and ethical issues.[11] Despite these resources there are still a limited number of case studies that address the decision-making process that is part of engineering design.

Case study learning has been found to increase a number of learning outcomes such as critical thinking, problem-solving skills, and motivation to learn in engineering students.[12] The approach is designed to engage learners using facilitated, yet unscripted discussions to explore a complex scenario. Preparation is critical for both the learner and instructor prior to class, but the burden of the discussion and discovery is primarily placed on the learner. The learner must come prepared to ask questions, support different points of view, and engage with his or her peers to derive meaning from the case study content. The instructor must have a thorough understanding of the case study materials. However, an instructor fulfills more of a facilitation or moderation role to guide learners through a scenario as opposed to actively lecturing and dictating on a specific topic.[13]

Political theorist Hannah Arendt once said "storytelling reveals meaning without committing the error of defining it."[14] Similarly, effective case studies do not deliver a single, well-defined learning outcome. Instead, the content is complex, introduces conflict, and asks learners to

consider all aspects of the larger issues at play and how they influence success and/or failure in a given scenario. For the SAGE course, each case study is studied through discussion about which design axioms are followed and which are violated. While there are specified learning objectives for the course and each case, there isn't one explicitly stated correct answer for each scenario.

In contrast, a factoid-based case is more focused on and explicit about the desired learning outcome. For instance, such a case may present the scenario of a satellite antenna that did not deploy properly due to a single technical flaw. The focus of this case narrowed and case may not look beyond the lone conclusion related to the technical flaw. In contrast, an analysis of a case study about the Deepwater Horizon accident yields more insight into engineering design than a single answer to why the failure occurred.

The case study approach provides course participants with the opportunity to apply their critical thinking skills to each scenario and exercise non-analytical insight as part of the design process. Ultimately, the methodology reinforces the practice of reflection upon past successes and failures within the context of the seven axioms and how they can inform future design endeavors.

Development of The Seven Axioms of Good Engineering

The seven axioms of the SAGE course are the product of in-depth engineering study, comprehensive research of the teachings and observations of recognized engineers, and the authors' observations for success or failure in engineering design. This process started with the creation of 23 axioms. This is a large number to present in a short course and so a goal was set to reduce this number through a rigorous process to become seven. Upon further study it was determined that a higher-level "umbrella" axiom could be developed that would represent several of the original 23 axioms, which would then act as corollaries to the new axiom. Throughout the process it was important to ensure that each axiom conveyed the intended conceptual content, and several of the axioms (e.g., Axiom 3) address a broader scope than others, covering a wider range of concepts. The axioms are intended to serve as general rules that lead to good engineering design. This list is not meant to be exhaustive but rather to present a cohesive learning module as part of an engineer's education. A brief description of the seven axioms follows:

1) Avoid Selective Use of Past Design Data

Viking Project Manager Thomas Young once said, "…risk is a little bit like radiation. It comes in small doses, but it accumulates until it kills you."[15] As time passes, it is easy to become used to a certain level of risk. Prior to the foam strike on space shuttle mission STS-107 in 2003, which damaged the leading edge of Columbia's left wing and ultimately led to the tragic loss of crew and mission, there were six recorded incidents of foam loss.[16]

One such incident occurred on October 7, 2002, during the launch of STS-112, when a piece of the External Tank bipod foam shed and struck the Solid Rocket Booster/External Tank Attachment ring. NASA investigated and confirmed that a debris event had occurred, but did not identify it as a serious threat to safety. Following the incident, the STS-113 Flight Readiness

Review assessed the STS-112 strike and classified it as an "accepted risk" and not a safety-of-flight issue.[16] NASA continued to fly.

What wasn't fully understood at the time was that the External Tank (ET) had a design concern. Trapped air pockets in the ET's outer foam expanded due to altitude and aerothermal heating, caused chunks of the foam to break free. The warning signs of this issue were present, but remained unaddressed.[17] Six days after the STS-107 foam strike, Chair of the Mission Management Team Linda Ham wrote in an email to Space Shuttle Program Manager Ron Dittemore, "…the ET rationale for flight for the STS-112 loss of foam was lousy. Rationale states we haven't changed anything, we haven't experienced any 'safety of flight' damage in 112 flights, risk of bipod ramp TPS [Thermal Protection System] is same as previous flights…So ET is safe to fly with no added risk. Rationale was lousy then and still is…."[16]

Ham's characterization of NASA's attitude toward the STS-112 foam strike during the STS-113 review illustrates a phenomenon called the "normalization of deviance," described by author Diane Vaughan in her book *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, whereby deviant behavior becomes commonplace and is no longer recognized as outside of the norm.[18] The deviance becomes accepted. This behavior has been observed across a variety of industries such aerospace, healthcare, energy, and even housing markets.

One component of this phenomenon is the human tendency to favor information that supports our beliefs regardless of whether that information is representative of reality. Typically referred to as confirmation bias, we are inclined (or biased) to attend to the data that supports our predetermined conclusions and ignore the rest. As a result, the entire data set is not objectively assessed.

There are always warning signs leading up to a design failure—and they are usually are easier to spot in hindsight. Among them is a tendency to not account for all of the data at hand, as was the case with Columbia. There were six close calls before Columbia and her crew was lost upon reentry. Ultimately, this axiom asserts that just because something is seemingly successful does not mean that everything was done right. Good engineering design involves being aware of what the data is saying—even if it tells a story we are not keen to hear.

2) Extrapolate Existing Data into Unknown Regions with Extreme Caution

Human nature is inclined to take what is known to be true in one scenario or environment and be tempted to apply it to an unfamiliar one. This holds true for both scalability (e.g., preparing a meal typically designed to feed a small family and scaling it to serve a large wedding party) and transfer (e.g., Henry Ford's attempt to apply his successful industry practices in Dearborn, Michigan to Fordlandia in Brazil).

Scalability was a significant challenge in product development during the nineteenth and twentieth centuries. Once a product was successful there was a tendency to scale it up, making it larger and/or more powerful. Bridges were made longer until issues that were not apparent at

small length became apparent at larger length. Ocean liners grew many times over in mass, power, and size with little understanding of the new environment that they operated within.

One such scaling challenge occurred during the design and development of the space shuttle. During the development, engineers were cognizant of the acoustic pressure wave produced by the shuttle main engines and solid rocket boosters, which, if too great, could threaten the integrity of the vehicle. To better understand the shuttle's performance in the harsh launch environment, NASA constructed a 6.4 percent propulsion scale model of the shuttle, which included the orbiter, propulsion system, and movable launch pad.[19, 20] The small-scale model was used to measure the effects of the acoustic launch environment on the vehicle and launch pad.[21]

During STS-1, the first flight of the Space Shuttle Columbia, the launch acoustics measured were much larger than anticipated.[22] If Columbia had been carrying a full payload, the orbiter would have been severely damaged. These findings led to the development of an appropriate sound suppression system on the mobile launch platforms. In scaling their understanding of the shuttle environment to its full size, variables not accounted for in the smaller model were introduced.

Years earlier, during World War II, the Navy developed the Mark 14 torpedo and acquired a poor reputation due to it's unreliable depth control, premature detonations, and failure to explode upon impact. Among the litany of design issues with the torpedo, one in particular resonates with the transference aspect of Axiom 2.

Intended for use in the Pacific Theater of the war, one of the flaws with the design was that it did not account for the specific environment in which the torpedoes would operate. The torpedo carried an exploder designed to detonate either when it made contact with the hull of a ship or when it passed through the magnetic field generated by the ship's keel. The latter was the preferred option, as ships were less armored and more vulnerable in this area.

Unfortunately, during the design and test phase of the torpedo, variations in the magnetic field were not taken into account. While the test torpedoes yielded positive results in the waters of Newport, Rhode Island, their performance in the Pacific Ocean was quite the opposite. Specifically, "the magnetic field generated by a metallic hull varies with latitude. Close to the equator the field spreads out, which is why torpedoes would often detonate 50 feet from a ship. Rolling seas, as well as surges in internal power supply to the coils and vacuum tubes that made up the hears of the magnetic detonator, were also sometimes enough to set off the device ahead of schedule."[23]

The designers failed to account for the change in environment (and latitude) while constructing the torpedo. While there were other contributing factors to the torpedoes' poor performance, this particular instance illustrates the dangers of extrapolating an understanding of a product's performance in one environment and applying it to another.

3) Understand the Design's Sensitivity and Robustness

This axiom can be interpreted a number of ways and further divided into three subparts:

1. Sensitivity with respect to design inputs.
2. Robustness with respect to statistical noise.
3. Robustness with respect to new loads and applications.

A good design continues to perform well even in off-nominal situations: it is robust with respect to sources of variation (e.g. temperature and mass), as well as functional requirements (e.g. a spacecraft carrying astronauts vs. carrying a space station). For instance, in the automobile industry, manufacturers design cars that will still drive straight even if the alignment isn't perfect.

Perhaps the quintessential example of this axiom is the Space Shuttle Challenger tragedy. At 11:38 a.m. on an unusually chilly Tuesday, January 28, 1986, the Challenger lifted off for the STS-51-L mission. Seventy-three seconds into launch the mission tragically ended in a ball of fire.

After investigation into the accident, a report from the House of Representatives Committee on Science and Technology cited a "failure in the aft field joint in the right-hand Solid Rocket Motor"[24] as the proximate cause for the Challenger explosion. Critical to the successful operation of this joint was a component called an O-ring. Manufactured by NASA contractor Morton Thiokol, the component's purpose was to contain the propellant's burning gases during lift-off and flight operations. The failure of the joint "was due to a faulty design, and that neither NASA nor [Morton] Thiokol fully understood the operation of the joint prior to the accident."[24] In other words, they didn't fully understand the design.

Prior to the accident, Thiokol had done testing on the O-ring at various temperatures, revealing troubling data about the component's performance. They found that the O-ring's ability to create an effective seal was compromised at temperatures of 50 degrees Fahrenheit and below. The day Challenger launched, it was 36 degrees Fahrenheit on the pad.[25] Investigation into the accident revealed a number of factors to which the joint sealing performance was sensitive, including contamination during assembly, reuse, and temperature.[26]

As exhibited by the Challenger story, the importance of knowing the most important variable in a design, what it's most sensitive to, how small changes impact it, and how small changes impact the system as a whole cannot be understated.

4) When Possible, Always Test in the Physical World

This axiom is known to engineers in a variety of ways. "Test as you fly, fly as you test." "Let the data speak." "Hear the voice of the design." When it comes to testing, it is tempting to rely on the output that a model, analysis, or risk assessment provides. While technologies such as computer-aided engineering (CAE) and simulation programs are powerful tools, they are not a replacement for the real thing: an end-to-end test.

Nobel laureate and James Webb Space Telescope Principal Investigator John Mather learned this lesson early in his career. During his graduate studies, Mather designed a balloon payload intended to measure cosmic background radiation. He and his team had grown tired of testing

and forewent some of their planned tests. The payload failed. "Testing is tiresome, tedious, boring, and essential," said Mather. "If you do not test it, it will not work."[27] Years later, after Mather set aside his involvement in research related to cosmic background radiation, NASA offered him the opportunity to fly the experiment in space on the Cosmic Background Explorer (COBE). A mission fraught with challenges and multiple redesigns, he carried the lessons of his failed graduate experiment with him: test, test, test. The mission yielded discoveries that earned Mather at Nobel Prize in 2006.[28]

Around the time of COBE's development, NASA was building the Hubble Space Telescope. Known for its issues with spherical aberration, the story of Hubble illustrates the importance of this axiom well. While some tests were conducted during the development of telescope, the execution was poor, yielding poor data, and enabling Perkins Elmer engineers to selectively use test data to support the results they desired. Had all the necessary testing been performed correctly and if the Optical Telescope Assembly (OTA), which contained the primary mirror where the spherical aberration existed, was subjected to an end-to-end test, the failure could have been avoided.

The Hubble Investigation Report noted, "An end-to-end test of the OTA would have been very expensive to perform at the level of accuracy specified for the telescope. The test could have cost on the order of what the OTA itself cost, because a flat or plano mirror would have been needed,"[29] and that "a range of feasible tests to verify the shape of the primary mirror were considered, but not carried out. Finally, no end-to-end tests were planned or implemented to verify the performance of the OTA."[30]

A fundamental part of testing is having at least two independent test mechanisms (e.g., numerical model, analytical model, experimental data, etc.) for a basis of comparison. Performing tests, walkthroughs, and building prototypes lengthens schedule and increases cost. However, the price of not doing comprehensive testing can yield more costs—as it did with the shuttle mission to fix Hubble—when a mission fails and the error has to be corrected. In the case of Hubble, NASA worked diligently and was able to correct the mistake. However, for some engineering feats such as the James Webb Space Telescope, there isn't always a second opportunity to get it right.

5) Guard Against Unanticipated Loads and/or Failure Modes

How does one guard against something that is unanticipated? While this sounds borderline illogical, complex feats of engineering heed this axiom, as they are particularly susceptible to unanticipated events. Anything can happen. Even the designs that intentionally plan for the unexpected can fall victim to the unthinkable and so-called "unknown unknowns." New designs fail in novel ways and as engineering systems grow and evolve, the governing mode of failure often changes.

On August 14, 2003, parts of Ohio, Michigan, New York, Pennsylvania, New Jersey, Connecticut, Massachusetts, Vermont, and the Canadian provinces of Ontario and Quebec were impacted by series of unfortunate (possibly unthinkable) events. At 12:15 p.m. Eastern Daylight Time (EDT), an employee at the Midwest Independent Transmission System Operator identified a problem with one of their software analysis tools designed to monitor power flow over timed

increments. While troubleshooting the error, the operator had to deactivate the system's timer. While he succeeded in restoring functionality to the tool, he did not restore the system to its normal, automated operation: the timer was never reactivated. Without realizing his mistake, the operator left for lunch.

Two hours later, in separate facility, the FirstEnergy Corporation's Energy Management System experienced a failure. Operators successfully rebooted the system to recover their ability to monitor the electrical grid, however they didn't realize that certain functions were not fully restored. One in particular, an alarm that alerted operators to off nominal behavior in significant components, remained offline. The loss of the alarm functionality went unnoticed until 3:42 p.m. EDT.

Meanwhile, a 345kV power transmission line in Walton Hills, Ohio sagged due to an increased load. Sagging transmission lines are an accepted occurrence and are typically managed by building structures that are high enough to provide power lines clear space away from objects like trees. However, at 3:05 p.m. EDT, this particular line made contact with an unpruned tree, caused the line to short-circuit, and then fail. Within the next thirty-five minutes, two more power lines began to sag as they took on the burden of the first failed line. They, too, short-circuited. The loss of the power grid operators' situational awareness and the transmission line failures ultimately led to a cascading a power outage that left 50 million people without power before anyone could stop it or explain what happened.[31]

While a detailed analysis of the 2003 Northeast Blackout is considerably more complex than what is described in this paper, the story illustrates that complex designs must be created with vigilance. The unanticipated event is the one not thought of, and this places a burden on the designer to carefully consider all possible failure modes. Failure modes and effects analysis is one tool that can be used to check that this axiom is followed.

With 200,000 miles of transmission lines serving over 283 million people, "the North American electricity system is one of the great engineering achievements of the past 100 years."[32] Maintaining regular operations on a normal day is complex. The possibility of a power failure was not lost on the designers of the electrical grid. Standards and practices were in place to prepare operators to respond to unexpected events. "The basic assumption underlying these standards and practices is that power system elements will fail or become unavailable in unpredictable ways."[33] And so they did.

6) Avoid Highly Coupled Systems Unless a Strong Benefit is Shown

During the Apollo program development, the computer systems for the Saturn V rocket and the Apollo Command Service Module (CSM) were separate from one another. For the Saturn V rocket, a dedicated 350-pound instrument unit housed in a ring atop the third stage provided the rocket's guidance and control. The CSM contained the Apollo Guidance Computer, an advanced digital computer and which was one of the first of its kind to contain integrated circuits. The use of two separate computers instead of one saved lives.

Within the first minute of the Apollo 12 launch on November 14, 1969, the spacecraft was struck by lighting—twice. The strikes resulted in electrical surges that temporarily knocked the command module's fuel cells and navigation systems offline, and permanently disabled nine non-essential instruments. It was another two minutes before the crew regained control of the situation and continued on their journey to the moon.[34] Throughout the disturbance, the Saturn V rocket's instrument unit was unaffected. Had it also been compromised, it is likely the crew would have been lost.

While the avoidance of a potential fallout from a possible lighting strike might not have been one of the benefits considered during the development of the Apollo and Saturn V computers (Commander Pete Conrad later remarked, "[I] think we need to do a little more all-weather testing."[35]), this axiom highlights that increased interdependency of systems can lead to the increased probability of a problem.

Ten years after the end of Apollo, NASA launched its first Get-Away Special (GAS) Program mission, a program that exemplifies the meaning of this axiom. Originally an idea hatched by former-NASA Associate Administrator John Yardley in 1976, the GAS Program intended to give anyone from amateurs to experts the opportunity to use any excess space in the space shuttle payload bay to conduct experiments in low-Earth orbit. However, because the program accommodated such a wide a range of technical experience and projects, the program's design needed to accommodate a wide range of outcomes.

Since the GAS payloads were secondary payloads, it was important they did not interfere with the success of the shuttle, primary payloads, and crew. Experiments and payloads flown as part of the program were housed within aluminum containers either 2.5 or 5 cubic feet in size, which were designed to contain potential hazards if something went awry, and weigh no more than 200 pounds. Experimenters were required to provide their own data recording, sequencing systems, and power, and not draw upon or interfere with shuttle resources. Astronaut crew involvement was limited to specific, simple actions such as turning a payload on and off, but not monitoring or servicing the payloads.[36]

The program successfully launched 159 payloads on 35 space shuttle missions between 1982 and 2003, when the Columbia accident prompted the cancellation of the program. As demonstrated by the GAS program, decoupling systems minimizes the impact of a possible failure propagating throughout the larger system. While not always possible, it is certainly worth considering.

7) Ensure a Human Understanding of How the System Works

Designing a system that functions well is one accomplishment. Designing a system so that its operations and functions are intuitive and comprehensible to a user is another. Complexity, safety, and technology contribute to the difficulty of designing systems that are fully understood by their operators.

At 4:00 a.m. on March 28, 1979, the Three Mile Island nuclear power plant experienced an unexpected malfunction, triggering an increase in temperature in its cooling system and causing

a reactor to shutdown automatically. Per protocol, a relief valve opened to restore the proper temperature balance. Ten seconds later the valve was supposed to close.

Inside the power plant control room, operators managing the situation monitored their instruments in order to understand what had transpired. Their instruments indicated that the command to close the relief valve had been sent. However, there was no instrumentation in the control room to confirm the command had been received and the valve had actually closed.

Without the operators knowing, the command was never received and the valve remained open. As a result, the system began to behave in ways that confused the operators. Since they had an incomplete understanding of the system's status, their response to the events that followed was uninformed and slowed their ability to control the situation. The control room's design and instrumentation were ineffective at communicating to the operators the information they needed to address the problem before them.

"Deficient control room instrumentation" was later identified as one of the root causes for the partial meltdown. [37] The report of the Presidential Commission on the accident recommended to the that future actions include the "review and approval of control room design; the agency should consider the need for additional instrumentation and for changes in overall design to aid understanding of plant status, particularly for response to emergencies."[38]

With any design, it is the responsibility of both the designer and operator to have an understanding of the system's the strengths and weaknesses in how it communicate its state. The safety the system and surrounding entities and an operator's ability to effectively respond to off nominal situations depends upon it. A good design should never leave an operator guessing what is happening behind the scenes.

SAGE Case Studies and Learning Materials

During the development of the SAGE course, the authors intentionally selected to teach case studies that addressed a variety of engineering disciplines, which included, but were not limited to aerospace. From energy to deep-sea drilling to military design, the cases cover a broad range of topics and technologies. To aid in understanding the authors start each case study with a review of the technologies involved and a summary of the readings. Table 1 displays each major case study taught in the course and the applicable axioms. The check mark means that the axiom is used as either a positive or a negative example and is therefore a topic of discussion.

Table 1: Main SAGE Case Studies and Applicable Axioms

Case Study	Axiom Cited						
	1	2	3	4	5	6	7
General Electric Refrigerator	✓	✓	✓	✓	✓		✓
Ocean Ranger			✓		✓	✓	✓
Pioneer 10		✓		✓	✓	✓	
Deepwater Horizon	✓		✓	✓	✓	✓	✓
Three Mile Island	✓	✓	✓		✓	✓	✓
DC-3 Aircraft		✓	✓	✓			
Tacoma Narrows Bridge	✓	✓	✓		✓		

Columbia STS-107	✓	✓	✓	✓	✓		
Mark 14 Torpedo	✓	✓	✓	✓	✓	✓	
Hubble Space Telescope Primary Mirror		✓	✓	✓	✓		

Many of these case studies are know and will not be described here. Students are asked to use the axioms as a guide in the evaluation of the suitability of each design.

Future Work

The current SAGE course has been offered over 20 times to technicians, engineers, project managers, and senior management across NASA's ten centers. Self-reported reviews of the course have been extremely positive (4.4/5 to 4.8/5), with many course participants commenting on their new insight into design and design decision-making. One unanticipated finding is the audience's positive interest in case study learning and in further reading of engineering case studies. Future evaluations will provide a more detailed review of the learning of each specific axiom.

Several of these cases have also been used in a capstone engineering design course taught at a major public university. One of the issues with this is that students are unfamiliar with the case study method of instruction and need motivation to complete all of the readings before class. Case study learning is idea in recitation classes which have less than 30 students.

Future offerings of the course will seek to build upon and refine several aspects of the learning materials and introduce new case studies. Planned updates include:

Categorization and expansion of the axioms. The axioms will be further categorized to identify those that involve the processing of past information, strategies to make good design decisions, the relationship of the design to the outside world, and the interfaces among the various parts of the internal design.

Incorporation of case studies focused on the small and medium design scale. Most of the current case studies address the challenges of large, complex products, projects, and systems. While these case studies provide an important and memorable learning experience, course participants often work on smaller projects. Including case studies about smaller projects will offer participants an opportunity to engage in thinking about the axioms on a different scale.

Reducing the burden of course preparation. One of the challenges of teaching the SAGE course on a compressed, three-day schedule is the amount of case study reading that is required beforehand. New strategies will be explored to provide learners with better ways to successfully manage the quantity of reading in conjunction with their full-time work at the agency.

Development of a dedicated section on engineering communication. The current course touches on various aspects the role of communication plays in engineering design. Future versions of the course will seek to dedicate more focus to this critical engineering skill.

Inclusion of design exercises. Some course participants have limited experience with engineering design and the decisions and judgments involved. Two in-class, hands-on group design exercises—one of which will be based on an Arduino robot board—will be added so as to reinforce participant knowledge of the design principles being taught throughout the course.

References

[1] "The Vision for Space Exploration," National Aeronautics and Space Administration, NP-2004-01-334-HQ, 2004. (*See also http://www.nasa.gov/pdf/55583main_vision_space_exploration2.pdf*.)

[2] Dym, C.L., Agogino, A.M., Ozgur, E., Frey, D.D., and Leifer, L.J., "Engineering Design Thinking, Teaching, and Learning," *Journal of Engineering Education*, Vol. 94, No. 1, 2005, pp. 103 - 120.

[3] Suh, N.P., *The Principles of Design*, New York: Oxford University Press, 1990.

[4] Petroski, H., *Design Paradigms - Case Histories of Error and Judgment in Engineering*, Cambridge University Press, UK, 1994.

[5] Ferguson, E., *Engineering and the Mind's Eye*, Cambridge, MA: The MIT Press, 1992.

[6] Tenner, E., *Why Things Bite Back - Technology and the Revenge of Unintended Consequences*, New York: Vintage Books - Random House, 1996.

[7] Chiles, James, *Inviting Disaster - Lessons from the Edge of Technology*, New York: Harper Collins Publishers, 2001.

[8] Perrow, C., *Normal Accidents - Living with High-Risk Technologies*, New Jersey: Princeton University Press, 1999.

[9] Atman, C.J., Kilgore, D., and McKenna, A., "Characterizing Design Learning: A Mixed-Methods of Study of Engineering Desginers' Use of Language," *Journal of Engineering Education*, Vol. 71, No. 3, pp. 309 - 326.

[10] Prince, M.J., and Felder, R.M., "Inductive Teaching and Learning Methods: Definitions, Comparisons, and Research Bases," *Journal of Engineering Education*, Vol. 95, No. 2, 2006, pp. 123 - 138.

[11] Online Ethics Center for Engineering and Research. Retrieved from http://www.onlineethics.org/Resources/Cases.aspx.

[12] Yadav, A., Shaver, G.M., and Meckl, P., "Lessons Learned: Implementing the Case Teaching Method in a Mechanical Engineering Course," *Journal of Engineering Education*, Vol. 99, No. 1, 2010, pp. 55-69.

[13] Kulonda, D.J., "Case Study Learning Methodology in Operations Engineering," *Journal of Engineering Education*, Vol. 90, No. 3, 2001, pp. 299—303.

[14] Arendt, H., *Men in Dark Times*, New York: Harcourt Brace & Company, 1983, p. 147.

[15] NASA Headquarters Oral History Project, Edited Oral History Transcript of A. Thomas Young, 2013. (*See also http://www.jsc.nasa.gov/history/oral_histories/NASA_HQ/Administrators/YoungAT/YoungAT_6-10-13.htm*.)

[16] "Columbia's Last Mission," Retrieved from http://go.nasa.gov/1iXguVH, 2011.

[17] "Columbia Accident Investigation Board," U.S. Government Printing Office, 2003, pp. 50 - 55.

[18] Vaughan, D., *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, Chicago: The University of Chicago Press, 1996.

[19] Sullivan, W., "Engineers Hoping to Prevent Pressure Peril to Shuttle," *New York Times*, October 31, 1981.

[20] MSFC Technical Standard: Development of Vibroacoustic and Shock Design and Test Criteria, MSFC-STD-3676, 2013. (*See also https://repository.msfc.nasa.gov/docs/multiprogram/MSFC-STD-3676.pdf*.)

[21] "Toward Lift-off: A Brief History and Chronology of the Marshall Space Flight Center's Role in Designing, Developing, and Testing the Space Shuttle Propulsion Elements for STS-1," NP-2001-04-72-MSFC, 2001, p. 11 (*See also http://history.nasa.gov/sts1/pdfs/msfc-full.pdf*.)

[22] Lai, S., "Development of space shuttle ignition overpressure environment and correlation with flight data," NASA Langley Research Center Shuttle Performance: Lessons Learned, Part 1, 1983, pp. 259 - 282.

[23] Murphy, D. "Hit or Miss," *Invention and Technology*, Vol. 58, 1998.

[24] "Investigation of the Challenger Accident: Report of the Committee on Science and Technology, House of Representatives," House Report 99-1016, U.S. Government Printing Office, 1986, pp. 4.

[25] Hoffman, E.J. and Kohut, M.K., *NASA's Journey to Project Management Excellence*, 2012. (*See also http://appel.nasa.gov/knowledge-sharing/appel-ebooks/*.)

[26] "Report of the Presidential Commission on the Space Shuttle Challenger Accident," Volumes 1-V, Washington, D.C., June 6, 1986. (*See also http://history.nasa.gov/rogersrep/genindex.htm*.)

[27] NASA's Masters with Masters 2: Dennis McCarthy and John Mather [Video file]. Retrieved from http://go.nasa.gov/1iXjq4C.

[28] "Redesigning the Cosmic Background Explorer (COBE)," September 2009. (*See also http://appel.nasa.gov/knowledge-sharing/publications/cobe-html/*)

[29] "The Hubble Space Telescope Optical Systems Failure Report," 1990, pp. 4 - 7.

[30] "The Hubble Space Telescope Optical Systems Failure Report," 1990, pp. 9 - 2.

[31] "Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What did We Learn?" North American Electric Reliability Council, 2003, pp. 32-46.

[32] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," 2004.

[33] "Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What did We Learn?" North American Electric Reliability Council, 2003, p 11.

[34] This Month in NASA History: Apollo 12 Lighting Strike, November 24, 2009, Retrieved from http://appel.nasa.gov/2010/03/11/aa_2-11_sf_history-html/

[35] Apollo 12 Flight Journal: Day 1 Launch and Reaching Orbit, Transcript, 2004. (*See also http://history.nasa.gov/ap12fj/01launch_to_earth_orbit.htm*.)

[36] "Get Away Special…the First Ten Years," Goddard Space Flight Center, Special Payloads Division, The NASA GAS Team, 1989.

[37] "Three Mile Island Accident," World Nuclear Association, last updated January 2012, http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Three-Mile-Island-accident/#.UnKqTpSG2tU.

[38] "Report of the President's Commission on the Accident at Three Mile Island – The Need for Change: The Legacy of TMI," Washington: U.S. Government Printing Office, 1979, pp. 63.