Implementing and Teaching Risk Mitigation in Project Courses

Robert Niewoehner
United States Naval Academy

Abstract

Faculty members teaching courses involving Design-Build-Operate projects have several distinct responsibilities regarding risk management. First, they have the obvious responsibility to safeguard the physical welfare of the involved students. Furthermore, they have a responsibility to instill in their students an appreciation for controlling risk in the operation of engineering systems. This paper applies industrial risk management processes to the educational design project both as a means of enhancing student safety and introducing risk management/mitigation as a distinct engineering process. Classroom-ready exercises are presented suitable for adoption in any engineering curriculum.

Motivation

Contrary to perception, Experimental/Developmental Flight Test is not supposed to be an exciting activity. In fact, considerable effort goes into making Flight Test mundane, the premise being that exciting flight test is typically undesirable, particularly if the excitement arises from the unforeseen. The processes by which the "excitement" is contained provide the substance of the flight test professional's identity. In contrast, the testing of student engineering projects is frequently ill-disciplined, supervised by faculty members who were otherwise very demanding in the rigor of other elements of their craft.

Two prominent issues arise. The first is safeguarding the safety of the involved students. Colleagues report the following episodes which have to be regarded as significant breeches in test discipline.

- At one school, in each of the past two years, during test flights of 25 lb. Radio-Controlled airplanes, the airplanes have struck test members pre-occupied with capturing video of the flight tests. Fortunately, the only injuries have been bruised shins.
- The first test operation of a SAE formula car was conducted along a narrow road lined on one side by parked cars, and on the other by a 3-foot concrete seawall which included a number of fixed protuberances (bollards, cleats, reinforcement stanchions at right angles to the road). Test speeds exceeded 45 mph during the first ten minutes of driving. The only obvious safety accommodation was a crash helmet, seat belts and a roll bar.
- A solar-powered car operating on public roads was involved in a collision with a private automobile, killing the student operator.[1]

The second is the negative educational element by which rigor and professionalism is demanded during the design, yet test practices are casual and ad hoc. The students fail to grasp that Test and Evaluation (T&E) is itself an engineering field in its own right, with its own processes and disciplines.

Professional T&E communities and their respective practices and disciplines have arisen as a consequence of the costs associated with poorly performed test and evaluation:

- Death or injury among test participants or spectators.
- The cost of tests can run tens of thousands of dollars per hour. Careful and methodical planning is comparatively cheap and can thereby yield enormous value by optimizing T&E resources.
- Schedule costs associated with damage or loss of test articles.
- Political costs associated with damage or loss of test articles. The loss of a test article can be spectacular and highly visible, and even if unrelated to the technical or business merit of the project, can cast an adverse political shadow over the program.

The origin of the problem is evident. The CDIO (Conceive-Design-Implement-Operate) initiative has highlighted the weakness of engineering faculties in direct industrial experience in design activities.[2] Fewer still have direct experience in professional test and evaluation communities. Furthermore, while professional organizations such as the Society of Experimental Test Pilots (SETP) and Society of Flight Test Engineers (SFTE) vigorously promote T&E safety, educate within their own ranks on this very subject and support their own specialized schools, their dialogue with the broader academic world is scant. Consequently, T&E risk management processes, while largely common sense, are foreign to many academic faculty. The challenge then is importing this body of developed processes from the T&E communities into the academic realm in a digestible format such that a faculty mentor for Design/Build/Test activities can readily embrace them as a foundational curricular practice. The material that follows is adapted from an Instructor Resource Module found on the CDIO website. Its format is derived from its origin and is intended to provide a self-contained lesson segment on test planning and risk mitigation.

Lesson Objectives

Introduce T&E practices and attitudes at the undergraduate level in order to:

1) Enhance student/staff safety in conjunction with design/build/operate activities by systematically identifying and mitigating test hazards.
2) Promote affective appreciation of T&E processes as the bridge from engineering development to operational deployment, and the business and technical incentives for disciplined T&E.

Content

Disciplined T&E depends largely upon the quality of the preparatory planning. Appropriate planning provides the principle means by which the following may be assured:

1) the testing will answer the sponsor's questions. It is possible to devote considerable resources to an extensive test program which fails to answer fundamental questions.
2) the testing proceeds efficiently.
3) the testing proceeds with minimum exposure to risk.

This paper is concerned with the risk mitigation and management, but the realities of program pressures (typically cost and schedule), will create tensions with risk mitigation, and

T&E risk will invariably be accepted to reduce test time and cost. T&E risk management seeks to comprehend the risks and reduce them to levels at which they can be accepted.

While no right way exists to manage the risk in engineering test processes, those organizations that do this well have adopted a fairly common structure, which could be regarded as "best practices." What follows is a distillation of the procedures common to many flight test organizations (both government and industry). Details, if desired, can be found in each organization's specific safety instructions.[3, 4, 5]

The process outlined below will include the following steps:

1) Hazard Definition
2) Cause Identification
3) Risk Assessment
4) Risk Mitigation
5) Residual Risk Assessment
6) Emergency Response

1) Hazard Definition

Test Specific Hazards are those that arise *as a direct consequence* of the test activity. There are many hazards that exist as the normal operation of a system, mitigated by design features and normal operational procedures. For example, every pneumatically wheeled vehicle risks blown tires, and the systems safety analysis during the design should have addressed this eventuality. A roll bar on a SAE formula car provides a measure of safety against this potentiality. This is not a test specific hazard. A blown tire becomes a *test specific hazard* only when the test activity directly increases the risk of the event. For example, a maximum braking test would elevate "blown tire" to the status of test specific hazard, because the nature of the test significantly elevates the likelihood of the hazard being experienced. Therefore it is the test team's intent to control those hazards uniquely introduced or aggravated by the testing, rather than revisiting the entire systems safety analysis presumably performed during the design. There is admittedly some ambiguity, as the test team will also need to provide safety margin for unknowns with respect to the design and its performance.

Risk management process begins then with a brain-storming session in which every imaginable test hazard is proposed. This must include considering some ludicrous "what-if's" and compound failures that might initially breech the bounds of plausibility. This process cannot be left to an individual, and the group's leadership must demand that team members have complete liberty to propose even outlandish hazards. Upon the completion of brain-storming, consideration should first be given whether the hazards are indeed test unique. Those hazards that are deemed routine may be set-aside at this time, as well as those that are indeed outlandish and inconceivable. Those hazards that might be judged implausible, yet conceivable, should be retained, as they may represent a category in which real danger exists, and the danger is elevated specifically because test team participants are blind to the real nature of the hazard. The professional T&E communities have lengthy archives of unforeseen/unimagined hazards which resulted in death, injury, damage or near brushes.

2) Cause Identification

Second, the likely causes of the hazard should be listed. Some hazards might have a single cause, but many may have multiple potential causes. All those causes must be listed.

3) Risk Assessment

Once a list of test specific hazards is composed, each event's consequences are listed. These consequences may run the spectrum from death and destruction to interruption of the testing. Each hazard is then coded for its severity and its likelihood. The codes below are representative of several T&E organizations. Definitions may vary from company to company, across or within industries, as may the number of levels and their resolution.

Many organizations employ a risk assessment code as a means of providing some objectivity to the process and a common vocabulary. The risk assessment code is a matrix describing both the severity of a test specific hazard and the likelihood of its occurrence.

Severity is commonly coded according to the following four severity levels of the consequents of an identified hazard, coded for our purposes by a Roman numeral (I-IV)

- I- Catastrophic- Death, serious injury, or destruction of an irreplaceable test asset.
- II- Severe- Injury involving lost work days. Damage to test assets requiring major repair and loss of schedule.
- III- Moderate- Injuries not involving lost work days. Non-minor repair (multiple shifts)
- IV- Minor- No personnel injury. Easily reparable damage (<1 shift). Cessation of that day's testing.

Likelihood is coded similarly according to a four or five point scale:

- A- Nearly certain- If the test is repeated multiple times over a lengthy testing campaign, the specified event should be expected to occur at least once.
- B- Probable
- C- Possible
- D- Improbable
- E- Remote

The likelihood is subjectively assigned, unlike the more rigorous values found in systems safety in which manufacturers quantitatively calculate component and system reliability. The counsel of experienced test personnel with diverse backgrounds, provide legitimacy to this process.

A 2-dimensional matrix is thus formed, which together capture the nature of the overall risk, ranging from Risk Assessment Code (RAC) I-A in the top left corner to RAC IV-E in the lower right. Figure 1 depicts an example from NASA's *Risk Management Procedures and Guidelines* (NPG 8000.4), similar to that used throughout the flight test communities.[6]

	LIKELIHOOD ESTIMATE				
CONSEQUENCE CLASS	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7
High Risk					
Medium Risk					
Low Risk					

Figure 1
Sample Risk Assessment Matrix

4) Risk Mitigation

Risk mitigation is then the process by which risks are reduced, moving them down and right in the hazard matrix. (The vocabulary *mitigate* or *mitigation* will likely be new and require definition for your students. The Latin root means *to soften*; the English verb means *to reduce harshness, hostility or severity*, precisely describing our very goal.)[7] Reduction in the severity level usually requires specific hardware changes to the test equipment (perhaps the installation of safety equipment installed solely for the purpose of the test, or the modification of the design to permanently reduce the hazard severity). Procedural precautions alone seldom reduce hazard severity. Hazard likelihood however can be reduced by hardware, instrumentation, or procedurally. Again at this point, brain-storming by a team of people is appropriate to devise mitigation measures to reduce the hazard level. Common risk mitigation techniques are listed below:

Hardware mitigation- Modifications to the hardware specifically to enhance the test safety.

a. Safety equipment- This is equipment specifically installed on a *test* article specifically to reduce *test* hazards. This is over and above the design features incorporated in order to enhance the safety of an in-service production article. This could include protective equipment for participants, power cut-outs, etc.

b. Instrumentation- Generally, the more the test team knows during the tests, the safer the tests. "Safety-of-test" parameters may be monitored in real time, or post-processed event to event during a build-up sequence (allowing a forecast of behavior on the next event). Note well that items identified in the test plan as "Safety-of-test" become "no-go" items; if that parameter isn't working, the test cannot be conducted, absent a suitable back-up.

Procedural mitigation- Procedures intended to reduce risk (typically the likelihood):

c. Codified normal and emergency procedures- Scrutinized, detailed procedures alleviate many of the incidental risks of operating equipment. For example- not applying electrical power until closure of panels, and then removal of power prior to any access. RC modelers habitually conduct antenna pattern checks and loss-of-signal checks as part of their pre-flight preparations. Those activities must be codified so that they are not lost in the anxiousness to operate a design.

d. Simulation- A huge discipline in its own right that spans a broad range of levels of expense and effort: batch, man-in-the-loop, hardware-in-the-loop, part-task, full-task, component, systems level, environmental, failure mode, etc. Simulation can be used for engineering analysis, procedure development, test team training (test rehearsal or emergency procedure).

e. Build-up/build-down. This is a fundamental technique in which performance in benign conditions is thoroughly understood prior to more stressing conditions. Build-up/down can be in speed, weight, loading, aggressiveness/abruptness, altitude, configuration. Build-up/down has the advantage of both incrementally increasing the stress on the system in test, and familiarizing a human operator (where applicable). Trends can then likely be observed and anomalous behavior more easily detected. Appropriate instrumentation enhances the likelihood of detecting adverse trends. Note: a cautious build-up/down improves the likelihood of detecting adverse behaviors, but must not be assumed to be wholly reliable. Many system exhibit non-linear attributes which can abruptly degrade system performance with little prior hint that 'cliffs' may be lurking.

5) Residual Risk Assessment

A single risk mitigation measure may not adequately address any one causal factor or hazard; indeed the best hazard plans include diverse, overlapping measures. After the mitigation measures have been applied, the hazard is again analyzed for both severity and likelihood, and a Residual Risk code assigned.

Presuming that test hazards cannot be eliminated all together (a rarity, frequently achieved only by test cancellation), T&E organizations must necessarily live with *accepted risk*. Accepted risks are those hazard codes for which tests may be allowed to proceed. Organizations vary in where they will draw the line through the risk matrix identifying the blocks they would regard as "acceptable." An organization's particular line invariably represents some stair-case running from lower left (inconsequential, and nearly certain) to upper right (catastrophic, but remote) . For example, some organizations accept all severity codes of III and IV, plus those category I and II hazards whose probability is "Improbable" or "Remote." Other organizations might allow for IIC, while prohibiting III-A, and ID. *The prerogative of drawing the line of acceptable risk must not reside with the test team, but with their executive leadership*. Indeed professional T&E organization convene review boards for tests exceeding certain thresholds of perceived risk, where senior engineers and managers outside the test team will critique the team's risk analysis and mitigation plans. These "murder boards" are vital for challenging the test team's assumptions; in truly high risk enterprises, their tone must border on adversarial. If not,

executive leadership is likely not adequately scrutinizing the work of their test team leaders, who will typically lack leadership's breadth of experience.

6) Emergency Response
Finally, to be complete, the Hazard Analysis should include some planning for a procedural response to event should it occur, despite the precautions. These then are included among the "Emergency Procedures."

A warning from the past

There is a real temptation to copy/paste the existing test hazard analysis of a prior program, and thereby short-cut the test hazard analysis process. There is genuine value in consulting the work of others for their ideas lest either some hazard or viable mitigating measure be overlooked. However, uncritical acceptance of another's analysis risks missing vital differences and a unique hazard, or one overlooked by others. Therefore, a prior analysis should be considered a baseline at best, or a check case after the initial brainstorming.

The purpose of the above module is two-fold. First, to elevate the safety of students involved in design-build-test projects. Secondly, to introduce the hazard management process as an engineering discipline in its own right.

Examples

Industrial Example (Flutter Flight Test):

Hazard:	Divergent Aeroelastic Event (an historic killer)
Cause:	Inadequate structural stiffness for the flight condition
Result:	Inflight disintegration of the airplane, loss of pilot
RAC:	I-C (presuming exhaustive design analysis)
Mitigation	>100 instrumented dynamic parameters
	Real-time monitoring by test team
	Incremental build-up in dynamic pressure
	Point-to-point clearance
	Test team training and consistency
	Minimum essential on-board crew
	Simulator rehearsal of high-workload points
	Simulator rehearsal of emergency procedures
Residual:	ID

Emergency Procedures:

"Abort, abort, abort" call from test conductor
Retard throttle, pull-up to reduce airspeed
Aerial inspection/ damage assessment

Automotive example:

Hazard:	Blown tire during anti-skid/maximum braking test
Result:	Dynamic Roll-over
	Loss of directional control- impact with surrounding objects
	Injury to driver
	Injury to spectators due to tire debris
Causes:	
	a. overheating during prolonged testing
	b. abnormal wear during testing
	c. seized calipers
	d. road hazards
RAC:	II-C
Mitigation:	Instrumented tire pressure and temperature
	Driver must wear full-protective equipment
	Tests will be performed on a test pad isolated from ground hazards
	Test pad will be swept/inspected prior to each day's testing
	Incremental build-up in speed and braking aggressiveness
	Brakes must cool to X deg prior to next test point
	Tires will be inspected through 360 deg of rotation after each test
	No personnel will be allowed downrange of the point at which braking begins, to a distance of 500 ft.
Residual	II-D
Emergency Procedures	
	Attempt directional control while lightly braking

In-class hazard mitigation exercise

This exercise is intended to provide a practice forum for the students preparatory to the development of their project test plan.

The class should be broken into groups of 2-3 students . Each group is assigned a distinct, plausible test hazard. These hazards could either be germane to the project on which the students were working or some other test with which they could conceivably have some familiarity. Teams are given 15 minutes to prepare their analysis for the assigned hazard, including the following elements:

1. Causal factors
2. Risk Assessment
3. Risk Mitigation
4. Emergency procedures
5. Residual Risk

Upon completion, each group can either present their Hazard Analysis and Mitigation by completion of a matrix on a chalk board, or via a transparency on an overhead projector (in which case each team should be provided with a Hazard Analysis Form and transparency marker).

In the case of a course in Flight Test Engineering, the following list is assigned to the students:

1) Overstress of landing gear/fuselage during max sink-rate landing
2) Engine flameout during spin testing
3) Blown tire during anti-skid brake testing
4) Store-to-aircraft collision during separation
5) Design-Build-Fly airplane impacts spectator

Vehicular design projects should have no trouble conceiving like lists of hazards. The risk to students however is clearly not restricted to vehicular projects. Other projects entail hazards that span projectiles, pressurized vessels, flammable or caustic materials, rotating machinery, electrical power, etc.

As an alternative to the above exercise, the material above could be presented in an inductive approach. Prior to introduction to the above material, have the student preview the website mentioned below, and come to class prepared to describe the motive and elements of the process that they see documented.

Other resources

Dozens of excellent examples of professionally prepared and reviewed hazard analysis forms can be found on the National Test Pilot School website.[8] The subject matter is clearly that of flight test, but the process and approach is evident from these samples.

The above model is synthesized from exposure to the flight test practices of Navy, Air Force, NASA, and diverse civilian companies. It represents no one organization, but resembles them all, the community of flight test professionals having collectively gravitated to this model over the past twenty years. Details can be found in various organizations' instructions, many of which can be found on the web.

Conclusion

The same care and rigor we demand of our student's analytical and experimental work should be shown in the test and evaluation phase. The material presented here constitutes an industrial best-practice among those who do this for a living. Even where the risks are slight, our students need to understand that managing the risks associated with the things they've built, is as much a professional responsibility as the analytical part of the design.

---

[1] Jane Stirling, "Solar car student dies in accident", http://www.engineering.utoronto.ca/userfiles/HTML/nts_1_1123_1.html, dated August 12, 2004.
[2] http:// www.cdio.org
[3] NASA Procedures and Guidelines *Risk Management Procedures and Guidelines* (NPG 8000.4), 25 Apr 2002
[4] Air Force Flight Test Center Instruction 99-1, *Test and Evaluation Test Plans*, 28 Jan 2002
[5] Air Force Flight Test Center Instruction 99-5, *Test and Evaluation Test and Control and Conduct*, 10 May 2002
[6] NPG 8000.4, pg 12.
[7] *Merriam Webster's Collegiate Dictionary, 10e*, Springfield, MA, 1997.
[8] http://www.ntps.edu/HTML/Downloads/TestHazardAnalysis.htm

Biographical Information
CAPT Rob Niewoehner, USN, is a Permanent Military Professor serving as Director of Aeronautics within the Naval Academy's Aerospace Engineering Department. He came to the Naval Academy after serving 17 years as both a fleet fighter pilot and experimental test pilot, including 3 years as the Navy's Chief Test Pilot for the development of the F/A-18 E/F Super Hornet. He is an Associate Fellow in the Society of Experimental Test Pilots.