A Hazard Analysis of Human Factors in Safety-critical Systems Engineering

Les Chambers

Chambers and Associates Pty Ltd
PO Box 593, Toowong 4066, Queensland

les@chambers.com.au

Abstract

Safety incident studies often cite human factors as a major cause of accidents. At Bhopal in 1984 human error - the failure to follow safe operating procedures - instigated the deaths of thousands of people from cyanide poisoning. In this case, human factors introduced a common cause fault that disabled four separate safety measures designed to prevent cyanide gas from venting to the atmosphere.

From this and other case studies I have taken the view that the competence and motivation of people responsible for the design and operation of safety-critical systems is our first and last line of defence against loss of life and property. The circumstances and influences that cause people to embrace or ignore best practice in safety-critical systems engineering invites detailed analysis.

In this paper I assert that lack of competence and safety awareness in developers and operators is a hazard that can have catastrophic consequences. However, by taking a risk management approach we can reduce the severity and frequency of accidents by developing insights into why individuals and organisations might choose to adopt international standards for best practice in safety-related systems engineering, and why they might not.

Keywords: human factors, EN50128, IEC 61508, safety-critical systems engineering.

1 Introduction

With distressing regularity throughout the world, individuals and organisations find themselves in situations that, when the dead are buried, the injured treated and the flames extinguished, are pronounced hazardous. Many of these situations come about through the interaction of normal, predictable and repeatable (but unsafe) human behaviour in the conduct of safety-related system design, development, operation and maintenance. The tragedy is that many of these behaviours can be recognised and their negative consequences avoided.

The objective of this paper is to make a small contribution to the catalogue of hazards that arise from our humanity. The way we act (or fail to act) on the basis of what we know (or don't know) and how we feel (or fail to feel) at the time. To this end I examine the behaviour of individuals, organisations and client-contractor teams formed to deliver safety-related projects. I investigate the factors that influence behaviour in two environments: self regulated in-house development and contracted systems development requiring compliance with CENELEC Standard EN 50128.

I draw my case studies from chemical processing process control system development with the Dow Chemical Company and railway station environmental control and smoke extraction projects for the Hong Kong MTR and the Taiwan High Speed Rail Corporation. In the context of these case studies I identify thirteen hazards that have human failings as their root cause and offer some ideas on how we can reign in the negative aspects of our humanity in the interests of building safer systems.

2 The Individual

Concerning how a safety-critical systems engineer should be trained.

Joe Simpson, high altitude mountaineer and author of the classic novel *Touching the Void* once wrote:

> *Experience is something you don't get until just after you need it.*

Joe learned the hard way. In 1985, he and friend Simon Yates embarked on a 21,000 foot climb of Siula Grande in the Peruvian Andes. Their strategy called for an alpine-style ascent, a technique where the climber attacks the mountain in "one great push", carrying minimal food and without setting up ropes or base camps ahead of time. This was a high risk strategy. In addition to the usual risks of death by exposure to sub zero temperatures, avalanche and lethal falls, any delays could cause them to be caught in the open with no food or heating oil. Due to Siula Grande's isolation there was also no possibility of rescue in the event of an accident. Joe's story has passed into legend. Breaking his leg in three places and ultimately having to be cut loose by Simon on the descent he cheated death at the bottom of a crevasse and managed to crawl back to base camp.

Joe and Simon knew they were taking substantial risks. They accepted them and suffered the consequences alone in the wilderness. You could say this was a fair thing as no one else was affected. At Bhopal, one year prior to the Siula Grande climb a small team of engineers took risks and 500,000 people suffered. This was not fair.

2.1 Case Study: Bhopal

Around midnight on December 2, 1984, for unknown reasons, a substantial volume of water found its way into a Methyl Isocyanate (MIC) storage tank in Union Carbide's Bhopal, India pesticide plant. The reaction of water and MIC formed carbon dioxide at high pressure, resulting in the passage of MIC vapour through the pressure release system, up the stack of a vent gas scrubber and into the atmosphere. At atmospheric pressure MIC decomposes into various components, the most toxic of which is cyanide gas. The immediate death toll from the cyanide release was in excess of 2000 people. Estimates of death and injury in the following days and years range from 30,000 to 500,000. Bhopal therefore represents the world's worst industrial accident.

In 2004 I had the pleasure of working with Jagdish, an engineer who lived through the disaster. He told me that it could have been worse. It turns out that nature was the only force working to mitigate the effects of the gas release that night. It was late at night, and cold, with a light breeze blowing and dew on the ground. Most people were indoors with their windows closed. Cyanide is readily absorbed by water and the low ambient temperature reduced the partial pressure of cyanide in the atmosphere. The lack of a high wind also limited the affected areas of the town. Around midnight Jagdish received a telephone call from his brother, an employee at the plant, who told him to seal all doors and windows with wet towels and stay indoors. His family survived, Jagdish had good fortune.

2.2 Are We Helpless Before Nature?

Reflecting on the catastrophe that was Bhopal, one cannot help but wonder "how far human affairs are governed by fortune and [by our actions] how fortune can be opposed". If we shift our focus to sixteenth century renaissance Italy we will find the man who wrote those exact words. His name is Niccolo Machiavelli. He is in a farmhouse on the outskirts of the city state of Florence. It's 1513 and he's just begun to write a book entitled *The Prince*. Machiavelli, a brilliant thinker, skilled diplomat and devoted servant of the Florentine state has just suffered genuine bad luck. In 1512 the government he faithfully served was overthrown and the powerful Medici family returned to power. Guilt by association with the past power structure caused him to be accused of sedition, imprisoned and tortured. His experiences became a metaphor for the dark side of the golden age that was the Italian renaissance. This was the time of Leonardo Da Vinci and Michelangelo, when artists and philosophers flocked to Florence to produce works of beauty that endure to this day. On the other hand Machiavelli's age was characterised by political turmoil and constant warring between the city states of Florence, Venice, Milan, Naples and the papacy based in Rome. In the resulting storm of political upheaval Machiavelli became one of the first western writers to formally deal with the concept of risk. His basic premise was that we are not helpless in the face of nature. That we can take steps to control our future but those steps must be calculated with a pragmatic insight into human behaviour. He wrote candidly of what men do as opposed to what they should do and advised princes on measures to be taken by the modern ruler to ensure that he stays in control of his principality.

Should they care to listen, Machiavelli can speak to today's systems engineers as they go about designing, building and operating safety-critical systems. I assert that we live in a modern renaissance surrounded by the creativity of emerging technologies. Whistling while we work we deploy them in a myriad of applications that can benefit mankind or, if they fail, take lives.

Like Machiavelli, our environment also has a dark side. The ebb and flow of power between warring city states has been replaced by a maelstrom of explosive technology growth in a cutthroat commercial environment; where compliance with standards for best practice comes into direct conflict with the fundamental unit of engineering, the dollar. How then should we conduct ourselves as individuals, organisations and contractual partnerships when faced with this conflict? Further, when put under pressure, what causes one engineer to aggressively pursue a best practice and another to ignore it, thus handing over the safety of future users, people who trust us with their lives, to the randomness of fortune.

2.3 Human Factors at Bhopal

The disaster at Bhopal came about through a series of human errors - critical decisions made by human beings. Given the potentially lethal consequences of an MIC release, the storage system had four separate safety protection measures. Based on the account provided in the book *Five Past Midnight in Bhopal* by D. Lapierre and J. Moro, safe operating procedures required that:

1. All MIC tanks were to be operated at 50% of capacity to allow for injection of a solvent to inhibit any reactions. I note that Jagdish's brother was unaware of this measure.

2. Tank contents were to be kept below 15° centigrade by a refrigeration system with a high temperature alarm provided in the control room.

3. Should the tanks become over pressured, the pressure relief system featured a scrubber designed to extract toxic chemicals from exhaust gases by injection of caustic soda.

4. Finally, should all else fail, all exhaust gases could be burned off by an ignition system installed at the top of a 34 meter flare stack.

The critical decisions that contributed to the accident were as follows:

1. The MIC tank levels were maintained above 50% and there was no awareness of the solvent injection measure.

2. The refrigeration system had not operated for months as plant management believed it wasn't necessary.

3. The scrubber had been off line for maintenance for a week.

4. The flare igniter was also out of service for maintenance.

Four separate safety measures were therefore defeated by two common cause faults: 1) lack of competence in process technology and 2) lack of safety awareness (the ability to recognise and deal with an unsafe situation). To abstract these causes further, the disaster was the result of poor education and poor attitude in human beings with decision-making power in a safety-critical environment.

What can be done about this? Answers are hard to come by. The engineering profession does not deal well with non-technical human issues. We tend to flick pass them to human resources specialists and go back to our calculations. This is no longer acceptable due to the devastating efficiency with which human factors can defeat the most elegantly engineered safety-related systems. Like it or not, engineers live at the pointy end of human factors, we should therefore know how to deal with them. How then, in an age of unfettered access to information and advanced educational technology, can lack of knowledge and bad attitudes come about?

2.4 The Origin of Safety Awareness

I'd like to discuss my own experience of how safety awareness comes about in an individual. To illustrate, I'd like you to picture yourself in the front room of my friend's house. It's a renovated workers cottage in the suburb of East Brisbane. Before she moved in, she took a risk management approach and had decorative bars placed on all the windows. It was a good move, hers is the only house in the street that has not been robbed.

You are standing at the window that opens out onto the front balcony. As a safety measure the bars on this window are hinged to allow for escape in case of fire. The procedure is to operate a lock, slide out a bolt, swing back the bars, open the window and make your escape. One day with a few minutes to spare I found myself in this room. My gaze fell on the locking mechanism and a scenario began to play out in my head.

It's midnight and the occupants of the house are fast asleep. Smoke curls up the hallway and finally sets off the smoke alarm mounted on the wall adjacent to the master bedroom door. Within 30 seconds my friend is awake with the realization that her house is burning down. By this time the smoke has thickened, making the blackness of night even blacker. She crawls across the hallway heading for the escape hatch. At this point in the scenario we can have many endings. The happy one plays out as follows: despite her terror, she can lay her hands on the key and operate the escape hatch lock in the pitch black. Given the high probability that the heat of the fire could make the bolt hard to slide and, in the worst case, impossible to touch without sustaining third degree burns, she also has a pair of pliers to pull it open.

Concerned at the absence of keys and pliers I engaged my friend in a conversation on fire safety. Today if you entered this room you would see below the window a key hanging on a hook and below the key a pair of pliers lying on the floor. Further, after several practice sessions my friend is capable of reaching the key and the pliers from any point in the house blindfolded.

Fire evacuation drills are a good idea for all residential homes. But this is not the point of my story. My point is, what would lead anyone with a few moments to spare in a strange room to have such a thought process? In my case the answer is: ten years of working in an environment where personal survival depends on heightened safety awareness. Ten years of participation in organised safety programs that required me to attend a safety meeting once per week, to reflect on safety hazards in my environment and to propose preventive action to reduce safety risks. This was the life of everybody working inside a chemical processing complex with the Dow Chemical Company. For me it occurred between 1975 and 1985, and shaped my attitude toward safety for the rest of my life.

2.5 How Safety Awareness Impacts Behaviour

My time with Dow impacted my behaviour in two important ways. Firstly, when dealing with a safety-related system I am more likely to think in terms of hazardous situations, risk and risk reduction. This has become an almost subconscious thought process. Secondly, I am more likely to challenge, with vigour, an unsafe practice being performed by another. Even to the point of incurring the wrath of my superiors when a management decision has the potential to create a hazard. For example, I once disobeyed a management edict to cease testing and deliver a software product I knew had bugs. I was reprimanded but to my great satisfaction found the bug.

A personal commitment to safety is a necessary safety driver. Having one safety zealot in a development team is an advantage, however this person can be marginalised by unmotivated team members especially if there is no support from management. In contrast, an entire team of zealots is a potent weapon against unsafe practices. It turns out that it is extremely difficult to order an entire team of people to do what they know in their gut is wrong. The net result is safety being engineered into a system. This is infinitely preferable to relying on after-the-event measures such as audits, reviews and testing to detect and correct safety-related defects. For example, Union Carbide's safety audits of the Bhopal plant did not prevent the disaster. A grass roots commitment to safety, developed through regular training and application, may have.

Hazard 1

Systems engineers do not value the safety engineering process. When put under pressure to deliver, the subject does not comply with established best practice in safety engineering even though he or she may be fully conversant with the process.

Risk: unsafe development practices or operational procedures cause failure of a safety-related system. In the presence of individuals that do not value safety, the probability that systemic defects will be injected into development and operational procedures is high. The probability that these defects will cause an accident must be evaluated on a case by case basis.

Risk reduction strategy: place systems engineers in an environment where they are constantly required to recognise hazards, evaluate risk and take preventive action. Reward engineers for good safety performance. Develop a culture where poor safety performance is career limiting.

If you are an engineering manager, monitoring the safety-related value system of all your subordinates should be a high priority activity. You could save a life. A steel worker was once pointed out to me on a multi story construction site. The comment was: "See him. He's careless. He's going to go." Two weeks later he fell six floors to his death. The man's poor safety attitude was transparent to everyone but nobody took action. What can be done? Step one is education.

2.6 The Safety-related Education

Bill McCarthy is a training captain for Cathay Pacific Airways in Hong Kong. Part of his job is to determine the competence of pilot applicants from other airlines on a flight simulator. Today he is witnessing a candidate pilot reliability and predictably crashing the simulator during the asymmetric flying test. Asymmetric flying skills are required when an engine fails on a multi engined aircraft. It transpires that to be a first officer with his previous employer the candidate wasn't required to demonstrate that skill! Asymmetric flying is a critical skill. In 2003 two Australian pilots were killed while practicing the procedure too close to the ground. This candidate pilot's lack of knowledge therefore represents a serious hazard.

In common with the aviator the systems engineer's education has a direct effect on safety. If we aspire to work with safety-related systems our profession should be explicit on what we are to learn, how we are to learn it and how our skills can be verified before we are given critical design responsibility.

2.6.1 Setting Learning Objectives

Whether it be asymmetric flying or dealing with overpressure in an MIC storage tank, human knowledge is the creator of safety integrity while ignorance can become its destroyer. The evolution of knowledge in human beings is well documented in the literature of education technology. In the 1950s a group of educators led by Benjamin Bloom developed a classification system for educational objectives. Known as Bloom's Taxonomy, the system partitions learning objectives into the following three domains:

1. **Cognitive domain.** Concerning how people think and take on knowledge.
2. **Affective domain.** Concerning the development of attitudes, beliefs, and values.
3. **Psychomotor domain.** Concerning skills requiring physical movement and coordination.

The Cognitive and Affective domains are most relevant to the education of systems engineers.

A related development occurred in 1984 when David Kolb modelled the experiential learning process with "The Kolb Learning Cycle". The cycle models the process by which individuals, teams and organisations learn from experience. Bloom therefore helps us set the objectives and Kolb gives us a process to reach them.

2.6.2 Cognitive Domain Learning Objectives

The cognitive domain is described by a hierarchy of learning objectives in increasing level of difficulty and sophistication as follows:

1. **Knowledge.** The ability to absorb and regurgitate facts. Example: the engineer can list hazard analysis as a safety engineering life cycle activity.
2. **Comprehension.** The ability to internalise and organise information identifying links between facts. Example: the engineer can explain in his own words the purpose and objectives of a hazard analysis.
3. **Application.** The ability to perform basic procedures such as solving problems. Example: the engineer can compute the probability of a hazardous event.
4. **Analysis.** The ability to think critically and in-depth, often characterised by the ability to abstract. Example: the engineer analyses the causes of hazards and gains insights into patterns of behaviour and hazardous situations that may be used to detect unsafe situations in future.
5. **Synthesis.** The ability to perform original and creative thinking as opposed to the mechanical implementation of a standard procedure. Example: the engineer reviews the hazard analysis and creates a new procedure to reduce the risk of an accident should the same situation reoccur.
6. **Evaluation.** The ability to judge the quality of an outcome or the merit of an idea. Example: the engineer performs an independent review of a hazard analysis from another project. He identifies systemic problems and missing risk scenarioes.

How can this information be applied to managing an effective safety program? Consider the following examples:

1. **Assigning a design manager.** Professional educators assert that unless an individual gets to the Analysis level he or she is unlikely to attempt real-life application of what has been learned. Overall design responsibility should therefore only be entrusted to engineers with demonstrated Analysis level skills.
2. **Setting up a safety program.** Establishing a safety management program requires the skill of Synthesis.
3. **Conducting an audit.** An effective audit of a safety program requires Evaluation skills.

2.6.3 Affective Domain Learning Objectives

Affective learning concerns the more emotional and spiritual aspects of gaining self-confidence, taking on responsibility, giving and receiving respect, exhibiting dependability and defending strongly held beliefs. The affective domain is structured as follows:

1. **Receiving.** The inclination to pay attention and ask questions. Example: the engineer sits erect and makes eye contact with the instructor in the hazard analysis training course. Questions are asked if the material is not clear.
2. **Responding.** Active participation in learning. Example: the engineer completes assignments and participates in discussions on common railway signalling hazards.
3. **Valuing.** The perception that the training material is worthy of consideration and action. Example: on completing a functional safety engineering training course the engineer prepares a management proposal recommending that a hazard analysis be performed on a target system early in its development life cycle as per IEC 61508.
4. **Organisation.** Integrating different values, resolving conflicts among them and building an internally consistent value system. Example: the engineer determines that, while full compliance with EN 50128 at SIL 2 might be a good thing for the smoke extraction system, a SIL determination exercise might reduce the overall development cost without impacting safety. His rationale is that SIL 2 development requirements are applicable to only the small subset of system components that are safety-related.
5. **Characterization.** Consistent and predictable behaviour in line with a deeply embedded value system. Example: the senior systems engineer informs the company's chief executive in a team meeting that his decision to shut down the safety requirement validation program has jeopardised the safety integrity of a new weapons system, placing pilots' lives at risk. He suspects that his outburst will have career limiting consequences but he can't help himself. Commitment to safety is in his DNA.

What does this mean in terms of the ability of an individual to function effectively as a safety-critical systems engineer? My view is that the Organisation level is a minimum requirement for a person's normal thought processes to include hazard awareness. For example, I had to have at least that level to spend a few minutes reflecting on the fire escape hatch in my friend's window. An individual who is at the Receiving level might listen politely to my tirade on what should be done, but secretly think I should get a life.

Most importantly, systems assurance managers (whose job is to champion the safety engineering process) must be at the Characterization level.

2.6.4 Learning from Experience

Legend has it that circa 450 BC Confucius uttered the following dictum:

> *Tell me, and I will forget. Show me, and I may remember. Involve me, and I will understand.*

Kolb took these Confucian sentiments several steps further with The Kolb Learning Cycle. Kolb modelled learning as a continuous cycle with four classes of activity. In the cycle, immediate experience creates a need for learning, which transfers to reflective observation of the experience, which is followed by the introduction of concepts to integrate the immediate experience into what is known. After integration, testing is induced and, because this action results in new experiences, the cycle repeats. The following is a real-world example of the cycle applied to organisational learning:

Immediate Experience. The subject has an emotional or behavioural experience either by accident or on purpose.

Example:

The Metropolitan Subway Authority in the South Korean city of Daegu experienced a subway fire. An arsonist set fire to a train stopped at the Joongang-ro station. The fire then spread to a second train which had entered the station from the opposite direction. Approximately 200 people were killed.

Reflective Observation. The subject takes stock of the experience in terms of any significance it might have and reflects on what has been learned. Significance maybe accepted or rejected.

Example:

The Daegu Metropolitan Subway Authority (DMSA) determined that corrective action was required to prevent a recurrence of such an incident. Causal analysis revealed that the following actions and conditions compounded the problem:

1. Subway officials allowed the second train to enter the station when they knew that the first one was on fire.
2. Power to the station was cut disabling the smoke extraction system.
3. The driver of the second train fled, leaving the 79 passengers locked inside the train. They subsequently died.
4. There was no emergency lighting in the station. Passengers became disoriented and died of asphyxiation while searching for exits.

Abstract Conceptualisation. The subject develops structures or explanations for the way things work. Theories and rules are developed that explain chains of cause and affect.

Example:

Policy decisions taken by the DMSA as a result of the Daegu incident are not well publicised, however an independent analysis conducted by the Taiwan High Speed Rail Corporation (THSRC) led to an internal policy decision that an operator shall not be capable of disabling the operation of a smoke extraction fan.

Active Experimentation. The subject tests structures and explanations against the real world. Predictions are verified against experience.

Example:

The THSRC changed its safety-related requirements for underground smoke extraction control systems and will monitor the effectiveness of this measure.

In the context of safety engineering, Kolb is telling us that regardless of how much learning material is handed to an engineer, progression to higher levels of insight in both the Affective and Cognitive domains depends on frequent practice and intellectual focus on the subject of building safe systems.

2.6.5 Safety Engineering Curricula

What are the elements of a well rounded safety-critical systems engineering (SCSE) education, and what training disciplines should be applied to guarantee an engineer's evolution in both the Cognitive and Affective domains? In my search for answers I recently came upon a vascular surgeon who had done a comparison of surgical and flight training. His conclusion was that pilots are probably better trained due to the extensive use of flight simulators. The pilot's ability to apply knowledge can be thoroughly tested in best and worst case scenarios before he takes responsibility for people's lives. In contrast the surgeon's training in worst case scenarioes happens on the job.

Pilot training techniques could well be applied to the systems engineering education. Although many of the pilot's skills lie in the Psychomotor domain, there is one aspect that is directly relevant to the SCSE profession. That is, in executing critical procedures, such as landing an aircraft, a pilot cannot make mistakes.

Intensive training targeting a no mistakes outcome would eliminate many of the systemic problems that plague the systems engineering profession. For example, it is well known that defects injected into complex software and electronics systems can be extremely hard to find. In the management context, wholesale abdication of safety responsibility by unenlightened management can destroy safety integrity with one blow. While audits, reviews and testing play an important role, the baseline competence of the people doing the work is the best defence against system failure. Imagine the outcome if a systems engineer took the same care with each development procedure as a pilot does when landing a jumbo with 300 passengers on board.

The long road to the command seat of a jumbo jet is documented in Appendix A. To summarise, pilot training is a mixture of book work and practical application in simulated and real aircraft, with and without passengers. A pilot's training and operational life is characterised by constant surveillance of competence. The surveillance never ends. The skills of working captains are regularly checked in the cockpit. Further, the captain's ability to recover from an error or deal with an external threat is rigorously examined in simulator sessions.

It's almost embarrassing to compare the systems engineering education with that of the pilot training discipline. Many of our people lack a professional education or are inducted from professions unrelated to systems engineering. Further, the output of the average systems engineer is subjected to zero or only cursory review and testing. There is no culture of, "gee, if I get this wrong I could kill someone". We are, by and large, bookish types who sit at desks and play with our abstractions, far removed from the real world that uses our products. Many of us would be offended if someone kicked down the door and demanded to do a line by line inspection of our documentation and code.

Hazard 2

Lack of formal safety-related system development training injects systemic defects into software.

Risk: poor design and careless implementation creates high defect densities in safety-related software. Defects go undetected in testing, causing failure of safety-related systems.

Risk reduction strategy: introduce safety-related training disciplines and conduct regular reviews of competence. Essential knowledge areas are as follows:

1. **Manage a safety-critical project.** Plan, staff, direct and control all life cycle activities associated with a safety-related project (refer to IEC 61508).
2. **Evaluate a safety program.** Confirm the existence of an operational safety management system in a development organisation and evaluate its effectiveness.
3. **Identify hazards.** Identify hazardous situations that could lead to an accident.
4. **Analyse incidents.** Perform causal analysis of safety incidents using modelling techniques such as fault trees.
5. **Evaluate risks.** Evaluate the possible negative outcomes of hazards and compute the probability of occurrence. Determine if perceived risks are acceptable to the organisation.
6. **Devise risk reduction strategies.** Identify system requirements, design solutions and manual procedures to reduce risk. Justify risk reduction strategies through quantitative or qualitative means. Determine required safety integrity levels.
7. **Document safety requirements.** Develop unambiguous, complete, correct, consistent and testable statements of safety requirements.
8. **Construct safety-related systems.** Design and build safety-related systems in compliance with safety requirements, using semi formal models such as state engines and Petri nets.

9. **Analyse design reliability.** Determine that a safety-related system will meet its required reliability goals using techniques such failure modes effects and criticality analysis.
10. **Procure safety-related systems.** Plan, solicit, select and administer the purchase of safety-related systems and services.
11. **Validate safety-related systems.** Validate safety-related systems against safety requirements.
12. **Justify the safety management approach.** Develop safety cases that present clear, comprehensive and defensible arguments that safety-related systems, as delivered, will be acceptably safe throughout their operational life.

SCSE training must be on-going, featuring regular practice and evaluation. Without repetition, an engineer will not reach the Characterization level of the Affective domain, where delivering a safe system becomes a personal goal rather than an organisational requirement. New recruits can also benefit from mentoring programs where experienced engineers accelerate personal development by flowing down practical knowledge and attitudes that can't be found in a classroom.

2.7 The Personal Safety Culture

If absorbing and applying the information listed in section 2.6.5 takes care of the Cognitive domain, what factors drive evolution to higher levels of insight in the Affective domain? Answers might be found in a comparison of other professions that deal with life critical matters.

James Reason, a psychology professor from the University of Manchester, has made a study of medical and aviation professionals. He compares their attitudes as follows:

Medical

- We've been trained for 14 odd years and we're perfect … infallible
- We feel shame in our errors
- We don't confess our errors.

Aviation

- We screw up, we're fallible
- We'll assume we're going to make errors so we're afraid and wary
- We value the ability to correct and compensate for errors
- We actively look for threats
- We'll report incidents because we can learn from our mistakes.

The systems engineering profession cannot be characterised by a single value system. Attitudes tend to be a function of experience, work environment and application domain. Immature systems engineers start out with a medico style attitude. They are fearless in the face of risk and supremely confident that technology will solve all. Training in risk assessment and management together with the experience of failure will move them to a healthier, more aviation oriented world view.

The SCSE education should be strong in both the Cognitive and Affective domains. A solid background in the knowledge areas identified in section 2.6.5 is a necessary but insufficient condition for safety risk reduction. Pure knowledge may qualify and engineer to recognise a hazard but will not guarantee that he will speak up and take action.

What events or conditions trigger transitions to higher levels of insight? I can tell you what influenced me with the following vignettes:

- **Immersion in a safety culture.** Ten years with Dow, surrounded by managers and peers with a strong commitment to safety imbues me with a safety-aware value system through social pressure.
- **High frequency drills.** Constant practice in safety incident analysis and hazard identification forces me to regularly focus on safety and ultimately value safe work practices.
- **Work environment.** Working at a desk with a 15 cm thick reinforced concrete blast wall separating me from the reactor area constantly reminds me of the ever-presence of unsafe acts.
- **Experience of failure.** The bloody face of a plant operator freshly sprayed with concentrated caustic soda; working with an emotionally disturbed man who undersized a pressure relief system and caused the death of an operator; having to explain to my boss that a chemical reactor had gone out of control because I allowed an inexperienced programmer to load a new algorithm unsupervised … reminds me of the consequences of unsafe acts.
- **Reward for safety performance.** Being told in a job performance review that my active participation in the company's safety programs impacts my next salary increment refocuses my efforts on safety.

Given all this, am I a perfect specimen of safety culture Characterization?

No.

When large amounts of money are involved, Machiavelli comes to me and advises that I should act in my own interests. It's a problem. One that can only be solved by socialising with others in a safety-aware organisation.

3 The Organisation

Concerning the use of systems engineering militia as opposed to mercenaries.

Machiavelli took a jaundiced view of the motivation of the mercenary. In *The Prince* he wrote:

> *For mercenaries are disunited, thirsty for power, undisciplined and disloyal; they are brave among their friends and cowards before the enemy; they*

> *have no fear of god, they do not keep faith with their fellow men; they avoid defeat just so long as they avoid battle; in peacetime you are despoiled by them, and in wartime by the enemy. The reason for all this is that there is no loyalty or inducement to keep them on the field apart from the little they are paid, and this is not enough to make them want to die for you. They are only too ready to serve in your army when you are not at war; but when war comes they either desert or disperse.*

Machiavelli's risk reduction strategy was to form a Florentine militia which proved to be highly effective in wars against minor enemies such as the town of Pisa.

Elements of Machiavelli's views are relevant to the construction of safety-critical systems. Should critical systems be built by contracting organisations or should they be constructed by the end user?

3.1 Employing Mercenaries

One could draw an analogy between the Florentine militia and the internal systems engineering groups that build safety-critical control systems for companies such as Dow Chemical. Like the militia they live on the battle field and are defending their homes. In contrast the systems engineering contractors (SECs) that railway authorities employ to install signalling and station smoke extraction systems could be compared to the Swiss mercenaries engaged in the defence of Florence. Like mercenaries SECs provide service for a fee, but, taking the analogy further, will they "die for you" when safety conflicts with profit?

At this point the Machiavellian view of life becomes transparently useful. We must view the world as it is rather than as it should be. Should we ask him to perform a safety risk analysis, Machiavelli would view all organisations as self-aware organisms that can be trusted, with 100% probability, to act in their own interests. He would lecture us that the first instinct of all self-aware organisms is survival. For the SEC the first and only threat to survival is financial failure due to under quoting or over engineering a development project, or both. This class of organisation will therefore deploy itself to minimise cost and maximize profit. Conversely, a company that must live with its inventions and has the capability to despoil the environment and destroy life will have safety as its first priority. This is so because to ignore safety is to expose the company to massive financial loss. Union Carbide is a case in point. It never recovered from Bhopal. In 2001 it became the subject of a takeover by the Dow Chemical Company.

3.2 Organisational Safety Culture

I have personally experienced both the mercenary and the militia environments. I can report that they spawn quite different cultures. Engineers brought up in the culture of the mercenary are constantly rewarded for cost minimisation. Engineers whose formative years are served in the militia are rewarded for hazard identification and safety risk reduction. Militia are also accustomed to relentless capital expenditure on safety improvement.

These two quite different environments breed quite different attitudes. For example, working for a chemical processing company such as Dow is often a lifestyle choice. Exciting careers and stable employment, the opportunity to do real engineering in capital intensive operations, often mean these companies are staffed with long-term employees with heavily embedded safety-related value systems. Over 30 years it can even find its way into your DNA. This is the optimum environment for developing the safety awareness alluded to earlier. In contrast, the SEC runs a high risk business with financial peaks and troughs and very little momentum to sustain long-term employment. Employee turnover is high and the ability to build a culture other than one of cost minimisation is therefore limited.

Tagging SECs as mercenaries is unfair however. Are they evil empires staffed by unscrupulous people? Clearly not. I have had the pleasure of working with many of them and can confirm that they are staffed with committed people trying to do the right thing, often providing control system features and engineering services that are technically not required by the letter of the contract. The SEC provides an essential service to organisations whose economics do not justify maintaining an in-house development capability. For example, railway authorities do not experience sufficient churn in system upgrades and new projects to justify home grown development groups. The important issue therefore becomes the mode in which the city state employs the mercenary and how that contractual relationship can be structured to preserve safety.

Hazard 3

An SEC building a safety-related system is placed in a position where it is losing money.

Risk: in a bid to survive, costs are cut by scaling back the safety engineering program, causing failure of a safety-related system.

In a serious cash crisis, safety engineering can be viewed as a nonessential activity and become a target for cost saving. A common strategy is to devolve responsibility to development teams where everyone is responsible but, by definition, no one is responsible. In my experience, instances of blatant non-compliance with the conditions of a contract are rare. However, substantial savings can be gained by militant clause by clause compliance with no leeway given for any omissions by the customer. The net result is that the SEC does not inject the same energy into the safety engineering effort as would be the case with an in-house development shop.

The probability that a cost reduction program will be instituted in a loss situation is 100%. The severity of the outcome must be evaluated on a case by case basis.

Risk reduction strategy: the customer must provide the safety culture. The customer must manage the contract in a proactive manner to ensure it does not have a contractor building a safety-critical system in a loss situation.

Customers must understand how strong survival instincts are in SECs. The senior executives driving these companies make their careers on profit performance, their antennae are finely tuned to financial risk and they will take action to reduce costs. Further, customers must take the Machiavellian view that this situation is not an indictment of the morals of the SEC. It merely represents the natural order of things and is therefore as predictable as the sunrise. It will never change. It must therefore be managed with a risk reduction strategy focused on formal conditions of contract supported by references to international standards for best practice such as IEC 61508. The customer should also have high visibility of work in progress and a productive working relationship with the SEC, a subject that I will now explore in detail.

4 The Contract

Concerning how the city state should organise its militia and its mercenaries.

My experience of the Hong Kong Mass Transit Railway and the Taiwan High Speed Railway projects has convinced me that effective personal and contractual relationships between customers and SECs has a major impact on the quality of the safety engineering in a contracted development. The quality drivers are as follows:

4.1 Unambiguous Responsibility for Safety

If one day you find yourself sitting in a railway carriage travelling at 300km per hour on a viaduct 20m from the ground in earthquake affected countryside, you could be excused for holding the railway authority responsible for your safety. Thinking in Machiavellian terms, the rail authority becomes the state. The state's primary duty then becomes the management of safety, its disciplines and outcomes, and most importantly, acceptance of final responsibility for safety.

What does responsibility for safety actually mean in terms of actions? If critical actions are not taken does this constitute a hazard? I assert that the following issues if not dealt with effectively can lead to hazardous events:

1. **Building a safety culture.** Concerning the extent to which the state should take responsibility for establishing and maintaining a safety culture in its own and SEC organisations.

2. **Evaluating capability maturity.** Concerning the visibility the state should acquire of the ability of an SEC to deliver a safe system.

3. **Taking the low bid.** Concerning the influence price should have on the selection of an SEC to build a safety-related system.

4. **Identifying all hazards.** Concerning the elements of the hazard analysis that must be performed by the state and those elements that can be delegated to the SEC.

5. **Complying with standards.** Concerning the extent to which the SEC should be required to comply with standards for best practice.

4.2 Building a Safety Culture

As discussed previously, a culture of safety awareness is developed by:

1. **Leadership.** Being forthright and unambiguous in communicating who is ultimately responsible for safety and what the individual's safety-related responsibilities are.

2. **Engagement.** Requiring all the members of a community, be they militia or mercenary, to consider safety issues and to formulate actions for safety improvement on a regular basis.

3. **Reward and punishment.** Rewarding good safety performance and punishing poor safety performance.

This is a manageable task in an in-house project. It is extremely difficult in the context of a major infrastructure project such as the development of a new rail network. These projects feature a diversity of contractors with a variety of safety-related attitudes that range from total ignorance to grudging partial compliance.

Sample hazards that emerge from these projects are:

Hazard 4

Abdication of leadership through SONO. The state does not show leadership in safety awareness. Quite the contrary, the state insists that the responsibility for safety is with the SEC and reinforces that assertion by refusing to formally approve progressive design submissions. Instead, the concept of "Statement of no Objection (SONO)" replaces approval. Not being a lawyer I have only a vague perception of the ramifications of SONO. My understanding is that it means, "we don't disagree but neither do we agree. In any event the responsibility is with you as at some later date we may choose to disagree."

Hazard 5

Lack of surveillance reduces safety engagement. A lack of regular audits and reviews encourages the SEC to pursue other priorities, thus neglecting the safety program. Contract engineers do not get the requisite time to engage in safety-related thought and action and never do develop effective safety awareness.

Hazard 6

Rewarding non-compliance devalues safety. Schedule pressure causes the state to relax safety-related conditions of contract. This often takes the form of allowing an SEC to deliver safety submissions after installation which, in turn, encourages the SEC to submit cosmetic documents or attempt to engineer safety into a system after delivery, a well recognized bad practice.

Risk: the SEC, left to its own devices, is likely to apply less energy to pursuing its safety management program, exposing it to scale back or shutdown in the face of schedule and budget pressure. Worst of all, the people working in the projects do not get the safety indoctrination required to produce the commitment to a safety program.

Risk reduction strategy: the state must send its zealous militia to live among the mercenaries, develop clear visibility of their safety engineering execution and imbue in them the culture of safety. This is achieved by uncompromising enforcement of the safety clauses in the contract through regular process audits and thorough review of submissions.

4.3 Evaluating Capability Maturity

Complying with the safety provisions of modern systems engineering standards such as IEC 61508 and EN 50128 requires substantial maturity in an SEC. The contractor requires skilled people working in well oiled procedural frameworks. For example, compliance with EN 50128 at safety integrity level two (SIL 2) requires fully operational project management, configuration management, quality management, verification and validation and systems assurance processes - together with the application of semi formal methods in design. This equates to at least a Capability Maturity Model (CMM) level of three. The state therefore needs to proceed with care when selecting a short list of bidders. My experience is that the state is fully aware of the need for competent SECs but tends to be overawed by size and international reputation. It pays little attention to the skills of the actual cast of characters that the SEC plans to deploy on the project. The reality is that multinationals tend to be highly compartmentalised across national boundaries and within their various business streams. They are a collection of autonomous business units responsible for their own profit performance. The net result is that although the multinational may have the skilled resources required to execute a contract, they will not be deployed across internal organisational boundaries because each business unit has its own priorities and the costs are prohibitive due to high internal charge out rates.

Hazard 7

Low SEC capability maturity compromises safety. The state employs an SEC that does not have the capability to comply with the safety-related clauses of the contract. Processes are not in place and people are not trained. The safety life cycle activities required by standards such as EN 50128 are not performed.

Risk: the state either relaxes the conditions of contract or terminates the contract and seeks another supplier. In both situations safety can be compromised. Once a contract is in place the act of cancellation with its legal ramifications is viewed by most states as an absolute last resort. It becomes more difficult as the project progresses and site works have been performed. Delays associated with awarding another contract, together with the ramp up time required by a new SEC inevitably delay the entire project. This can expose the state to substantial financial penalties. For this reason, in my experience, the state is more likely to sweep safety under the carpet and put up with a bad situation. If the state does take the step of replacing the SEC the unfortunate successor comes under massive schedule pressure which in turn is an invitation to cut back on perceived “non essential” activities such as safety. The integrity of safety functions delivered in either case is therefore questionable.

Risk reduction strategy: the state conducts a capability audit on all short listed SECs to verify their ability to perform and takes this step with extreme vigour **prior** to contract award.

4.4 Taking the Low Bid

Sam Walton founded the world’s biggest retailer Wal-Mart on the credo “stack it high and sell it cheap”. Everyone loves a bargain, even the state finds it difficult to resist a good price. Competitive pricing is a critical success factor in any business but in the case of a safety-related system “silly” pricing can kill. The state must therefore be diligent and look under the cover before loading the shopping cart. In safety-related work a low bid is a sure indicator of one of two situations:

1. The bidder does not understand the requirements of the contract, specifically the engineering effort required to comply with an EN 50128 or IEC 61508 style standard.
2. The bidder is out of work and is buying a contract to keep its shop running.

Safety-critical systems engineering is expensive. It employs highly trained people and systems engineering processes that are costly to implement. For example, the act of maintaining full traceability from requirements through to delivered code introduces substantial costs into a project.

There are two common hazards which flow from accepting a bargain price:

Hazard 8

Safety life cycle activities are not funded in the contract. The state accepts a low bid which is transparently inadequate to cover the cost of safety systems engineering.

Risk: the state employs an incompetent SEC or a SEC who may be competent but is focused on cutting costs to the exclusion of delivering a safe system. There is a 100% probability that inadequate project funds will produce an unsafe system.

Risk reduction strategy: the state performs a detailed cost inspection of bids. The most effective process I have yet seen is the issuing of a common detailed work break down structure to all bidders to allow for easy cost inspection and bid comparison.

Hazard 9

Responsibility for awarding safety-related contracts is delegated to incapable organisations. The practice of delegating the contract award task to other organisations such as civil construction contractors is a hazard to be avoided.

Risk: civil construction contractors award contracts to incapable organisations. Construction companies excel in designing structures and pouring concrete, they have no knowledge of the state of the art in safety systems engineering and therefore no capability to recognize a capable bidder. They can however recognize a low price and rejoice in the saving.

Risk management strategy: if the state is to be responsible for safety it must take responsibility for awarding and administering safety-related contracts.

I note that a common risk management strategy is to hire only multinational companies with substantial financial bulk. The logic is that, in the event of a funding shortfall, a safe system will be delivered in the name of corporate pride and regardless of the loss. This logic is flawed as the state will most likely be dealing with an autonomous business unit within a corporation. A business unit that is a self-aware organism with a will to survive and a plethora of stop-loss strategies (refer section 3.1).

4.5 Identifying All Hazards

The hazard analysis forms the core of a safety program. No amount of systems engineering will protect the end user from the harm that might flow from an unidentified hazard. Capturing and dealing with all reasonably predictable hazards at both project commencement and during project execution is therefore critical to the success of a safety program. Dysfunctional contractual relationships between the state and the SEC inject a disconnect in the hazard analysis process causing hazards to fall through the cracks. This disconnect becomes a hazard in itself. The following sub-sections identify hazardous situations I've personally witnessed:

4.5.1 To not Know What is not Known

In the case of a railway project, a system wide Preliminary Hazard Analysis (PHA) is performed by the railway authority. The required safety integrity level of various subsystems is then determined and individual contractors are tasked with delivering compliant products.

The SEC is responsible for identifying elements of the PHA that relate to its target system. The target system might mitigate the effects of a hazard or, should it not function correctly, create the hazard. For example, the mission of a smoke extraction system is to remove smoke from an underground station or tunnel given that a fire has occurred. It therefore mitigates the effect of smoke on passengers and staff. Once the relevant subset of hazards has been identified the contractor must design a safety-related system that will respond reliably to the hazardous event. The degree of required reliability is set by the SIL that is usually mandated by the railway authority.

Hazard analysis does not cease at PHA. The contractor is commonly required to maintain a hazard log throughout the project. The function of a hazard log is to document hazards identified subsequent to the PHA. Recognition of a new hazard may trigger the discovery of new safety requirements and the addition of additional safety features to the system under construction. But what if the hazard identifier can't identify hazards?

Hazard 10

A contractor with no experience in the application domain is tasked with hazard identification. For example, a control systems contractor is tasked with identifying operational hazards in a rail network.

Risk: hazards that would normally be identified by an experienced person go undetected. Safety-related systems are designed to deal with an inadequate subset of real life hazards.

Risk reduction strategy: the customer takes responsibility for ongoing hazard identification with in-house staff or consultants knowledgeable in the application domain.

4.5.2 The SIL Determination Game

The SIL associated with various system components is often negotiable. If it can be proven that the failure of a system component cannot contribute to a hazard or is not required to mitigate the effects of a hazard, it can be downgraded to SIL 0. This substantially reduces the cost of development to the contractor. Contractors therefore pursue SIL negotiation with extreme vigour.

Vigorous SIL negotiation is also fuelled by the reality that all control systems vendors have product lines of varying vintage. Some may be ten to fifteen years old. Justifying a SIL level greater than zero for any legacy software is extremely difficult. One common approach is the "proven-in-use" argument. The vendor points at multiple installations operating world wide with thousands of trouble free operational hours. This argument looks good on the surface but does not stand up to close scrutiny. All software products are living organisms that undergo constant change. A multinational control systems company may have a system installed all over the world but each installation has its own custom modifications and version deltas. In the software business no one has a standard product that remains unchanged for more than a few days. It is therefore impossible to argue that installation B will be as reliable as installation A, given that the introduction of one defective line of code in a software product can destroy its integrity. The only solution for the contractor therefore, is to argue the product's SIL level down to zero. Dealing with this unfortunate business reality has a Machiavellian side effect. How can one expect a contractor to identify a hazard that would require a SIL level greater than zero for legacy software that, by virtue of its history, cannot comply?

Hazard 11

Commercial conflict of interest causes a contractor to ignore or downgrade the importance of a hazard.

Risk: hazards are ignored or risk reduction delegated to complex manual procedures (see section 4.5.3). There is a high probability that a commercial conflict of interest will arise if responsibility for hazard analysis is over delegated to a contractor in a fixed price project.

Risk reduction strategy: customers must retain responsibility for application domain hazard analysis. Take care when allocating safety functions to legacy software. Ensure that debates over the integrity of legacy software do not mask the need for safety functions.

4.5.3 Operator Superhero Syndrome

The legalistic argument over SIL levels is often protracted. A target system can actually be installed before agreement is finally reached on its component SIL levels. The customer is therefore often put under pressure to accept suboptimal solutions such as safety functions being devolved to excessively complex manual procedures. Hazardous event mitigation then becomes the responsibility of operators. In the minds of the SIL negotiators operators become caped crusaders, superheroes capable of great feats of problem solving under high stress emergency conditions.

Hazard 12

Lack of automation in a safety-related system requires operators to perform complex manual procedures to avoid accidents.

Risk: operators are incapable of following complex procedures in an emergency. The safety-related system fails due to operational mistakes or inaction. The probability that operators will not respond correctly to a once in a lifetime emergency if a complex procedure is required is extremely high.

Risk reduction strategy: evaluate the ability of an operator to respond to emergency situations. For example, do not expect a station operator to have the reflexes and situational awareness of a combat pilot. Make manual emergency procedures simple. Where possible automate complex hazard mitigation steps. If complexity cannot be avoided, conduct regular training and retraining.

I offer the following legend in support of this strategy:

> *One day a very very senior manager of the Dow Chemical Company walked into the control room of an ethylene production plant. He pointed to a pipe rack in the production area and asked an operator, "Tell me, what would you do if the flange on that ethylene line cracked and ethylene poured all over the deck?"*
>
> *"Well." said the operator. "Unless there is a shut off valve in the car park. Nothing!"*

4.6 Complying with Standards

In his epic Ulysses, Lord Tennyson mused:

> *Yet all experience is an arch wherethro'*
> *Gleams that untravell'd world, whose margin fades*
> *For ever and for ever when I move.*

This verse could apply to industry standards which are an ideal we aspire to but seldom reach. For example, EN 50128 represents an aggregate of industry knowledge and experience. A concise statement of best practice in systems engineering. As a systems engineer I can't fault it. There is a dark side however. In a competitive bidding situation the winning bid seldom supports the cost of full compliance. In the best case customer and supplier come to an accommodation on partial, practical, compliance. In the worst case the customer goes into denial insisting that it's the supplier's problem. In response the supplier engages in dysfunctional behaviour such as producing light weight "show" documents. Plans describing processes that bear no resemblance to the methods actually being used. High level requirements specifications that never become design inputs.

Project execution begins. The supplier's wordsmiths write, the customers engineers read. While deep in the supplier's catacombs the real work of building a system proceeds undisturbed and unobserved. Intellectual capital is wasted on shuffling paper when it could be better applied to bullet proofing the systems engineering process. In the context of railway projects requiring SIL 2 compliance I offer the following hazard:

Hazard 13

Full standards compliance is not economical at the prices being paid for SIL 2 railway systems. In response, contractors find ways to affect cosmetic compliance.

Risk: effort expended on cosmetics distracts from the real work of building a safe system. Systemic defects are injected into life cycle activities causing failure of safety-related systems. Developers don't follow proper process because it's perceived as being too expensive. The people with the knowledge and experience to establish and maintain proper process are distracted, producing politically correct documentation that adds no value. In my experience the probability of this occurring is 100%.

Risk reduction strategy: the railway authority ensures that the winning bid has sufficient funds to properly cover compliance costs. Alternatively if the authority is working on a tight budget, consideration is given to requiring compliance with only an appropriate subset of the practices identified in the standard.

An example of tailoring requirements for standards compliance is as follows: the requirement to provide traceability from all documentation into code could be relaxed with the elimination of the design-code link. This would not compromise safety. In a real world project a traceability matrix incorporating design-code links is very quickly rendered useless during testing and installation. As thousands of changes are made, the traceability matrix update task becomes impractical and is typically abandoned.

Other measures include the merging of some document submissions and the elimination of the need for detailed design documents when self documenting graphic programming techniques are used.

It is not unreasonable to tailor out or de-scope some practices, but is there a short list of practices that should never be compromised? If one were to apply the 80/20 rule to standards compliance, what are the 20% of practices that account for 80% of the safety integrity? Please consider the following:

1. A thorough hazard analysis performed by specialists with a deep understanding of the application environment.
2. Developing complete, correct, unambiguous, consistent and testable safety requirements.
3. Applying self checking and highly testable semi formal methods such as state engines to control system design.
4. Module, integration and system testing conducted by an independent test group with full visibility and approval authority over requirements and design documentation (and possessing slightly less compassion than the grim reaper).

5 The Future

Concerning how we princes of engineering could lose our states.

Each day we average citizens entrust our lives to machines either knowingly or unknowingly. We assume that our brakes will work, that aircraft will not fall from the sky and nuclear missiles will not explode in their silos. We make these assumptions and have no fear, and that is as it should be. But to maintain this state of bliss in the general population a small group of us, the safety-critical systems engineers, must learn to be very afraid. We must take the view that to avoid being helpless in the face of nature we must actively look for the circumstances that predictably lead to dangerous failure and take action to avoid their consequences.

In this paper I have identified several hazards that come about through predictable human behaviour. Hazards that will have inevitable consequences if no action is taken. I have identified the human factors hazard as a particularly dangerous phenomenon due to its ability to break through multiple safety protection layers with a weapon as simple and primal as a bad attitude. My personal view of what should be done is encapsulated in the prayer I say as I descend the air bridge into the latest shiny new computer controlled aircraft.

> *Let the people who built this aircraft be well educated in systems engineering practice.*
>
> *Let them care enough about safety to do battle with commercial forces that would denigrate safety engineering as overkill.*
>
> *Let any contractors who worked on this aircraft be properly funded and closely supervised.*
>
> *Let the organisation who built this aircraft have a safety culture with a focus on verifying competence and fostering good attitudes in its people.*

I take my seat, the aircraft taxies, jet engine thrust kicks in and the ground falls away. I imagine Machiavelli sitting up in business class, his crimson gown of office folded about him, his fathomless black eyes gazing at the receding earth. I know what he is thinking. In a time of peace he's thinking about war. As others feast he's thinking about famine. While others gain he's thinking about loss. Especially, how a prince could lose his state and what actions, taken now, could stop it happening.

Niccolo Machiavelli speaks to us from 1513.

> *So these princes of ours, whose power had been established many years, may not blame fortune for their losses. Their own indolence was to blame, because, having never imagined when times were quiet that they could change (and this is a common failing of mankind, never to anticipate a storm when the sea is calm), when adversity came their first thoughts were of flight and not of resistance.*

Should we care to listen we might see that the engineering profession is a state over which we rule. Things remain quiet as long as the engineering standards and practices under which we operate are fit for the systems we build and are followed. But things never remain calm for long. Machiavelli's storms appear on the horizon and roll over us with monotonous regularity. The latest storm has been triggered by the relentless march of large and complex software intensive systems into safety-related applications. Today they fly aircraft high in the jet stream and out into space. Tomorrow they will take control of motor vehicles with drive-by-wire technology. The fundamental change is the transition from the high cost, low volume "gee wiz" interstellar application to the cheap-as-chips, ubiquitous system in everyday use. Their wide scope of application will mean that, more than ever, these systems will need the reliability, availability, maintainability and safety integrity of a steel bar.

The engineering profession rose to meet this challenge in 1998 with the release of standard: IEC 61508 *Functional safety of electrical/electronic/ programmable electronic safety-related systems.* This standard provides a framework under which we can build and operate safe systems. It falls to we engineers to put it into practice. This can be achieved by the following actions:

1. Training and certifying engineers in safety-related systems engineering principles and practice
2. Building personal commitment to safety through high frequency application of these practices
3. Developing a safety culture within the organisation so it may be trusted to build a "trusted system"
4. Structuring contracts to ensure that safety integrity is not corrupted by commercial conflict of interest
5. Ensuring safety-related product development is properly funded
6. Actively taking responsibility for safety.

Only by these actions we will ensure that the safety integrity of our systems is not "governed by fortune" (or luck), but by good management. Only at this point will we have fully embraced Niccolo's parting advice.

> *The only sound, sure, and enduring methods of defence are those based on your own actions and prowess.*

6 References

Bloom, Engelhart, Furst, Hill, Krathwohl (1956): *Taxonomy Of Educational Objectives: Handbook 1, The Cognitive Domain*

Bloom, Masia, Krathwohl (1964): *The Taxonomy Of Educational Objectives: Handbook II, The Affective Domain*

CENELEC (2001): *Railway Applications - Software for Railway Control and Protection Systems*. EN50128

International Electrotechnical Commission (1998): *Functional safety of electrical/electronic/ programmable electronic safety-related systems*. IEC61508

Kolb, D. (1984): *Experiential Learning: Experience as the source of learning and development.* See also: http://www.learningfromexperience.com/

Lapierre, D., Moro J. (2002) *Five Past Midnight in Bhopal*, Warner Books

Machiavelli, N. (1961): *The Prince*, Penguin. Available at: http://www.ilt.columbia.edu/publications/machiavelli.html

Reason, J. (2005): *The Health Report: 16 May 2005 - Absent-mindedness/Risk Management*, ABC Radio National. Available at: http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s1366797.htm

Simpson, J. (1998): *Touching the Void*, HarperCollins

Software Engineering Institute (2002): *Capability Maturity Model Integration for Software Engineering (CMMI)*, CMU/SEI-2002-TR-028

7 Appendix A. Pilot Training

Criteria/Rank	**Training Requirements**
Entry Requirements	**Cadets** • Flight hours: no flight experience required, 12 months basic flight training provided • Education: year 12 science and mathematics required; candidates usually degree qualified; candidates who display good interpersonal skills and personal maturity will be accepted with year 12 A levels • Attitude: acceptable level of social and personal maturity
	Direct Entry • Flight hours: 3000 hours • Experience: First Officer, Second Officer or ex Air Force • Testing: comprehensive interviews, technical and coordination testing and a flight simulator test.
Second Officer	**Initial Training** • Three months conversion training on target aircraft • One week of orientation for airline operations • Three weeks of ground school • 10 sessions in a simulator • Line (in service) training, 10 sectors[2] including a line check[1].
	Recurrent Training • Six, four hour flight simulator sessions per year including two instrument ratings and emergency procedure checks • One aircraft line check[1].
Selection criteria for upgrade to First Officer	• Three years as a Second Officer functioning as a relief pilot (able only to sit in a control seat in the cruise) • 100 tests to allow upgrade to First Officer.
First Officer (prior to flying with passengers)	**Initial Training** • Three days general airline operation training.

Criteria/Rank	Training Requirements
	• Three weeks technical training • 14 sessions of simulator training including, aircraft operation, emergencies, non technical skill training in crew resource, threat/error management • 60 hours line check[1] • 15-20 landings in an empty aircraft with a Base Training Captain to consistent competency
First Officer (flying with passengers)	• First four sectors[2] with a Base Training Captain to ensure landing skills are embedded. • six sectors with a Check Captain to consolidate. If all is well the third safety pilot is removed. • Up to 30 sectors with Training Captain to complete the syllabus. • A line check[1] is then done and the candidate becomes a Junior First Officer for six months. • Ex cadets get a further two to four sectors a month with a Training Captain. A final line check[1] will confirm them to full First Officer.
	Recurrent Training and Testing Five simulator sessions per year as follows: • Two practice sessions featuring aircraft handling with engine failures, selected emergencies and other topical handling problems. These sessions are performed on a three year cycle. • Two tests of aircraft handling, instrument rating, emergencies etc. • Optionally one session devoted to real time problem solving as experienced on a normal passenger flight. This is referred to as Line Orientated Flying Training (LOFT). This is conducted as a pilot approaches command.
Relief Captain	• Responsibility: in charge during a long haul flight when the Captain is resting. • Skills: a higher level of knowledge, skill and attitude expected. • Testing: required to pass an assessment board, technical tests and line check[1].
Captain	**Initial Training** • Aircraft type conversion training if required as per First Officer conversion. • Three additional simulator sessions as problem solving exercises. These are difficult sessions, run in real time with a First Officer in the other seat. The objective is to train and evaluate the candidate's crew management, prioritisation, problem solving and decision making skills.
	Recurrent Training and Testing As per First Officer (LOFT excluded)

Notes:

[1]line check	The objective of a line check is to verify that the candidate is operating in compliance with company procedures and to check knowledge levels in appropriate areas. A line check is conducted over two to four sectors of normal passenger operation with a Check Captain who is either operating in the co-pilot's seat or observing two candidates from the jump seat. The candidate operates without prompting or interference from the Check Captain unless safety becomes an issue.
[2]sector	One flight, one take-off and landing.

Source: Mr Bill McCarthy, Training Captain, Cathay Pacific Airways.