The University of New South Wales

ELEC4122/GSOE9510

On hazards & risks

A major concern of engineering profession is safety. It is integral to professional practice. Indeed, you will find it embedded within Engineers Australia's *Code of Ethics* (2010):

> *"Practise engineering to foster the health, safety and well-being of the community and the environment."*

Remember that no technology is ever perfect; our knowledge remains incomplete. Consequently, engineers need to be able to make decisions while facing multiple uncertainties. Not the least of these is that we cannot know the future. Things go wrong; accidents happen; and when they do, people might get hurt.

The two fundamental principles of safety are your knowledge and your attitude.
(i) **Know the dangers** (or 'hazards') so that you can take precautions and know how to take them. This may mean you need to do some research; it may mean a lot of research. Military strategy will tell you that you can never know too much about your enemy. Don't be amongst those who don't want to know something, believing (?) "What they don't know can't hurt them." Your knowledge of the hazard allows you to implement suitable features in the system's design and to make suitable administrative arrangements.
(ii) Knowing is insufficient. Whether you choose to implement safety precautions or not follows from **your attitude to safety** and is a demonstration of what you think is important (ethics again – your duty of care'). Safety comes from your wanting to be safe and being concerned for the safety of others. All knowledge of safety is irrelevant if it makes no difference to the designs chosen. Note that 'others' may include people who have no direct involvement in the project but are still affected; note, too, that it is a concern that endures beyond the initial implementation of a system.

In many respects, safety is about good habits, both habits of thought and habits of action. Start them now. Remember that it is more difficult to break a bad habit than start a good one. Remember: *Think first. Act carefully.*

While nobody wants them, **accidents do happen**. Not wanting an accident means actively seeking to **prevent** one. It also means **preparing** for one should it happen. There are several causes for accidents. Typically,

- human error (One could include deliberate sabotage here and count that as an ethical error.);
- human ignorance;
- the physical failure of artefacts (hardware), e.g. metal fatigue; and/or
- random external events.

As an engineer, you have a duty to minimise both the *chance of the system failing and the effects of a failure*, if and when it occurs.

When it comes to fulfilling this responsibility for safety, there are some well-established, useful processes to follow.

Principles of Hazard Management

The following steps outline one established procedure for handling a hazard. Remember that a *hazard* is anything that could compromise any of the stakeholders of a system.

1. *Identify the hazard*.
The hazard is the *causal* agent (e.g. the laser, electricity, sulphuric acid, curiosity of children) of what might go wrong. Until you know what the actual hazard is, no mitigation is possible.

2. *Assess the risk* of the hazard (see below).
This involves two steps: determine the *severity of all possible consequences* and also the respective *likelihood of each of these occurring*. This, in turn, may require research and may end up being both very time-consuming and very uncertain, particularly as some consequences are unknown.

3. *Control the hazard*, to reduce the risk (see below).

4. *Monitor the effectiveness* of the controls.
As with all innovation, there is an element of experimentation about any safety measures so collecting information will be informative.

5. Periodically *review* the management of the hazard.
New information may become available, not least from the experience of operating the system, as in the previous step. New people may be involved or the existing personnel become more competent. You can think of more possibilities.

Hierarchy of Hazard Controls

After any hazard is identified, it can be controlled in the following ways. This is in the **decreasing** order of effectiveness.

1. Try to *eliminate* the hazard.
Clearly the safest option is to remove the hazard completely, for then the associated risk vanishes. However, in most cases a hazard is intrinsic to the activity and so must remain.

2. Seek to *substitute* the hazard with a less dangerous hazard.

3. Re-design the system (*engineering controls*)
   (i) to limit human contact with the hazard,
   (ii) to reduce the possibility of human error (see previous notes), and
   (iii) so that, should the system fail, it will fail with minimal adverse outcomes
   (i.e. provide *safe exits*).
In your re-designs, always consider the whole system, not just particular components. A hazard may only be a hazard because of the context, e.g. being used by students!

4. Introduce relevant procedures (*administrative controls*).
These may include such things as restricting access, having suitable emergency procedures, training people, or simply posting warning signs. (Incidentally, as a professional engineer, you should learn to recognise the safety information provided by signage.)

5. Issue *personal protective equipment* (PPE).
PPE may be clothing or eye-protection, and also items such as insulated tools that protect the user.

Assessing Risks

1. As always, first *identify the context*.
Who is or might be involved? Where will the activity occur? When is it scheduled? The level of risk may depend upon any or all of these.

2. Identify the *hazards* associated with the activity, noting the *control measures* already in place for each of them.

3. Only now identify the *possible adverse consequences*.
Then, for each consequence, estimate the likelihood of it's happening, given the controls that are in place. Sometimes the probability is easy to determine, based on historical events. However, most 'extreme' outcomes are what are known as *very low likelihood events* and their probabilities are, thus, very, very hard to calculate reliably on the basis of the past. Extrapolating into the future assumes continuity with the past and an accident is a form of discontinuity, almost by definition. The risk associated with each hazard follows as the product of the probability of the outcome and its consequence. Within this analysis, a minor but frequent consequence is as big a risk as a catastrophic outcome that is very rare. The *overall risk* is determined by considering all these different outcomes simultaneously.

$$effective\ risk = \sum_j hazard_j\ severity \times hazard_j\ likelihood.$$

It is only illusory to accept risk assessments as 'objective.'

Remember that engineers work with incomplete and evolving information; it is auditing that needs certainties. Any assessment depends on the quality of the data. It is difficult to assign probabilities to an untried innovation; nor can we honestly quantify 'severity,' although aspects of severity (e.g. how many broken bones) can be measured. Again, it is entirely subjective which things are chosen as a measure. Beware! Often a risk assessment uses probabilities estimated at a level to validate what someone wants to do anyway and severities are indexed by an aspect chosen to support that same decision.

Furthermore, a *risk assessment can never determine whether a given risk should be taken*. That is a subjective decision and depends not only on the overall risk, but also on both the possible benefits and who is bearing the risk. From the perspective of ethics, an important question is who makes that decision. Is it the party who benefits from the activity? Or the party who bears the risk? Ideally these should be the same, but rarely are in most non-trivial systems. This shows why the person with the authority to make to choice should *consult* with those affected.

(Note that this discussion about risks is phrased around considerations of safety and a technological system. You can use the same ideas equally well anywhere there is a risk associated with the uncertainty of the future. For examples, financial institutions use an analogous process for managing the risk associated with lending.)

References

Martin & Schinzinger, ch 4; Kletz ch2 & appendix; Perrow, ch 1; AS/NZS4360