

A risk-based approach to supporting the operator role in complex monitoring systems

Kevin Anderson

Hyder Consulting Pty Ltd
16 /31 Queen Street, Melbourne VIC 3000
kevin.anderson@hyderconsulting.com

Abstract

Many facility and infrastructure Central Monitoring Systems have functions that relate to the protection and resilience of critical infrastructure protection and resilience. Issues of concern include terrorist threats. To counter such threats, use is made of defensive layers which include biometrics, smart cards, CCTV and perimeter screening. There is much interest in virtual training and crisis management techniques to train staff to recognise and effectively respond to scenarios and incidents (and, from time to time, the real thing).

The examples given here are hypothetical, but based on experiences with Functional Safety Assessment (FSA) of actual Traffic Control Centres (TCC), Operations Management and Control Systems (OMCS) and Central Management Systems (CMS). It is concluded that a complex control centre remains vulnerable to human error if only one operator is present at the time a critical alarm is raised.

Keywords: SIL, IEC 61508, facilities, infrastructure, monitoring, safety, critical, tunnel.

1 Introduction

Reliability, availability, maintainability and safety (RAMS) techniques are employed in many industries, but only a few have adopted the risk-based approach outlined in the Functional Safety standard IEC 61508. This standard provides a 'due diligence' framework within which to set various methods and techniques.

One concept is to determine the risk of dangerous failure of the equipment-under-control (EUC), the EUC control system and associated human factor issues in terms of frequency and consequence. Then it is necessary to determine the tolerable risk which is to be accepted in a given context based on the current values of society.

The difference between EUC risk and tolerable risk is the necessary risk reduction. This can be partially covered by three means:

- external risk reduction facilities (ERRF), e.g. fire walls, refuges,
- other technology safety-related systems, e.g. deluge system, and
- electrical /electronic /programmable electronic (EE/PE) safety-related systems.

Note: a person can be part of a safety-related system. For example, a safety action may be performed based on information received from a programmable electronic device.

The paper summarises the risk assessments (mostly fire and life safety) that lead to various Safety Integrity Level (SIL) 1 conclusions in complex systems such as road tunnel - plant and traffic control.

The paper then considers the human-machine interface and carries out a task analysis leading to recommendations on operator training and competence in dealing with both accidents and deliberate attacks.

This paper concludes that a complex tunnel control centre remains vulnerable to human error if only one operator is present at the time a critical alarm is raised.

2 Road and Rail Tunnel Emergency Experience

This section lists the mitigations employed to date, based on experience with actual incidents. Typically these have comprised fire extinguishing equipment and warnings to drivers. The extent to which ventilation and extinguishing equipment should be automated is still open to debate.

One such international debate occurred in Marseilles, France in 2003. The following highlights are taken from the 5th International Conference Safety in Road and Rail Tunnels (Tunnel Management International).

Up until the Mont Blanc tunnel fire on 24 March 1999, engineers were confident that their designs were safe. In longitudinally ventilated tunnels with unidirectional traffic the design objective is to prevent smoke from backlayering i.e. to ensure all smoke is driven in one direction.

Bi-directional and congested tunnels are different and users must be protected on both sides of a fire. In longer tunnels, separate air ducts are used to extract smoke,

either continuously (fully transversal) or at intermediate points (semi-transversal).

At Mont Blanc, a semi-transversal ventilation system was normally in operation; the whole tunnel was ventilated by only one ventilation plant at each portal serving ducts under the carriageway.

Sensors were installed to identify fires, as were devices to measure opacity and carbonic oxide level, with video cameras connected to these systems, to raise the alarm at a threshold of 20% opacity.

A key requirement identified by Borchiellini et al (2003) is that when a fire event occurs in a tunnel, two different actions must be carried out as soon as the fire is detected:

- control of smoke propagation, and
- activation and display of danger signals to the drivers in the tunnel and those about to enter the tunnel.

If the users had stopped when and where the traffic lights were turned on, they would have been far from the smoke front and able to reach shelters or wait for the rescue teams.

Other actions identified in relation to human factors include:

- the choice of ventilation system configuration,
- the decision time,
- the observance of traffic light signals and
- the question of how to make users, supervisors and fire detection systems respond as required.

From Henke and Gagliardi (2003), the 2001 Gotthard fire involved a head-on collision of two trucks, ignition of spilled fuel and rapid spreading of the fire. The nearest involved drivers evacuated the zone, warning and urging incoming vehicles to return and go out of the tunnel.

Rescue personnel had difficulty persuading some motorists to leave their cars. Apart from those directly involved in the 23 destroyed vehicles and unable to escape, there were no further consequences.

Regular radio messages are now deployed to educate the public as to correct behaviour in such circumstances. Other measures adopted to inform users about the way to get to a safe place include:

- automation of radio information in four languages,
- lighting and signs every 50m indicating distance and direction to the nearest shelter,
- green and white colours and lighting highlighting shelter entrances,
- information signs and communication packs inside shelters.

The Daegu Metro fire disaster of 18 February 2003 involved loss of many lives and damage to two trains and the station. Issues raised by Burns et al (2003) included:

- station egress design,

- systems 'failing' to unsafe conditions,
- lack of clarity as to staff responses in the event of emergencies,
- lack of coherent consultation processes, and lastly,
- how to deal with malevolent acts?

Ward (2003) discusses the use of communications as a safety device in tunnels. Direct person-person communication in very short tunnels is wryly described as 'shouting'. Communications facilities to enable radio communications to users have a broader range. Public address systems and fixed-point telephones are also germane.

Dual redundant systems with separate fibre optic cables are also an option to maintain availability. For effectiveness, communications must be seamlessly integrated with other tunnel safety systems, such as dynamic road signage, ventilation systems, telephone and broadcast systems and video coverage.

Yae and Mizuno (2003) outline human factors and systems engineering issues for tunnels. Experiments and simulations were conducted in relation to the preservation of the evacuation environment in cases of tunnel fires.

Human factor incidents are classified into four stages:

- information receipt;
- recognition;
- decision-making and
- operation /direction.

They conclude that operations at each stage of the emergency operation should be automated if possible so as to mitigate human factor incidents.

Stroppa and Seebacher (2003) discuss the use of simulation tools to train operators in operation of tunnel ventilation systems in fire mode. Operations staff are not usually ventilation experts and can be overburdened by the demands of manual operation.

Setoyama et al (2003) extol the virtues of automatic water spray operation, notwithstanding European concerns that water can cause explosion in petrol and other chemical substance fires and possibly create hazards for evacuation in the fire and smoke zone. A number of experiments and eight actual cases were cited as evidence that water spray systems are effective.

Sanchez (2003) recounts the US experience as it relates to the New York subway. Ventilation systems are designed to provide a tenable environment long enough to allow passengers to reach a safe haven.

Miclea (2003) covers design challenges and dilemmas facing tunnel ventilation systems in the US for both road and rail. He suggests a risk-based approach to contingency planning.

Nakanishi et al (2003) note that actuation of water spray systems in Japanese tunnels is dependent on operator judgement at the time. A risk assessment approach is presented in the form of an event tree which concludes

that the greatest effect of the water spray system for fire extinguishing in a tunnel is obtained by starting the system 3 min after a fire is detected in a unidirectional tunnel and 10 min after in a bi-directional tunnel.

These times are based on when evacuation is deemed to be completed i.e. the times relate to theoretical evacuation, after which deluge is commenced to protect the tunnel structure.

The Australian perspective (MacDonald and Messenger, 2003) describes the many additional features not necessarily required by the international authority, the World Road Association formerly known as the Permanent International Association of Road Congresses (PIARC). Deluge systems are deployed for early intervention, with the support of Australian fire authorities.

Robinson et al (2003) present a cause-consequence model of a heavy commercial vehicle (HCV) 50 MW fire for a longitudinally ventilated tunnel. This showed that automatic deluge systems provide superior risk reduction for fires in stalled traffic compared to manually activated deluge and emergency longitudinal air handling systems, the usual design for Australian tunnels.

The loss of control point was considered to occur when the smoke /fire overwhelms the usual air handling systems placing remote persons at risk, i.e. at about a 5MW fire. Deluge systems can control such fires.

Otherwise, with stalled traffic and a smoky environment where smoke has to be blown one way or the other, safe evacuation of those people is very, very difficult.

The role of the Operator in deciding whether or not to intervene in response to an alarm is further discussed below:

3 Road Tunnel Case Study

3.1 Issues

Despite the multiple sensor alarms, the Chicago telephone exchange fire at Hinsdale in 1988 was ignored by the Operators. Large areas of the City were left without communications.

There are similar questions regarding road tunnels today, for example, as to whether deluge system activation should be totally automatic with an operator override. Fires are not uncommon and occasionally result in multiple fatalities, as unfortunately occurred recently on 23 March 2007 in the Melbourne CityLink Burnley Tunnel.

The conventional expectation is that the deluge (drencher) sprinkler system will not be actuated until all persons in the tunnel are safely evacuated. The view is that all the combustion gases from the fire remain buoyant and above the heads of any persons in the tunnel. Once the deluge system activates, hot gases will cool and fall placing any persons on the ground at risk.

The size of a fire can be correlated to the number of possible fatalities. The larger the fire, the faster is the

rate of build up and the more urgent the need to complete evacuation before the onset of flashover conditions. Flashover is a period of rapid fire growth, where an enclosed space dangerously bursts into flame, with little chance of persons escaping.

Complex, expensive, hard to model and unpredictable emergency measures invoked after the loss of control point attempting to bring a situation back under control are legally difficult to defend, especially where a sensible pre-loss of control precaution is available.

The automatic activation argument contends that small fires should be the norm and flashover should not occur.

Spurious activation remains a hazard requiring commensurate safety assurance, such as assigning a Safety Integrity level (SIL) pursuant to the Functional Safety standard (AS /IEC 61508:1998-2000).

These questions raise the issue of the risk trade-off between false alarms and real trouble – to ‘cry wolf’ too often results in the alarm not being believed when the threat actually happens.

3.2 Tunnel Systems Dependability Criteria

A typical road tunnel systems specification leaves the onus on the designer to demonstrate Reliability, Availability, Maintainability and Safety (RAMS). This includes dealing with the trade-off between safety (shut-down in face of danger) and availability (maintain operations at all costs)

For example, on various New South Wales road tunnels, 99.995% availability has been specified for the Operations Management and Control Systems (OMCS) to be demonstrated ‘through the conduct of a rigorous failure analysis prior to the finalization of the detailed design using an internationally recognised failure analysis methodology’. The selection of an appropriate standard is discussed in section 3.3 below.

Other relevant requirements included ‘a suitable and robust OMCS computer system ... duplicated for redundancy ... configured for high availability’:

where availability = $MTBF / (MTBF + MTTR)$

where MTBF = Mean Time Between Failures

MTTR = Mean Time To Repair

(MTTR < 3 hrs as specified by Road Authority)

A further requirement is to facilitate the effective management of incidents in the tunnel through the integrated control of all tunnel control, monitoring and communications devices.

3.3 Relevant Standards

There are various relevant RAMS standards such as the BS 5760 series and the EN 50126, EN 50128 and EN 50129 Railway series.

These echo many of the measures and techniques and concepts such as Safety Integrity Level (SIL) first espoused by the Functional Safety standard IEC 61508

(adopted in Australia as AS 61508). The choice of 61508 was to apply the risk-based ‘due diligence’ Part 1 rather than a RAMS standard.

Assurance measures and techniques considered relevant here are:

- Cause Consequence Model Diagrams (CCM)
- Event Tree Analysis (ETA)
- Fault Tree Analysis (FTA)
- Common Cause Failure Analysis (CCF)
- Markov Analysis Models (MA)
- Reliability Block Diagrams (RBD)
- Failure Mode Effects and Criticality Analysis (FMECA)
- Monte-Carlo Simulation

A FTA or FMECA may have sufficed simply to establish the numbers. The specified system availability was not adopted as a basis for determining the required dangerous failure rate.

Rather, from a risk viewpoint, the question was: Is the specification ‘safe’? Safe in this context means freedom from unacceptable risk of harm.

The Society of Automotive Engineers’ (SAE) aeronautical standard ARP 4761 ‘Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment’ provides a cogent worked example of an aircraft Wheel Brake System, progressively applying FTA, RBD and MA to the same mechanical and electrical problem. Nowhere else is the commutability between techniques expressed so cogently.

The cause-consequence model approach was selected here as an elegant combination of FTA (leading up to a critical event) and ETA (as to what consequences escalate).

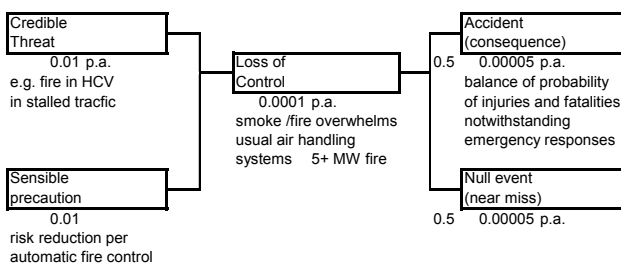


Figure 1 Cause-consequence model

These analysis techniques provide for the detailed quantification, but not the overall risk-based safety argument approach of IEC 61508.

The claim for risk reduction through automatic fire control of 0.01 is consistent with Safety Integrity Level SIL 2 (assumes the fire control system is a low, failure on demand system) which suggests that the fire detection, monitoring and control systems should be separate and independent from the Operations Management Control System (OMCS).

A complete Functional Safety Assessment under IEC 61508 was therefore adopted by the Contractor for the New South Wales road tunnel OMCS.

This was grouped into three Phases:

- Concept & Scope (Part 1 #7.2-3)
- Hazard and Risk Analysis (Part 1 #7.4)
- Requirements Definition and Allocation (Part 1 # 7.5-6)

The following sections apply these Phases for the Road Tunnel example and its human factors.

3.4 Concept & Scope

A typical configuration comprises two separate longitudinally ventilated carriageways with unidirectional traffic. There may be intermediate entry and exit ramps.

Escape doors are provide every 120m and these lead to cross passages, stairs and in some cases blind refuges. These areas are pressurised to prevent smoke ingress. Thus to pass through an escape door is to reach a safe place.

Door open events are detected and monitored by CCTV cameras as are the numerous other systems provided in a modern road tunnel.

The Operations Management and Control System (OMCS) consists of two separate systems; the Traffic Management and Control System (TMCS), and the Plant Management and Control System (PMCS). Each has its own field device I/O and independent backbone and hardware, but the systems use a common interface to the operator.

TMCS includes Closed Circuit Television (CCTV), Traffic Devices, Radio Rebroadcast, Barrier Enforcement Systems and Traffic Authority Interface.

PMCS comprises Tunnel Air Monitoring and interfaces to Heating, Ventilation and Air-conditioning (HVAC) & Egress Pressure, Fire and Emergency Systems, Power System, Ventilation (Jet Fan) System and Hydraulic System.

Whilst independent in the field and at the server level, the two systems TMCS and PMCS share common operator workstations and displays in the Tunnel Control Centre (TCC).

The human factors and in particular those relating to the system users, take account of the shared user interface for both the TMCS and PMCS. The most concern with OMCS is the likelihood that the operator (user) will rely on the information displayed, i.e. the concern is with the veracity of the information, not what the operator would do with it.

There would seem to be some common mode failure issue here. However, the TMCS and PMCS systems are serial – i.e. not redundant.

For example could the PMCS alarms mask more severe TMCS alarms? TMCS is the lead system, certainly more dynamic, if not more severe and the traffic displays,

video wall and CCTV drive most of the operator decision time.

If TMCS, or indeed the TMC, are down, plant can be controlled from a laptop patch into PMCS servers. An emergency setup is provided in one of the switch-rooms for the purpose.

The Fire System has a separate Fire Panel located in the TCC behind the Operator i.e. instantly accessible. A failure on demand approach is taken to this.

For the OMCS, the high demand /continuous mode is appropriate as OMCS is required to monitor hundreds of devices in near real time.

From this, the OMCS availability requirement has been applied to the 'monitor and control' functions and not the individual availability of the hundreds of field devices, that is, the criterion applies to the level of assurance that the operator will be given information that a secure door has been breached or that a routine status poll has failed.

Depending on the level of concern, devices can be scheduled for repair at the next maintenance cycle or sooner if necessary, data from multiple sources including CCTV can be correlated and emergency team(s) can be dispatched.

3.5 Hazard & Risk Analysis

An energy-damage view has been taken of likely sources of hazards: this view considered mechanical /electrical /chemical /fire /explosion /confined spaces /pathological /psychological /human factors /flooding and so on.

For each credible hazard, sensible precautions had to be developed covering matters such as hardware and software failure, power failure, interface /integration failure /accidental human error and deliberate acts /damage.

The key threats arise from the traffic itself and include:

- traffic congestion
- vehicular breakdown
- vehicular accident
- vehicular fire
- prohibited users /trespassers
- civil disturbance /bomb threat /terrorism

The severity of each threat depends on circumstances, particularly whether traffic is free flowing or congested.

Passenger Car /Light Commercial Vehicle represent the base case while the involvement of Buses /Heavy Commercial Vehicles in a breakdown /accident represents an escalation. Dangerous Goods are a major concern and, while usually prohibited, transgressions have been noted.

For each identified threat, the role of OMCS was defined in terms of how important /what level of assurance is required that the Operator will receive a correct and timely message from a field device. These assurance levels were expressed as SIL levels ranging from SIL 0 – not urgent, SIL 1 – some urgency, SIL 2 – urgent.

Fire systems were rated at SIL2 as was CO exposure monitoring.

Examples of SIL 1 included alarms regarding traffic breakdown, management and lane closure, UPS battery condition, jet fan vibration, toxic and flammable chemicals, dangerous goods, confined spaces, security access /monitoring, software, intrusion, emergency communications channels, incident recording and monitoring and flooding.

Functions rated at SIL 0 nevertheless have availability requirements and include alarms regarding mechanical, electrical and ventilation systems, chemical storage, access ways, maintenance facilities, storage and handling, operational, maintenance and emergency guidelines and procedures, facilities and sub-system interfaces,

3.6 Requirements Definition & Allocation

For each particular threat, it is assumed that appropriate sensors are installed and responses planned accordingly.

For example, pre-computed ventilation scenarios can be devised to deal with fires in different zones, so as to prevent backlayering upstream of the fire.

Note: The backlayering phenomenon is the case where the smoke moves against the provided ventilation upstream of the fire causing a dangerous environment to the tunnel users.

Other risk mitigations also involve incident response planning and resourcing, accessibility, management and public education. For a unidirectional longitudinally ventilated road tunnel, these involve:

- monitoring and detection of traffic speed, congestion and accidents
- tunnel message signs, public address, radio rebroadcast and education programs
- automatic deluge devices and smoke extraction (to suppress /extinguish the fire (protecting proximate users) and smoke extraction capable of dealing with a 50 megawatt fire (Heavy Commercial Vehicle fire) with no backlayering (protecting upstream users),.
- provisions for tunnel closure and traffic diversions (assuming free-flowing traffic, allowing downstream users to drive away).
- emergency access and escape (including pressurised cross- passages at regular intervals – such safe havens being pressurised areas @ 120 m intervals).

3.7 Human factors

The role of the operator is vitally important in recognising where circumstances deviate from the plan. For example, in the case of fire, he /she has to consider safety of users, even those distant from that fire (noting some proximate users may be involved in the fire in any case).

The risk mitigation features in 3.6 assume free flowing traffic. Where traffic is congested, reliance has to be placed on the deluge system alone. A concern is that a 30 second delay is available in the otherwise automatic deluge system within which time the operator can use a 'Cancel' function to prevent activation. This function is available presumably to avoid unnecessary water deluge occurrences. But what is a reasonable balance between inconvenience and potential catastrophe?

A false alarm in free-flowing traffic seems no more than akin to driving into a rain storm, while to override a real alarm in congested traffic could have extreme consequences if smoke overwhelms the ventilation system.

Information available to the operator includes flow and occupancy data computed from integrated loop detectors every 120 m, CCTV, fire detection sensors, PABX Phones and receipt of 000 calls via Emergency Services Dispatch Centre from user mobiles.

Thus there are at least four ways in which the visual surveillance, communications and fire detection systems can get the message of the reality of smoke and heat through to the operator. Similarly, multiple means of communication to tunnel users are available to the operator include:

- Tunnel Message Signs (TMS)
- Public Address (PA)
- Radio Re-broadcast (RRB)

Users who do not understand the need to evacuate may remain in their cars for too long. Activation of deluge systems to contain fire size may still result in smoke affecting downstream users.

This analysis was concerned mostly with the hardware and software techniques relevant to Safety Integrity Level 1 (SIL 1) with some calculations as to core redundancy and diversity. The Safety Argument included 'necessary risk reduction' from other Technology (OT) and External Risk Reduction Facilities (ERRF) – the human factors side.

The 99.995% availability criterion is the same as 0.005% unavailability, in scientific notation 5.00 E-5. At 1 hr MTTR as specified, this is the same as MTBF 20,000 hours, a failure rate of 5.00 E-5 per hour.

Unavailability is 1-Availability. From 3.2, this is $1 - \text{MTBF}/(\text{MTBF} + \text{MTTR})$. $\text{MTBF} = 1/\lambda$, where λ is the failure rate. Through substitution and reduction, $\text{Unavailability} = \lambda \text{MTTR}/(1 + \lambda \text{MTTR})$. For small λMTTR , Unavailability approximates to λMTTR . Therefore for a 1hr MTTR (or Mean Down Time), $\text{Unavailability} = \lambda$.

Clause Part 1 #7.5.2.4 of AS 61508 allows where failures of the EUC control systems place a demand on one or more E/E/PE or other technology related systems and/or external risk reduction facilities, and where the intention is NOT (author's emphasis) to designate the EUC control

system as a safety-related system, the following requirements shall apply:

- a) the dangerous failure rate claimed for the EUC control system shall be supported by data acquired through one of the following:
 - actual operating experience of the EUC control system in a similar application,
 - a reliability analysis carried out to a recognised procedure, or
 - an industry database of reliability of generic equipment.
- b) the dangerous failure rate that can be claimed for the EUC control system shall not be lower than 10^{-5} (1.00 E-5) per hour. This equates to tolerance of one dangerous failure per 11.4 yrs. Thus, a claim that failure rates are lower than this has to be supported by a SIL, which is much more than just to do (a) above.

Following consideration of diversity and redundancy at the systems level, compliance to SIL 1 with respect to software requirements provides the strongest safety argument that a number around 1.00 E-5 per hour can be claimed, notwithstanding that failure modes of software are systemic rather than random.

A budget allocation was made that the requirements should be:

- PMCS Hardware	1.00 E-5 per hour
- TMCS Hardware	1.00 E-5 per hour
- Software	1.00 E-5 per hour

This left 2.00E-5 for the Operator External Risk Reduction Facilities (ERRF). Note: This is only so far as the Equipment-under-Control (EUC) is concerned. This comprises the OMCS backbones and servers which are considered to be part of a continuous control & protection system.

As previously stated, the separate fire protection function is considered to be a "Protection only" system, and therefore the Failure on Demand frequency is more apt.

The next section considers how this relates to the question: Should TWO operators be involved in such decisions?

4 Human Error Rates

Anderson (2005) summarises Human Error rates:

Key references in the field of human reliability assessment (HRA) include the seminal US Nuclear Reactor Safety Study (1975), Lees (1995) and Swain (1983).

Numerous techniques including HEART (Human Error Assessment and Reduction Technique) and THERP (Technique for Human Error Rate Prediction) are described by Villemeur (1992) and Kirwin (1994). Publications by Leveson (1995), Storey (1996) and Redmill (1997) also draw attention to the subject.

The following Tables stems from the failure rate of humans performing different tasks from the 1975 US Nuclear Reactor Safety Study (Table 1) and according to type of activity (Table 2 - Smith, 1993).

Type of Activity	Probability of Error per Task
Critical Routine Task (tank isolation)	0.001
Non-Critical Routine Task (misreading temperature data)	0.003
Non Routine Operations (start up, maintenance)	0.01
Check List Inspection	0.1
Walk Around Inspection	0.5
High Stress Operations; Responding after major accident	
- first five minutes	1
- after five minutes	0.9
- after thirty minutes	0.1
- after several hours	0.01

Table 1: Human Error Rates

(Source: US AEC Reactor Safety Study, 1975)

Type of Activity	Probability of Error per Task
<i>Simplest Possible Task</i>	
Overfill Bath	0.00001
Fail to isolate supply (electrical work)	0.0001
Fail to notice major cross roads	0.0005
<i>Routine Simple Task</i>	
Read checklist or digital display wrongly	0.001
Set switch (multi-position) wrongly	0.001
<i>Routine Task with Care Needed</i>	
Fail to reset valve after some related task	0.01
Dial 10 digits wrongly	0.06
<i>Complicated Non-routine Task</i>	
Fail to recognise incorrect status in roving inspection	0.1
Fail to notice wrong position on valves	0.5

Table 2: Human Error Rates

(Source: Smith DJ 1993)

There are differences between errors of commission and errors of omission but the figures below have proven remarkably robust and accurate in the author's experience. This includes air and sea pilots, car and train drivers and industrial situations generally.

A coarse summary has it that human errors in trained tasks occur typically at the rate of 1 in 100 per demand, checklist errors are notorious (1 in 10) and even critical tasks can evince error rates of 1 in 1000.

For example, recent monitoring of 2000 train movement orders found a handful of mistakes, none critical, but suggesting a human error probability of 2 in 1000.

Kirwin (1994) collates generic guideline data from a number of sources:

Description	Human-error probability
1. General rate for errors involving very high stress levels	0.3
2. Complicated non-routine task, with stress	0.3
3. Supervisor does not recognise the operator's error	0.1
4. Non-routine operation, with other duties at the same time	0.1
5. Operator fails to act correctly in the first 30 minutes of a stressful emergency situation	0.1
6. Errors in simple arithmetic with self-checking	0.03
7. General error rate for oral communication	0.03
8. Failure to return the manually operated test valve to the correct configuration after maintenance	0.01
9. Operator fails to act correctly after the first few hours in a high-stress scenario	0.01
10. General error of omission	0.01
11. Error in a routine operation where care is required	0.003
12. Error of omission of an act embedded in a procedure	0.003
13. General error rate for an act performed incorrectly	0.001
14. Error in simple routine operation	0.001
15. Selection of a wrong switch (dissimilar in shape)	0.0001
16. Selection of a key-operated switch rather than a non-key-operated switch (EOC)	0.0001
17. Human-performance limit: single operator	0.00001
18. Human-performance limit: team of operators performing a well-designed task, very good PSFs, etc	0.00001

Table 3: Human-error probability

(Source: Kirwin, 1994)

The value of applying such Tables to other situations, such as Airspace Risk Modelling, is to invite

Stakeholders such as Pilots and Air Traffic Controllers to estimate whereabouts in a list a particular scenario might lie.

Using Table 3, is the error a #10 or #11? The answer is the same, 0.01.

A variant of the Delphi group consensus technique is the Shang method which assists practitioners in estimating and calibrating risk-based model parameters.

Each participant is asked to provide a range of estimates and the mean of the group high and mean low is then calculated. The higher than high and lower than low are then invited to explain their rationale.

From this debate, the members vote high or low of the overall mean so as to reach a consensus. For example, votes of #10, #11, #12 and #15 translate to the set of numbers 0.01, 0.01, 0.003, 0.001. In this example – a geometric mean of 4.2 E-3, a high vote could lead to adopt 7.9 E-3 while a persuasive argument for low, say 2.9 E-3.

The value of this technique lies more in the documentation of the reasons for a decision than the numbers per se. The numbers are simply an expression of the articulated reasons.

The conclusion to be reached after a number of such studies is that systems ought not to rely on human performance being any much better than 1 in 1000 for any given critical task. Multiple (different tasks) or teams of people are required to reach safety-critical levels of performance.

With railway signals for example, the Train Driver is always given a second chance: The caution signal is saying: 'Warning, the next signal is at stop' (indicate 0.01 error rate). Then the stop signal means, of course: 'Stop, the next section is occupied' (indicate 0.001 error rate, giving an overall error rate at best 0.00001).

A number of Signal Passed At Danger (SPAD) studies in New South Wales and Queensland, the UK and Europe have indicated that 2.00 E-4 (0.0002) is not unusual as an error rate per red signal sighted and 2.00 E-5 (0.00002) for SPAD greater than 50m past the signal.

5 Application to Case Study

The application of these ideas to this case study suggests that one should not rely on a single person to carry out a single critical task without allowing for that human error rate of 0.001 (1 in 1000).

It has been shown that there are numerous pathways and a high degree of integrity whereby the operator would be alerted to a critical event such as a fire in the tunnel.

But does the fire involve a car or a bus or a heavy commercial vehicle? The consequences escalate rapidly. That is why water deluge systems are provided in Australian tunnels, even though that is not the norm in most other countries.

Various scenarios are pre-planned, especially in relation to operation of ventilation systems in fire mode. The key

concern expressed here is with the congested traffic scenario where downstream traffic may not be free to drive away, thus negating the assumed ventilation scenarios.

It has also been shown that multiple means are available for the operator to communicate with tunnel users, if only the gravity of the situation is appreciated.

6 Conclusion

Given that to override a real alarm could have extreme consequences in such circumstances, it is concluded that a complex control centre remains vulnerable to human error if only one operator is present at the time a critical alarm is raised.

The recommendation is that TWO operators (or a Supervisor) should be involved in such decisions, i.e. both operators need to agree to override otherwise automatic activation.

Alternately, scenarios, such that of fire detected AND congested traffic detected should be interlinked and the deluge system set to automatic in this particular mode, and NOT to involve the operator.

7 References

- Anderson K. *Risk and reliability – An introductory text*. Self-published. Kevin J Anderson & Associates Pty Ltd.. 1995.
- Borchiellini R, Cali M, Giaretto V, Vanelli G, Verda V. *Reflection on the importance of monitoring and control after the Mont Blanc Tunnel fire event*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Burns D, External observations of the Daegu metro fire disaster 18 February 2003. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- EN50126, *Railway applications – The specification & demonstration of reliability, availability, maintainability and safety (RAMS)*, 1999, CENELEC.
- EN50128, *Railway applications – Communications, signalling and processing systems – Software for railway control and protection systems*, 2001, CENELEC.
- EN50129, *Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling*, 2003, CENELEC.
- Henke A and Gagliardi M. *The 2001 Gotthard fire: response of the system, behaviour of the users. How was the fast reopening of the tunnel possible?* TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003
- IEC 61508, *Functional Safety of electrical /electronic /programmable electronic safety-related systems*, Parts 1–7, 1998–2000, International Electro-technical Commission. Also known as AS 61508:2000.

- Kirwin Barry. *A Guide to Practical Human Reliability Assessment*. Taylor & Francis, London. 1994.
- Lees F P. *Loss Prevention in the Process Industries*. 2nd Edition. Butterworth- Heinemann Ltd, Oxford, UK, (3 Volumes). 1995.
- Leveson Nancy G. *Safeware - System Safety and Computers*. Addison-Wesley. 1995.
- MacDonald C and Messenger S. *Life safety facilities in Australian road tunnels*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Miclea P. *Tunnel ventilation systems designer's challenges and dilemmas. Dealing with extreme conditions, assumptions and circumstances*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Nakanishi T, Uamamoto K, Yokota K and Uehara Y. *Risk assessment analysis for water spray operation*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Redmill Felix and Jane Rajan (editors 1997). *Human Factors in Safety-Critical Systems*. Butterworth Heinemann.
- Robinson R, Francis G and Anderson K. *Lessons from cause-consequence modelling for tunnel emergency planning*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Sanchez, *Emergency conditions requirement for modern air conditioned stations in the New York subway*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Setoyama S, Ichikawa A, Shimuzu K, Gunki S and Kimura T. *Effective operation of water spray system for a tunnel fire*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Smith David J. *Reliability, Maintainability and Risk. Practical Methods for Engineers*. Fourth Edition. Butterworth Heinemann, Oxford. 1993.
- Society of Automotive Engineers, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, (SAE ARP 4761, 1995)
- Storey Neil. *Safety-Critical Computer Systems*. Addison- Wesley. 1996.
- Stroppa W and Seebacher J. *The development of tunnel ventilation simulator: A tool to train operators and fire brigades*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Swain Alan D and Bell Barbara Jean. *A Procedure for Conducting a Human Reliability Analysis for Nuclear Power Plants*. 1983.
- US Atomic Energy Commission *Reactor Safety Study*. 1975.
- Villemeur Alain. *Reliability, Maintainability and Safety Assessment*. John Wiley & Sons. 1992.
- Ward S, *Communications a safety device*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.
- Yae H and Mizuno. *Preventing tunnel fires becoming disasters – human factors and systems engineering*. TME 5th International Conference 'Safety in Road and Rail Tunnels', Marseilles, 2003.