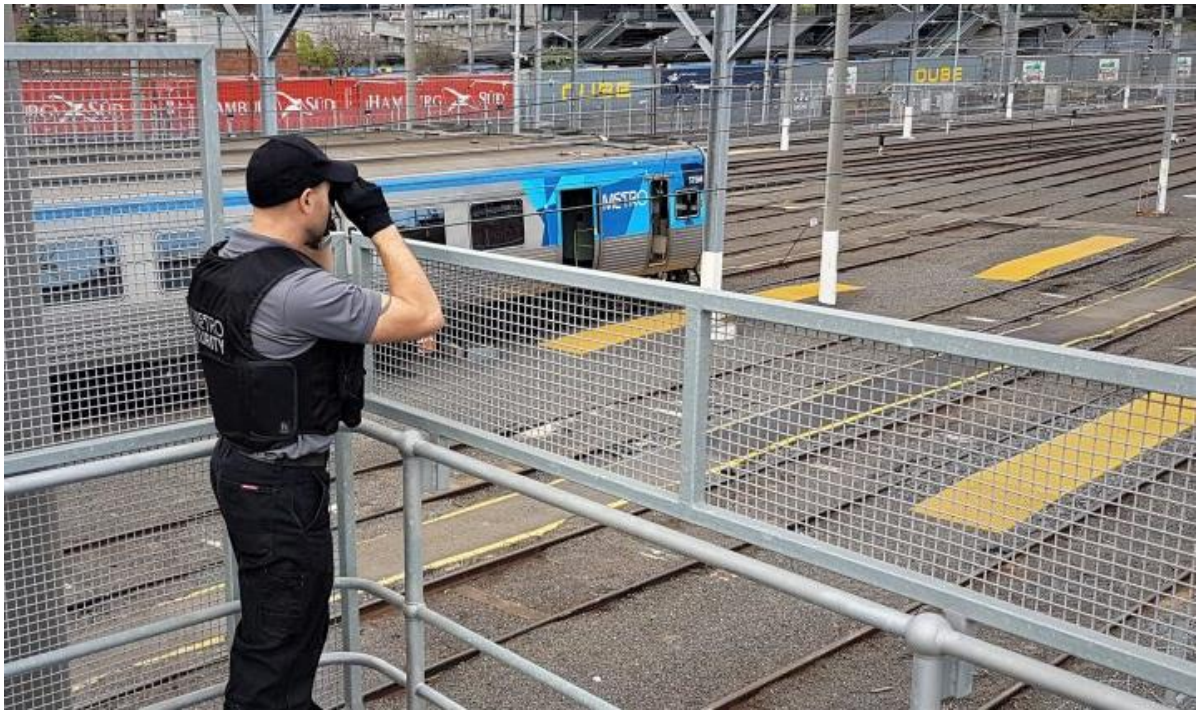
Security Considerations for the NSW Rail Infrastructure Network

By Zachariah Reisch

08 October 2020



Background

As NSW becomes more interconnected and densely populated, its needs for transport infrastructure will continue to grow. With numerous road, rail and airport projects being funded in the coming years, many are concerned with the cost, efficacy, or political buying-power of such undertakings. Amidst the storms around these projects lies an issue often overlooked – with an exponentially complex transportation system being developed over the coming years, how should their designers and operators best approach the issue of security?

Of these three project types, this article will focus on rail projects. This is due to the fact that road projects encounter comparatively few security concerns that are often handled by emergency services or in-built infrastructure measures, and airports intrinsically receive robust security consideration.

Within Australia and globally, rail exists in an interesting realm where it is both an attractive target for crime and/or terrorism, but has a minimalist approach to security design. And, what security does exist is often being reduced – for a domestic example, NSW rail workers have refused to staff a new fleet of trains due to its overreliance on CCTV as opposed to the presence of additional rail staff. Decisions regarding the minimisation of security on rail networks are often not as unwarranted as they appear, or they are done for the sake of a better service - as will be covered - however, it is still necessary to appreciate the impact this has on the safety of our rail networks and those who use them.

While many of the security concerns fall at the smaller end of impact, such as graffiti, concerns such as assault and even higher end terror threats do require dedicated attention to address.

Indicative Security Issues

The following are some of the threats that rail systems, their staff, and their users may face:

Category of Threat	Type of Threat
Physical	Graffiti, Malicious Damage to Property, Arson
	Assault, Sexual Assault, Robbery, Theft, Homicide
	Antisocial Behaviour, Drug Offences, Intoxication
	Littering and Dumping
Cyber	Theft or unauthorised viewing or information
	Control of any systems including trains, signals, communications etc.
	Targeting or associated public-facing communication infrastructure – e.g. train timetables
	Internal Sabotage
Terrorism	Use of IED on a train, train track or platform
	Knife or ballistic weapon attack
	Targeting of a particular user of the rail system
	Any of the crimes as above

While many commuters may not perceive rail premises as crime targets, and the above examples may seem disconnected from their experience, looking closely at the statistics highlights that these premises do indeed have their fair share of crime. For example, in the Sydney LGA, from July 2019 to June 2020 there were 130 recorded incidents of (Non-Domestic) Assault, 135 incidents of Malicious Damage to Property, 330 incidents of Theft and 382 incidents of Drug Offences at rail premises. Similar statistics can be seen by LGA or Suburb across NSW, including in the areas of recently developed or upcoming rail projects.

Additionally, the previous decade has shown us that rail systems are recognised globally as high-value targets for terrorist action. In the previous decade there have been attacks on rail systems globally in Russia, India, Belarus, Turkey, Germany, Belgium, The U.K. and China. Australia's railways have been fortunate to avoid these attacks, but this should be attributed to the robustness of our broader national and state security networks rather than our rail networks and infrastructure being poor targets for such attacks.

A counter-argument to the crime data is that rail premises aren't the cause of the crimes, but rather simply where they occur; obviously if rail premises are frequented by large portions of the population, inevitably a criminal element will also exist. While this is true, it is also important that this fact is used to strengthen the commitment to safety and security at these sites, rather than absolve their designers and operators of responsibility for creating safer environments. If the threat of crime is inevitable, then it is doubly important that security and safety considerations are given due attention in both design and operational stages.

Doing so allows the decision-makers for our rail networks to actively shape their security environment and create safer spaces for all users.

As is briefly touched on with 'internal sabotage', while many threats are external to the system, it is apparent that those who are within it have the greatest capacity to do harm should they wish. What to do about this reality will be discussed in a later section.

Why is Security lighter for Rail networks?

Obviously if security were the only concern, train stations would look a lot closer to airports than their current style. Rail is built on minimalistic security principles for two other main reasons – efficiency and cost. If the security process interferes with the journey of the rail passenger on anything more than a minor and inconsistent rate, the service loses its identity as a convenient and fast method of transport. Commuters won't tolerate an overly-securitised rail system. Similarly, if the security requirements are too expensive, they won't be feasible to adopt on a large scale, as is necessary for a major transport infrastructure framework. Essentially, rail will never have the same design philosophy as airports because it is seen as an unnecessarily intrusive and costly set of measures that is overly alarmist.

While the sentiment is understandable, and the idea of armed guards and metal detectors at every train station is rather hyperbolic, unfortunately our everyday use of these rail networks has desensitised us to the point of believing threats do not exist - as detailed above, they are a definite reality. Although not as susceptible to individual damage as a plane, trains are susceptible in that an incident can often cripple the entire system, having rippling impacts that cause widespread disruption.

Although there are definite reasons security cannot be as airtight as our airports, the foregone conclusion that our rail networks are safe or 'safe enough' should be retired in favour of maintaining a manageable security scheme in line with expert analysis of relevant threat and risk considerations. While existing industry and government standards in this regard are evidence of efforts to achieve a secure rail network, and are commendable, it is vital that these are used as a foundation for a reliable security framework that evolves with the changing risk context, rather than an inflexible rulebook.

How can these threats be combated?

Understanding the threat context is key to devising a holistic strategy. The typical process is to engage a Licensed Security Consultant to conduct a Security Risk Assessment and develop a Risk Control Plan that mitigates an evolving risk context through design, construction and operational stages of the projects. Whilst traditional approaches to security tend to focus solely on its physical aspects, there are strong imperatives to view security as a holistic construct and consider aspects such as governance, personnel security, and information security within the overall risk management framework.

Video Surveillance

Given the apparent steadfastness with which the industry is heading, it appears unlikely that the trend towards increased reliance on video surveillance will revert. Therefore, it is vital that those involved in the security of rail systems employ such surveillance in the most efficient manner possible.

Cameras should be twofold in use (at least in their totality, rather than *individual* cameras), being useful for both evidentiary purposes (the current predominant use) and information gathering for rapid response. As rail systems are increasingly integrated into new areas, some of which with higher than preferable crime rates, solely focusing on evidence gathering for past crimes is rapidly becoming an outdated and insufficient model.

Development of a system by which presently occurring 'serious' crimes (Assault, Sexual Assault, Arson etc.) can be monitored for and responded to is highly recommended as a measure that improves safety and reduces the cost of repair over time, as well as strengthens community perception of safety and takes command of the security environment without excess intrusion.

Internal Threats

Regarding the threat posed by internal staff or ex-staff, as noted above, a politically motivated or disgruntled employee can cause significant or even catastrophic damage if they are inclined.

Therefore, maintaining checks and balances with a necessary degree of oversight is advised, both in terms of physical oversight of day-to-day functions and periodic review of work and checks for malfeasance of any sort. This includes risk managed approaches to conduct police checks, background checks and financial credit checks not just at the commencement of employment, but also on a regular basis - dependent on the risk assigned to the role in question.

Automating this and/or building it into the function of roles – for example automating reviews, having managers work in the same physical space as employees, and ensuring work-checking is a mandatory part of the process – will reduce the tax this has on regular operation, as it will be a permanent component of work rather than an intrusive nuisance.

Additionally, obviously, access permissions and restrictions should be utilised to the necessary level across systems and locations, and care should be taken to ensure that ex-employees are unable to access any of the physical or cyber infrastructure they had access to during the performance of their role.

Further Employment of CPTED

CPTED stands for Crime Prevention Through Environmental Design and broadly addresses the use of the physical environment to minimise situational crime. CPTED in NSW has traditionally involved the use of the four principles of Surveillance, Access Control, Territorial Reinforcement and Space Management. These principles can be augmented through concepts such as target hardening, while also factoring in considerations of social ecology, liveability, public health and sustainability that are part of second and third generation CPTED thinking.

Leaning further into CPTED principles is encouraged, particularly those related to vision. The style being adopted for many urban rail systems – particularly light rail – of open platforms is excellent for visibility and ensuring that being seen is an active deterrent against crime.

Lighting is another key issue; lighting should be maintained at all hours of operation and should only light 'safe' areas that include the platform and its necessary surrounds, not any areas which may raise risk by entering – for example, any unmonitored areas. The visibility of trains should also be noted; many previous train models have had windows with a low degree of transparency that precluded individuals from seeing into the train carriage. It's recommended that trains have large, transparent, non-tinted, ad-free windows to reduce the risk of crime occurring on or off the train where criminals may feel they cannot be seen from the other location.

Personnel

Lastly, addressing the decrease in personnel; despite the urge to cut back on drivers, security guards and station staff, it is important that these are *at the least* maintained at their current level. The presence of staff – particularly security staff – on trains and platforms reinforces the idea that both are well-monitored, well-cared for and crime-repellent.

It is also necessary that 'footage monitoring' staff are employed if the exponential use of cameras is to yield benefits in stopping any ongoing crime. Despite the initial cost of this, it will yield benefits in reduced levels of crime and allow ongoing 'serious' crimes (as above) to be halted when they occur.

Conclusions

With the rapid expansion of rail networks to meet the travel demands of the NSW population, appreciation of the necessary security considerations is essential in order to ensure the developments are safe and sustainable. In line with State and Federal Police and Intelligence bodies, as well as the expectations of commuters, rail developments should address crime and terrorism concerns as a matter of course.

The above recommendations are a non-exhaustive list and should be considered to the extent relevant for specific rail developments – but the underlying intent is to highlight that although existing security attitudes and frameworks appear to be 'good enough', they can and should be built upon to actively reduce the risk of crime and terror threats. Although there may be some increased initial and/or ongoing costs and hassle involved, the security of our rail networks and their commuters should be viewed as the key concern – and through engaging actively with these security concerns with an eye for cost reduction and innovation, new and more effective methods will inevitably be produced.