SECURITY OF ROAD INFRASTRUCTURE

World Road Association TF2 – Security Task Force
STATEMENTS

The World Road Association is a nonprofit organisation established in 1909 to improve international co-operation and to foster progress in the field of roads and road transport.

This report was developed as a special project by the World Road Association after this issue was identified as a priority by the Association’s Executive Committee.

This report is available from the internet site of the World Road Association

http://www.piarc.org

This paper was prepared under the auspices and with the approval of the PIARC Task Force 2 on “Security of roads” chaired by Roberto Arditi, SINA/ASTM-SIAS Italy, with the following membership:

• Steve Ernst, DOT USA
• Jürgen Krieger, BASc Germany
• Bine Pengal, ZAG Slovenia
• Dominique Schmitt, IFSTTAR France

A special recognition to the advices and contributions delivered by the UK Government’s Centre for the Protection of National Infrastructure (CPNI), whose officers first proposed the drafting of this paper.

Some members of the World Road Association, external to the working group and other experts contributed to this paper by giving a scientific contribution to the international workshop organized by the World Road Association Task Force 2 and hosted by British Authorities in London on June 10th 2014.
There is a wide range of threats potentially affecting infrastructure and the operation of roads: e.g. threats to individuals, threats to the operators and threats targeting, more generally, society. This paper is addressing threats directed to the infrastructure.

Roads have previously been a target of terrorist organizations. Transport infrastructure supports national economic and provides freedom of movement. Protection of citizens whether they be highway users, pedestrians or maintenance staff is an issue for governments. A wide range of hazards and threats may impact roads, bridges and tunnel infrastructures. Terrorism, e-crime, theft and hoaxes have to be considered. For low frequency, high-consequence events, it is difficult to avoid complacency and this can impact on the motivation of the guard force, the reaction of users who may find it difficult to know what should be reported as suspicious and the actions of Road Authorities in determining relevance and cost-effectiveness of preventative or protective measures.

A correct understanding and a suitable handling of the security of road infrastructure is not only important to safeguard the infrastructure itself, but is also relevant to cover the protection of the social and economic values for those activities that rely upon road facilities, the protection of the environment and even the security of other transportation modes.

The objective of this paper is to:

• provide an overview of the range of security threats and issues that affect road infrastructure, operations and users.
• promote thought and discussion within the road community in order to raise awareness and allow Road Authorities and Operators to step forward with international good practices on “Road Infrastructure Security”.

The paper outlines the following topics of interest for the security of roads:

• assessment of physical security;
• different methodological approaches;
• safety and security programs;
• application of knowledge in security by design;
• retrofit of existing infrastructure.
There is a wide range of threats potentially affecting infrastructure and the operation of roads: e.g. threats to individuals, threats to the operators and threats targeting, more generally, society.

In this first cycle of study, the World Road Association decided to concentrate on threats directed to the infrastructure.

Theft, threats to the operation of roads (e.g. attacks to individuals, to truck drivers, attacks to the operation of roads, fraud of tolls) are also important topics for road authorities, to be covered in the scope of the World Road Association’s action, but not addressed by this leaflet.
THE NEED FOR THIS PAPER

Reliable road infrastructure is necessary for sustainable mobility and makes an important contribution to quality of life of the citizens. To achieve a satisfactory level of reliability on the roads, it is necessary to consider the safety and security of both infrastructure and traffic. Requirements for road infrastructure are changing with increasing traffic volume and composition and from changing societal needs.

Roads may not have a high direct attractiveness as potential targets, but terrorist organisations have previously targeted transport infrastructure. Transport infrastructure supports national economic well-being and provides freedom of movement. Protection of citizens whether they be highway users, pedestrians or maintenance staff is an issue for governments, but a wide range of hazards and threats impact roads, bridges and tunnel infrastructures. We protect against accidents, crime and other user safety threats, but also must now consider terrorism, e-crime, theft and hoaxes (photo 1). For low frequency, high-consequence events, it is difficult to avoid complacency and this can impact on the motivation of the guard force, the reaction of users who may find it difficult to know what should be reported as suspicious and the actions of Road Authorities in determining relevance and cost-effectiveness of preventative or protective measures.

A correct understanding and a suitable handling of the security of road infrastructure is not only important to safeguard the infrastructure itself, but is also relevant to cover the protection of the social and economic values for those activities that rely upon road facilities, the protection of the environment and even the security of other transportation modes.

The objective of this paper is to:

- provide an overview of the range of security threats and issues that affect road infrastructure, operations and users;
- promote thought and discussion within the World Road Association’s community in order to raise awareness and allow Road Authorities and Operators to step forward with international good practices on “Road Infrastructure Security”.

Photo 1 - Road interrupted by direct action
BACKGROUND

Road infrastructure is necessarily open and accessible and offers a convenient means of mobility for those wishing to do harm. Road infrastructure may be perceived as a soft target if there are few visible protective security measures in place. If roads are also crowded places, as in city centres, then they may prove even more attractive as a target for those with malicious intent. Good protective security measures have been shown to deter and displace the threat.

Due to the nature of man-made risky events, it is difficult to anticipate security issues in terms of time and location. Unpredictable or unlikely, even catastrophic events are possible and it is one of the roles of road authorities to reduce the possible consequences of attacks by making attacks more difficult to carry out and/or potentially less effective. Cost is always an issue and a good goal is to strive for strategies that are both proportionate and cost effective. Criticality of the asset should be considered for any countermeasure.

A process of assessment for the road security risks and a plan for effective mitigation implementation assists authorities, road administrations and road operators to make choices and investments in a scientific and realistic way.

“Security by design” is easier/less expensive than applying measures to existing infrastructure elements (retrofitting). In fact, a major issue is not only that retrofitted security measures may not be as robust as those included in the initial design process, but that retrofitted measures can be extremely expensive requiring a separate project thus causing delays. Incorporating security early in the design process has many advantages for both effectiveness and cost savings.

For both intentional acts of terrorism and the unintentional act of barge collision, a waterway pier can be protected by rock islands, dolphins or fenders. The best security improvement, against intentional ramming and from explosives, might be the rock island (like the one shown in photo 2B), but it is likely that this option is available only if the planning process has considered
the impact of the island footprint on the waterway and adding such a feature late in design would be expensive in both time and money.

There is the challenge of the “Black Swan”, the low frequency, high impact event that is difficult to foresee and the challenge coming from more predictable events that require our constant attention. Road infrastructure security is subject to both of these challenges. We certainly must deal with the predictable, every-day events and it is often a good option and perhaps cost-effective to take actions to eliminate or reduce catastrophic consequences from the infrequent ones.

Some security incidents may represent low level impact with high frequency of occurrence (for example attacks on HGV drivers, e-fraud of tolls, metal theft). They have an aggregated and erosive impact but do not attract high media coverage. In Europe, a high number of lorry drivers are attacked and robbed, as more secure parking facilities are often perceived to be too expensive.

Terrorism represents a high impact but low frequency incident, designed to attract extensive media coverage. Significant investment in protective security measures is normally required to mitigate this type of attack.

It is important to understand the nature of the threats to the network, which elements are critical, where the main vulnerabilities are, before one can target an appropriate response.

In order to implement countermeasures on critical elements, a threat and vulnerability assessment is required involving consideration of the capability and malicious intent of hostiles, identification of possible scenarios and determination of the vulnerability of the asset and its important components. The identification of vulnerabilities and criticalities is essential to prioritise spending, but these terms are often wrongly interchanged. It is also necessary to consider the resilience of the critical infrastructure as well as any interdependencies with other infrastructure and sectors.

Partnerships with different stakeholders is a key to success in protecting critical infrastructure. Consideration has to be given to the neighbouring facilities and to the relationships with everyone with a security role and with others who may not necessarily have a direct responsibility for security. Negotiation and partnering are important skills when working with adjacent site operators, whose facilities may be part of critical infrastructure. Complacency can also be a challenge, therefore training and information dissemination is vital to ensure that stakeholders are up-to-date and engaged early on in the process of protecting their infrastructure.

Stand-alone security solutions are difficult to implement without a legal framework. Cost-efficient security solutions can be achieved where synergies with mandatory safety measures exist.

There is no universally accepted method for security risk assessment and management. Among experts, the debate is on-going as to what is appropriate, effective, economical and what user tolerance and trade-offs exist. An “all hazards”, risk-based design approach is not yet state-of-the-art. The monetization (or different estimation) of loss of life, disruption of service and quantification of iconic value underpin this kind of approach. A constant review process would be advisable for criticality and vulnerability.

---

1 Nassim Nicholas Taleb: The Black Swan - The Impact of the Highly Improbable
2 According ITF (15 February 2013, Palais des Nations, Geneva): 1 in 6 (or 17%) of drivers attacked in the past 5 years (30% more than once). Source: http://www.unece.org/trans/events/2013/inlandsecurity_forum13.html
What makes up the Risk?

**Threat**
Anthropogenic hazards or human-made hazards can result in a human-made disaster. In this case, anthropogenic means threats having an element of human intent, negligence, or error; or involving a failure of a human-made system. It results in loss of life and/or property. It further affects a person's mental, physical and social well-being. This is opposed to natural threat such as flood or earthquake.

**Vulnerability**
Means the characteristics, parameters and conditions of a structure, infrastructure, system or population that make it susceptible to the adverse effects of a threat. Factors that define vulnerability are of physical, social, economic and environmental natures. Vulnerability varies significantly within a community and over time.

**Critical Asset**
Asset having significant potential to impact on the achievement of economic, operational and security objectives of National Authorities.

**Resilience**
It is the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events.

**Soft measures**
These are measures assumed in operation, organization and staff training. Retrofit of the asset may be included in the range of soft measures.

**Risk**
A measure of the probability that damage to life, health, property and/or the environment will occur as a result of a given hazard.

The speed of change in society, complexity, technology and interconnectivity all have an impact upon security. Society is undergoing an internet and technology-based revolution and there are unprecedented opportunities to exploit new systems. Technology is playing a key role in road systems becoming more complex, with opportunities to utilise Intelligent Transport Systems and the constant need to keep up-to-date with developments and new vulnerabilities. The world is currently experiencing a major wave of innovation related to ever increasing opportunities from communication (mobile, internet, etc.). This kind of innovation is entering automotive technology, improving safety and efficiency of transport through vehicles connected among themselves (from cooperative systems towards autonomous vehicles) and with the Infrastructure. Although expected to give a positive outcome for citizens, security of the transport system will become more complex, as the new threat of cyber-attacks could directly impact the safety of road operations, tunnels and bridges. Although the cost of security is a concern “Who owns the risk?” and “Are there cost efficient measures?” are among the more tricky questions to be considered.
ASSESSMENT OF PHYSICAL SECURITY

Threats to road infrastructure are varied, for instance from terrorism, stand-off weapons, Vehicle-Borne Improvised Explosive Devices (VBIEDS), hand emplaced explosives, contact explosives, non-explosive Cutting Devices, cutting charges, thermal lances, fire (hydrocarbon, hazmat), impact, metal theft, vandalism, trespassers, crime, contamination, natural hazards, drugs and alcohol and accidental damage. There is no internationally accepted definition of critical infrastructure. Risk is a function of consequences and the vulnerabilities of the asset or component.

It is not possible to protect everything, therefore a proportionate and a layered approach to security must be used, which includes consideration of what is critical on site and concepts of deterrence, detection and delay. To face all the mentioned threats a holistic approach is required: the nature of the infrastructure and the environment, personnel and cyber security needs to be considered.

Planning, coordination and monitoring are required to improve detection and response capability. Tools like CCTV with video analytics have proven useful for good operation (e.g. using CCTV to verify an alarm). Additional soft measures can be deployed at times of increased threat. In some countries, Road Authorities undertake to train staff on security matters: hostile reconnaissance training, penetration testing and live multi-agency contingency/response planning exercises.

Criticality assessments are a complex problem requiring social investment. An assessment process needs to be traceable, transparent and reproducible. A combination of engineering techniques and appropriate models for comparison and decision making is required. Typical questions are:

1. How does an owner decide to spend money to protect a road, a bridge or a tunnel?  
2. How does the owner need to describe the contract requirements?  
3. How does an owner or operator integrate security into asset management plans?

Effective planning includes identification and selection of critical elements on the road network, examining critical components for each major element in the network (bridge or tunnel for example), analysis of the threat, identification of those with criminal intent, identification of means of attack, analysis of infrastructure vulnerability, processing of threat scenarios by evaluating threats, vulnerabilities and consequences, definition of countermeasures and combining the level of risk of the critical elements with specific actions.

The interest for physical security is not limited to intelligence and patrolling activities. More effective solutions can be easily achieved when the issue is included in asset management programs and project management.

Protecting this way even the functioning of the overall network.
National and cooperative research and development with programmes covering physical, personnel and cyber security, is advisable – this means that countermeasure development is objective. There is a need for holistic design of security measures. Even cyber security can have an impact on physical security.

Even more difficult is the assessment of the probability of attacks and the stretching of resources that may occur in the event of simultaneous attacks. Generally speaking, the lack of information regarding probability of an attack makes it harder to identify the cost-effectiveness. If a countermeasure has multiple benefits, this may be useful for the decision process.

Indicators for the structural assessment could be general durability and resilience under various threats, structural risk, time required for repair after a damage and estimated cost for repair.

Indicators for the assessment of user safety could be quantitative risk assessment in regard to local constraints and specific scenarios, estimation of probabilities, consequences and accumulated risks and possible implementation of mitigation measures. Indicators for the assessment of lifecycle costs (LCC) are costs of initial investment (construction, equipment, countermeasures, etc.), follow-up costs (maintenance and repair), costs of decommissioning and possible revenues in cases of Public-Private Partnerships (PPP).

Indicators for the system criticality assessment are the impact to the surrounding infrastructure network, partial or a full loss of a structure and loss of service.

Soft criteria include the symbolic value of an asset like a bridge or tunnel.

Rough filter criteria for estimating risk of bridges and tunnels are: high Annual Average Daily Traffic (AADT) or High Goods Vehicle (HGV), sensitive construction below, over or near the structure; long reconstruction period; high symbolic value (attractiveness for man-made attacks); long-span bridges and tunnels. The criticality assessment can be performed transforming physical values into utility classes (e.g. 1 to 5), weighting of indicators and using uniform default values with owner input. When traffic system criticality is based on additional travel times, further indicators can be added such as emissions, accidents etc.
A few remarks on the organising process:

- in some sectors and disciplines, operators are thinking about security in advance of the Regulator; security sells and organisations believe they understand their operations best and are keen to act, assuming there is room in their budget;
- the presence in the organization of a safety and security culture devoted to the protection of infrastructure could be helpful to consolidate advice to owners, operators, regulators and police;
- security only solutions are difficult to implement without a legal framework.

In some countries the priorities are to stay ahead of potential attackers and to educate and influence owners - who may not have experienced attacks. Threat data can be used to map the direction and progression of malicious intent and attack methodologies.
DIFFERENT METHODOLOGICAL APPROACHES

Owners of road infrastructure (in most cases road authorities) are responsible for the overall maintaining, consequently, from owner’s point of view, the procedure “per se” is not so important. What is important is the final result which must be comprehensible and adapted in the way that the procedure can easily fit with bureaucratic reasoning and forms. That is the only way that solutions will ever be financed and implemented. So, it is more the question what experts can learn from the owners and road authorities and their reasoning that can be of benefit when designing the methodological approaches.

There are a lot of approaches and different variations of making a security assessment (criticality and vulnerability) of a certain structure on road network. These approaches vary according to the sector of the infrastructure itself (transport, energy, water management, etc.), according to different countries, history and experiences of direct attacks on the infrastructure and so on. The end result of such analysis should however include at least the following information for the owner:

- pinpointing of the structures in the network (bridge, tunnel, crossing, etc.) needing protection;
- clear and comprehensive list of threats to this structure;
- clear and comprehensive list of proposed countermeasures;
- detailed and clear calculation of estimated costs for implementation of preventive /protective measures;
- cost-benefit analysis considering even other possible benefits (e.g. for safety).

With this basic information the owner of the infrastructure can competently decide about investments. Image below represents steps of basic procedure for focused security analysis for certain structure that at the end provides answers to all above mentioned issues for the owner.
An example of open literature, providing an interesting approach at national level, is the “TRANSEC Compliance Framework” produced by the United Kingdom Department of Transport. This aims to protect travelling public, transport facilities and people employed in the transport industries (primarily against acts of terrorism). TRANSEC Compliance Framework has security objectives over several modes of transport, including roads (transportation of dangerous goods only).

The objectives are:

- to organise a proactive and reactive programme of compliance monitoring activity to maintain and, where necessary, enhance standards of security; to take timely action, in line with the stepped approach, where deficiencies are identified;
- to engage with industry at all levels to influence their strategic and tactical thinking so that security forms part of the business planning and decision-making process;
- to encourage industry to take ownership and responsibility for security and adapt their quality assurance activities accordingly.

Germany performed research in the field of road infrastructure security at National level (within the “National Security Research Programme”): projects SKRIBT and SKRIBT+. Furthermore, results from various research projects on European level projects like SERON, SECMAN are available. Links for these projects are available in the following chapter “Resources on road security”.

References and brief descriptions for some tools used in the United States for evaluating risk and for designing countermeasures are described below.


This paper describes a risk-based method to prioritize mitigation strategies on a bridge by matching each component on the structure to specific risks from terrorism. Results are measured against the impact from mitigation measures and their cost to help owners identify effective protection. This process has been adopted in the United States by the Federal Highway Administration and the Department of Homeland Security for strategic bridge evaluation.


This report describes the response of concrete bridge columns subject to blast loads, design and detailing guidelines for highway bridge columns subjected to these loads and the results of experiments to validate models for these columns. The results were adopted as a guidance specification in the United States by the American Association of Highway and Transportation Officials Load and Resistance Factor Design Code. The design examples demonstrate how the methodology can be used to design more resistant columns and evaluate existing designs against a reasonable set of standards.

CAPTOOL, Users Guide for CAPTA, USDOT Volpe Centre, available from the USDOT Federal Highway Administration. This guide will be updated with the new version of CAPTA.

These two documents (CAPTA and CAPTOOL) describe a method for transportation agencies to manage risk, using consequence-driven attributes to evaluate high-level funding decisions for multiple assets exposed to multiple hazards. The report details the methodology and CAPTOOL is a user guide developed by the Federal Highway Administration to make using the tool easier. This is a cost-based tool that recognizes limits to transportation funding and the need to balance investment decisions among many competing factors, including terrorist threats. Both documents are available and useful in their current form and they are under revision with expected completion in 2015.

To find French literature about methodological approaches to security is not an easy exercise in general. Security of road transport in particular do not escape to this general rule. In fact the Government of France has a strong culture of national defense secret. So, when methodological guides exist, they are often classified “confidential defense” and consequently are available for authorized people only. For the same reason, books on the subject are not so many.


Consequently, you can find authorized guidance about security of hazardous goods transport by road in circular n°2005-62 of October 7th 2005 and more particularly, in the guide produced by an inter-professional association published as an annex of it. About security assessment of ports and relevant facilities, guidance can be found in the circular of 2004, having more details in the annex of an act of April 22nd 2008.

Then came the time for the implementation in France of an act on “vital interesting sectors” (Act 2006-212 of February 23rd, 2006), a French concept that later inspired even UE to develop its own Directive 2008/114/CE of December 8th, 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

French government’s agency SGDSN published a Guide for development of Operator Security Plans and other useful, but classified, documents. The protection of critical infrastructures is now resumed through the inter-ministerial instruction n°6600. Road infrastructures are considered as one of the 12 vital sectors treated in this device.

---

5 http://www.bulletin-officiel.developpement-durable.gouv.fr/fiches/BO200520/A0200044.htm
Whatever the targeted field, the guiding principle of French method is still about the same: threat assessment, resilience and risk reduction measures, planning (organization, procedures, training), detection and alert, action and rehabilitation, feedback.
SAFETY AND SECURITY PROGRAMS

Cost efficient security solutions are needed. There is a large overlap between safety and security (the boundaries are often not clear) which can be used to strengthen both. It is easier for owners to implement cost-efficient security solutions where synergies with safety exist. Methodologies and tools to take advantage of this synergy need to be available to owners and operators. There is a need to identify critical objects and/or road sections and to undertake vulnerability analyses with regard to relevant threat scenarios and to assess the effectiveness of security measures. Are road safety and security issues analogous from the point of view of programs? For road safety, if there is a reduction in road casualties from an action, then there is a demonstrable payback and ample data to support it. It is different for security with little base data and low incident numbers that make interventions appear to be subjective and too expensive.

An example: road tunnel technology is mature for safety. Incidents in tunnels could be safety or security related (e.g. fire or terrorism) and existing structural and operational safety installations could be used to prevent and mitigate both safety and security related events. A legal framework exists for tunnel safety. Additional measures such as innovative detection systems could be used for selected vulnerable and/or critical bridges or tunnels and for detection of suspicious vehicles, persons and objects with a focus on prevention.

Only few security measures are cost-effective when focusing strictly on security aspects. Measures with relevant risk reduction potential and additional benefits (such as safety impacts on multiple scenarios) should be considered. National European projects demonstrated the use of “Real Time Safety Management System” for tunnels (existing detection systems plus new innovative detection systems) that enable risk-level visualization for the tunnel operator in the control centre in real time and an expert system suggesting preventive or mitigation measures in case of “yellow” or “red” risk level.

Intelligent Transport Systems (ITS) integrate technologies to monitor traffic behaviour (e.g. Bluetooth, mobile phones and license plate recognition) and are designed to improve traffic flows and road safety. These monitoring systems can sometimes be used specifically for security purposes\textsuperscript{11}. For instance, ITS can be used in emergency situations to support crisis managers. They can also be adopted for enforcement purposes. Connected vehicle technology has great potential for the driving public, but introduces a new set of threats as well. Malicious intent, including cyber-attack, will require the concerted attention of system designers and operators.

\textsuperscript{11} Aspects of data privacy need to be considered when safety/security measures are considered; in some countries (e.g. Germany) the protection of privacy rights makes more and more difficult the action to secure assets.
APPLICATION OF KNOWLEDGE IN SECURITY BY DESIGN

Following extensive research into infrastructures and acts of terrorism, a growing number of consulting engineers and scientists have the knowledge to design structures against acts of terrorism.

Some protective measures could cost less than 1% of the total project budget; however, design codes do not require protective actions and owners usually do not request them. General principles and existing specifications can be consulted for security design and there is considerable information about protective measures and protective design available outside of specifications. Certainly, there is room for development of improved security practices and codes and a need for international information sharing for which the World Road Association can play a significant role. Following are some key points from the World Road Association Security Task Force Workshop concerning security by design.

There are some straightforward protective security measures. Keep people away from critical components. Plan in advance for access control (for example, lock hatches etc.). Provide stand-off (for example from the columns). No system is impenetrable (for example, people will climb bridges) and it needs to be decided how much access control is reasonable to deploy. Ensure surveillance devices and sensors link to an adequate response force, with a concept of operations for response.

As might be expected, a sizeable proportion of international terrorist threats against bridges has been directed at suspension bridges and other iconic structures (i.e. the most visible ones), though a large percentage of actual attacks has been directed at more common bridges. Columns, bridge cables, towers and girders can be vulnerable due to their direct exposure to blast and large fire effects. In this threat environment, inches of stand-off make a difference.

Protective measures can be classified:

- by type: structural, operational and organizational;

For new designs, there is the opportunity to focus on enhanced system behaviour, to improve asset-level redundancy and to deploy stand-off measures for vulnerable components. Robustness has value for all hazards and there is opportunity to take advantage of the benefits of mitigation for more than security alone.

The design of bridges for security is not as mature as for the design of buildings. Still, there is plenty of opportunity to use lessons from the building industry to influence transportation security design.
RETROFIT OF EXISTING INFRASTRUCTURE

It costs more to retrofit existing infrastructure than to include measures at the outset, however, a list of possible measures for retrofit is needed, including benefits, maintenance requirements and good design practice. Measures need to be robust, secure and proportionate. They should provide value for money, not compromise inspection or maintenance, be environmentally appropriate and fit with the image desired by relevant authority.

Key concepts for consideration are redundancy, recovery, structural hardening and blast stand-off. It is recommended that a simple toolkit of measures be employed – these measures should be complementary to the response plan. There is a requirement for low budget solutions, with security being embedded into main business practices. The terms “protection” or “mitigation” may be more readily accepted than “security”. Sample clauses based on good practice for implementation in contracts should be identified.

Physical protection includes fences, mesh screens, crash barriers, vehicle access gates, security doors and lockable access covers, bollards (PAS, CWA or IWA rated\(^2\), non-rated and safety bollards), gabions, berms and ditches, cameras with analytics, incident detection systems and cyber locks.

Redundancy provides resilience and it is vital to eliminate single points of failure or reduce vulnerability to attack in these critical components. There are differences between the stand-off for buildings and bridges. For bridges there are often no redundant systems, therefore the sudden loss could cause a progressive collapse. An asset owner may need to harden critical components when adequate stand-off is not feasible.

Several tools to plan and design are available. A few examples are listed in the following section of this paper.

It is necessary to prevent access to internal areas such as box girders and arch ribs and prevent the placing of an explosive device against the critical elements (for example flanges, cables and bearings). There needs to be means to detect whether a protected area has been unlawfully accessed. Bearings can be protected using mesh or fence and small service shacks. Strong shrouds should be used for padlocks. Sterile zones can be created using camera monitoring with video analytics or laser incident or intrusion detection systems and alarms. These systems should be monitored in the Control Room. It is important to prevent unscreened vehicles from parking under the bridge or next to the piers.

Soft measures (local patrols, signs, liaison with local population) may be beneficial. Special surveys will be required for critical infrastructure and an armed response may be required. There can be added benefits from reduction in other crime (for example metal theft, general crime, preventing trespass and vandalism).

In retrofit it is often necessary to implement redundancy, with a focus on blast mitigation measures that can meet multiple threats.

---

\(^2\) PAS = Publicly Available Specification published by the British Standards Institution. CWA = CEN Workshop Agreement. IWA = International Workshop Agreement.
The response to the threat must include a range of measures such as cameras (CCTV) and incident or intrusion detection systems (IDS). These and other detection and physical security measures should be integrated to give police time to respond. It is necessary to protect critical elements such as columns, towers, cables, girders and bearings. The question needs to be asked “What is a proportionate response for a publicly-owned asset?” Major issues for consideration are the size of the asset, economic importance, relationship with other infrastructure, location, site-specific attributes and the complexities of land ownership and use agreements. In many cases, the road owner does not control the land under its assets. There is a need for a clear concept of operations (ConOps) for all security features.
RESOURCES ON ROAD SECURITY

A few references to open documents of interest to the content of the current background paper:


[6.] European Project SERON (Security of Road Transport Networks) concerning the identification and designation of European critical infrastructures and the assessment of the need to improve their protection www.seron-project.eu

[7.] SKRIBT: two German programs for the assessment of infrastructure security (in German only) http://www.skribt.org/

[8.] ESIMAS German research program for the real time monitoring of road tunnels http://www.esimas.de/


[10.] AllTrain: All-Hazard Guide for Transport Infrastructure; http://www.alltrain-project.eu/


[25.] OECD « Security of intermodal container transportation » [https://books.google.fr/books?id=tTXHR0OUtEC&pg=PA97&dq=s%3C%BBret%3CA9%+des+transports+routes%26hl=fr&sa=X&ei=zcX4VM-aFoyrUd7JgJgN&ved=0CDoQ6AEwAQ#v=onepage&q=s%3C%BBret%3CA9%20des%20transports%20routes%26f=false](https://books.google.fr/books?id=tTXHR0OUtEC&pg=PA97&dq=s%3C%BBret%3CA9%+des+transports+routes%26hl=fr&sa=X&ei=zcX4VM-aFoyrUd7JgJgN&ved=0CDoQ6AEwAQ#v=onepage&q=s%3C%BBret%3CA9%20des%20transports%20routes%26f=false) or [http://ebiz.turpin-distribution.com/products/191057-container-transport-security-across-modes.aspx](http://ebiz.turpin-distribution.com/products/191057-container-transport-security-across-modes.aspx)


[27.] TRANSEC COMPLIANCE (UK)

