Login or Register Join The IET Shop Help A-Z Contacts Home Search the IET website Search

The IET Engineering Communities Careers & Education Policymakers & Media Events & Venues Publishing & Inspec

Home Engineering Communities Industry Sectors **Computing and Control**

ENGINEERING COMMUNITIES

Computing and Control

Services supporting the growth of knowledge in engineering and technology

Industry Sectors

Computing and Control sector:
Technical Articles
Industry News
Events & Training
iet.tv - Event Webcasts
Website Directory
Jobs & Career Development
Discussion Forum
Current Awareness
Recent Publications
Magazine

Select Sector or Network

Tunnels of Terror

by Konstantinos Koumpis, Lesley Hanna and Stephen Hailes

Computing & Control Engineering
February 2006

Responding effectively to emergency situations such as earthquakes, forest fires, terrorist attacks and chemical spills involves a complex interaction of engineering, technology and people. The objective of the architects, builders, operators and regulators of related systems is to ensure that they provide an acceptable level of safety for their users and staff.

The level of safety depends upon well-designed, reliable equipment operated in accordance with effective procedures for tasks such as data gathering, analysis, detection, response and recovery.

Major incidents have shown that current safety systems are vulnerable mainly because traditional data acquisition systems and control systems are not seamlessly integrated and they do not support redundancy for components that have failed or been destroyed. Advances in embedded computing systems have led to the emergence of devices that integrate sensing, computation, and wireless communication.

Such embedded systems will be increasingly carried around by people and fitted into vehicles and fixed infrastructure. Our particular focus is on the case of road tunnel fires, although the know-how and tools may be applied more broadly across the field of emergency response.

Tunnel Fires

Tunnels are complex engineering structures built in order to save transportation time and costs, as well as to protect the environment. Their design and construction represents a balance between the demands of function, safety and cost at a particular point in time. Statistics show that the risk of accidents in tunnels is lower than on open roads and motorways. This is primarily due to the minimal effect of weather conditions, speed limits, steady lighting conditions, as well as the low number of junctions in tunnels. But when a fire breaks out in a tunnel, vehicle occupants are changed from spectators of an accident into participants in a potential disaster, since they can be easily exposed to toxic flame and smoke and trapped in areas where rescue teams have very restricted access.

Over 200 people have died in Europe as result of tunnel fires in the last decade (See Table 1). According to a report by the European Commission the direct costs of recent tunnel fires, including reparation amounting to 210m Euros per year. With more tunnels (35% extra tunnels over 1km in length are to be constructed between 2002 and 2010 in Europe), the number of accidents and tunnel fires is likely to increase.

Testing times

Consider the future scenario in around 2012 of a fictional road tunnel. It has been in existence for over 30 years and offers a major transport route. The amount of traffic is moderately high and any alternative route is much longer so it is a preferred route for goods vehicles. Because of its age, the tunnel does not have an optimum design for safety and, as a result, hazardous and explosive cargoes are refused passage or allowed through under restrictions. This is enforced following the scanning of obligatory RFID tags that provide information on the contents, quantity and hazard. The age of the tunnel means also that ventilation is poor and, as a result, air quality monitoring equipment has been installed. Temperature, humidity and some gases are measured. Information on air quality is made available to anyone who may be concerned about the potential hazard to their health (e.g. asthmatics) via a suitably-equipped PDA.

On a busy weekday a collision occurs deep within the tunnel between several vehicles including a tanker loaded with vegetable oil, which suffers penetration of the tank and begins to leak over the road surface. A small fire, started as a result of the collision, spreads to the oil, which begins to burn, producing clouds of thick smoke as well as heat and flame.

The traffic stops quickly when the accident occurs. Even regular tunnel users are unlikely to have experienced the tunnel while outside their vehicles and so will not be familiar with the safety features available in the tunnel. However, given the speed with which a fire develops, their own actions towards self rescue will most likely determine their chances of survival.

Virtually all the tunnel users have personal communication devices. Many will call the emergency services for help and some could seek information from local information systems about the location of safe havens unaffected by the consequences of the unfolding incident. Some of the tunnel users may have medical problems that result in them carrying personal medical monitoring equipment and some of these may be disproportionately affected by the incident, requiring priority evacuation. Normally, a person with a medical problem would prefer to keep this information confidential, however the nature of the emergency means that some of those injured or having prior medical conditions will require priority evacuation. Commuters involved in the resulting traffic jams but not affected by the fire risk will also require information on the cause of the problems and anticipated delays or diversions.

As soon as the fire detection system within the tunnel picks up the fire and triggers an alarm, the tunnel operators have the responsibility to close the tunnel to incoming vehicles, activate the fire ventilation system and summon the emergency services. In the meantime, the operators should give information and orders to tunnel users by using the public address system.

To support emergency services, the tunnel operators need to provide information on the course of events, number/type of vehicles inside the tunnel, availability of access passages and possible change of operational mode of technical systems. Since the tunnel operators are remote from the devices being monitored or controlled, much of the control will be performed through generic computer interfaces as opposed to the sort of bespoke control mechanisms one might find in traditional embedded systems. Thus, tunnel operators must be insulated from the complexities of adaptive system behaviour in these environments, while retaining appropriate control.

On their way to the accident scene the rescue teams will be briefed on the situation by downloading the tunnel's details and operational options, although it is likely this information may be incomplete and the situation could change rapidly. The first major challenge will be to gain access to the tunnel. The traffic resulting from closure of the tunnel will present a serious delay to any road vehicle. Road infrastructures already allow traffic signals to be changed to facilitate access for rescue vehicles and there is little reason why this should not be coupled with information from vehicle networks that identify the fastest possible route.

On arrival, the immediate priorities are to establish the situation inside the tunnel in order to rescue survivors and tend to the injured without endangering the lives of the rescuers unnecessarily. To understand what the situation is within the tunnel, a variety of sensors will be brought into play. These will include CCTV cameras and fixed fire detection equipment but could also include sensors on people and on vehicles whose primary role was not the support of the emergency services.

In a very simple case, an engine management system that reports an engine is still running is indicating that there is sufficient oxygen to allow that system to run. Likewise, engine temperature sensors could be used to indicate the approximate location of a fire front. For example, the temperature and air quality sensors may take readings that would normally be considered erroneous due to being too high. There may be a need to download data from vehicle on-board systems, which would not normally make data available for security reasons.

Once the situation is sufficiently understood, the first rescue workers will enter the tunnel. Such personnel will have personal location devices and health monitoring equipment to allow the command and control outside the scene to recognise risk to their operatives. An alternative possibility is use of robots, which can be sent into the tunnel to locate hazards such as poisonous gases. Their sensing systems could be added to the network as required and they might have the facility to distribute sensors in areas where existing ones had been destroyed or rendered inoperative.

Rescue workers may also require temporary medical monitoring information on victims. Casualties with pre-existing conditions may already have some medical monitoring originally linked to their primary healthcare provider. Previously healthy people injured in the disaster may be fitted with medical monitoring devices at the scene because they are trapped, to provide historical data for when they can be evacuated and allow specialists to monitor their conditions.

Technical Implications

Because such emergencies can last from several hours to days and are highly dynamic, the response systems must adapt to the changing conditions, must be robust, must utilise the limited available resources efficiently and must provide accurate, timely, information requirements. A wireless sensor network, comprising low-cost, low-power wireless sensing devices throughout a physical area, can only meet part of the requirements and, therefore, a more complex network that supports an overlay of mobile and fixed wireless networks, existing networking infrastructure, and sensors/robotic services is required.

The problems associated with incompatibility of communication equipment of different emergency services are already known. In our scenario, these problems must be addressed in the context of personnel who not only have radios but also personal telemonitoring, handheld sensor devices and, in the case of paramedics, telemonitoring equipment for use with casualties.

Various sensors are expected to be available to collectively assess the situation as it develops, but a means is required to access the data from them and to provide control information back to them that dictates what data they capture. This is a challenge for several reasons. The first is the degree of heterogeneity in the system: the sensors will be of many different types, capabilities and ages; they will use different physical and MAC layer protocols; they may require continuous reconfiguration within the network as parts fail. Given the need to adapt response over time, the second challenge is to provide support for the semi-automatic uploading of software components and the dynamic retasking of nodes, some of which will not belong directly to the emergency services. Finally, both the capture of data and the control of the system must be achieved securely: if emergency services are allowed to retask sensors, then there is the possibility that the same retasking may also be achieved by malefactors or that the power to do this may be misused by errant emergency service personnel.

In traditional, distributed security, authentication is established after contacting a trusted authority responsible for maintaining up-to-date records of each user's access rights. However, in an emergency response case, communi-cation with this authority might be poor or impossible. In such a case, a best-effort security model may be appropriate, but it is unclear what this might look like and how effectively a balance can be achieved between the responsibility on the emergency services to preserve life and the liberty of the citizen as expressed through the right to exercise effective control over their surrogate computer devices.

In order for the surviving parts of the sensor and communication network to remain operational for enough time to allow the rescue mission to be completed successfully, the sensor nodes must be supplied with power. Replacement of batteries is often impossible or impractical and solutions relying on power scavenging could be of great value.

Health monitoring

Commercial health monitoring systems already exist, but are limited, for example, by carrying out the monitoring process only in a defined area (the patient's home or within a clinical environment) and there is no evidence of interoperability at present. In this use case we are examining widespread monitoring of healthy people (rescue workers) in order to check for the effects of heat, smoke, fumes, fatigue and injury. In addition, there is scope for monitoring of casualties who are trapped, cannot be evacuated, for triage purposes or to provide a record of health status from first contact with paramedics until arrival at hospital. Quickly identifying the most severely injured patients poses unique challenges, as does efficiently monitoring and transporting victims. Wireless vital sign monitor devices can be attached to victims to help throughout this process.

Security and privacy issues are important in emergency response systems, since medical records should remain private. However, in a large-scale emergency, particularly one involving rescue teams from many organisations, these concerns are likely to decrease in importance compared to those associated with dealing with data from large numbers of people, how to react when personnel or casualties show a significant change in status, and transferring data from patients to hospitals. A consensus is needed on what security and privacy may be relaxed.

For the road tunnel fire use case it may be more appropriate to consider using mechanical devices to identify areas where temperatures, chemical concentrations or other risks make it inappropriate for human presence, or to establish safe routes by mapping and characterising the infrastructure. The devices may have some on-board sensing capability but would also be able to obtain data from local sensors. The communication and middleware infrastructure should be able to assign priorities for the control and data transmission among the nodes of the network. There are several key factors to take into consideration when designing autonomous robots for rescue missions including perception, planning, navigation and learning and adaptation.

The RUNES Technology

Emergency response in road tunnels can be achieved through a composite of facility design, operating equipment, hardware, software subsystems and procedures. The software fabric of networked embedded systems tends to be ad hoc though, limiting the convergence of the above. Power, computational capabilities, and communication bandwidth limitations demand new approaches in software design. Embedded software components must be designed and reused at an abstraction level independent of the underlying hardware platform, operating system, and even programming language. These components must be small, simple and efficient so that the resulting systems are highly tailorable.

As part of the EC-funded project RUNES (www.ist-runes.org), a consortium of 22 partners has been designing and implementing software and hardware platforms that aim to deliver consistent mechanisms for configuring, deploying and reconfiguring networked embedded systems. The RUNES technology is ideal for addressing issues associated with: gaining an understanding of the environment resulting from natural or man-made disasters; for assisting the command authorities in understanding the situation of people and assets in the emergency zone; and for allowing tasks to be carried out to locate or rescue victims, in many cases using systems that are already present at the scene and that can be used for purposes for which they were not originally designed.

Apart from designing middleware, networking protocols, wireless gateways and robots, we believe it is necessary to build demonstrators in order to test the feasibility of the proposed architecture in real settings. The road tunnel fire use case, which is the subject of a RUNES project demonstrator, combines both the developing market of emergency response and the proven area of medical monitoring in an application that does not require the use of patients.

Since the all-important testing during the development phases in large or specialised locations is both prohibitively expensive and time consuming, we have also given emphasis to simulators that enable test tactics and strategies without risking lives and property. They allow evaluations to be conducted under a number of degraded system conditions (bandwidth, connectivity, preferred I/O missing etc.), and we expect it to play a significant role in mission preparation, rehearsal and training.