D5.2 – TERTIARY SYSTEM ARCHITECTURE

Project Acronym:	**Smart RRS**
Project Full Title:	**Innovative Concepts for smart road restraint systems to provide greater safety for vulnerable road users.**
Grant Agreement No.:	**218741**
Responsible:	**Robert A Pinnock, Principal Product Engineer** **Peter E M Frere, Principal Product Engineer** **TRW Conekt**
Internal Quality Reviewer:	**Mouchel**

Status	**Changes**	**Version date**
Provisional	Version circulated prior to the Brussels review	12 Jul 10
Final Review	Addition of explicit details of the AHP process (rather than just a reference to the document describing the process). Summary revamped.	29 Sep 10
Final, final review!	Post Mouchel review of 17 Nov 10. Additional notes about radio topology included in Overview and Gateway Module Requirements sections. Notes about the control of power to the RF sub-system included in section 3.2.2. Reasons for choice of location (i.e. on post) enhanced in Section 7.1. Also included comments about number of sensors per unit length of barrier (7.1). Additional sensor module requirements relating to sensor spacing, sensitivity and discrimination included. Added points in section 3.2.2 item 2 about the need for local signal processing and the fact that the algorithms will be developed during the project. Added new section 5 about the Vehicle Activated Display Emulation. Conclusion and Summary expanded.	19 Jan 11
For release	Mouchel's formal quality review with minor modifications	15 Feb 11

SUMMARY:

The Smart RRS Tertiary Safety System is intended to identify when a barrier collision has taken place and then to alert a control centre whence appropriate action from the emergency services can be initiated.

This document is intended to take the requirements and to identify a first level system architecture that will achieve them – identifying the functionality of a number of modules and sub-systems. From these requirements it proposes a Tertiary Safety System based around a gateway module monitoring the output of a number of crash sensing modules. The sensing modules are arranged as a star network with the gateway - all communications taking place through the gateway at the hub of the network.

The key modules for the system are the sensing modules, the gateway, a control centre, an emulation of a vehicle activated display and an approaching vehicle sensor.

The crash sensing module detects when a crash event takes place. The gateway forms the communications hub for the system. The control centre is the place where crash alerts are displayed for human action and intervention. The display and approaching vehicle sensor provide the means by which oncoming traffic is warned that a barrier collision has taken place.

The crash sensing modules will comprise crash sensors (a combination of accelerometers and acceleration sensing switches have been identified as the best candidates for this task); a processing function to check acceleration data for false triggers and to provide some measure of crash intensity as well as controlling the power and communications sub-systems; a radio subsystem to communicate using a wireless personal area network (WPAN) protocol with the gateway and a power subsystem to provide long-term power to the sensing module. The document argues that these modules should be mounted on the posts of the crash barrier.

The gateway will monitor sensing modules using a WPAN protocol and communicate to a remote control centre using GPRS. In addition to communication functions, the gateway module will also provide some logic for controlling a vehicle activated sign, based on data from the sensing modules combined with detection of approaching vehicles. The gateway will also have the function of providing some time synchronization for the sensing modules.

The control centre will store status data from the sensing modules and provide means for examining this data as well as displaying an appropriate alert to control centre staff when a crash has taken place.

Contents

Figures

Tables

1. INTRODUCTION

This document gives an overview of the architecture for the Tertiary Safety System and identifies the requirements on the various sub-systems.

This document is aimed primarily at defining the sub-systems for the demonstration systems. Where these are likely to be significantly different from a production system the document makes this clear.

Top level requirements for the system (from D5.1) are as listed in the following sub-sections.

1.1 TOP-LEVEL FUNCTIONAL REQUIREMENTS

FR.1. During installation, it shall be possible to register the location of each data source (e.g. sensing node) and to store that location at each data source.

FR.2. The system shall detect or infer that a barrier collision has taken place.

FR.3. The system shall be capable of distinguishing between different crash severities. Note that discrimination between different kinds of vehicles or number of vehicles is anticipated to be very difficult to achieve. Such discrimination may be a future goal achieved only through the gathering of a large amount of operational data.

FR.4. The system shall communicate to a control centre. It shall communicate:

a. That a barrier collision has taken place.

b. An indication of the severity of the event. This is likely to be limited to such measures as the number of sensors triggered by the crash event, the duration of the event and the magnitude of the signal during the event.

c. The location and time of the collision.

d. Within a few seconds of the event taking place. The exact timing will be dependent on the latencies in the communication sub-systems. It is anticipated that these will be investigated during the course of the project.

Consideration needs to be given as the project progresses to the issues of both false and missed detections which might undermine the credibility of any practical system.

FR.5. The system shall be capable of demonstrating how it might communicate to drivers approaching the road section on which the system is installed. It shall communicate an appropriate messages relating to the crash event using the messaging system to be developed and demonstrated in the Primary Safety System.

Note that this aspect of the demonstration may only be a simulated representation of messages away from the roadside – for example displaying simulated roadside messages on a remote laptop monitor.

FR.6. The system shall be capable of investigating how it might communicate to an approaching driver in a timely manner (as per the Primary Safety System).

FR.7. The system shall also communicate to the traffic control centre more detailed messages as shall be necessary for monitoring the performance of the system itself.

FR.8. The traffic control centre shall have means to display and store the data received from the system.

It may be possible for the traffic control centre to request additional information from the system, for example (if appropriate to a future implementation) still images from a camera. It is unlikely that this will be demonstrated within the scope of this project.

FR.9. It shall be possible to remotely request simple diagnostic information from each element within the system.

1.2 TOP-LEVEL OTHER REQUIREMENTS

OR.1. At least the sensing part of the Smart RRS system shall be mounted on the crash barrier.

OR.2. The mounting of any part of the Smart RRS system on the barrier shall not present an additional hazard to a PTW or other vulnerable road user in collision with the barrier.

OR.3. The mounting of any part of the Smart RRS system on the barrier shall not interfere with the containment or energy absorption functions of the barrier.

OR.4. The system shall make minimal demands on the wired infrastructure for power.

OR.5. The system shall make minimal demands on the wired infrastructure for communications with road users and traffic control centres.

OR.6. All external (outdoors) elements of the system shall meet a rating of IP54.

OR.7. All external elements of the system shall be able to withstand an ambient temperature range commensurate with homologation requirements for roadside infrastructure.

OR.8. The system shall comply with EMC standards called for by the homologation requirements for roadside infrastructure.

2. OVERVIEW

The tertiary safety system will consist of 4 modules:

- A sensing module that detects and evaluates the crash event and communicates it to the Gateway (GW) module.
- A GW module that gathers data from a number of sensing modules and passes it back to the control centre. It might also take commands or data from the control centre and forward those to the sensing modules.
- A control centre which is the point within the Smart RRS system to which crash alerts are ultimately sent. This will also monitor the performance of the other modules and allow simple diagnostics of these to take place.
- A Vehicle Activated Display emulator which will be able to inform oncoming vehicles that a barrier collision incident has taken place.

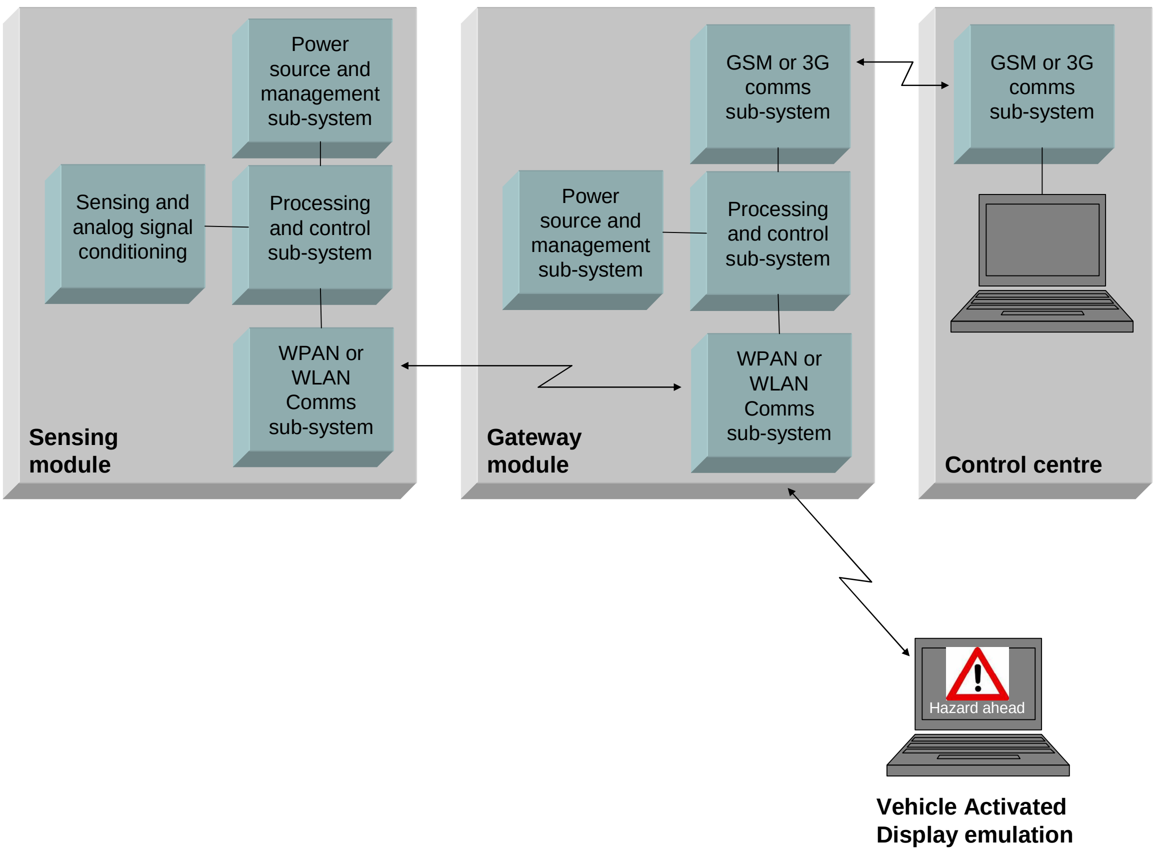

Figure 1: Top Level View of Tertiary Safety System

The system will use a "star" topology with the GW module as the hub for all communications and the sensing modules communicating only to the gateway (rather than allowing peer to peer communication between the sensing modules). This is in order to keep the system simple for the purposes of demonstration and to minimize the power requirements of the sensing modules.

Communications between the GW module and the sensing modules will be initiated by the sensing modules – i.e. they will communicate either when they have information to transmit or at a fixed time interval for status updates. This relieves the sensing module of the power-burden of an RF receiver continually listening for data requests from the GW module. Information communicated by a sensing module is automatically passed through to the control centre.

Each of the four modules (Sensing, Gateway, Vehicle Activated Display and Control Centre) is considered in more detail in the following four sections of this document.

3. SENSING MODULE DESCRIPTION

3.1 SENSING MODULE REQUIREMENTS

The sensing module requirements listed below are derived from the "top-level" requirements given in Section 1. Some additional "desirable" features are also listed below: whilst not "requirements" as such, these are things which may also help to drive the choice of system components and architecture.

Requirements (must haves) for tertiary safety system sensing module:

SMR1 – The sensing module shall detect (or infer) that a collision has happened.

SMR2 – The sensing module shall be capable of distinguishing between different crash energies (intensities).

SMR3 – The sensing module shall be able to derive a figure representative of crash energy which it can communicate to a control centre.

SMR4 – The sensing module shall be attached to (mounted on) the crash barrier.

SMR5 – The sensing module shall not [in itself] represent an additional hazard.

SMR6 – The sensing module shall not adversely interfere with the safety / energy-absorbing functionality of the crash barrier.

SMR7 – The sensing module shall make minimal demands on the wired infrastructure for power.

SMR8 – The sensing module should be able to survive roadside environmental conditions.

SMR9 – The sensing module shall be capable of detecting a "minimum detectable event" (see note below).

SMR10 – The sensing module shall be capable of distinguishing between a "minimum detectable event" and noise events such as vibration induced by passing vehicles, wind or even maliciously generated vibrations such as a post being hit by a hammer.

It is suggested that a "minimum detectable event" should be the minimum event which produces permanent deformation of the barrier rails or their mounts. Note that the magnitude of a "minimum detectable event", the maximum sensor spacing, the required sensitivity of the crash sensor, and the characteristics of noise events will be investigated and determined through the course of the project.

Desirables (nice-to-haves) for tertiary safety system sensing module:

SMD1 – The sensing module may be able to determine [more information about] the nature of the crash event (for example, vehicle types).

SMD2 – The sensing module may be developed into a product – implies that the sensing module may be: (i) integrated with the "crushable" part of the Smart RRS barrier assembly or alternatively be a standalone unit independent of the energy absorber; (ii) novel (no prior art or IP).

SMD3 – The sensing module cost should be minimized.

SMD4 – The sensing module should be powered through energy harvesting techniques if battery life is insufficient.

3.2 SENSING MODULE SUB-SYSTEMS – REQUIREMENTS, CONSTRAINTS AND OPTIONS

A simplified diagram of the Smart RRS Sensing Module generic architecture is shown in Figure 2. The architecture is split into sensing, processing and radio sub-modules, the constraints and options for which are described in the following sub-sections.

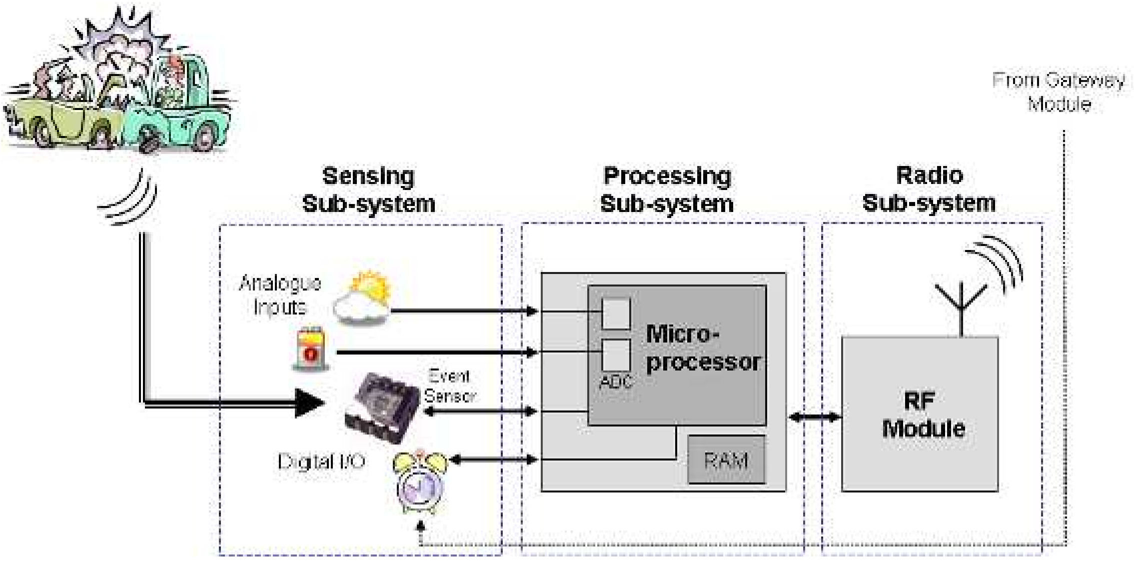

Figure 2 : Smart RRS Sensing Module Simplified Generic Architecture

3.2.1 SENSING SUB-SYSTEM

The purpose of the tertiary safety system sensing sub-system is to detect the occurrence of crash events and enable data to be gathered during such events. The data gathered should be such as to enable subsequent processing that will, as a minimum: (i) confirm that a crash has occurred; (ii) determine (in some manner) the "size" of the crash event.

Simulated crash event data provided by the University of Zaragoza[1] shows that considerable displacements, velocities and accelerations are imparted both to the horizontal crash barrier structure and to the support posts: common experience also indicates that there is an acoustical signature associated with a crash event. One or more of these parameters may be sensed by the sensing sub-system to provide the required indication of the crash event.

In considering possible sensor types for this application, a number of things must be considered. These include:

- Can the sensor provide data which can be processed to determine: (i) if a crash event has occurred; (ii) the "size" of the crash event? How complex is processing the sensor signal to extract this data likely to be? (Note – it is acceptable that an individual sensing module may not be able to determine the size of the crash event on its own, but that it can do so in combination with other adjacent sensing modules. This allows the use of simple switches to be considered as possible sensing elements). For analogue sensors, is any form of signal conditioning (gain / offset control, filtering, etc.) required prior to analogue-to-digital conversion?

[1] Document: Dummy_impact_results.doc; 15 January 2010;

- What are the power requirements of the sensor? Does it need power at all? Does it have low-power operating modes? How long does it take to "wake up" and settle following a period in a low-power or "sleep" mode?
- What sort of packaging is required to enable the sensor to operate in the environment? Can the sensor (at least in principle) survive a crash event?
- How does the sensor operate? How does it respond to the type of physical parameters which are available to be sensed when a crash event occurs? How must the sensor be mounted on the crash barrier structure? How many sensors will be necessary to ensure that no crash events are missed?
- How much does the sensor cost?
- How novel is the use of the sensor in this type of application? Are there IP issues which may prevent its use in future production systems?

The process which has been used to select the most suitable sensor for the sensing sub-system is summarized as follows:

- Brainstorm potential sensor types which could conceivably meet the key requirements of being able to detect the occurrence of a crash event, and provide some sort of measure of the size of the crash event.
- Perform an initial evaluation of the sensor types identified in the brainstorm process against the general issues for consideration bulleted above. The purpose of this step is to reduce the number of sensor types under consideration to a more manageable proportion.
- Perform a more rigorous and systematic analysis of the selected sensor types against a carefully evaluated set of criteria derived from the system requirements and the "things for consideration" above. The technique used for this step is called the "Analytical Hierarchical Process" (AHP). AHP is a structured technique used to help determine the best solution to a complex decision, where multiple potential solutions need to be assessed against multiple – and possibly conflicting – criteria and constraints. The technique, and the way it has been implemented to help determine the best sensor type for the Smart RRS tertiary safety system sensing sub-system, is described in detail in a separate report[2].

By way of a summary of the AHP, Table 1 shows the shortlist of candidate technologies that were considered, Table 2 gives the criteria against which the candidates were evaluated and Figure 3 gives the results of the process. It can be seen that the post mounted accelerometer, the travelling acoustic signal and the inclinometer all scored well along with a simple extensometer idea. The latter concept was later discarded on grounds of reliability. The former three concepts can all be considered to be forms of accelerometer.

The Tertiary Sensor Selection process also went on to evaluate a number of switch-based concepts which all scored highly from the point of view of low power consumption.

The final system will carry forward both the ideas of using some form of accelerometer and a switch based sensing trigger.

[2] **R A Pinnock, P E M Frere**; *Tertiary Sensor Selection*; 57536-17c Ver 1 28May20 Tertiary Sensor Selection.doc

Table 1: Candidate technology shortlist for Tertiary sensor selection

S1:	Acoustic Microphone	A support-post-mounted microphone will detect the acoustical noise generated during a crash event.
S2:	Accelerometer (on post)	A support-post-mounted accelerometer will detect the barrier motion generated during a crash event.
S3:	Camera	A camera (suitably triggered) can record images of a crash event
S4:	Wire Extensometer	A wire (or wires) running along the length of the crash barrier will be extended during a crash event as the barrier distorts. A potentiometer or encoder can measure the amount of extension.
S5:	Travelling Acoustic Signal	Accelerometers (or microphones) mounted at intervals along the crash barrier can detect crash-induced vibrations travelling along the barrier.
S6:	Piezoelectric "Pad"	A pad of piezoelectric material mounted inside the energy absorbing part of the barrier system will generate a voltage "spike" when a crash event occurs.
S7:	Inclinometer (on post)	Sporadic interrogation of a support-post-mounted inclinometer will indicate when the post has been displaced as a result of a crash event.
S8:	Load-sensing Bolts	Load-sensing bolts used to join the sections of the crash barrier together will detect barrier distortions resulting from crash events.
S9:	Magnetometer	A magnetometer will detect the near-approach of vehicles to the barrier, indicative of a crash event.

Table 2: Criteria for evaluation Tertiary sensor candidates

C1:	Signal to Noise	The more easily the sensing system can distinguish a crash event from extraneous noise (e.g. noise of passing traffic), the better (from R1)
C2:	Information Content	The more crash information that can be derived from the sensor data, the better (from R2, D1 and D4)
C3:	Ease of Data Extraction	The more easily the crash data can be derived from the sensor data, the better (from R3, D3 and D5)
C4:	Range of Detection	The longer the range over which a sensor can detect a crash, the better (from R1, R4 and D3)
C5:	Suitability for Integration	The more easily the sensing system can be formed into an integrated product, the better (from R4, R5, R6 and D2 (i))

C6:	Novelty	The more novel the proposed sensing technology, the better (from D2 (ii))
C7:	Inexpensiveness	The less expensive the proposed sensing technology, the better (from D3)
C8:	Crash Robustness	The more capable of surviving a crash event the sensing system is, the better (from R7)
C9:	Low Power Operation	The more capable at operating at low power levels the sensing system is, the better (from D5)

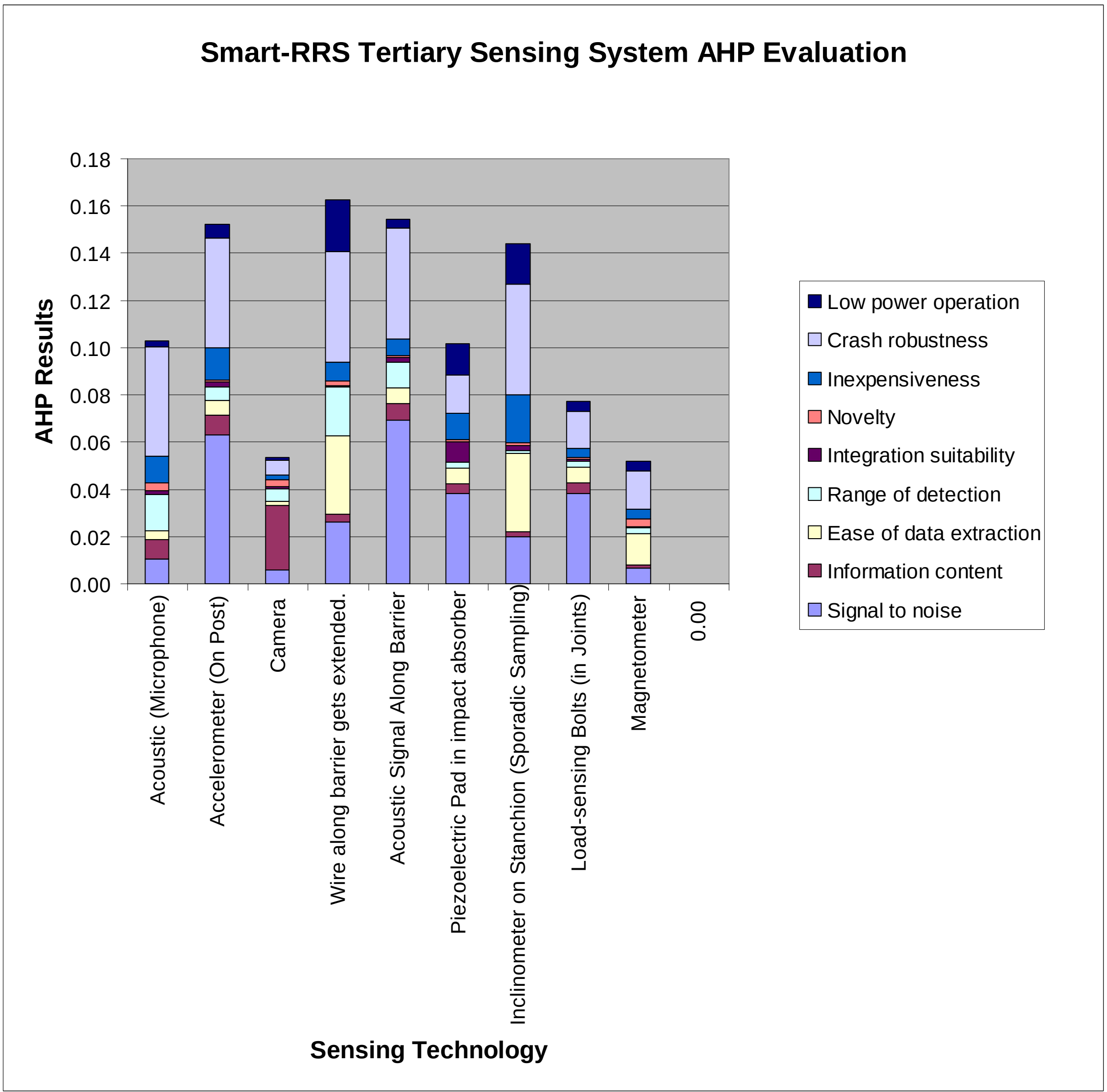

Figure 3: Results of AHP for Tertiary sensor selection[3]

[3] The scale of Figure 3 is a relative one and is used as a comparison scale for each technology. The size of each rectangle (a different colour for each criterion) reflects not only how well the technology scored for this criterion but also the relative weighting given to that criterion.

In addition to the actual crash sensor, additional sensor channels (for example, battery power level, ambient light level, etc.) may be desirable for system status updates, etc.

3.2.2 SIGNAL PROCESSING SUB-SYSTEM

The purpose of the tertiary safety system signal processing sub-system is to identify, from the sensing sub-system signal, when a crash event is occurring, and to derive some measure of the "size" of the crash event. It also needs to control the data gathering and data transmission system functions. The processing sub-system needs to derive appropriate data for subsequent transmission over the wireless link to the GW module.

The essential tasks of the processing sub-system are as follows:

1. Sample / receive sensor data from the sensing sub-system (which may be in analogue or digital form). For analogue sensors, an analogue-to-digital converter (ADC) will be set to sample at some specified sampling rate and to convert the sampled signals to digital format. The ADC may be a peripheral found on a microcontroller, or could be a stand-alone device, depending on how the processing is implemented and the specification of the conversion (sample rate, number of bits etc.)

   Required sampling rate will depend on: (i) the allowable time period between the initial occurrence of a crash and the start of data collection; (ii) the bandwidth of "features of interest" within the crash signature.

   Required sample resolution will depend on required fidelity of transmitted data for crash analysis.

   The number of channels required (per sensing sub-system) will depend on: (i) the selected type of crash sensor (for example, it might be that a two- or three-axis accelerometer is selected, rather than a single-channel) device; (ii) any additional signals which may be monitored (for example, ambient light levels, battery voltage, etc.)

2. Process and interpret the sensor data to identify: (i) that a crash has occurred; (ii) the "size" of the crash.

   The precise features of the sensor crash signature which will enable the system to recognize a crash condition need to be established. Possible candidate features of the sensed crash signature are:

   – signal amplitude (either occurrence of signal or change in level)
   – signal rate of change
   – occurrence of or amplitude of particular frequency components
   – the general frequency characteristic

   For lowest complexity, non-frequency-based analysis (such as the first two features identified above) will be used for crash recognition, provided suitable signal thresholds can be set to enable this to be achieved without too many false crash events being identified (for example, through the occurrence of extraneous noise from traffic or other sources). For more detailed crash analysis (for example, identifying the type of crash, the vehicles involved, and so on), some form of frequency analysis may be needed.

   For the envisaged applications, the data processing will probably be handled by the capabilities of the microcontroller alone, but if more complex signal processing is required (for example, frequency analysis by FFT), additional hardware may be required. However, low-power microprocessors, such as the MSP430 range from Texas Instruments, are available which should be capable of performing the type of analysis required for crash recognition in the Smart RRS tertiary safety system. Some versions of the MSP430 range include hardware multipliers and other peripherals such ADCs and comparators (for example, the MSP430x5xx family of devices), potentially capable of doing all the required analysis in low power operating mode.

Note that it is important that the signal processing takes place at the sensing node in order to minimize the data-traffic needed to be sent to other parts of the system. Minimizing the transmitted data is a key technique for reducing the power consumption of the node (and the system as a whole) as RF transmission is relatively wasteful of power.

Note also that the exact nature of the processing of the sensor data will determined through the course of the project and cannot be specified at this stage.

3. Control the "system wake-up", data gathering and data transmission functions. The precise nature of this control will depend on the wider system architecture and functional partitioning.

   Several questions need to be considered when establishing a "wake-up strategy" for the Smart RRS tertiary safety system. These include:

   - How quickly does the system need to wake up in order to capture the important parts of the crash signal?
   - Is a separate sensing system required in order to wake the system or can the crash sensor itself be used to wake the processor up, for example when a certain crash amplitude has been reached?
   - Does the system need to be woken up or is the current consumption while it waits for an event to happen low enough?

   The answers to these questions will depend on analysis of crash signatures to determine at what point features of interest occur during a crash event, but initial analysis of modelled crash data suggests that this period is likely to be of the order of ten milliseconds. Waking up a microprocessor from a stand-by mode typically might take only a few µs (or even less). However, some "settling time" will also be required for the crash sensor (whichever sensor technology is chosen) if it is not left operating continually: for MEMS-type accelerometers, for example, this is likely to be of the order of a few milliseconds.

   In terms of wake-up strategy, a number of options are possible and need to be evaluated, for example:

   - Continually-repeated interrogation: in this case, the system "wakes up" at repeated intervals and interrogates the crash sensor input to check for crash events
   - System wake-up on interrupt: in this case, the system remains in quiescent mode until some form of interrupt or trigger signal (which indicates a crash event is occurring) is received.
   - "Always on" system front end: in this case, the crash sensor and front-end conditioning electronics are continuously powered: the sensor effectively triggers the microprocessor when a crash event occurs.

Another aspect of the system wake up control is the need to control the power to the radio sub-system. The radio sub-system will be on only when the sensing module has a message to transmit. Thus the radio sub-system will not remain on to *listen* for messages from the gateway.

3.2.3 RADIO SUB-SYSTEM

The choice of wireless protocol will depend on several factors, including:

- Range over which data must be transmitted (sensing sub-system modules to GW modules)
- Amount and frequency of data transmission
- Power requirements (transmission power and power management functionality)
- Cost and availability of components
- System topology and operating mode
- Degree of vendor support / level of familiarity and expertise already present within Smart RRS consortium

For the tertiary safety system, the following types and approximate frequencies of transmit and receive messages are anticipated:

- Gateway to sensing module (~ once per day): status request and time re-synchronisation
- Sensing module to Gateway (~ once per day): status update
- Sensing module to Gateway (occasional - ~ once per year?) processed crash data

Each message may include additional bytes for additional features such as message ID, sensor ID, forward error correction, time data, etc. However, analysis (see Table 3, Section 4.2.5) of all the message sizes by their corresponding frequency of transmission and number of sensing nodes per gateway for all Smart RRS module types (including crash sensing module) gives a total average data rate of about 61 bit s^{-1} .This is extremely low and allows for the choice from among a wide range of low bandwidth wireless technologies to communicate with the sensing nodes.

A number of wireless protocol options are being evaluated, including:

- ZigBee (many vendors; many module options)
- Bluetooth (as ZigBee)
- DASH7 (433 MHz low bandwidth protocol with extended range; (very) limited number of vendors)
- WiFi (802.11 standard – long range but more power-hungry; many vendors and module options)
- Proprietary 802.15.4-based protocols (many variants available from many vendors)

The choice of wireless protocol will depend not only on the general system requirements, but also on the need to communicate reliably with the GW module which is intended to be an off-the-shelf product: hence, the choice will in reality be limited to those protocols which can be supplied by the supplies of the GW modules which are currently being evaluated.

3.2.4 POWER SUB-SYSTEM

In order to minimizing system cost and installation complexity it is expected that the Smart RRS tertiary safety system will be battery-powered rather than making use of existing wired infrastructure. Two options for powering the systems are envisaged:

- Battery power alone
- Battery power "topped up" with additional power derived from power scavenging

The choice between these two options will depend on the total power levels required for the system to operate successfully over a time period of at least 10 years. A range of factors will determine the potential for achieving this operational period; for example:

- Sensing Sub-system Sensor:
  - Excitation requirements (voltage, current…)
  - Availability of "low power" or "sleep" operating modes (and corresponding "wake-up" characteristics…)
  - Other operating characteristics (bandwidth, number of channels…)
- Sensing Sub-system ADC /Microprocessor:
  - Power requirements (voltage, current…)
  - Availability of "low power" or "sleep" operating modes (and corresponding "wake-up" characteristics…)
  - Other operating characteristics (resolution, sampling rate, filtering…)
  - Data processing requirements (amount of processing, type of processing…)
  - Data storage requirements at sensor node (how much, how often…probably not required for Smart RRS tertiary safety system)?
- Sensing Sub-system Wireless Transceiver:
  - Transmission power (depends on range, environment, legislated limits…)
  - Time spent in different operating modes (transmit, receive, "sleep"…)
  - Amount of data (number of data bits, overheads…)
- GW Module:
  - In Smart RRS case, this will also be powered by battery or battery with scavenged power. The powering will be separate to that used by the sensing sub-system, but the operation of the GW module will have some effect on the sensing sub-system operation (frequency of up-dates, etc.), and hence on its power requirements.

For demonstration purposes, it is unlikely that the sensing sub-system will require a power scavenging system since the demonstrations will take the form of limited number of planned events. The actual product will need to operate continuously for many (≥ 10) years so that power management will be important. The demonstration system will show how it can operate from a limited power budget. Appropriate choice of components and system architecture in terms of the factors identified in the bullet points above may enable the eventual product itself to operate only from battery power: this would simplify the system considerably.

In the event that power scavenging technology is required to "top up" the available power, the most likely option is to make use of solar-derived power. Initial calculations suggest that, using this technique, for a horizontally mounted 100 cm^2 solar panel, an average of 170 mW of power[4] should be available throughout the year, with the minimum being around 30 mW in the worst (winter) months.

In order to utilize solar-derived power, appropriate power conditioning circuitry will need to be incorporated in the sensing sub-system. Off-the-shelf components are available for this type of application: these are currently being investigated.

[4] This figure comes from the Smart RRS D4.1 requirements document and represents the power averaged over both day and night *throughout* the year. The figure of 30 mW quoted in the same sentence is based on the fact that the average solar irradiance for December is less than a fifth of the average power for the year.

4. GATEWAY (GW) MODULE DESCRIPTION

4.1 GATEWAY MODULE REQUIREMENTS

The GW module is intended to aggregate data from a group of sensing modules in its vicinity using an appropriate wireless personal area network (WPAN) or local area network (WLAN) protocol. It then communicates this data to the control centre module via a long distance communication technique such as GSM-based technology.

The aim is to purchase an "off-the-shelf" GW module for the Smart RRS demonstration systems. A number of suppliers of such modules have been identified. Evaluation of the different product offerings is currently on-going to identify the best option.

4.1.1 INSTALLATION FUNCTIONAL REQUIREMENTS

Ideally, there will be a mode for installation during which each sensing module can be identified, located and registered in a database (both at the GW module and the control centre). Automation of this process would be beneficial, but this might involve the integration of a GPS receiver in each sensing node. It is likely that this process will be carried out semi-manually (e.g. the installer entering location and identification code of each node into a PDA or the like) with the data being uploaded into the system prior to it's becoming live.

In addition to the system knowing the location of each sensing module, the communication network between the sensing module and the GW module needs to be set up. The exact nature of this task depends on the particular wireless protocol chosen.

4.1.2 OPERATIONAL FUNCTIONAL REQUIREMENTS

This section lists the top level operational functional requirements for the GW module. Note that the GW module is common to both the Tertiary and the Primary Smart RRS safety systems. Thus, some of the requirements are more appropriate (or, indeed, only appropriate) to one or other of these safety systems.

GFR1 The GW module shall be capable of communicating with up to 25 sensing modules.

GFR2 The GW module shall be capable of an aggregate communication bandwidth with the sensing modules of at least 1 kbit s^{-1}.

GFR3 The GW module and the sensing modules shall form a star network with the GW module as the hub or centre of the star.

GFR4 The GW module shall be capable of sending data to and receiving data from the following sensing modules: a crash sensing node, an environmental sensing module and an obstruction sensing module

GFR5 The GW module shall be capable of maintaining a time reference (Accuracy to be determined through the course of the project). It will be necessary to determine if it is sufficient just to communicate a single clock timing to the sensing nodes and for the control centre to monitor these and make allowances for GW module clock drift).

GFR6 The GW module shall receive daily status requests from, and at the same communicate time sync data to, each sensing module (The spacing of these events across a day will be determined through the project).

GFR7 The GW module shall receive event or risk data from each sensing module and communicate that immediately to the control centre.

Figure 4 illustrates the operation of the GW module in normal operation. Note that, for the demonstration system, it is not intended that communication from the control centre to the GW module will be demonstrated. In a real system, the ability to make such communication may be necessary. For example, it will be necessary to "cancel" a displayed message indicating that a crash event has occurred once the carriageway has been cleared (as indicated in Figure 4): in a real system, such a cancellation request is likely to come from the remote control centre, being passed via the GW module to the display sign. For the demonstration system, this functionality is likely to be implemented simply via a "cancel display" button on the vehicle-activated display emulation (lap-top).

Situations can also be envisaged where it might be useful for requests for "additional data" to be sent from the GW module to one or more sensing modules at times other than the normal "once-per-day" intervals. However, this functionality will not be implemented in the demonstration system.

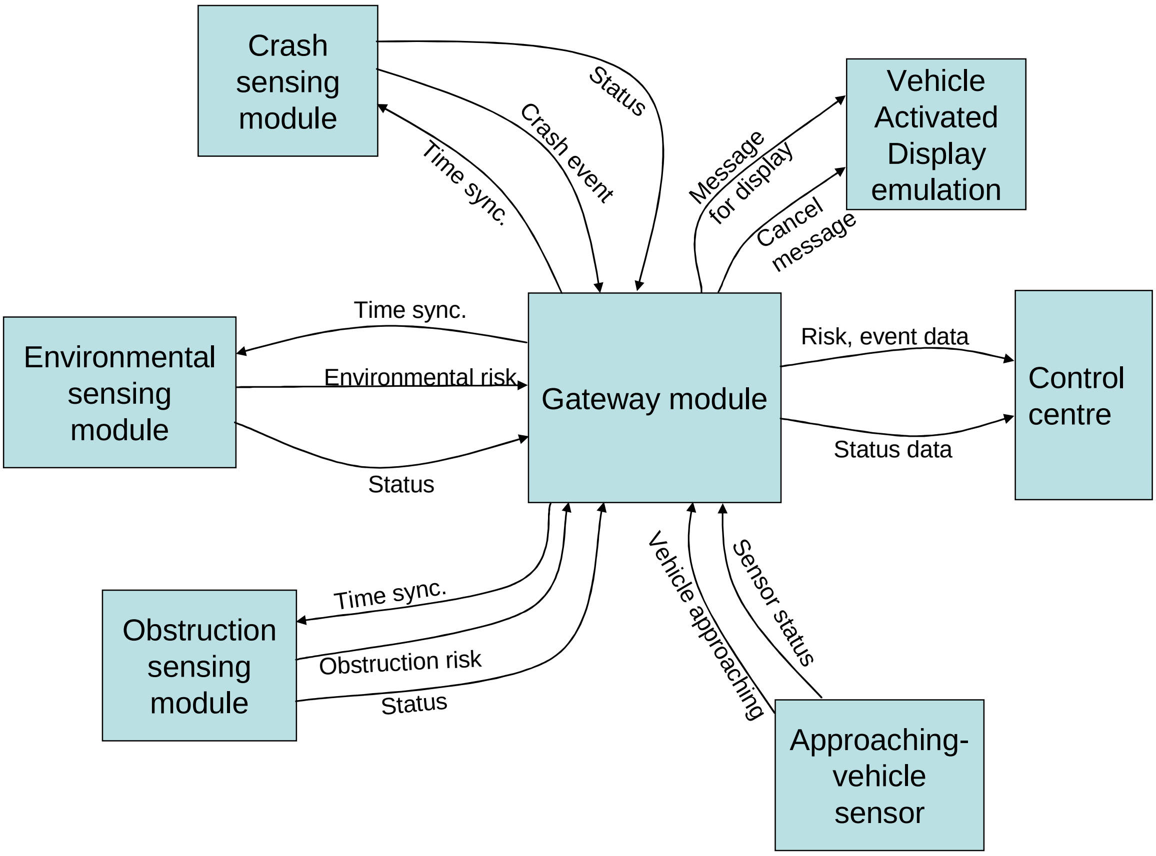

Figure 4: Gateway Message Traffic in Normal Operation

4.1.3 SERVICE FUNCTIONAL REQUIREMENTS

GFR8 The GW module shall generate its own status information which it will communicate back to the control centre along with the status information of the other modules.

Note that no specific service mode is envisaged for the purposes of the demonstration system.

4.1.4 OTHER REQUIREMENTS

Size and location requirements

GOR1 There shall not be more than 5 GW modules per kilometre.

GOR2 The GW modules shall be located such that they can communicate with a control centre (for a GSM-based system this implies within line-of-sight and range of a GSM basestation).

Resource requirements

GOR3 The GW module shall make minimal demands on the wired infrastructure for power.

GOR4 The gateway shall make minimal demands on the wired infrastructure for communications with road users and traffic control centres.

The requirement GOR3 implies that battery and / or power scavenging techniques will be required for the system. Requirement GOR4 implies a wireless communications system.

Environmental Requirements

GOR5 The GW module shall be designed to withstand the roadside environment for the duration of the demonstration.

Economical Requirements

No specific requirements are given but the design process shall bear in mind that that this is to be a low-cost system.

4.2 GATEWAY (GW) MODULE SUB-SYSTEMS – REQUIREMENTS, CONSTRAINTS AND OPTIONS

A simplified diagram of the Smart RRS GW Module generic architecture is shown in Figure 5.

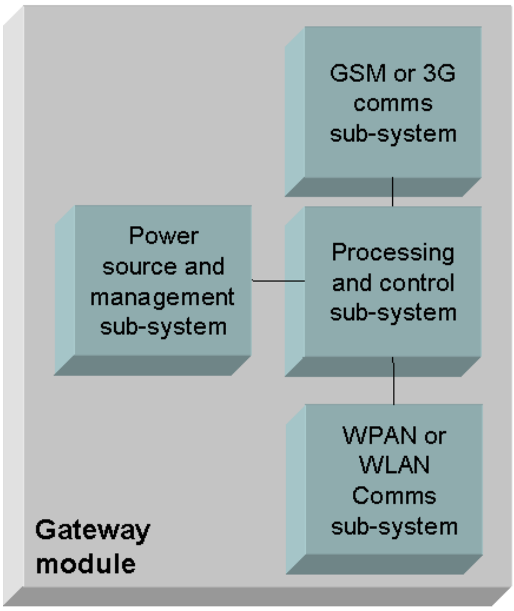

Figure 5 : Gateway Module Generic Architecture

The GW module will interface with the sensing modules using a wireless RF protocol, effectively operating as a personal or local area network.

Long range connection to the control centre will be using standard mobile phone technology (GSM / GPRS).

At present, it is anticipated that the processing tasks of the GW module will be relatively limited. Its primary tasks will be to pass data between the sensing modules and the control centre, and to maintain time synchronisation between itself and the sensing modules.

The GW module links wirelessly to several sensing modules on the one hand, and to the system control centre on the other. It therefore has to receive the data from the various sensing modules, manipulate it appropriately (for example, remove any overhead data, and – possibly – undertake additional data processing in addition to that done at the Sensing Module), and present the data as appropriate for transmission to the Control Centre. The GW Module may also act in the reverse direction: to transmit signals or commands sent from the Control Centre to the Sensing Modules to control their operation. Data communications may be via one or more types of RF link.

These main tasks of the GW Module are discussed in more detail below.

4.2.1 CONTROL OF SENSING MODULES

Each GW Module acts as the 'access point' for the Sensing Modules in its vicinity. It controls "membership" of the Sensing Modules to its "local" wireless network and manages local security. Assuming a wireless link between the GW Module and the local Sensing Modules (and also assuming no wireless communication between Sensing Modules), the number of Sensing Modules handled by each GW Module will depend on the maximum wireless transmission range. This document defines the maximum number of Sensing Modules per GW Module as 25 (see GFR1 in Section 4.1.3): for example, assuming a maximum wireless transmission range of 50 m and a Sensing Module spacing of 4 m, each GW Module will (in principle) control 25 Sensing Modules in a star network formation (also a requirement – see GFR3 in Section 4.1.3).

Any configuration information for the Sensing Modules will also be generated by, or relayed through, the GW Module. Some of this may be autonomously handled by the radio PHY and MAC (for example, autonomous control of the RF transmitted power), but other higher-level information (for example, calibration values for sensors or control instructions to start and stop the Sensing Modules) will be handled by GW Module.

4.2.2 DATA RECEPTION, PROCESSING AND FORWARDING

The data received at the GW Module from the Sensing Modules will need to be processed to remove any unnecessary overhead information. This might include error correction, decryption, de-compression or other signal processing functions. Again, some of these functions (for example, error correction) may reside in the radio PHY and MAC layers, but others will need to be provided by the GW Module. The processed data will then be forwarded to the system Control Centre.

4.2.3 SYNCHRONIZATION

The reference clock for the system will be contained within, or referenced by, the GW Module. Multiple GW Modules within a complete system will also need to be synchronized (for demonstration purposes, this might be managed by a single 'master' GW Module). Each GW Module will then communicate with its local Sensing Modules as appropriate, to enable all clocks on the Sensing Modules to be synchronized to the reference.

4.2.4 BULK STORAGE

If required or desirable (perhaps for demonstration purposes), the GW Module could potentially provide fixed or removable data storage capacity.

4.2.5 DATA FLOWS

In order to estimate the amount of data traffic each GW module must handle, Table 3 has been constructed. Note that this table covers the GW message requirements for all types of sensor module (that is, primary safety system environmental and traffic obstruction sensing message requirements as well as those associated with the tertiary safety system). The table is not definitive for the system – it is only a tool to provide an estimate for the amount of data traffic.

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
Crash Event			15	1.1E-04	10	Message from crash sensing module to the GW module when a crash event occurs.
	Message ID	1				Code that identifies this message as a crash event.
	Packet ID	1				Identifier for this instance of this message. A bit like the rolling counter, it's not clear how important this is for these single packet messages.
	Sensor ID	1				Code uniquely identifying the crash sensing module. 1 byte is more than enough for the project – but once we get into volume production…!
	Gateway ID	1				Code uniquely identifying the gateway to which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where the least significant byte (LSB) is 10ths of seconds. 24 hour clock. We felt that date information is not needed at this point in the system and that there should be a way of resolving any ambiguities occurring at the midnight rollover. Could be binary encoded into 3 bytes if we are getting really precious about message size. Date stamping would more likely take place on receipt of the message at the control centre.
	Magnitude	1				A 0…255 indicator of the magnitude of the crash – e.g. related to the maximum displacement during a crash event. Note that we felt that for development purposes, the raw acceleration data could be stored on board the sensor for later download. We need to define

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
						functionality to do this.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are "1 off's" like this one?
Crash Sensor Status			17	1	10	Message from crash sensing module to the GW module transmitted hourly (on receipt of Time Sync message) indicating the status of the crash sensing module.
	Message ID	1				Code that identifies this as a Status message from a crash sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the crash sensing module.
	Gateway ID	1				Code uniquely identifying the gateway to which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover.
	Battery Voltage	1				Binary representation of the battery voltage.
	Sensor status	1				Byte identifying any error codes from the acceleration sensor (single byte should cover all three axes).
	Solar charge status	1				Whether the solar cell is providing any charging current.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are "1 off's" like this one?
Crash sensor time sync			14	1	10	Message from GW module to the crash sensing module transmitted hourly resetting the internal clocks of the sensing modules. It's not

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
						entirely clear how the latency of the transmission and reception of this message can be accounted for.
	Message ID	1				Code that identifies this as a Status message from a crash sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the crash sensing module to which the message is being sent.
	Gateway ID	1				Code uniquely identifying the gateway from which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are "1 off's" like this one?
Environmental risk			16	12	5	Message from environmental sensing module to the GW module when an environmental risk occurs, confidence level changes or disappears.
	Message ID	1				Code that identifies this message as an environmental risk alert.
	Packet ID	1				Identifier for this instance of this message. A bit like the rolling counter, it's not clear how important this is for these single packet messages.
	Sensor ID	1				Code uniquely identifying the environmental sensing module. 1 byte is more than enough for the project – but once we get into volume production…!
	Gateway ID	1				Code uniquely identifying the gateway to which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
						that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover. Could be binary encoded into 3 bytes if we are getting really precious about message size.
	Risk Type	1				Potential for 256 messages
	Risk Confidence	1				0…255 confidence level indicator for the particular risk type. 0 = clear this risk.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are “1 off’s” like this one?
Environmental sensor status			17	1	5	Message from environmental sensing module to the GW module transmitted hourly (on receipt of Time Sync message) indicating the status of the environmental sensing module.
	Message ID	1				Code that identifies this as a Status message from an environmental sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the environmental sensing module.
	Gateway ID	1				Code uniquely identifying the gateway to which the message is being sent. It’s not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover.
	Battery Voltage	1				Binary representation of the battery voltage.
	Sensor status	1				Byte identifying any error codes from the various environmental sensors.
	Solar charge status	1				Whether the solar cell is providing any charging current.
	FEC	2				Forward error correction

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
	Rolling Counter	1				Not clear this is needed where messages are “1 off’s” like this one?
Environmental sensor time sync			14	1	5	Message from GW module to the environmental sensing module transmitted hourly resetting the internal clocks of the sensing modules. It’s not entirely clear how the latency of the transmission and reception of this message can be accounted for.
	Message ID	1				Code that identifies this as a Status message from an environmental sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the environmental sensing module to which the message is being sent.
	Gateway ID	1				Code uniquely identifying the gateway from which the message is being sent. It’s not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are “1 off’s” like this one?
Obstruction			18	360	4	Message from obstruction sensing module to the GW module when an obstruction risk occurs, confidence level changes or disappears.
	Message ID	1				Code that identifies this message as an obstruction risk alert.
	Packet ID	1				Identifier for this instance of this message. A bit like the rolling counter, it’s not clear how important this is for these single packet messages.
	Sensor ID	1				Code uniquely identifying the obstruction sensing module. 1 byte is more than enough for the project – but once we get into

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
						volume production…!
	Gateway ID	1				Code uniquely identifying the GW to which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover. Could be binary encoded into 3 bytes if we are getting really precious about message size.
	Risk Type	1				Potential for 256 messages
	Risk Velocity	2				Value representing the speed at which the obstruction is travelling (not sure if this is needed but let's put it in for the time being).
	Risk Confidence	1				0...255 confidence level indicator for the particular risk type. 0 = clear this risk.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are "1 off's" like this one?
Obstruction sensor status			17	1	4	Message from obstruction sensing module to the GW module transmitted hourly (on receipt of Time Sync message) indicating the status of the obstruction sensing module.
	Message ID	1				Code that identifies this as a Status message from an obstruction sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the obstruction sensing module.
	Gateway ID	1				Code uniquely identifying the gateway to which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a

Message	Data	Data size (Bytes)	Message Size (Bytes)	Frequency (hr^{-1})	No. Sensors per Gateway	Notes
						way of resolving any ambiguities occurring at the midnight rollover.
	Battery Voltage	1				Binary representation of the battery voltage.
	Sensor status	1				Byte identifying any error codes from the obstruction sensor.
	Solar charge status	1				Whether the solar cell is providing any charging current.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are “1 off's” like this one?
Obstruction sensor time sync			14	1	4	Message from GW module to the obstruction sensing module transmitted hourly resetting the internal clocks of the sensing modules. It's not entirely clear how the latency of the transmission and reception of this message can be accounted for.
	Message ID	1				Code that identifies this as a Status message from an obstruction sensing module.
	Packet ID	1				Identifier for this instance of this message.
	Sensor ID	1				Code uniquely identifying the obstruction sensing module to which the message is being sent.
	Gateway ID	1				Code uniquely identifying the gateway from which the message is being sent. It's not clear whether this is needed at this stage.
	Time	7				HHMMSSS where LSB is 10ths of seconds. 24 hour clock. We felt that date information is not needed and that there should be a way of resolving any ambiguities occurring at the midnight rollover.
	FEC	2				Forward error correction
	Rolling Counter	1				Not clear this is needed where messages are “1 off's” like this one?

Table 3 : Gateway (GW) Module Message Formats and Requirements

Multiplying all the message sizes by their corresponding frequency of transmission and number of sensing nodes per gateway together and adding them all up gives a data rate of about 61 bit s^{-1}. This is extremely low and allows for the choice from among a wide range of low bandwidth wireless technologies to communicate with the sensing modules.

5. VEHICLE ACTIVATED DISPLAY EMULATION

This is used to display a message warning drivers of vehicles approaching the instrumented section of road that a hazard exists. In a real-life system, the VMS will be powered by energy-harvested power (wind, solar): in principle, it need only be powered when there is actually a "hazard" message to display. For the purposes of the demo system, the VMS will be emulated by a lap-top computer display, because of the practical difficulties of erecting and using an actual VMS.

The display is fundamentally part of the Primary Safety System but will naturally serve to provide warning of the events detected by the Tertiary Safety System. It will have the following functions.

- Receive data from the GW Module relating to Tertiary warnings and when to display them.
- Display a variety of messages (most of these will relate to Primary hazards) warning the driver of hazards they will shortly encounter. Proposals for the nature of these displays messages are made in the Primary Safety Requirements document[5].

[5] Smart RRS deliverable D4.2 – Requirements for the Primary Safety System

6. CONTROL CENTRE MODULE DESCRIPTION

The control centre is likely to undertake the following functions:

- Receiving data via the Gateway Module.
- Storing the data arriving from the Sensing Modules via the GW Module for future analysis.
- Displaying events and status of various parts of the system (Sensing Modules, GW Modules) in such a way as to successfully demonstrate the system.
- Providing a means for displaying simulated warning signals generated by data from the Sensing Modules.
- If time and budget allow, there may be some mechanism (e.g. a web-site) that enables the simulated warning signals to be made available to road users for the purposes of demonstration.

The system shall be built from off the shelf components and systems but will require additional software to be written.

7. MODULE-TO-MODULE INTERFACE REQUIREMENTS

The proposed distribution of the Smart RRS safety systems is as shown schematically in Figure 6 (note that this diagram includes both tertiary and primary safety system elements).

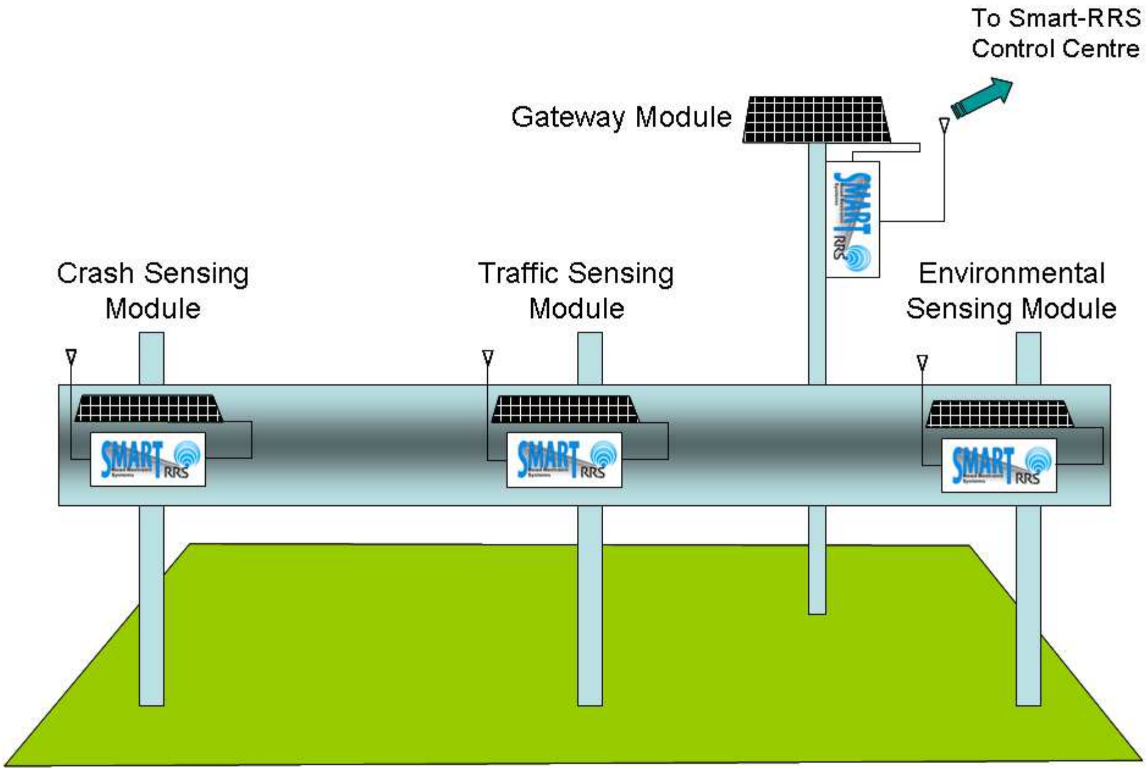

Figure 6 : Smart RRS Safety System Distribution

For the tertiary safety system, the main "lines of communication" are between:

- The crash barrier and the crash sensing module
- The crash sensing module and the GW module (and vice versa)
- The GW module and the control centre (and vice versa)

As stated in the Overview (Section 2) the communications topology will be a star with the Gateway as the hub. As also stated, there is no direct communication between sensing modules, nor between the control centre and an individual sensing module (all control centre messages will pass via the GW module).

7.1 CRASH BARRIER TO SENSING MODULE

Disturbances of the crash barrier arising during a crash event must be picked up by the crash sensor. Such disturbances potentially have a large dynamic range, since they may arise as a result of anything from a minor "glancing blow" of a light vehicle with the crash barrier, to the head-on collision with the barrier of a large and heavy vehicle. Preferably, therefore, the chosen sensor technology should be capable of:

- Detecting crash signals across the full potential dynamic range
- Surviving the crash event

There are some additional constraints on the manner of attachment to the crash barrier of the sensing module arising from the tertiary safety system requirements discussed in Section 3.1. In particular, the sensing module should:

- Be attached to (mounted on) the crash barrier.
- Not [in itself] represent an additional hazard.
- Not adversely interfere with the safety / energy-absorbing functionality of the crash barrier.

The most likely places for attachment of the sensing module to the crash barrier structure are:

- At the top of, and behind, the crash barrier support post.
- Within the "crushable" part of the additional barrier structure to be implemented as the secondary Smart RRS safety system.

The perceived advantages of the first of these options are:

- that the post is likely to see lower accelerations than a directly impacted rail so that any given sensing module is more likely to survive a collision,
- that attachment to the post is less likely to compromise the post's integrity than attachment to a rail is likely to compromise the rail's integrity
- and high up on the post is likely to be in the best position for wireless transmission to and from the GW module.

Some uncertainty exists over how well signals originating in the crash barrier itself may be transmitted to the post structure, but the simulation results provided by the University of Zaragoza (See Footnote 1, p9) indicate that this should not present a problem.

A possible advantage of the second option is that it potentially provides a more integrated solution (possibly with a better chance of intellectual property being generated). It is not such a good position from the point of view of wireless transmission to and reception from the GW module, since it is lower down, and the metal barrier is may block the wireless signal unless the aerial can be mounted separately in some way (though this detracts from the "integrated" format). If energy harvested power is required, getting wiring to the integrated unit may also be more problematic than for a module mounted at the top of the post.

It is also worth noting that it is unlikely that it will be feasible to house the primary safety system sensing modules within the crushable part of the Smart RRS crash barrier, so that – from a whole system" point of view, there may not be a lot of advantage in mounting the crash sensors in this way.

Another question that arises regarding the architecture of the system is the spacing of the tertiary sensing modules. From a system cost point of view, the greater the spacing the better. On the other hand there must be sufficient sensors along the rail to ensure that the minimum detectable event is always sensed. The nature of the minimum detectable event and the spacing of the sensors will be a matter to be determined through the project.

7.2 SENSING MODULE TO GATEWAY (GW) MODULE

Communication between the sensing module and the GW module will use one of the low-power wireless protocols discussed in Section 3.2.3. It is anticipated that the following signals will need to be transmitted from the sensing module to the GW module:

- Signals relating to a crash event itself (very infrequently – e.g. once per year!)
    - Time of event
    - Location / identification of sensing module (gives crash event location)
    - "Size" (energy) of crash event
    - (Code relating to the likely type of vehicle involved? – depends on selected sensor signal characteristics and processing. Note that this is currently not included in the "Message Requirements" listed in Table 3)

- Regular diagnostic updates (once per hour?)
    - Time of update
    - Location / identification of sensing module
    - Additional diagnostic measurement data (e.g. battery voltages, ambient light level)

Details of the message characteristics and requirements associated with this various signal types may be found in Table 3 (the exact details of the overhead data will depend on the wireless protocol chosen for this application).

7.3 GATEWAY (GW) MODULE TO CONTROL CENTRE

The GW module will transmit the following types of message to the control centre, via GPRS / GSM:

- System status updates.
- Crash event messages (gateway ID / location; time; crash "size").

In the latter case, the messages need to be passed from the GW module to the control centre within only a few seconds to ensure rapid response.

7.4 CONTROL CENTRE TO GATEWAY (GW) MODULE

- Future implementations of the system may have the capability of transmitting messages (for example, requests for additional and / or diagnostic data) via GPRS / GSM from the control centre to the GW module (and hence from the gateway to the sensing modules). However, it is not intended that this functionality will be implemented in the demonstration

7.5 GATEWAY (GW) MODULE TO SENSING MODULE

The GW module will communicate with any / all its associated sensing modules as required. The following types of messages will be transmitted from the GW module to the sensing module(s):

- Status requests (either "regular" – e.g. once per day updates).
- Time synchronization data (to be communicated to the sensing module when the sensing module makes a status update).

8. CONCLUSION

This document has reviewed the requirements for the system and from these has proposed a Tertiary Safety System based around a GW module monitoring the output of a number of crash sensing modules. The sensing modules are arranged as a star network with the gateway - all communications taking place through the gateway at the hub of the network.

The key modules for the system are the sensing modules, the gateway, a control centre, an emulation of a vehicle activated display and an approaching vehicle sensor.

The crash sensing module detects when a crash event takes place. The gateway forms the communications hub for the system. The control centre is the place where crash alerts are displayed for human action and intervention. The display and approaching vehicle sensor provide the means by which oncoming traffic is warned that a barrier collision has taken place.

The crash sensing modules will comprise crash sensors (a combination of accelerometers and acceleration sensing switches have been identified as the best candidates for this task); a processing function to check acceleration data for false triggers and to provide some measure of crash intensity as well as controlling the power and communications sub-systems; a radio subsystem to communicate using a wireless personal area network (WPAN) protocol with the gateway and a power subsystem to provide long-term power to the sensing module. The document argues that these modules should be mounted on the posts of the crash barrier.

The gateway will monitor sensing modules using a WPAN protocol and communicate to a remote control centre using GPRS. In addition to communication functions, the GW module will also provide some logic for controlling the vehicle activated sign, based on data from the sensing modules combined with detection of approaching vehicles. The gateway will also have the function of providing some time synchronization for the sensing modules.

The control centre will store status data from the sensing modules and provide means for examining this data as well as displaying an appropriate alert to control centre staff when a crash has taken place.

More detailed design description will be given in the Tertiary Design Document, Smart RRS deliverable D5.3.