EXECUTIVE SUMMARY

Integrated Safety Systems and Interoperable Systems of Systems catering to the need of Life and Society is an important emerging need in this Information Age. Governments across the field, both local administration and Central Administration are developing standards, systems and procedures towards this important mission. Communications is an Important Aspect in Systems of Systems Realization and since Internet Protocols(IP) have emerged as an Common Universal Communications mechanism, system designers and engineers tend to use IP i.e. TCP – IP as a common backbone for communications. In this premise Emerging Public Safety Broadband Networks, Machine to Machine (M2M) all tend to utilize the ***All – IP Flat Network*** as the Communication Language, while there could be different medias like Ethernet, Cellular (2G, 3G, and LTE), Specific Wireless Bands i.e. in WiMAX, Airport Networks etc.

Safety Management can be defined as a businesslike approach to safety. It is a systematic, explicit and comprehensive process for managing safety risks. As with all management systems, a safety management system provides for goal setting, planning, and measuring performance. A safety management system is woven into the fabric of an organization. Globally governments have begun to adopt a national broadband plan and also provide a dedicated spectrum for Public Safety utilizing the Evolved Packet Core Long term Evolution cellular technology. Safety Management deals with both the prevention of accidents and as well as managing emergencies. The suitability of the LTE networks and the architectures for emergency response has been detailed out by the Dept. of Homeland Security. The systems thinking paradigm creates a human centred approach in the systems design and the overall system safety is then a function of interactions, interfaces and risk reduction by proactive monitoring and probabilistic failure models.

The objective of this research journey was to Design the Communication Systems for Cooperative Life Safety Systems, in a ***next generation All – IP Flat Network*** running over different physical media like Public Safety Networks, General Broadband Backbones and the like.

The Communication Systems Design of this Cooperative Safety Systems was governed by four major elements

- Accident Analysis and functional safety
- Interpretations of cognitive elements related to safety
- Information Model and Actors identification
- Communication Definition & suitability analysis.

With regard to this, the research was planned to develop these four work items.

a) Review of functional Safety Models for Safety Management Systems.
b) Functional & Cognitive Safety Aspects for Disaster Preparedness & Management.
c) Safety Information Modelling in the IoE context
d) Safety System Design – Architecture, Models & Communications.

The Scope of this entire research project was limited to Modelling Hazards related to Fire, Gas & Chemical. The derived models shall be capable of handling the Generalization to other Safety Related Instruments.

During the course of the research and review of accidents, chemical storage tank was identified as the element with higher probability of risk and its construction, operation and maintenance was used as the CASE for this research.

In Chapter 1, the accidents and accident models are reviewed for the cause of the accidents. The relationship between process safety management and public safety management was compared and correlated with findings from New Zealand's public safety management systems handbook. Based on different accident models causal and systemic a hypothetical communications backbone was elucidated comparable with IEC 61850 Smart-Grid standardization called as the safety grid. Aspects related to Cyber security were selected out of the scope of this research on the premise that cyber security behaviour can be in conformance with IEC/ISA 62443 standards.

In Chapter 2, the hypothetical model was subjected to detailed analysis with respect to disaster preparedness and management scenarios. The analyzed accidents indicated that the cause for major accidents was related to chemical storage tanks, their design, operation and maintenance. Based on the accident models reviewed in Chapter 1, a total of 118 requirements for tank construction, operation and maintenance was categorized into Theory of Constraints, Functional Safety and Cognitive Aspects. Based on Sam Mannan's report to the US senate on the accident of City of West the need for manual verification or automated verification or periodic audits through certified third parties was cited. The requirements were further classified to with respect to different sensing or inspection methods. A clear majority of the requirements skewed to the direction of Cognitive abilities.

In the disaster management scenario Boyd's OODA loop was used as the basis for examination of the OSHA 1920.10 requirements and categorized against Operational Requirements (Theory of Constraints) , Fail-Safe /Functional Safety and Cognitive abilities between different agencies co-operating during a disaster. For this purpose the National Information Exchange Model Emergency Management domain was analyzed. There was a clear need for inter-agency communications and NIEM model was insufficient to represent the scenarios. This was also corroborated with similar findings from APCO's high priority needs for communications. The hypothetical model also met the needs of the APCO recommendations with service orientation and stronger information models.

In chapter 3, the information model was developed. Disaster preparedness and control requires information that is regularly sampled and informs about compliance adherence. The overall Disaster Management takes into account both the conditions, i.e. the mitigation planning and the disaster containment after an incident as occurred i.e. Disaster prevention and Disaster containment. The Safety Information Model for the former provides the view about the compliance on constraints of a systems boundary and a safety practitioner could verify or correlate the details for measuring the practice- compliance integrity. The Disaster Containment module post incident is used to aggregate the safety information and present a situational awareness view for the containment personnel including the incident commanders.

The goals with observables categorize into three types of categories, i.e. the Key Performance Indicators, Asset Design & Construction, and the last on the periodic compliance and categorized across the People, Process & Things. The "things" are either **Smart Tags** or **Smart Sensors**. The connectivity process is described as **Rules** – If this then that, **Verify** – manual verification procedures, **measure** – a method or system to measure, and **simulate** – conditions are artificially injected and simulated. The people in the entire chain are either **associated** or **informed** or people **acknowledge** the measurements or process and are consciously aware.

In the case of disaster containment as studied earlier in Chapter 2, the ***O***bserve ***O***rient ***D***ecide ***A***ct OODA model was able to accommodate the needs with clear inter agency communications. The classical OODA enacts a strict decision action chain and does not include evidencing. This is evident from the roots of the OODA model owing to tactical military operations i.e. Cursor on the target. In case of safety management the needs for evidencing exists to avert future situations and post incidence analysis. Thus the OODA framework is constructed as a E-OODA framework for Disaster containment.

Finally in chapter 4, Constrained Applications Protocol was chosen as the communication protocol for its suitability over LTE networks. There are open challenges with respect to M2M connectivity and data communication with respect to bandwidth. Some of the developments in CoAP over control plane could address these challenges. At this point in this research the application of CoAP is considered to satisfy the use cases identified earlier. The system structure is further modelled with a **Thing Architectural Model** defined by an **OR3C communication interface**. The thing model is based on the IEC 61499 function block model. The safety management service orientation is realized using the CoAP service orientation with CoAP URIs. The OR3C interfaces are defined as extensions to the options field in the CoAP protocol.

Detailed architecture and working software prototype were developed to test the communications and information flow.

A visual information modeller based on the Thing Architectural Model was developed as a windows application to further model use cases and perform parametric research in the future. Appendix 1 displays sections of the visual information modeller.

A high level LTE communications topology study was performed and find suitable for Safety Management needs. However few recommendations for further research are identified as shown in Appendix 2.