4. INFORMATION MODEL

SAFETY INFORMATION MODEL IN INTERNET OF EVERYTHING – PROCESS, PEOPLE AND THINGS

Abstract

The next generation of Internet of things that connects the things, people and the process through which the people and things interact is coined as Internet of Everything. Safety management is constructed as a complex system of systems design coordinating with each other like the Fire Alarm System or Gas Detection System as well as the Emergency response like the Fire Fighters and Para-Medicals like the Ambulatory services. The governments have been setting up national broadband plans and separate dedicated spectrum for Public Safety Communications used for effective information rich emergency management and response. This paper outlines the evolution of the public safety LTE network and its applicability in the safety management system and safety preparedness. It also describes the role of Smart Objects and Internet of Everything in Safety Management. To achieve this, this paper develops the information models for safety management systems to be used in IoE utilizing the broadband LTE networks.

Key words **—** Safety Management Systems, Information Modeling, Internet of Everything, Public Safety LTE.

1. INTRODUCTION

Internet of Things (IoT) is widely known and typically brought to the fore in the context of Ma-chine-to-Machine (M2M) communications. IOT evolution has given rise to the genesis of new subject called Internet of Everything (IoE). IoE connects the products, the users(people) and the process through which these interact. IoE has been a subject of debate for many applications such as improving operation effectiveness in a business, to increased safety or better management of urban facilities and smarter cities [1]. The concept of IoE is piloted by Communications Company such as Cisco or Qualcomm. IoE thus is a heterogeneous connection of smart-products with consumers (users) and the process in which these are operated.

Safety management on the other hand 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(SMS) provides for goal setting, planning, and measuring performance. A SMS is woven into the fabric of an organization. It becomes part of the culture and is the way people do their jobs [2]. Globally, governments have begun to adopt a national broadband plan and also provide a dedicated spectrum for Public Safety using the Evolved Packet Core Long term Evolution.

In this paper we describe how the new media of IoE, the LTE may facilitate the increased system-safety and deduce the information models for effective safety management systems. We take inspiration from Building information modeling [3] that has steadily grown and captured the minds of Architects, builders and operators alike to deduce the Safety Information Model.

Safety management deals with both the prevention of accidents and as well as managing emergencies. [4]. The suitability of the LTE networks and the architectures for emergency response has been detailed out by the [5]. Safety Life Cycle encompasses design corrections, periodic maintenance, layers of protection to emergency management; this paper derives the information models useful for safety management.

2. Public Safety Communications using 3GPP LTE

Public safety networks provide communications for services such as police, fire and ambulance. In this realm the requirement has been to develop systems that are highly robust and can address the specific communication needs of emergency services. This has fostered public safety standards – such as TETRA and P25 – that provide a set of features that were not previously supported in commercial cellular systems. These standards have also been applied to commercial critical communications needs such as airport operations or Industrial Management.

The shortcoming of these narrowband applications is their insufficient bandwidths for high data rate applications i.e. file transfers and streaming media. [6] Initially the thought to adapt nationwide broadband communications originated in the United States around late 2009 and slowly different countries across the globe have begun to adopt a similar thought. The availability of high data throughput to these essential services not only helps them in informed decision-ing but also in evolution of applications that are integral to safety Management.

The TETRA and P25 systems on the other hand provided specific communication access methods like the Push-To-Talk(PTT), ease of deployment with minimal central controller(network router). These features are critical for emergency communications. The 3GPP group is adding the following specifications as part of release 12 and release 13 to meet these specific needs.

Table 11-3GPP Evolution [7]

Work Item	3GPP Release	Work Item Document Reference
Proximity-based Services Specification (ProSe)	12	SP-130030 [5]
Group Communication System Enablers for LTE (GCSE_LTE)	12	SP-130326 [6]
Public Safety Broadband High Power User Equipment for Band 14 for Region 2	11	RP-120362 [7]
Study on Resilient E-UTRAN Operation for Public Safety (FS_REOPS)	12	SP-130240 [8]

Texas A&M University & the EDGE Innovation network are also working on Safety LTE evolution and the advancement of associated telemetry equipments, mobile handsets and situational awareness applications. [8]

3. SAFETY MANAGEMENT AND SAFETY PREPAREDNESS

A safety management system provides a systematic way to identify hazards and control risks while maintaining assurance that these risk controls are effective. SMS 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. It becomes part of the culture, the way people do their jobs [9]

In general Safety is defined in terms of identified hazards (HAZID) and achieving lower Risk levels as in ALARP “As Low As Reasonably Practicable”.

Dr. Wayne Blanchard and Dr. Cortez Lawrence in 2007 set up a working group for defining the principles of Emergency Management & Disaster Preparedness and they developed the eight principles presented in **Table 12**.

Emergency management is a subset in the overall safety life cycle as in Safety management and both are constructed by design and expect risk reduction by clear objectives, continuous monitoring and collaboration amongst different entities. Internet of things is evolving and getting applicability in multiple domains, and as Internet has become a pervasive way of collaboration, Safety and Emergency management would drive on the new era of Internet of Things or Internet of Everything.

#	Principle	Description
1.	Comprehensive	Emergency managers consider and take into account all hazards, all phases, all stakeholders and all impacts relevant to disasters.
2.	Progressive	Emergency managers anticipate future disasters and take preventive and preparatory measures to build disaster-resistant and disaster-resilient communities.
3.	Risk-driven	Emergency managers use sound risk management principles (hazard identification, risk analysis, and impact analysis) in assigning priorities and resources.
4.	Integrated	Emergency managers ensure unity of effort among all levels of government and all elements of a community.
5.	Collaborative	Emergency managers create and sustain broad and sincere relationships among individuals and organizations to encourage trust, advocate a team atmosphere, build consensus, and facilitate communication.
6.	Coordinated	Emergency managers synchronize the activities of all relevant stakeholders to achieve a common purpose.
7.	Flexible	Emergency managers use creative and innovative approaches in solving disaster challenges.
8.	Professional	Emergency managers value a science and knowledge-based approach; based on education, training, experience, ethical practice, public stewardship and continuous improvement.

Table 12 Principles of Emergency management [10]

4. INTERNET OF EVERYTHING & SMART OBJECTS

Smart Objects are things that can communicate with users and other things about possible interactions with itself. The Auto-ID project in MIT Labs conceived these things as devices equipped with RFID tags and one can know more information by querying these devices. With the rise of Ubiquitous and pervasive networking, the concept grew to a level that the devices communicate with each other over Internet and also connect to god-like data banks i.e. the cloud computers. Several methodologies are being developed to make internet of things being a reality. These include CoAP (Constrained Applications Protocol) similar to SOAP services, MQTT (Message Queuing Transport Telemetry) and RESTful http services. [11].In early 2013 Cisco & Qualcomm began discussing about Internet of Everything and the definition provided by Qualcomm was

"The Internet of Everything is based on the idea that everyday objects can be readable, recognizable, locatable, addressable, and controllable via the Internet. Although the market defines the Internet of Everything in terms of connected everyday objects, the nature of the connection remains to be determined."

Cisco on the other hand defined the Internet of Everything (IoE) as "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries".

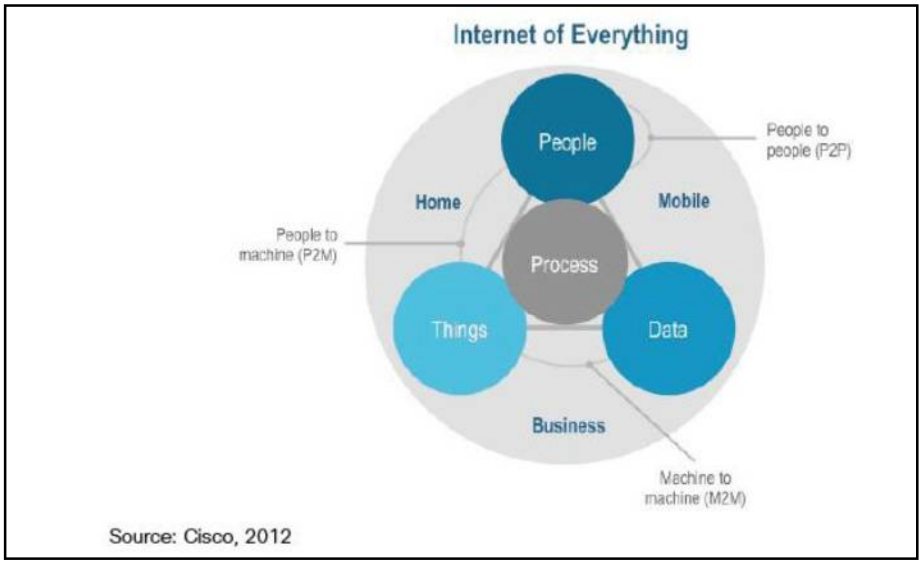

FIGURE 8 Internet of Everything (IoE) [12]

Internet of Everything finds application in different areas i.e. Energy Management & Smart Grid, Manufacturing and Retail and the concept of Internet of Everything is being pursued in building smarter cities from Songdo (South Korea), Nice (France) etc. The aspect of connecting devices and people has been widely utilized in more commercial and comforting applications. The aspect of safety governance is not yet been widely studied and as noted earlier the Safety communications have been in specific networks like TETRA. The connection of the safety applications with the Internet is evolving with the broadband wireless initiatives.

The CAPSCOM program of California Public Safety [13] outlines the need of the Broadband-ing work to evolve as a Systems-of-Systems solutions rather than a single System solution. In this context the IoE solution fits well as a set of coherently defined federated services. The systems-of-systems solutions require different systems to communicate seamlessly which necessitates **building the semantics of the information and modeling it**. In this paper we take up this case and devise the information model for the safety systems or in-short **S**afety **I**nformation **M**odel.

5. Information Modeling for Safety management & Compliance

As discussed earlier, Safety management provides a systematic way to reduce the risk levels to as lowest as possible in theory. The effectiveness of a safety management system is heavily dependent on the practice maturity, compliance to standards adherence and continuous monitoring. The Public Safety LTE global research is geared up towards emergency management that is one element of the Safety management System [5]. The disaster preparedness and control requires information that is regularly sampled and about compliance adherence. The evolution of the information model is represented as a mind-map with information labels representing the Nodes role in the IoE context (People, Data or Process). For the study purpose, the scope was restricted to Fire & Gas Hazard Management.

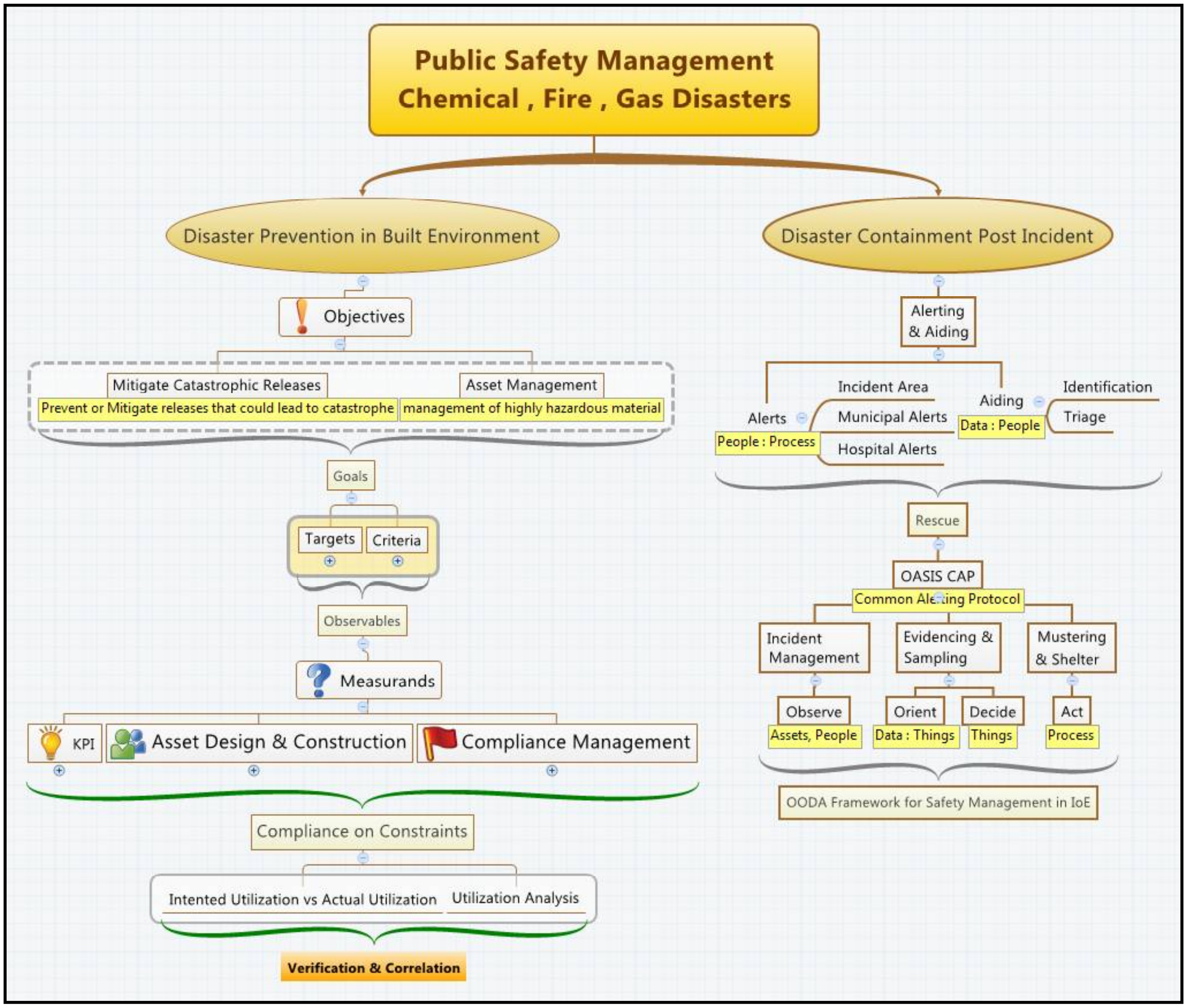

FIGURE 9 Safety Information Model Overview

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's including the incident commanders.

The goals of Safety management Compliance are depicted below.

FIGURE 10 Goals for Safety management for Disaster Mitigation

Upon these goals, the observables are presented that categorize into three types of categories, i.e. the Key Performance Indicators, Asset Design & Construction, and the last on the periodic compliance. The basis of Safety management is built on Periodic Proof Testing to measure the integrity of the system. The information model map in **Figure 12**, **Figure 13**, & **Figure 14** depicts the three attributes. The Labels (Process, Data, or People) hanging below an item classifies the category of the element.

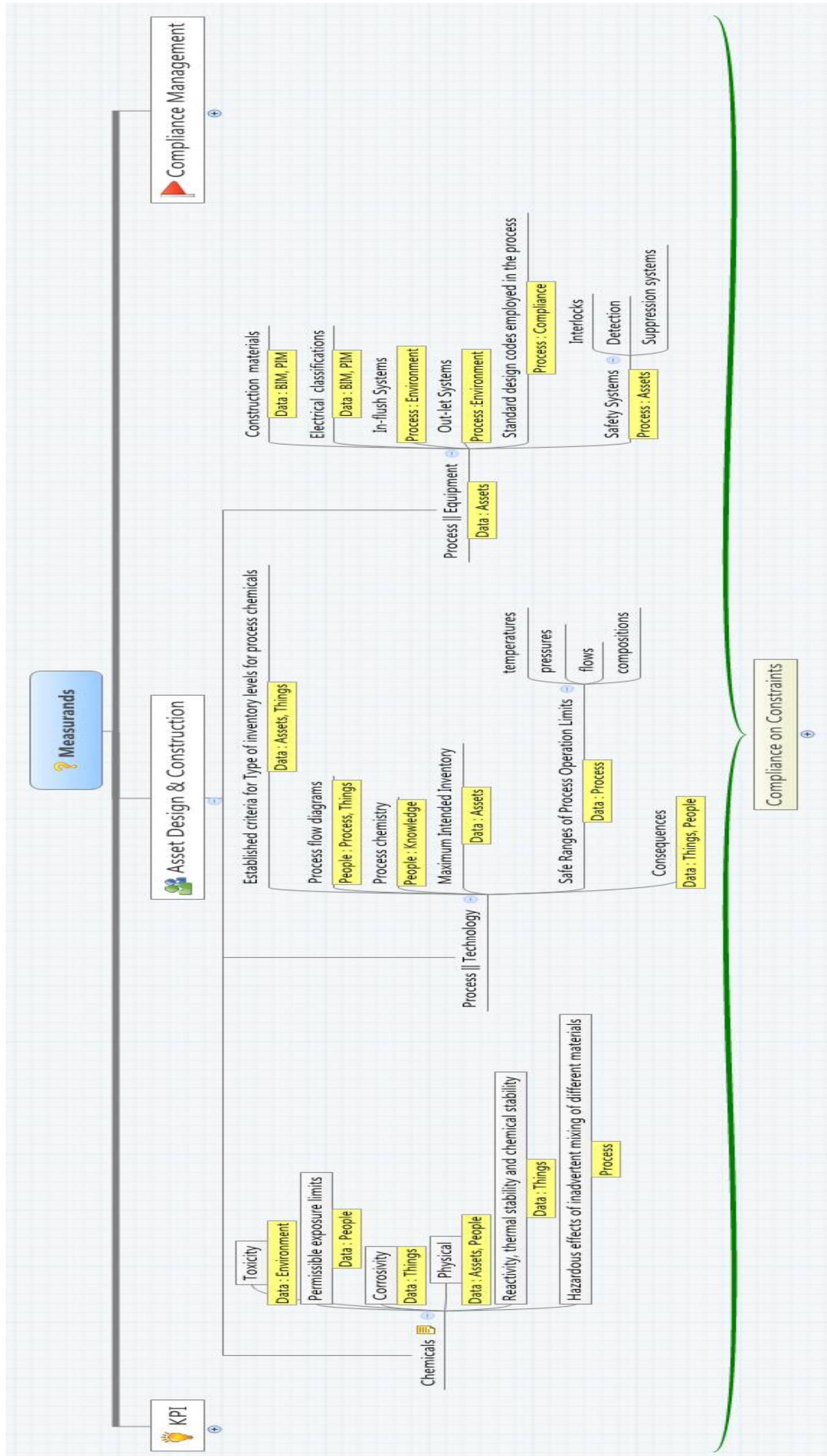

FIGURE 11 Asset Design & Construction

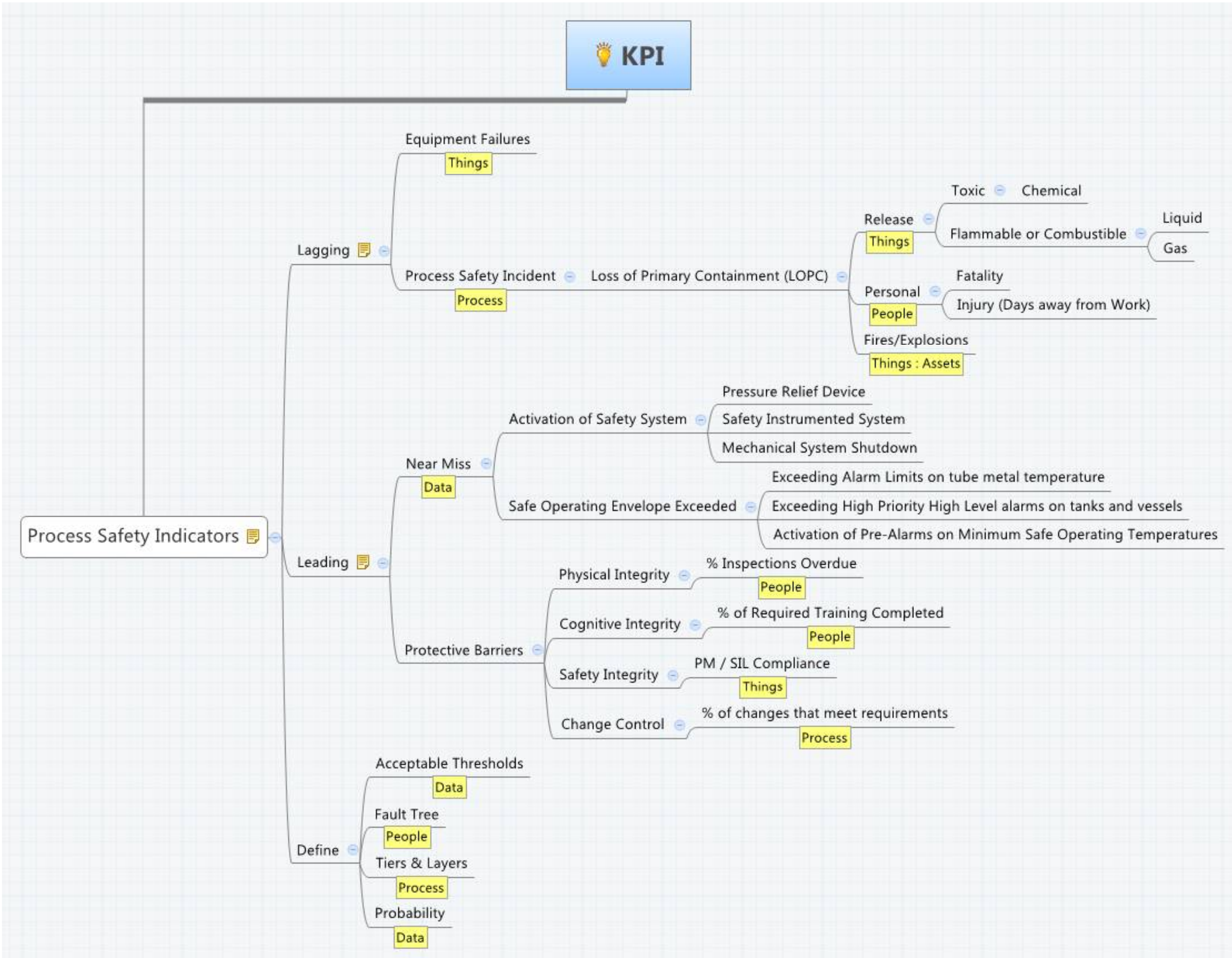

Figure 12 Key Performance Indicators

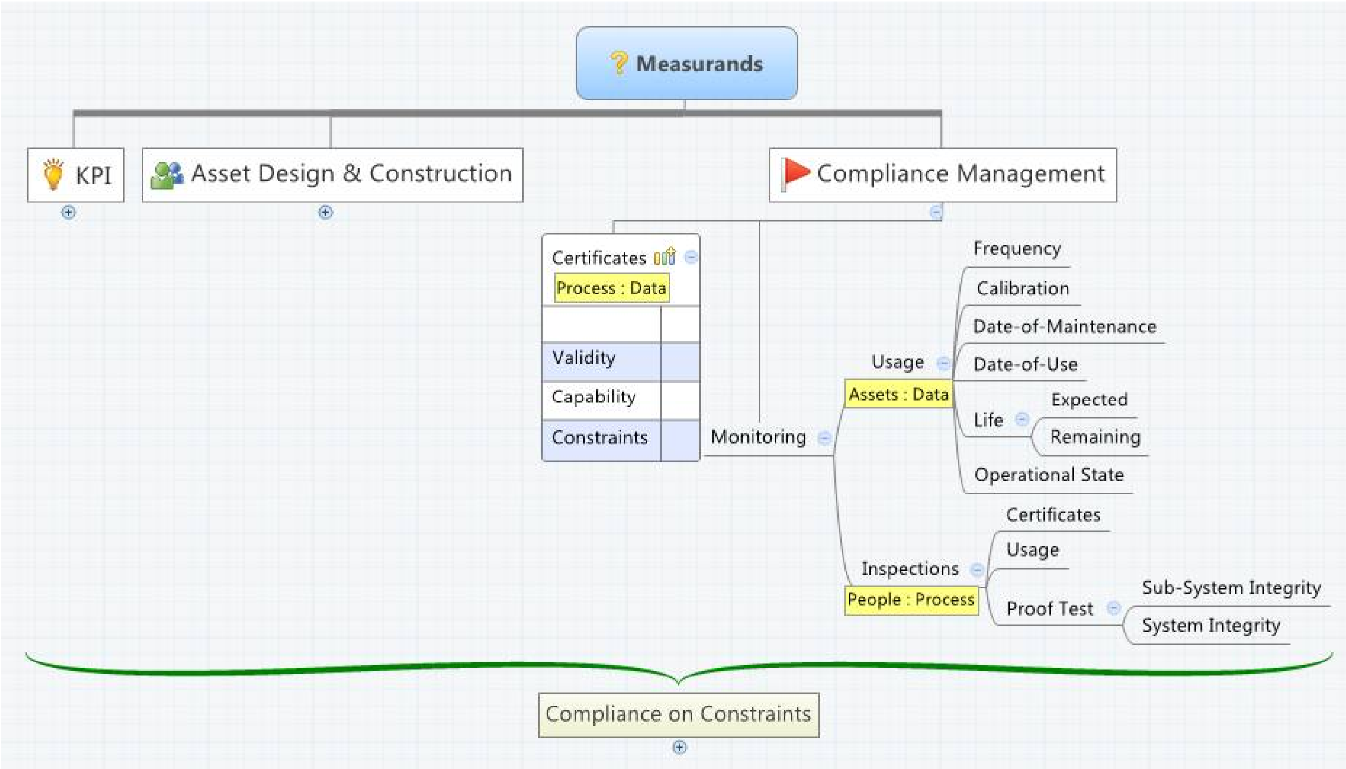

Figure 13 Compliance Management

The disaster containment view provides a view in which the Alert gets transported meaningfully to the respective recipients. The DoD uses information presentation frameworks like Cursor on the Target(CoT) which is derived from the Observe-Orient-Decide- Act(OODA) framework for situational awareness. [14].

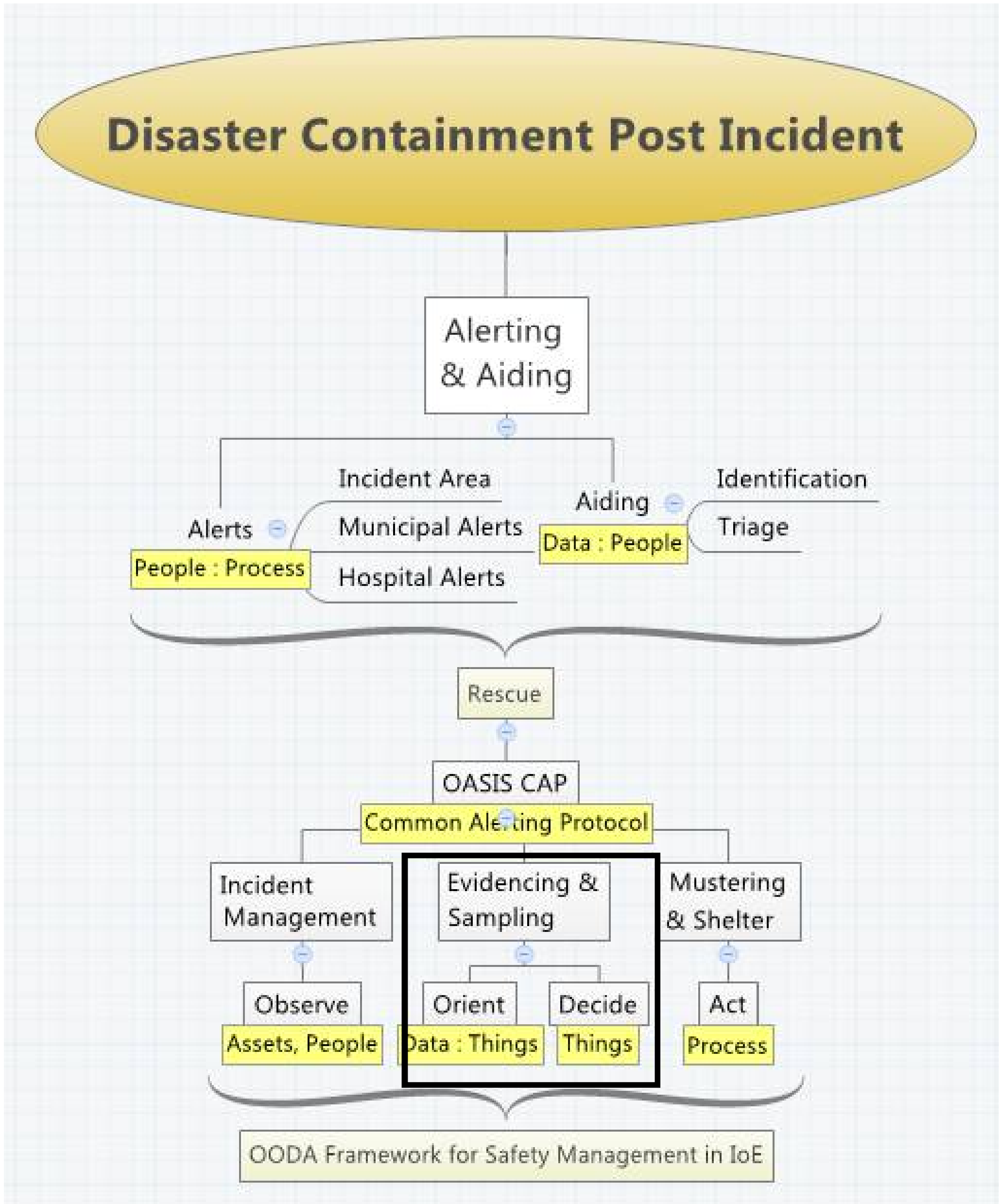

Figure 14 Disaster Containment OODA Framework

The OASIS group for open information exchange has developed a standardized protocol for communicating critical alerts called the Common Alerting Protocol [15], which is now in version 1.2. This protocol has also been standardized by the International Telecommunications Union. The normal OODA framework, does not seek to obtain evidences as it is tied to the strict decision-action chain. This enhancement of adding the Evidencing module to the classical

OODA helps in incident control and post incident analysis. This paper shall not further discuss about E-OODA in the current context.

6. DISCUSSION

The information models, along with the IoE label - classification representation shows the different facets of the relationship of the data that exist among the three categories in the Safety management. A pivot table was used to order the nominal relationship among the three elements viz. (People, Process and Things) and KPI, Asset design, and compliance management. In **Table 13** the types of People, Process and Things are described. 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*.

People	Process	Things
Inform(I) : are Informed	***Rules(R) :*** are available for processing	***Static Smart Tag (T):*** communicating tag's with Reference Constant readings embedded inside.
Associate (A): take passive part in the role.	***Verify (V) :*** people are expected to verify	***Smart Sense (M):*** communicating smart sensors.
acKnowledge (K) : take active role in the process and are consciously aware.	***Measure (M):*** system measurements are made.	
	Simulate (S) : conditions are simulated to verify system behavior	

Table 13- IoE Classification

In **Table 14** represents relationship between Design & IOE. The process here describes a system or system component in which the connected system behavior executes.

Asset Design & Construction			
Process	Things	People	Category
Rules	**Tag**	**acK**	o Permissible Exposure Limit
			o Storage
			o Max. Inventory
			o Toxicity
		Associate	o Construction, Electrical
	senseM	**acK**	§ - Capacity
			§ - Composition
			§ - Flow
			§ - Pressure
			§ -Temperature
			o hazardous effect
			o Stability
		Inform	o Inventory Levels for Process Chemicals
Simulate	**senseM**	**Inform**	o Consequences
Verify	**Tag**	**acK**	o Design Codes
			o Process Chemistry

			o Process Control System
			o Safe Operating Range
			o Corrosiveness
		Inform	o Reactivity
			o Process Flow Diagrams
	senseM	**Associate**	o Inlet , Outlet

Table 14 IoE in Asset Design & Construction

During Asset Design & Construction, a smart tag is placed that defines the overall Permissible Exposure Limit in the defined area. There exists a rule in the system that checks for the exceptions to the permissible exposure limits. *There is then a super rule that checks for the exception of either non-availability of rules or absence of tags for authorities to enforce.* Similarly accidents are caused predominantly by extremities rather than the process itself. Thus uncontrolled or leaky inlets or outlets are cause of concern. Users are associated to such points and the sensors are used to measure for un-desired behavior and such users shall verify the behavior periodically. *There is then a super verify function that checks for user association and a rule to raise exceptions.***Table 15** represents relationship in KPI and IoE.

KPI			
Process	**Things**	**People**	Category
Measure	**senseM**	**acK**	**o Equipment Failures**
		Inform	**§ Chemical Release**
			§ Fires / Explosions
Rules	**senseM**	**Inform**	**§ Change Control**
			§ Cognitive Integrity
			§ Physical Integrity
			§ Safety Integrity
Verify	**senseM**	**Associate**	**§ Personnel Injury**
		Inform	**o Near Misses**
	Tag	**acK**	**o Fault Tree**
			o Normally Accepted Thresholds
			o Probabilistic Failure Modes & SIL Level

Table 15 IoE & KPI

Table 16 represents relationship between Compliance Management & IOE. As discussed earlier, in the compliance management scenario, the user is associated to the proof testing process and acknowledges the behaviors and is recorded by a sense(Measure) process. *There is then a Super Measure function to assimilate the over-all proof test observations to calculate system integrity.* Smart tags are used to place certificate credentials and rules are placed to manage exceptions. The user plays a consciously aware role to acknowledge the compliance validity. *There is then a super rule to measure compliance invalidation as above and raise exceptions.*

Dr. Sam Mannan, in his statement to the US Senate on the City of West, Texas accident (2013) highlights the need for certifying 3rd party agencies to assist OSHA and DHS in periodic inspection and verifying the authenticity and integrity of the plants or facilities to avoid such further catastrophes [16]. *The broad-banding work of the public safety telecom networks presents as a boon to use the computing powers to help the first-responders and civic authorities to do mandated compliance checks and as well plan well for emergencies.*

Compliance Metrics			
Process	**Things**	**People**	**Category**
Measure	**senseM**	**acK**	**§ Proof Test – Sub System Integrity**
			§ Proof Test – System Integrity
		Assoicate	**§ Frequency**
			Assoicate
		Inform	**§ Remaining Life**
Rules	**Tag**	**acK**	**§ Certificates**
			§ Usage
			o Capability
		Inform	**§ Expected Life**
			o Validity
Verify	**Tag**	**acK**	**§ Last Date of Maintenance**
			§ Last Date of Use
			§ Operational State

			o Constraints

Table 16 IoE & Compliance Metrics

The following depicts one set of information representation view for compliance management.

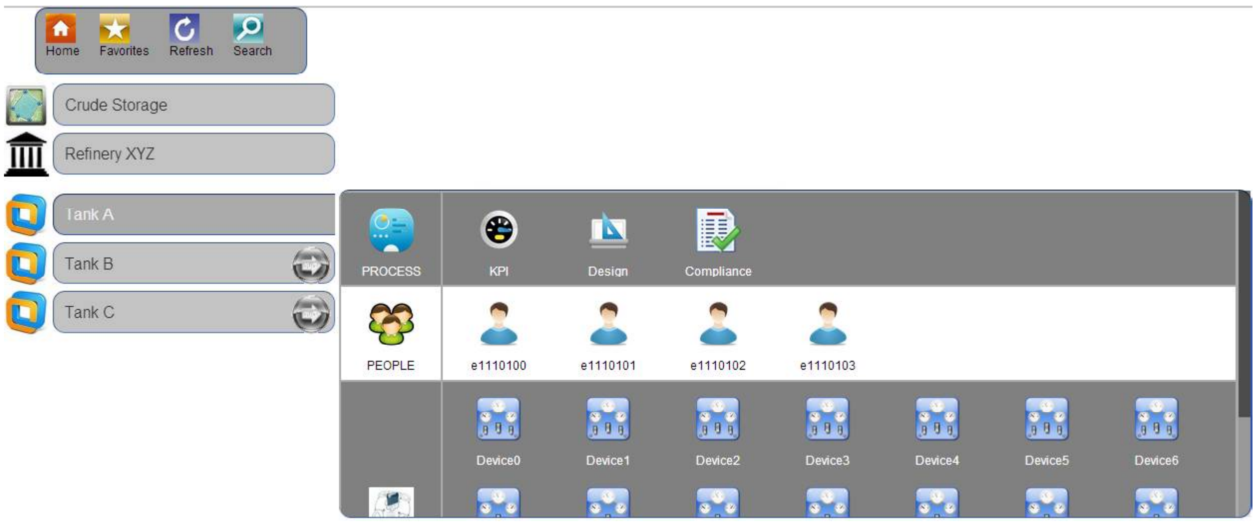

Fig 15 Safety Information Model IoE Realization

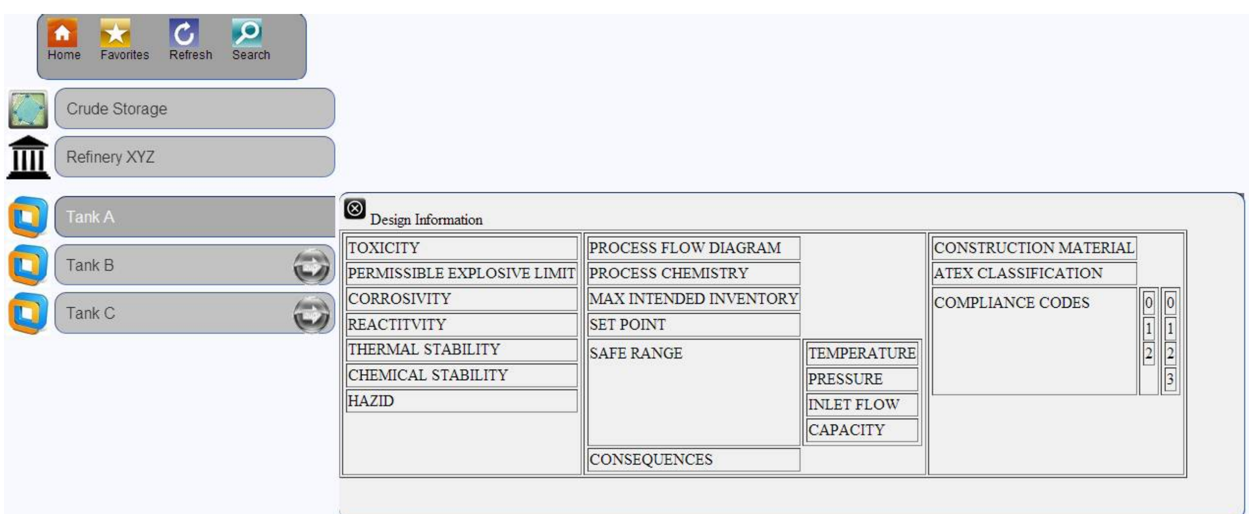

Fig 16 SIM Design Information Details

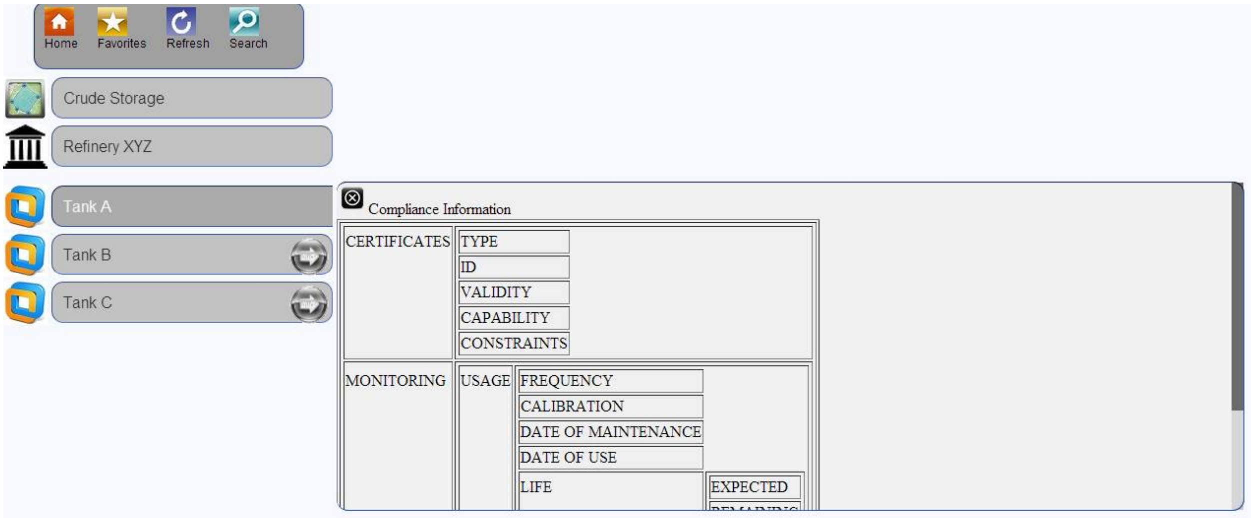

Fig 17 SIM Compliance Information View

As depicted in figure 8, plant information can be viewed as the detail list of assets inside the plant segregated by different geographical areas and each one of the assets such as the tanks, effluent pipes or distillation units can have associated users, process and the devices within the system. In a compliance conformance view the safety in-charge or the federal user can use the user-interface element for recording or observing the safety information.

In the case of City of West Fertilizer company accident, if the compliance information was recorded regularly, the mismatch in the designed tank storage content could have been identified and necessary actions could have been taken. The advancement of sensor networks and internet of everything could help in increasing compliance and averting such future accidents.

In the aftermath of an incidence i.e. a disaster the operational view of this public safety dashboard could include information from the medical agencies, first responders and also the legal compliance for post incident investigations.

Figure 18 Public Safety Operating Picture

7. Conclusion

The setup of Building Information Model (BIM) has helped the building management and construction safety industry with tools to design, manage and protect the facilities. Similarly a Safety information model, coupled with Industrial / federal compliance management solutions would aid in achieving cumulative public safety. As [4] hope that a Systemic Safety Management System (SSMS) would be a potentially preventive management system, this information model studies the different use cases of construction, compliance adherence, key performance indicators for preventive/compliant safety management system. The OODA attributes required for managing an aftermath are also discussed and an enhancement is proposed specifically for safety management system. This method of information segregation and aggregation helps in providing higher order compliance and an overall safety. This information model also seconds and aids Sam Mannan's report on the City of West, Texas accident signifies the need for effective information management and periodic compliance audits required in the industry to avert such accidents happening in the future.

REFERENCES

[1] O. Vermesan and P. Friess, Internet of Things-Global Technological and Societal Trends From Smart Environments and Spaces to Green ICT, River Publishers, 2011.

[2] T. P. Kelly, Arguing safety: a systematic approach to managing safety cases, University of York, 1999.

[3] S. Zhang, J. Teizer, J.-K. Lee, C. M. Eastman and M. Venugopal, "Building information modeling (BIM) and safety: automatic safety checking of construction models and schedules," *Automation in Construction,* vol. 29, pp. 183--195, 2013.

[4] J. Santos-Reyes and A. N. Beard, "A systemic approach to managing safety," *Journal of Loss Prevention in the process industries,* vol. 21, pp. 15--28, 2008.

[5] Dept. of Homeland Security, "Public Safety Architecture Framework Volume I, II, III," Department of Homeland Security, 2006.

[6] K. Balachandran, K. C. Budka, T. P. Chu, T. L. Doumi and J. H. Kang, "Mobile responder communication networks for public safety," *Communications Magazine, IEEE,* vol. 44, pp. 56--64, 2006.

[7] 3G Partnership Program, "3GPP Public Safety," July 2013. [Online]. Available: www.3gpp.org/public-safety.

[8] Edge Innovation Network, "Edge Innovation Center of Emergency Informatics," Sept 2013. [Online]. Available: http://www.edge-innovation.com/.

[9] Wikipedia, "Wikipedia Safety Management Systems," Oct 2013. [Online]. Available: http://en.wikipedia.org/wiki/Safety_management_systems.

[10] D. W. B. a. D. C. Lawrence, "Principles of Emergency Management," 2007.

[11] N.-T. Dinh and Y. Kim, "RESTful Architecture of Wireless Sensor Network for Building Management System.," *KSII Transactions on Internet & Information Systems,* vol. 6, 2012.

[12] D. Evans, "The Internet of Everything: How More Relevant and Valuable Connections Will Change the World," *CISCO White Paper [Online]. http://www. cisco. com/web/about/ac79/docs/innov/IoE. pdf, last access: July,* 2013.

[13] "Capsnet Strategic Plan," California Technology Agency, 03 03 2011. [Online]. Available: http://www.caloes.ca.gov/PSC/Documents/PDF/CAPSNET_Strategic_Plan_03-03-2011.pdf. [Accessed 10 10 2012].

[14] J. R. Boyd, "Organic design for command and control," *A discourse on winning and losing,* 1987.

[15] OASIS Open, "Common Alerting Protocol," 1 July 2010. [Online]. Available: http://docs.oasis-

open.org/emergency/cap/v1.2/CAP-v1.2-os.html.

[16] D. S. Mannan, "Environment and Public Works," Mary Kay O'Connor Process Safety Center Texas A&M Engineering Experiment Station, 27 June 2013. [Online]. Available: http://www.epw.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=12b33b05-57d8-474a-a5d2-ded91814b20c. [Accessed 29 June 2013].

[17] OHS Body of Knowledge, Safety Institute of Australia, Models of Causation : Safety, Safety Institute of Australia, 2012.

[18] Gas Association of New Zealand, SMS for Public Safety – Handbook for ESI & GSI Companies, New Zealand: Electricity Engineers Association , New Zealand, July 2011.

[19] Wireless Innovation Forum, "Use Cases for Cognitive Applications in Public Safety Communications Systems Chemical Explosion Scenario," Wireless Innovation Forum, 2010.

[20] Wireless Innovation Forum, "Information Process Architecture," Wireless Innovation Forum, 2012.