5. ARCHITECTURE, MODEL & TRANSPORT

SAFETY MANAGEMENT: COMMUNICATING SYSTEMS DESIGN AS IN INTERNET OF EVERYTHING

Abstract

With the evolving broadband public safety network, the next generation of safety management system is defined as a SafetyGRID. In relation to Internet of Everything (IoE), the system structure is modeled with respect to People, Process and Things with a Thing Architectural Model defined by an OR3C communication interface. The thing model is based on the IEC 61499 function block model. The IEC 61158 CPF-1 (Foundation Fieldbus) and the IEC 61850 smart grid communication profiles are compared and the application layer communication profile is defined. The case of safety management for tank storage compliance management is characterized by this system. The physical and transport layer from M2M communication over LTE is selected and the presented IoE model is demonstrated over Constrained Applications Protocol. The OR3C model is further extended to map to the requirements for Situational awareness and emergency response SoA.

1. INTRODUCTION

The idea of SafetyGRID emanated from the ongoing research on Public Safety LTE Communication systems design for disaster management[1]. During the analysis of accidents, it came to fore that compliance management is a deeper issue and tracking them is an un-solved problem, where governments and industries still are finding solutions. Mannan, in his latest report on accidents quotes the need for a effective auditing systems and third party agencies to support government agencies i.e. OSHA[2]. The communication design research across the globe is happening in the areas of emergency management[3] i.e. disaster site operations and tactical radio cognitive networks. Problems related to issues in reporting from field devices and taking all the way to government agencies were identified. The notion of probabilistic functional safety is well accepted in the industrial world today with standards i.e. IEC 61508 and its derivatives for Process (IEC 61511), Vehicular (IS0/IEC 26262), Nuclear (IEC 61513), Medical systems (IEC 62304). Review [1] of System Safety emanated human and systemic aspects beyond probabilistic aspects. The cause of accidents in chemical plants was mostly concentrated around storage tanks and hence it was used as the case.

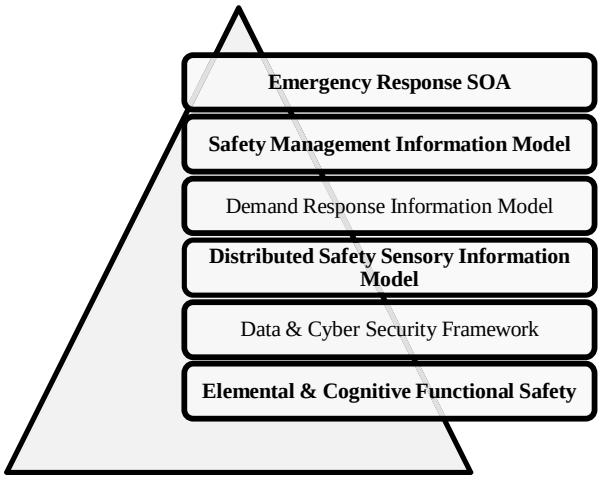

FIGURE 1 SAFETYGRID

These prompted us to develop the functional safety aspects and cognitive aspects and identify the needs for communicating systems amongst different stakeholders i.e. the Incident bearers, Law enforcement and first responders. The hypothesis was corroborated with the high priority needs developed from APCO; the design requirements were need for information model, public safety LTE API shared amongst different public safety personnel. The information model was developed as a function of People, Process and Devices (Things) against the backdrop of KPI, Design & Construction **and Compliance Management. In this** paper we develop a consistent architecture for LTE connected devices, people equipped with public safety LTE gadgets and an observing

server engine. Since the process safety and public safety share similar attributes[4], we tend to inspire from the device models defined for process control and smart grids and suit a Function Block architecture yielding service oriented APIs. This paper describes the PPT model, the function block architecture and chooses between two IoE protocols CoAP and MQTT-S for the system and goes on to describe the APIs and validates with the suitability with the storage tank case study. The paper set's the path for LTE channel scheduling mechanisms and network architecture which is not dealt in this paper.

2. THE SYSTEM CONTEXT

Disaster preparedness and control requires information that is regularly sampled and informs about compliance adherence. 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 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.

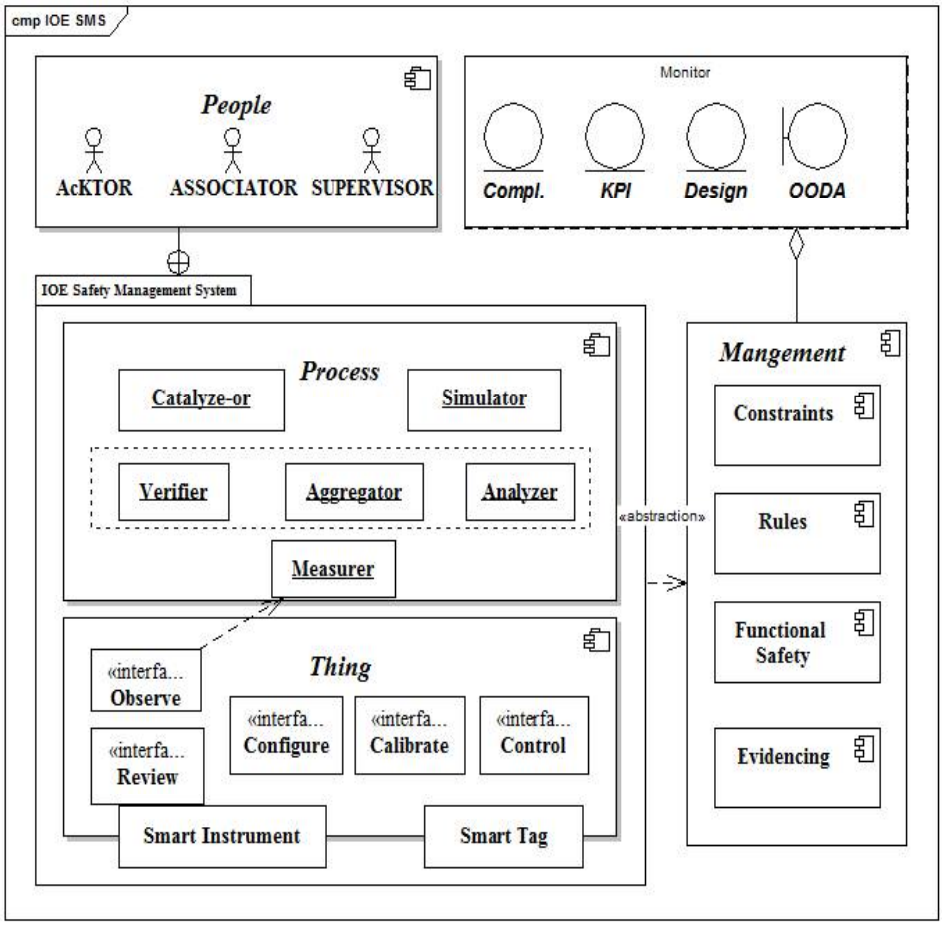

FIGURE 2 SMS IOE CONTEXT

In system structure depicted in Figure 1, smart instruments and tags are depicted with 5 different interfaces i.e. 1) Observe, 2) Review 3) Configure, 4) Control and 5) Calibrate. Observe and Review interfaces are used for reading the device parameters and while the rest are used to update or control the behavior of the devices.

The process is described in two blocks as Process and Management. The catalyze-or block acts on Rules and transforms the measurer blocks outputs. The verifier block acts in conjunction with Functional safety, while the Analyzer block acts with Constraints, measuring the compliance on constraints. The aggregator block represents a long range time window function and works with Evidencing block specifically for the disaster containment scenarios.

The communication architecture thus should be able to connect these different actors. As discussed earlier the Public safety management and process safety management share similar

traits with Functional safety as the fundamental base, process control communications were reviewed. In one view the system safety problem here is viewed as a control problem with *Monitoring and Periodic inspection* as the *Control variable (Handle)* and Compliance *Management and Audit as control function*. The communications used in the process industry has been standardized per IEC 61158 /IEC61499 [5] standards with certain communication profiles. The CPF - 1 utilizes the Foundation Fieldbus technology while the CPF – 2 utilizes Profibus communications. Both the technologies utilize Function Block architecture for process control and manufacturing automation respectively. CPF - 1 is called "Control on the wire" with a controller less configuration. Smart-Grid standardization [6] by IEC (IEC 61850) also took similar function block oriented approach. In this research, we tend to follow the similar architecture for the device model with different function blocks and a way to transport the parameters.

3. FUNCTION BLOCKS & COMMUNICATION PROFILE

The function blocks for the different actors i.e. People, Smart Instruments and Smart tags are categorized using terminologies from CPF -1 of foundation Fieldbus. Every hardware physical unit is associated to an object called Resource Block, which handles all the platform specific events. Instruments in this case are primarily sensor nodes raising analog (Pressure, temperature, Gas etc.) alarms or discrete (level) alarms. Such instruments then have Analog/ Discrete Alarm Blocks. Smart Tags and people contain information blocks, which could contain capabilities, certifications and validity. In one sense the people and assets have similar attributes applied in different contexts like storage tanker containing information about corrosiveness, material used, and last inspected date, a person operating the equipment containing required permits, training and injury history. A logical view of the system component structure was drawn as in Figure 3.

TABLE 17 OR3C DEFINTION

Interface	Rationale	*a	*b
Observe (O)	An interface used to observe set of critical parameters like Alarm points, Query Lists etc	✔	
Review (R)	An interface used to review Function block parameters from individual entities	✔	
Configure (C)	An interface used to configure the function block parameters and schedule individual entities		✔
Control (C)	An interface used to schedule individual entities blocks to a particular mode of operation either to raise manual alarms or to simulate behaviors		✔
Calibrate (C)	An interface used to update the operating state of the devices i.e to calibrate / re-position sensors or to update questionnaires		✔

*a – Typical Operation by Public Safety Personnel

*b – Typical Operation by Process Engineering Personnel.

The kernel shown encapsulates the platform building blocks which are abstracted away from the communications design. The communications package displays the OR3C interface and an Alerting interface. The communication interface acts as the common interface to communicate between the PPT elements. The OR3C interface is explained in Table 17. The observe and review interfaces are required primarily for the public safety operations to measure exceptions and compliance factors. The other three interfaces are primarily used by the field personnel to operate these devices. The basic block definition contains the parameters shown in Figure 4. There is a parameter called Block Alarm (blk_Alarm) a 16-bit bit flag member variable which denotes the alarm status of the block. Each block could have its own definitions as shown in Table 19.

The Alerting service interface shown in Figure 3 utilizes this Block Alarm bit-string object to transmit alarm status. One bit is reserved for communicating OUT_OF_SERVICE status to recipients. During the analysis of safety models and accident it was found that accident causations can be classified to Functional Safety or Cognitive Requirements or Theory of Constraints. Smart Tags are activated in the model either through *Rules* or *Human interaction*

(Diagnostic Sensing, Manual Verification and Periodic Inspection). Thus the smart tags information block provides Alert in these categories as shown. People information blocks are shown with respect to people operating the equipments. In this case it is predominantly personnel in the process industry. The first bit represents if the people have actively ACKNOWLEDGED the Safe Operating procedures. Bit 5 represents alarms arising because of lack of training or pending trainings.

With this set of information, the choice of protocols was made. A protocol design was intentionally avoided to add new protocol layers and complicate the system. The IOT protocols MQTT-S [7] & CoAP[8][9] were compared to find suitability for the Safety management application needs. As our medium is LTE dependent, CoAP had the capabilities of delivering contents over control plane[10] and promises to evolve with innovations in LTE networks and backing of Lightweight M2M Alliance. The Table 18 shows the details of the comparison and based on the analysis CoAP was chosen.

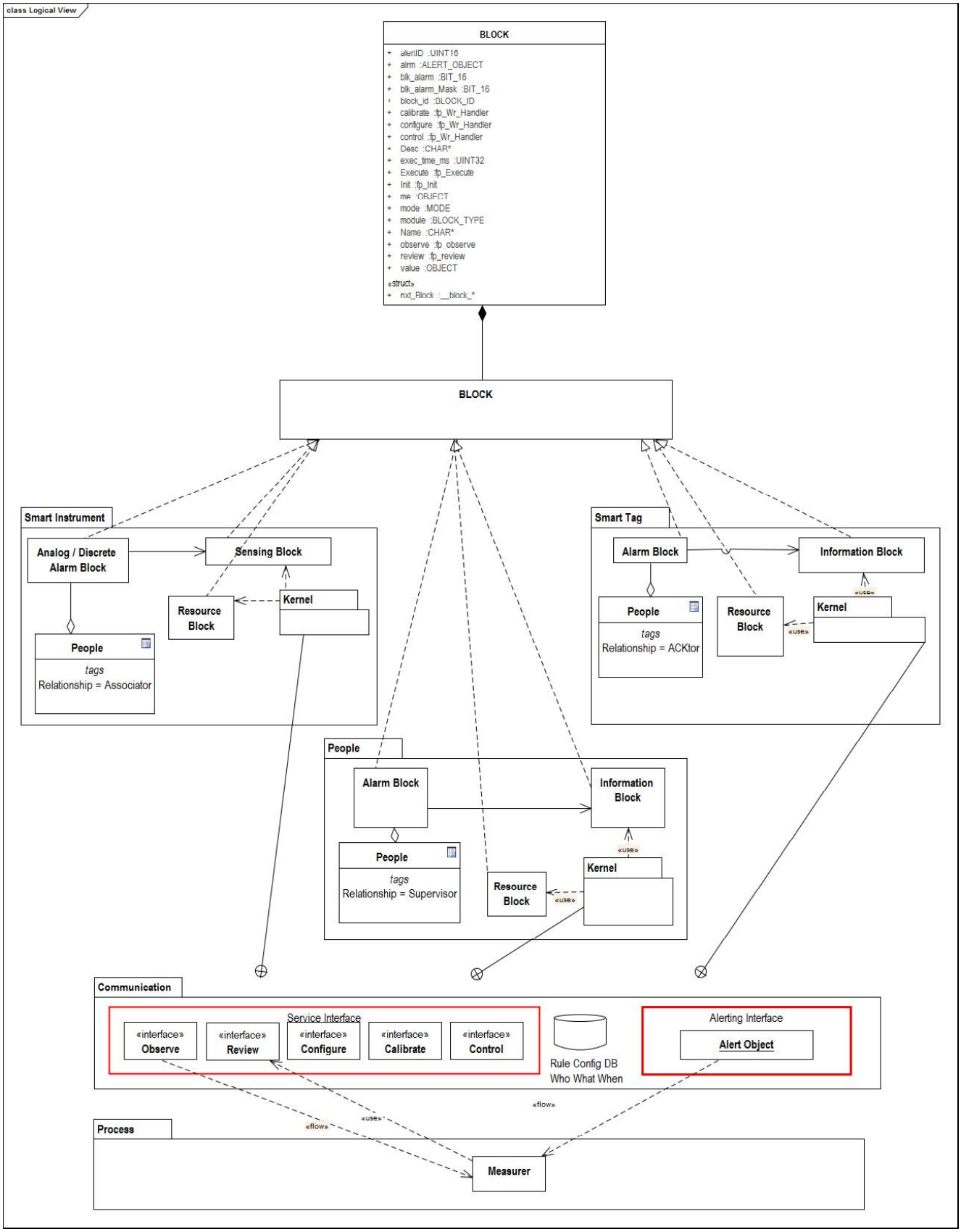

FIGURE 3 DETAILED COMMUNICATIONS ARCHITECTURE

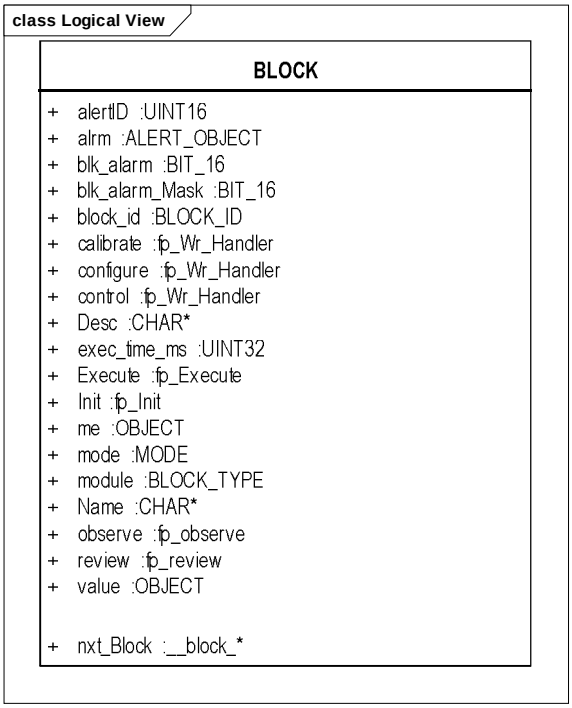

FIGURE 4 BLOCK DEFINITION

TABLE 18 PROTOCOL COMPARISON

MQTT - S	CoAP
Protocol Broker Oriented Architecture	**Web Services Oriented Architecture**
Network Address Traversal	Server discovery
Messaging and Publish Subscribe	**Responsive (Request Response) + Publish Subscribe Option**
Communications in user application plane	Possible to communicate in control Plane.

Table 19 Alert Bit

Bit Field	Resource Block	Analog Alarm Block	Sensor Block	People Info Block	SmartTag Info Block
i.	DIAG_OVER_DUE	CFG_ERR_SET_POINT_HI_HI	CHNL_TIME_OUT_ERR	UN_ACK_STATE	CR_ALARM
ii.	POWER_FAILURE_FAULT	CFG_ERR_SET_POINT_HI	CHNL_LP_BACK_ERR	TASK_ALARM_1	FS_ALARM
iii.	FOSC_FAULT	CFG_ERR_SET_POINT_LO	CHNL_VARIANCE_ERR_HI	TASK_ALARM_2	TOC_ALARM
iv.	ABNORMAL_REBOOT_FAULT	CFG_ERR_SET_POINT_LO_LO	CHNL_VARIANCE_ERR_LO	TASK_ALARM_3	
v.	ROM_FAULT	CFG_ERR_DEADBAND	CALIB_DUE	TRAINING_PENDING	RULE_ACTIVE_ALERT
vi.	RAM_FAULT	CFG_ERR_HI_RANGE	ZERO_FAIL_TOO_HI	INJURY_ALARM_1	DIAG_FAIL_ALERT
vii.	BOOT_ERROR	CFG_ERR_LO_RANGE	ZERO_FAIL_TOO_LO	INJURY_ALARM_2	PER_INSPC_FAIL_ALERT
viii.	RES_CFG_ERROR	ERR_TRANSDUCER	SPAN_FAIL_TOO_HI	INJURY_ALARM_3	PER_INSPEC_OVERDUE
ix.		ALARM_HI_HI	SPAN_FAIL_TOOO_LO		
x.		ALARM_HI			
xi.		ALARM_LO			
xii.		ALARM_LO_LO			
xiii.	RES_LOW_BATTERY	ALARM_OOR_LO			
xiv.		ALARM_OOR_HI			
xv.					
xvi.	OUT_OF_SERVICE	OUT_OF_SERVICE	OUT_OF_SERVICE	OUT_OF_SERVICE	OUT_OF_SERVICE

4. SERVICE API & OR3C INTERFACE DEFINITION

Having chosen CoAP as a protocol of choice, the service APIs are defined based on the basic CoRE technology definitions. CoAP provides the following messages

GET , PUT, POST, & DELETE.

Each CoAP server node is discoverable with the following uri.

coap://<Device Name or ID >/.well-known/core/

a request framed like this

GET /.well-known/core helps to discover different objects or endpoints that the CoAP server contains.

In the case of PPT model for safety management described above, the following URIs shall form the basic structure

GET /.well-known/core shall return

/model_type

/resource_block

/analog_alarm_block

/sensor_block

for the "Smart Instrument Category". All the three elements i.e. People, Smart Tags, and Smart Elements contain the same URI definition for **model type** and **resource_block.** The other block definitions are characteristics of the individual model elements.

The basic block definition is same for all the blocks and hence, each Block shall provide a URI of the following form

GET /<block>/blk_error

GET /<block>/mode

With these URIs each of the block status can be individually monitored.

On a bigger view, the functionality beyond monitoring, i.e. for active query / update cycle is necessary. Use cases like associating people or reviewing check lists through Tags or updating

alarm thresholds or setpoints becomes necessary. In this context the CoAP protocol is extended to support binary read write functions conforming to OR3C interface definition.

CoAP provides ways to add new request types in the GET and PUT requests using Options field in the CoAP header.

A GET request with a URI goes with a OPTION field of URI.

In this research to extend the CoAP for binary M2M communications we utilize an additional option type called OR3C. A generic GET request is defined in this form

GET OR3C BLK_ID MEMBER_ID

PUT OR3C BLK_ID MEMBER_ID VALUE

This definition of Block identifier and member identifier is similar to the definitions used in CPF -1 in IEC 61499 / Foundation Fieldbus.

The type definitions of different MEMBER's may not be available at the client end and hence for this reason, each CoAP server block provides auxiliary service to discover the parameter dictionary through a query like

GET / <block> /dictionary

TABLE 20 SUMMARY OF SERVICE API DEFINITION

Service Type	Method	Remarks
DISCOVERY	GET /.well-known/core	Enables identifying the end points in each of the service end points
OBSERVE the device	GET /observe /	Returns a composite object containing the basic function Blocks Status & Value
OBSERVE the blocks	GET OR3C : Observe : Block ID : View#	Returns a list of parameters stored in a view collection identified by the view number.
PUT values to the block Parameters	PUT OR3C : Configure Block ID Member ID Value	Writes the value into the specified block parameter.
GET dictionary	GET /<block>/dictionary	Returns a type dictionary and object definition of Blocks stored in the device.
POST /.well-known/core	POST /.well-known/core	Enables the CoAP discovery agent to collect information about different nodes

5. CASE ANALYSIS

In order to validate this protocol design for the Safety GRID, the case of Storage Tank Safety is analyzed.

The following messages are used

CoAP MSG Type	Purpose
OBSERVE	Is available to a multicast set of Subscribers in a particular group.
GET	Is available upon directed read request
PUT	Is available upon a directed write request.
POST	Is used to POST messages to known set of entities i.e. to Public Safety Bodies

Table 21 Asset Design & Operation

Things		**SmartTag**					
	People	Parameter	Bloc	Member	Type	Method	Use cases
Rules	AcK	Permissible Exposure Limit	INF	PEL	Float32	OBSERVE	**Ops. People :** Automatic updates for PEL values **Public Safety :** Rule based verification if PEL values are set and within range.
				UNIT	String		
		Storage	INF	STOR	String	GET PUT POST	**Ops People:** Know what chemical is stored or change to what chemical is stored. **Public Safety:** Monitor what material is stored in the specific tank and monitor against non compliance.
		Max. Inventory	INF	MAX	Float32	OBSERVE	
				UNIT	String		
		Toxicity	INF	TOX	Boolean	OBSERVE	
	Associate	Construction Work	RES	CSTR	String	GET	**Ops People:** Know the details about design and seek clarifications for change management.
		Electrical Work	RES	ELEC	String	GET	
Verify	AcK	Design Codes	INF	CODE	String	GET	**Ops People:** Know the details about design and seek clarifications for change management.
		Process Chemistry	INF	CHEM	uri	GET PUT POST	**Ops People:** Know what chemical is stored or change to what chemical is stored. **Public Safety:** Monitor what process used and audit change management.
		Process Control System	INF	CTRL	Uri	GET PUT POST	
		Safe Operating Range	INF	RANG	Float32 Float32	GET	**Public Safety:** Monitor what process used and audit change management.
	Associate	Corrosiveness	INF	CRVS	List	GET PUT POST	**Ops People:** Verify corrosiveness checklist and update. **Public Safety:** Audit corrosiveness verification procedure.
	Inform	Reactivity	INF	REAC	uri	GET	**Ops People:** Know the details about design and seek clarifications for change management.
		Process Flow Schematics	INF	PRCS	uri	GET	

Things		Smart Instrument					
Rules	Ack	Capacity	AIO	CPCT	Float32	GET	Level Transmitter to measure actual level available.
		Composition	AIO	CMPS	String	GET	Stored parameter to display actual composition of chemical
		Flow	AIO	Value	Float32	OBSERVE POST	Get actual flow value. POST alarms for exceptions
		Pressure	AIO	Value	Float32	OBSERVE POST	Get actual pressure value. POST alarms for exceptions
		Temperature	AIO	Value	Float32	OBSERVE POST	Get actual temperature value. POST alarms for exceptions
		Hazard. effect (Gas/Chem Sensor)	AIO	Value	Float32	OBSERVE POST	Get actual chemical conc. value. POST alarms for exceptions
Verify	Inform	Stability	INF	STBL	String	GET	Usable for Cognitive Audits and digital record keeping.
		Inventory Levels	INF	LVL	String	GET	Usable for Cognitive Audits and digital record keeping.
		Consequences	INF	CNSQ	String	GET	Usable for Cognitive Audits and digital record keeping.
	Associate	Inlet	AIO	Value	Float32	OBSERVE POST	Get actual flow. value. POST alarms for exceptions and diagnostics
		Outlet	AIO	Value	Float32	OBSERVE POST	Get actual flow. Value. POST alarms for exceptions and diagnostics

TABLE 22 COMPLIANCE

Things		SmartTag					
	People	Parameter	Bloc	Member	Type	Method	Use cases
Measurer	AcK	Proof Test – Sub System Integrity	ALL	BLK ERROR	Bit-string	GET POST	Smart devices enable diagnostics and send the updates via Block Error.
		Proof Test – System Integrity	ALL	Not Applicable		GET POST	The system integrity shall be measured in common monitoring gateway or controller to cumulatively raise alarms.
	Associate	Frequency	ALL	PT_DATE	Date-time	GET PUT	The next test date is updated in the system or each of the block. The appropriate user is also associated, i.e. the person can perform necessary activity.
Rules	Ack	Certificates	INF	CERT	Uri	GET PUT POST	Certificates are updated from latest 3rd party / agency certifications.
		Expected remaining Life	INF	LIFE	Float32	GET	Used by ops. Person for knowing the remaining life of the product.
Verify	Ack	Last Date of Maintenance	INF	MAINT	Date-time	GET PUT POST	Used by ops. Person to update the maintenance and usage status.
		Last date of Use	INF	USE_DATE	Date-time	GET PUT POST	For remote monitoring it is desired to use Caching POST interface than on demand GET interface.
		Operational State	ALL	MODE	Mode	GET PUT	A status parameter as enumeration indicating different states in which the entire block can function. OUT_OF_SERVICE MAINTENANCE MANUAL NORMAL CONFIG_ERROR

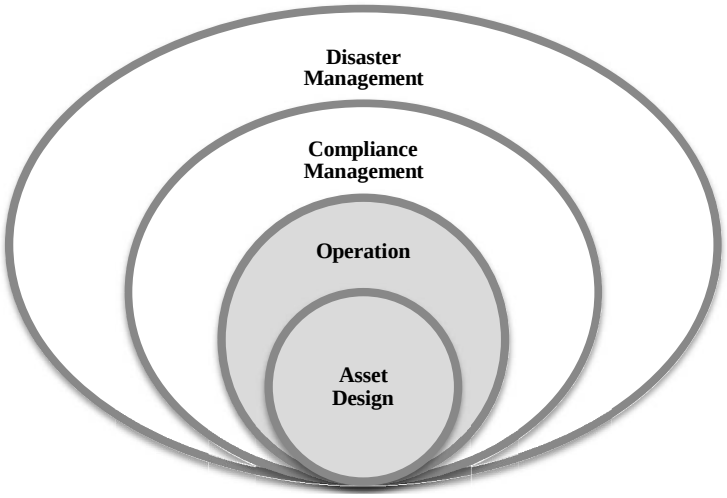

FIG. 5 LAYERS OF PROTECTION SAFETY MANAGEMENT STRUCTURE

Title	Description	Protocol Usage	Coverage Bodies		Coverage%
Records Management	Availability of Onsite Plans, Jurisdiction, Compliance Adherence Information – *OBSERVE* *5) Tank Size* *6) Stored Chemical Identifier* *7) Tank NDT – Proof Testing Information* *8) Mandatory regulatory Health Check Records*	Possible to GET values from Smart-Tags INF Blocks. All requests disperse as GET coap: //<DeviceID >// OR3C	LE EMS FR ECC	Source Covered Covered Covered	100 %
Rapid Assessment	Situational Assessment, typically available from the first crew to investigate damages, typically the First Responder – Initiator - *ORIENT* *4)* Identification of Gas Leak or Chemical Spill *5)* Estimated number of People / Life under threat *6)* Best Muster Zone	1) Covered by the Smart-Instrument to respond with stored chemical details and the quantity just before the disaster. 2) Need support from ECC and Jurisdiction to share people data. – Not covered. 3) Annunciate Mustering area through Alarm systems. Communication to Alarm systems can be carried out traditionally. - Smart Annunciator can be a variant product.	LE EMS FR ECC	Not Required Covered Covered Source. *Sharing of people occupancy information has to be investigated further.*	66%
Hazard Assessment	Typical Assessment of Hazard and potential cause. – *ORIENT – OBSERVE* *4)* Identifying Safe resorts and Musters *5)* PPE Identification and call for specialists *6)* Identifying known and unknown chemicals.	1) & 2) are carried out traditionally. Both these require strong Voice over LTE capabilities and other technologies. 2) Smart Instruments provide different chemical composition data and shared via POST messages with Block ID, chemical Type and measured concentration / quantity.	LE EMS FR ECC *Requirement 1&2 require human cognition to seek specialties and schedule the resources through interaction.*	Not Required Covered Covered Covered – Common End point for all the 3 agencies	33%
Resource Management	Deployment Planning of Trained Resources, PPE, Hospital Management – *DECIDE*	Status of used /in-use devices or people are measured using GET interface.	LE EMS FR ECC	Source Source Source Source	100 %
Tasking	Execution Strategy and real-time availability of information - *ACT*	Public Safety personnel and Para med's are scheduled and tasked using PUT services in respective PEOPLE blocks or Muster Zones block. PEOPLE – Operating Mode – Transition from **Normal to Occupied** Each people block has Personal Protection Parameters like Short Term Exposure, Long Term Exposure, SCBA Status etc.	LE EMS FR ECC	Covered – Generally not required but for Accident Investigation and Post Incident Analysis the LE People are used. Covered Covered Covered	100 %

Legend	
EMS- Emergency medical Services **LE – Law Enforcement** **FR - First Responders** **ECC – Emergency Command Center**	*Items in italic are not satisfactorily answered by the systems / communications design and would need further investigation / research.*

Table 23 Emergency Management Scenario

The Safety Management structure is constructed as shown in Fig. 5. The Object in the center is the entity or asset to be safeguarded. The asset includes both physical objects i.e. as Industrial plants and people working or occupying in the vicinity. The layers of protection are shown as Compliance Management (Regulatory with regularized audit processes) followed by the Disaster management group. The described communications are studied against the cases of Asset Construction and operation, Compliance Management and Disaster Management detailed in , Table 22 and Table 23.

CASE 1: Asset Design / Construction and Operation

The information model defined for Asset, Design and Construction contained elements listed in Table 21. The table is structured to provide the information on BLOCK, MEMBER and Communication Method or interfaces and potential use cases by the Operations people and the public safety / law enforcement agencies. ***As seen from the table all the information elements can be sufficiently expressed in the proposed communication layer***. Many of the PUT methods also give rise to a POST message to Public safety end points, enabling easier change management policy tracking. The information model structured the underlying Safety Process to be either Rule based or physical action (Verification/Measurement) based. This communication structure enables the scheduling of these actions based on the occurring events through Smart Tags or Smart Instruments.

CASE 2: Compliance Management

The information model expressed the compliance management elements as measuring

a) Proof Testing at System & Sub System Level
b) Verifying Certificates, remaining life, operating state etc

as seen in the Table 22.

The Function Block Structure is constructed of Block error parameter that was discussed in Table 19. In compliance management scenario these bits express the sub system integrity and as per the IEC definition of Safe Operation, each block can force its behavior to a known – fail safe

state i.e. Out_of_Service when in error. ***The overall system integrity though cannot be measured by this scheme, needs an integrator or aggregator device to compute the overall system integrity.*** All other information elements are sufficiently expressed by the communication method proposed.

CASE 3: Emergency Management

In emergency management scenario, the needs of different agencies where compared in the safety management information needs. APCO also identified similar findings in their recommendations[11]. In Table 23 , the information sharing needs for common operating picture is listed and compared with the proposed communications definition as described in column 'Protocol Usage'. There are certain requirements from Rapid assessment and Hazard Assessment that are not met by the proposed design and would require further investigation. ***The information required are like occupancy of people, best mustering zones and specialty of people and scheduling their availability for task in hand needs. This requires further research to connect these requirements to this communication model.*** The other information requirements meet the communication design model defined.

6. CONCLUSION & FUTURE WORK

A cohesive function block architectural model was developed with CoAP as the basic means of transport for Smart Things (Instruments and Tags). The new enhancement of options field was CoAP protocol was developed to satisfy the communication needs and cohesively verify that the information needs in Asset Design & Construction, compliance management and public safety audits is covered by the design enhancement. Most of the disaster management needs are covered by the protocol scheme. Some aspects in emergency management require further investigation i.e. estimating number of people affected by the disaster and establishing human organizational chain to utilize competent people to task for disaster containment. Different solutions exist to select specialists and also track/associate PPE today. These do not conform to the common communications requirement and may require stronger standardization initiatives. These Information model & API definitions provide a means for the Emergency command center and law enforcement to fuse and operate this larger set of data. This work considers LTE as a

medium for establishing communications. The presented work considers the devices and people connect in a typical M2M network as LTE UE (user equipment) nodes. In the public safety LTE work by 3GPP , the focus is on enabling TETRA replacements with LTE systems. This research in the future would focus on specific optimizations in the LTE network for a SafetyM2M network deployment.

7. *REFERENCES*

[1] C. K. N. S. S B Aanandh, "A Review of Functional Safety Models for Public Safety Management Systems," *Journal Of System Safety*, pp. 20-31, 2014.

[2] 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].

[3] "Public Safety Architecture Framework Volume I, II, III," 2006.

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

[5] V. Vyatkin, IEC 61499 function blocks for embedded and distributed control systems design, ISA-Instrumentation, Systems, and Automation Society, 2007.

[6] S. Lehnhoff, W. Mahnke, S. Rohjans and M. Uslar, "IEC 61850 based OPC UA Communication-The Future of Smart Grid Automation," in *17th Power Systems Computation Conference (PSCC 2011), Stockholm*, 2011.

[7] U. Hunkeler, H. L. Truong and A. Stanford-Clark, "MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks," in *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, 2008.

[8] Z. Shelby, K. Hartke, C. Bormann and B. Frank, "Constrained Application Protocol (CoAP), draft-ietf-core-coap-13," *Orlando: The Internet Engineering Task Force--IETF, Dec*, 2012.

[9] B. C. Villaverde, D. Pesch, R. De Paz Alberola, S. Fedor and M. Boubekeur, "Constrained application protocol for low power embedded networks: a survey," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, 2012.

[10] M. Becker, K. Kuladinithi and T. Ptsch, *Transport of CoAP over SMS and GPRS*, 2011.

[11] APCO International, "Unified CAD Project," 2013. [Online]. Available: https://www.apcointl.org/component/docman/doc_download/375-high-priority-info-sharing-needs-for-emerg-comm-and-first-responders-final-pdf.html?Itemid=725.

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

[13] 3G Partnership Program, "3GPP Public Safety," July 2013. [Online]. Available: www.3gpp.org/public-safety.

[14] "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].

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

[16] 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.