EVALUATION OF SMART SENSOR BASED SOC ARCHITECTURE FOR THE INDUSTRIAL INTERNET OF THINGS

[1]K HANUJA, [2] Dr SARDAR KHAME SINGH, [3] P MOUNIKA
[1]Research Scholar, LPU &Associate professor, [2]Professor, [3] Assistant professor
[1,2,3]ECE Department, St. Martin’s Engineering College, Secunderabad

ABSTRACT

Historically, Industrial Automation and Control Systems (IACS) were largely isolated from conventional digitalnetworks such as enterprise ICT environments. Where connectivity was required, a zoned architecture wasadopted, with firewalls and/or demilitarized zones used to protect the core control system components. Theadoption and deployment of ‘Internet of Things’ (IoT) technologies is leading to architectural changes to IACS, including greater connectivity to industrial systems. The main contribution of this paper is the design,implementation and experimental verification of an architectureof a Smart Sensor that satisfies the operational requirementsneeded by the Industrial Internet of Things (IIoT). Consideringthe software and hardware adaptability that a Smart Sensorshould have, this work takes advantage of the characteristicsof the current Field Programmable Gate Arrays (FPGA) andSoC to implement a Smart Sensor for the IIoT. In this sense,the proposed Smart Sensor architecture incorporates real-timeoperation features, the ability to perform local data analysis, highavailability communication interfaces such as High-availabilitySeamless Redundancy (HSR) and Parallel Redundancy Protocol(PRP), interoperability (industrial protocols) and cyber-security.The architecture was implemented with hardware available inthe market, IP cores and Python libraries developed by thirdparties. Finally, to validate the applicability of the architecturein the industry, two test environments were implemented. In thefirst case, interoperability, high availability, synchronization, andlocal data processing are validated.

1. INTRODUCTION

The concept of Industrial Automation and Control Systems (IACS) iswell established. These systems, often referred to as OperationalTechnology (OT), are employed in diverse industries including manufacturing,transportation and utilities, and are sometimes referred to ascyber-physical systems (CPS). Since the term Internet of Things (IoT)[1] was first used in 1999, it has been applied to connected devices inconsumer, domestic, business and industrial settings [2]. Althoughthere is a significant amount of literature attempting to define IoT, itsuses, and its typical components, it is rarely made obvious how any ofthis applies in the industrial setting.

Because current definitions of IoT invariably imply a similar approachto the high-level architecture of a system, the ubiquitous use ofthe term IoT to refer to the use of digital technologies in industry isunhelpful as it hinders the analysis of alternative system architectures,including the location and nature of the data or information processing,and associated performance and security issues. The aims of this paperare to improve on existing definitions of Industrial IoT (IIoT) and topropose a framework for IIoT components as a basis for analysing theuse and deployment of IoT technologies in industrial settings. In undertakingthis research our aim was to establish a framework that allowsus to analyse the nature of IIoT devices and their uses, which is tobe used as part of a vulnerability and threat analysis process for thesedevices. By being able to characterise the devices in a systematicmanner, we anticipate being able to analyse cross-cutting threats andvulnerabilities and identify patterns that may be obscured whenfocusing on the technology employed or sector specific issues.

The Industrial Internet of Things (IIoT) is a logical consequence of widely presentcomputing ubiquity and interconnectedness. With simple beginnings in 1982, CarnegieMelon University researchers connected a vending machine to the Internet allowingto query the state of Coke in the machine (empty, warm, cold) before walking to buya soda [3]. In this sense, the vending machine was the first Internet of Things (IoT)device. It was actively sensing its environment, storing and processing information andhad connectivity to its stakeholders. The current trend of IIoT (digitalization) seenaround the world is an evolution of this simple scenario.

Technological and business opportunities and challenges within IIoT have given riseto a \zoo" of software solutions. In this context \zoo" implies variations of size, domain,methods, forms (web app, smart app, libraries, tools), solutions and more. Computing domains in industry are commonly grouped into operational and informationtechnology (OT, IT). They are shaped by different requirements and environments:one focused on control (automating mechanical processes), real-time requirements, reliabilityand long life cycle etc.; the other focused on data management, process efficiency,business process management and frequent updates etc. This impacted the developmentof hardware, communications and software.

Smart sensors are necessary devices for the developmentof the Industrial Internet of Things (IIoT). In IIoT,in addition to the real-time operation, high availability, interoperability,and cyber-security characteristics that SmartSensors provide, IIoT also takes advantage of the enormousamount of data that Smart Sensors generate and Machineto-Machine (M2M) communication to incorporate automaticlearning and Big Data technologies into the production system. The philosophy behind IIoT is that machines with ahigh level of intelligence are better than humans at capturingand communicating data accurately and consistently. With thisdata, companies can more quickly detect malfunctions andproblems, even before they occur, saving time and money.Particularly, in the manufacturing industry, the IIoT will allowbetter product quality control while maintaining traceabilityand efficiency in the supply chain, with the aim of achievingsustainable and ecological production.

The main contribution of this paper is the design, implementationand experimental verification of an architectureof a Smart Sensor, which can be implemented in a SoCplatform, considering the operational requirements that theIIoT needs. In this context, the proposed architecture incorporatesreal-time operation features (latency, determinism,synchronization), the ability to perform local data analysis,high availability communications (HSR/PRP), interoperability(industrial protocols) and cyber-security.

2. LITERATURE REVIEW

1.Menon et al.(2013) The purpose of this investigation is to know the credibility ofrealizing Internet of Things in transport transportation system in Singapore.Singapore is known for its advancement movements, still has scope for improvementto the extent development being used for transportation purposes. There is anecessity for the customer to understand and survey particular transport options in acompelling way and this is the place Internet of Things structure can offer help.

2.**Quan et al.(2013)** As indicated by them There are such a large number of issuesin security of Internet of Things (IoT) shouting out for arrangements, for example,RFID label security, remote security, organize transmission security, securityinsurance, data preparing security. This paper depends on the ebb and flowexamines of system security innovation. Also, it gives another way to deal withspecialists in certain IoT application and outline, through investigating andcompressing the security of IoT from different ways .

3.**Zhou et al. (2013)**The Internet of Things gives the client a novel methods forspeaking with the Web world through universal question empowered systems.Distributed computing empowers an advantageous, on request and adaptablesystem access to a mutual pool of configurable registering assets. This paperprimarily concentrates on a typical way to deal with incorporate the Internet of Things(IoT) and Cloud Computing under the name of Cloud Things design. We survey thebest in class for coordinating Cloud Computing and the Internet of Things. We lookat an IoT-empowered shrewd home situation to break down the IoT applicationnecessities. We likewise propose the Cloud Things design, a Cloud-based Internet ofThings stage which suits Cloud Things IaaS, PaaS, and SaaS for quickening IoTapplication, improvement, and administration.

4.Vishwajeet H. Bhide(2014) gives completely keen condition observing by differentsensors for perusing vital information to consequently alter the solace level in homesby streamline utilization of vitality. he likewise utilized estimation here forconsequently discovery and determination of any issue in the gadgets. For that he isutilizing Naïve Bayes Classifier calculation for information mining. It will convey emailor SMS to required specialist for administration and it will likewise tell the proprietor.This gives a colossal favourable position on the brilliant home frameworks utilizingIoT.

5. SapandeepKaur and IkvinderpalSingh(2014) kept an eye on the Internet ofThings. The Internet of Things continues ensuring its basic position with respect toInformation and Communication Technologies and the change of society.Distinguishing proof and following advancements, wired and remote sensor andactuator systems, upgraded correspondence conventions and conveyed knowledgefor keen items are only the most applicable. As one can undoubtedly envision, anygenuine commitment to the progress of the Internet of Things should essentially bethe consequence of synergetic exercises led in various fields of learning, forexample, media communications, informatics, hardware and sociology. In such anunpredictable situation, this study is coordinated to the individuals who need toapproach this mind boggling control and add to its improvement.

3. INDUSTRIAL INTERNET OF THINGS (IIOT)

Whilst there are numerous IoT definitions, those of relevance toindustrial application make explicit the kinds of smart components thatget embedded into ordinary objects so that those objects can count

asIoT devices, and form constituents of cyber-physical systems (CPS).
Three relevant definitions are:
• A definition for the IoT would be a "group of infrastructures, interconnectingconnected objects and allowing their management,data mining and the access to data they generate" where connectedobjects are "sensor(s) and/or actuator(s) carrying out a specificfunction that are able to communicate with other equipment" ;
• "The terms 'Internet of Things' and "IoT" refer broadly to the extensionof network connectivity and computing capability to objects,devices, sensors, and items not ordinarily considered to be computers.These"smart objects" require minimal human intervention togenerate, exchange, and consume data; they often feature connectivity to remote data collection, analysis, and management capabilities"; and
• "The IoT represents a scenario in which every object or 'thing' isembedded with a sensor and is capable of automatically communicatingits state with other objects and automated systems withinthe environment. Each object represents a node in a virtual network,continuously transmitting a large volume of data about itself and itssurroundings…".
On the basis of these, an initial definition of IIoT might be: the use ofcertain IoT technologies – certain kinds of smart objects within cyberphysicalsystems – in an industrial setting, for the promotion of goalsdistinctive to industry. Similar simple definitions were found in ourliterature search, for example:
• "The Industrial Internet of Things (IIoT) is the use of Internet ofThings (IoT) technologies in manufacturing" ; and
• "Industrial Internet: A short-hand for the industrial applications ofIoT, also known as the Industrial Internet of Things, or IIoT".
Such a simple conception is not sufficient for our purposes in thispaper, however. We need something substantive and a precise conceptionto inform our proposed IIoT framework. The simple conceptiondoes provide a template for a definition of IIoT, for it correctly attemptsto define IIoT by appeal to two essential features: (a) the kinds of technologies that are used in an IIoT setting and (b) the distinctive aimsand purposes to which those technologies are put. We need a definitionwhich has that structure, but which gives us a more substantial expansionof (a) and (b).An advantage of the simple conception is that because it makes itclear that the relevant technologies are used for purposes distinctive toindustry, it satisfies the basic criterion of enabling us to distinguish IoTdevices from IIoT devices. For example, devices such as smart bike locksand smart kettles are not useful from the point of view of industry per se,the simple conception correctly classifies those items as non-IIoT devices.
Despite this advantage, the definition remains uninformativenevertheless.A further pitfall to avoid when attempting to arrive at a definition ofIIoT is defining IIoT in terms of some other notion, which is not obviouslydifferent from the notion of IIoT itself, which would render thedefinition uninformatively circular. That sort of problem is exemplifiedin the industry-driven literature by, for example:
"The IIoT vision of the world is one where smart connected assets(the things) operate as part of a larger system or systems of systemsthat make up the smart manufacturing enterprise".Since 'smart manufacturing enterprise' is essentially an industrialenterprise that exemplifies the features of IIoT, this definition is alsouninformatively circular.
In seeking to formulate an improved conception of IIoT we searchedthe contemporary academic and industry-driven literature for moreinformative definitions than those already cited. We found a few thatimproved on the simplistic and circular definitions already presented.A definition that improves incrementally over the simple definitionis:
"Industrial Internet or Industrial Internet of Things (IIoT) is built forbigger 'things' than smartphones and wireless devices. It aims atconnecting industrial assets, like engines, power grids and sensor tocloud over a network".
This definition goes beyond the simple conception by making itexplicit that it is industrial assets which are counted as connected in anIIoT setting, and it tells us a little about the nature of that connection that the relevant assets are connected to a cloud, over a network.A second definition which adds some further details is:"The Industrial Internet of Things (Industrial IoT) is made up of amultitude of devices connected by communications software. Theresulting systems, and even the individual devices that comprise it,can monitor, collect, exchange, analyse, and instantly act on informationto intelligently change their behaviour or their environment– all without human intervention"
The central advantage of this still admittedly vague definition is thatit makes it clear what the function of IIoT devices is: to monitor, collect,exchange, and analyse information so as to enable them to change theirown behaviour, or else instruct other devices to do so, without humanintervention.
A number of researchers writing in German, offer a cluster of definitionsof IIoT that share a focus on the kinds of technologies which areput into operation in IIoT settings, and the ways they are put to use inthose settings. It is suggested that a central element of IIoT is its reliance, in an industrial setting, on objects, systems and machinery whichhas been upgraded to the status of a CPS, so that products and servicescan be guided through the supply and value chains in an

autonomousmanner. Another perspective is that IIoT relies not just on CPS, butalso on embedded systems, cloud computing, edge computing, thegeneric technologies associated with the smart factory, and associatedsoftware. A further insight relates to the aims and purposes of IoTtechnologies, suggesting that they should not merely function to enableautonomous production, but enable real-time information to users,consumers and other processes.

4. METHODOLOGY

A Smart Sensor consists of a processing unit, a dataacquisition module and communications module. Fig. 1shows a high-level block diagram of the architecture of ageneric Smart Sensor.The data acquisition module is responsible for collectingdata (such as temperature, pressure, image, sound) from thephysical environment and sends it to the processing unit. Thismodule is composed of one or several transducers, signalconditioners, Analog to Digital Converter (ADC) and DigitalSignal Processors (DSP). At present all the elements that makeup the acquisition module can be integrated into a single circuitcalled MicroElectro-Mechanical Systems (MEMS). MEMSuses microfabrication technology to integrate miniaturizedmechanical and electromechanical elements into electronicdevices, such as accelerometers and gyroscopes.The processing unit is responsible for controlling all theelements that make up a Smart Sensor. It also manages the useof resources such as the communications module, memory, Input/Output (I/O) peripherals and application execution. Thereare several types of devices that can be used as processingunits, for example, microcontrollers, SoC and FPGA. Thechoice of each depends on the complexity and functionalityof the Smart Sensor. Also, in the processing unitis where the data is manipulated using specialized software,and the results can be sent to central stations or presented graphically to the user or in tables easy to interpret. Softwaredeveloped for a smart sensor must be able to adapt to changesin the structure of the smart sensor and be easy to use. Itis required collaboration and cooperation between informaticsexperts, those responsible for the management of the systemto which the application is directed and users.

The communications module is responsible for transferringthe data generated in the Smart Sensor to local or remotecontrol and monitoring stations. Depending on the amountand distance of data transmission, the communications moduleincorporates several low (RS-232, RS-485) and highspeed(Ethernet, SPI) interfaces. The universality together withthe communication protocols that can be implemented overEthernet make it the ideal means to link different devicesin the industrial environment. Ethernet allows sensors in theprocess network to be interconnected directly with the devicesin the management network, eliminating the use of protocolconverters (gateways) that increase runtimes and limit theiruse in real-time applications.

Technological advances in the fields of FPGA and SoC hasrevolutionized the way electronic systems are designed. TheFPGA has evolved from being a simple tool for the creation ofprototypes to being an essential solution for the developmentof devices that require high processing capacities, real-timeoperation requirements, interoperability, flexibility, safety, andhigh availability. The current FPGAs, in addition to the large

Resources they integrate (millions of logical cells, various typesof memory and peripheral interfaces), also integrate ARMprocessors implemented in silicon. Thanks to these new FPGAmanufacturing techniques, the sensors are getting smaller andcan perform more processing, allowing the execution of morecomplex applications, such as machine learning algorithmsand data analysis, introducing the Big Data concept in thefield of sensors, giving rise to so-called Smart Sensors. Theflexibility of the FPGA offers the possibility of adding thesenew features, some developments in this respectare outlined. Describes the design of neural networksin FPGA. Intel proposes the use of OpenVINO as atool for the development of artificial intelligence and machinelearning projects. The use of accelerators for use as IP cores inmachine learning is proposed. Finally in wecan find an extensive review on this area of research. At thesoftware level, the Linux operating system offers possibilitiesto extend the capabilities of the Smart Sensor, for examplewith the use of development tools such as Python it is possibleto provide the system with the ability to execute industrialcommunication protocols such as Modbus. The fundamentalchallenge of this work is to take advantage of the features ofthe current FPGAs that integrate silicon-embedded processorsto propose a hardware-software architecture of a Smart Sensor.

The proposed work considers the use of a SoC platform(microprocessor + FPGA) for the implementation of an intelligentsensor for the IIoT. In the proposed architecture, allIIoT requirements have been considered, in this sense, the architectureincorporates: a) A processing unit (microprocessor)to run the architecture management software, and to performdata processing and analysis (Big Data). b) An IP Core 1588 toensure synchronism in the order of nanoseconds. c) An IP CoreHSR / PRP to provide high availability in communications andan IP core for industrial communications such as PROFINETto ensure interoperability with other devices. d) An IP Core toperform asymmetric encryption of layer 2 Ethernet frames usingthe AES-GCM algorithm. e) I/O module are also includedin order to add more functionality to the Smart Sensor. Theuse of an encryption module fully implemented in hardwarereduces the use of resources in the microprocessor.

The scheme of the Smart Sensor architecture proposed forthe IIoT is presented in the Fig. 2. Five modules can be identifiedin the architecture to support the different functionalitiesthat Smar Sensor must have, which are presented below:

The processing module (PS), allows executing the necessarysoftware to manage all the components of the architecture,to run specific libraries of a communications protocol and toperform data processing and analysis (Big Data). The PS hasEthernet and serial interfaces (RS-232, I2C) to communicatewith the exterior or with the internal modules (HSR/PRP, IEEE1588, etc.). In the processing module, a 1Gbps Ethernet port(GMAC1) can be identified. This port will be used as aninterface to access a local network or the Internet, to providethe system with access to services such as web, FTP, database,cloud, among others. Additionally, the GMAC0 is used tointerconnect the PS with the IP Cores that are implemented inthe PL. There are also two serial interfaces, the first (UART0)is used to implement industrial communications via serial fieldbuses (Modbus, Profibus), and the second (UART1) is usedas a terminal for monitoring, configuring and controlling.

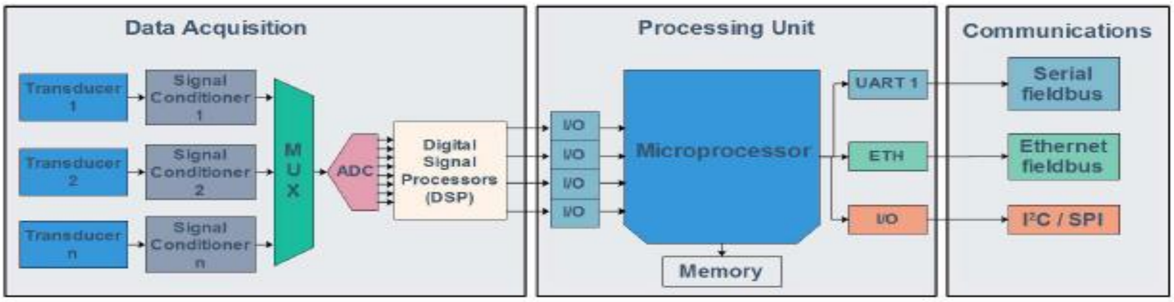

Figure 1. Generic architecture of an intelligent sensor. The Data Acquisitionmodule is responsible for collecting data. Processing Unit is responsible forcontrolling all the elements that make up a Smart Sensor. Communicationsmodule is responsible for transferring the data generated in the Smart Sensor.

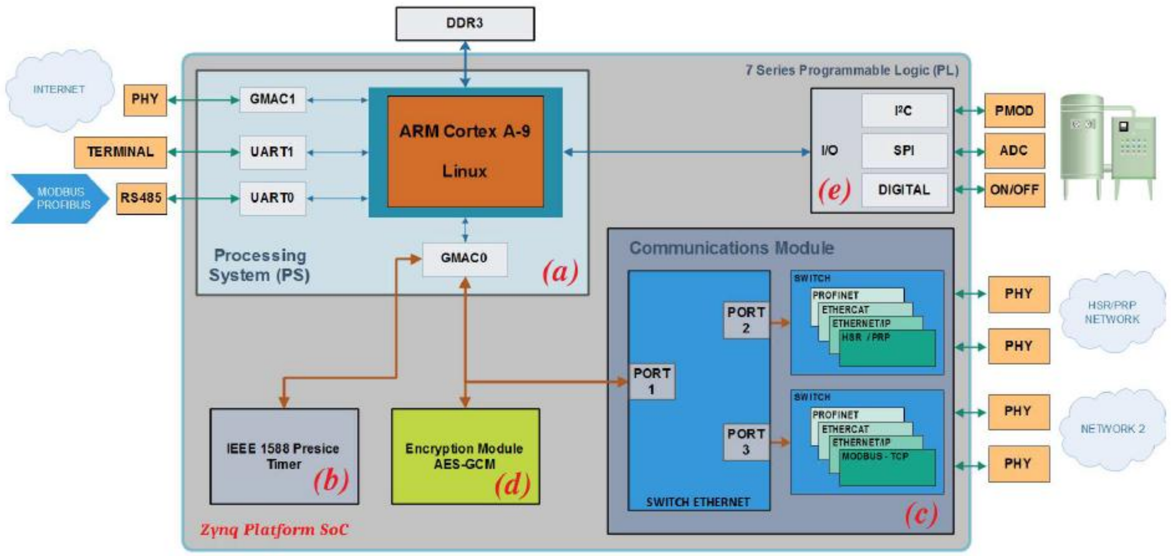

Figure 2. Block diagram of the architecture of a Smart Sensor for the IIoT.IEEE 1588 module is used to support applications with lowsynchronization time and timestamping.

This IP provides anexceptional synchronization mechanism that requires only anEthernet connection for nanosecond range synchronization. Allprocesses are carried out using hardware modules and do notneed any software to manage their operation. This IP corecan run on CPU-less boards and can be embedded into anyEthernet IP Switch or IP cores compatible with TransparentClock operation. The IEEE 1588 module is used to performtime stamping and supports the HSR protocol.

The communications module, allows managing high availabilitycommunications (HSR/PRP) and industrial communications(Profinet, EtherCAT, EtherNet / IP, among others).This IP implements Ethernet connectivity ensuring zero-delayrecovery time in case of network failure and no-frame lost. TheIP supports the latest version of Highavailability SeamlessRedundancy (HSR) and Parallel Redundancy Protocol (PRP)standards in combination with redundant IEEE 1588-2008.The communications module used consists of four Ethernetinterfaces, two of which are used as logic inputs to handlehigh-availability communication protocols (HSR / PRP), andthe other two allow the connection of Ethernet devices (SAN)that do not have HSR/PRP functionality, through the Redboxconfiguration.

CONCLUSION

In conclusion, having laid out the background including an overviewof related terms in section two, we provided a survey of existingdefinitions of IIoT in section three and developed our own definitionwhich we hope improves on those. The latest generation of programmable devices (FPGA,SoC) have allowed the development of electronic devicesthat are interconnected and are responsible for more complexactivities. FPGAs have reached a high level of developmentregarding performance, energy consumption and cost. Thefundamental challenge of this work is to take advantage of thefeatures of the current FPGAs that integrate silicon-embeddedprocessors to implement a hardware-software architecture ofa Smart Sensor. The processing of frames with real-timerequirements will be implemented as logic circuits (hardware),and the highest level algorithms will be performed in thehigh-performance processor (software). These two systems areclosely linked together on a single chip, and the success ofthe whole depends on the selected architecture for exchanginginformation between them.

REFERENCES

[1] K. Rose, S. Eldridge, L. Chapin, The internet of things: an overview, Internet Soc.(2015) 7.

[2] Beecham Research, M2M Sector Map, (2014) Available: http://www.beechamresearch.com/download.aspx?id=18.

[3] D. Lukač, 'The fourth ICT-based industrial revolution', 23rd TelecommunicationsForum Telfor, IEEE, 2015, pp. 835–838.

[4] Industrie 4.0 Available: vailable: https://www.bmbf.de/de/zukunftsprojektindustrie-4-0-848.html.

[5] Industrial Internet Consortium, What Is the Industrial Internet? [online], (2018)Available: https://www.iiconsortium.org/about-industrial-internet.ht.

[6] M. Hermann, T. Pentek, B. Otto, Design Principles for Industrie 4.0 Scenarios: ALiterature Review, TechnischeUniversitätDotmund, 2015, p. 11 Working paper(Accessed 12 September 2017).

[7] NIST, Framework for Cyber-Physical Systems. Release 1.0, NIST Cyber PhysicalSystems Public Working Group, (2016), p. 1. Available: http://www.nist.gov/.

[8] CHESS, Chess – Center for Hybrid and Embedded Software Systems. [ONLINE],(2017) Available at: http://chess.eecs.berkeley.edu/.

[9] R. Baheti, H. Gill, Cyber-physical systems, in: T. Samad, A.M. Annaswamy (Eds.),The Impact of Control Technology, vol. 2, IEEE Control Systems Society, New York,2011, pp. 161–166. Available: http://ieeecss.org/main/IoCT-report.