Concept of System for Surveillance and Monitoring of IoT HFSWR Network

Nikola Stojkovic, *Member, IEEE*, Vladimir Orlic, *Member, IEEE,* Miroslav Peric, *Member, IEEE,*
Dejan Drajic, *Senior Member, IEEE,* Aleksandar Rakic, *Member, IEEE*

***Abstract*—The IoT (Internet of Things) concepts for maritime surveillance systems represent an interesting, but rather unexplored area. This paper presents the IoT architecture for the High Frequency Surface Wave Radar (HFSWR) network within the well-known Integrated Maritime Surveillance (IMS) concept. An overview of the topology of a typical HFSWR network is given, and IoT architecture layers and distributed middleware functionality are defined. The architecture is implemented and tested in the Gulf of Guinea, Africa, where an aggregated surveillance and monitoring Web application operates in the private cloud, supported by the Web REST services and SNMP. Effectiveness of the solution is demonstrated in both network monitoring and surveillance aspects by giving details of a SNMP agent testing and the system-level insight to the network operation from the application layer.**

***Index Terms*—HFSW Radar, OTH Radar, IoT concept, HFSWR network, Integrated Maritime Surveillance.**

I. Introduction

Monitoring of remote sea areas inside EEZ (Exclusive Economic Zone) of maritime nations could be performed via satellite and aviation surveillance or by the deployment of HF-OTHR (High Frequency Over-the-Horizon Radar). Application of HF-OTHR network, without doubts, provides significant advantages in terms of deployment price and availability of sensor data over the aforementioned solutions. There are many possible technological implementations of HF-OTHR and one the most common types is HFSWR (High Frequency Surface Wave Radar).

HFSWR network is a Integrated Maritime Surveillance (IMS) subsystem, therefore conformed with HFSWR based IMS concept, defined in [1]-[2]. From this conformity certain assumptions could be made about HFSWR network's topology and disposition of its nodes. First of all, IMS concept assumes aggregate data processing node and arbitrary number of remote nodes, from where surveillance data originates. This certainly indicates a star-shaped topology of the network. Yet, some specifics of the topology need to be properly defined. Every remote node of this subsystem has potential problem with its communication channel, since remote nodes are installed on locations where is a lack of desirable communication infrastructure to support the work of HFSWR network. Besides measurement data, there are other secondary sensor data related to infrastructure state, like device calibration results or diagnostic information, that need to be transferred to processing nodes. Besides main sensors, there are other sensors and controllable devices on site nodes, e.g. ambient, power measurement sensors, routers, power distribution units (PDU), power amplifiers etc. All these facts define HFSWR network as a complex system for distributed measurement and control, whose elements are often resource-limited either by communication channel or by the construction of sensors itself, or even by both of these factors. This is the reason for creating a detailed conception of mechanism for control and monitoring, which should provide functional and uninterrupted flow of data and monitoring reports. For this purpose, the Internet of Things (IoT) conceptual scheme will be used, mainly based on SOA (Service Oriented Architecture) paradigm. It will, at some extent, follow principles of interaction with resource-limited sensors, given in [3], good practices of infrastructure monitoring, e.g. [4] and [5]. Note that HFSWR is a sensor, which resource limitation is predominantly regarding its communication ability, rather then computational capability. This fact is taken into account when building IoT infrastructure for HFSWR based naval surveillance systems.

Sensors and devices in the system have various built-in interfaces and an unified external access should be provided via Web service implementations. Additionally, HFSWR network can be controlled via external NMS (Network Management System) applications. These monitoring systems usually deploy SNMP protocol, and, in order to comply, middleware layer should contain one or more SNMP agents [6], for those components which do not own such interface.

To formulate the concept, topology of HFSWR network will be explained in Section II, together with network requirements in terms of security and planning and IoT architecture layers and its elements. Then, distributed middleware details will be presented. In Section III details of implementation are described, where details about Web

Nikola Stojkovic is with the School of Electrical Engineering, University of Belgrade, 73 Bulevar kralja Aleksandra, 11020 Belgrade, Serbia and the Vlatacom Institute, Belgrade, Bulevar Milutina Milankovića 5, 11070 Novi Beograd, Serbia, (e-mail: nikola.stojkovic@vlatacom.com)

Vladimir Orlic is with the Vlatacom Institute, Belgrade, Bulevar Milutina Milankovića 5, 11070 Novi Beograd, Serbia, (e-mail: vladimir.orlic@vlatacom.com)

Miroslav Peric is with the Vlatacom Institute, Belgrade, Bulevar Milutina Milankovića 5, 11070 Novi Beograd, Serbia, (e-mail: miroslav.peric@vlatacom.com)

Dejan Drajic is with the School of Electrical Engineering, University of Belgrade, Bul. Kralja Aleksandara 73, 11120 Belgrade, Serbia, (e-mail: ddrajic@etf.rs)

Aleksandar Rakic is with the School of Electrical Engineering, University of Belgrade, Bul. Kralja Aleksandara 73, 11120 Belgrade, Serbia, (e-mail: rakic@etf.rs)

service specification, SNMP agent solution and CC (Cloud Computing) platform utilization are given. Finally, fully functional IoT architecture, based on deployed HFSWR network in Gulf of Guinea, will be evaluated in Section IV via demonstration of applications from IoT application layer. Section V concludes the paper and provides details about future work.

II. HFSWR NETWORK IOT ARCHITECTURE

A. HFSWR Network Topology

HFSWR network, typically, has a star-shaped topology, in which external nodes represent individual remote sensor installations or operator nodes, with central node collection, representing the location of a Command and Control (C2) center, as presented in Fig.1. Remote sensor nodes (nodes of remote sites) represent installations, in general, of one or more homogeneous or heterogeneous sensors. Hence, by its nature, nodes of remote sensor sites can be elemental or mixed. Mixed remote sites usually contain combination of two, or even all, elemental sites. Types of elemental sites are:

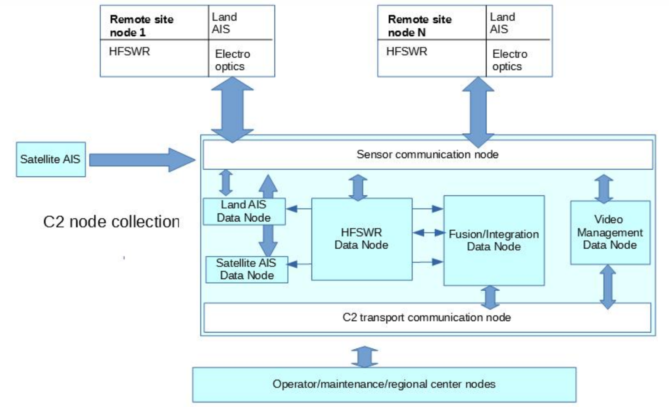
Satellite AIS reception site. This site contains satellite receiver equipment, necessary to connect to the satellite AIS (Automated Identification System) provider services. Note that satellite AIS node could be installed near C2 center facilities.

HFSWR site. This node contains HFSWR sensor, namely, the equipment that enables its function, other sensors for ambient and power measurements and server equipment for in-node primary processing of sensor data.

Land AIS base station site. Node contains AIS transceiver base station and network equipment for further data exchange.

EO surveillance site. On this node video surveillance cameras of different type (thermal, low-light etc.) are installed, which allow detection and identification of sea vessels on relatively large distances.

Another group of external nodes is dedicated for organized user installations, in forms of central or regional operation centers, which can be divided in three groups, maritime surveillance operator centers, supervision and maintenance operator centers and regional center node collections for surveillance and supervision.



.Figure 1. Typical star-shaped HFSWR network topology.

All nodes of the HFSWR network, located at C2 center installation, are represented in Fig. 1 as a collection of C2 center nodes, which form central point of topology. . Described nodes can be classified in following categories:

Sensor communication nodes. These nodes contain communication link and part of the C2 center infrastructure, with the task of reception of all sensor data in the network.

C2 transport nodes. Final results of integral data processing, including the system state related data is transmitted to this node, to which external user node communication link is joined, usually in the form of ethernet network. Final conditioning of data and its transport to end-users is performed in this node.

Aggregation AIS nodes. All LAIS (Land AIS) and SAIS (Satellite AIS) links are connected over sensor communication nodes to this node, where all data is processed in concentrated manner.

HFSWR data reception node. Data from all HFSWR sensors is concentrated in these nodes, filtered, processed and delivered to later stages, usually integration and monitoring nodes.

Sensor fusion / integration nodes. These process nodes perform fusion processes of different sensor data, HFSWR and AIS at the first place.

Video management nodes. Their main role is reception and resource management of video images from remote sensors for maritime and security surveillance.

Note that there are other possible topologies, e.g. a regionally grouped variant, with multiple regional processing nodes, but this topology is the most common and with significant advantages in terms of availability and implementability. HFSWR network, installed in Gulf of Guinea, also follows the star-shaped topology, presented in Fig. 1.

B. HFSWR network IoT architecture details

When establishing IoT architecture, one can start with the best IoT framework examples from [7] and radar IoT applications [8]. Block scheme of IoT architecture is consisted of sensor, network and application layer as shown in Fig. 2.

Sensor layer consists of already mentioned main measurement devices and services: HFSWR, LAIS, SAIS, video, GPS, ambient and power measurement sensors.

Network layer represents a bridge between sensor and application layer [4]. It is consisted of following blocks:

VPN (Virtual Private Network). End-user of the system is, most likely, military navy or a specialized state organization, which implies the need for security of exchanged data in HFSWR network.

Satellite network. Quite often, satellite link is the only way of communication between remote sites and the C2 center. Details about the role of satellite network in IoT concept of HFSWR network, deployed in Bay of Guinea can be found in [9].

GSM/3G/4G network. A convenient way to alternatively address the issue of communication link is the available cellular network, and, at the same time, the economic cost is much lower than the satellite network. The problem is that the number of cellular network access points on remote sites is usually one or none at all, and the quality of the connection could be quite low.

Integration of heterogeneous networks. In general, there are many different networking solutions present in the HFSWR network. From the use of VPNs in some domains of, or in the whole network, through satellite or cellular network data link. These are all factors of a heterogeneous network and the integration represents a complex task.

Remote access. Remote access is the principle of monitoring the HFSWR network, in which sensors and various devices are controlled and monitored over the Internet by client applications or processes, managed by people or expert systems.

M2M (Machine to Machine) wireless access. Certain parts of the HFSWR network on the remote sites may have a wireless interface or have provided access to the HFSWR network through fixed or even mobile access points.

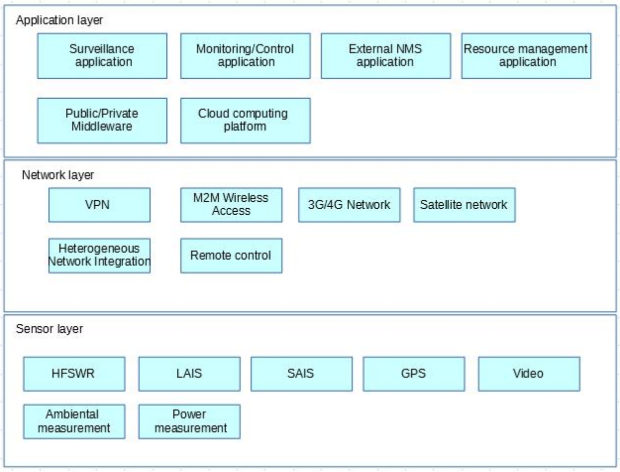


Figure 2. Basic IoT architecture concept of HFSWR based IMS system

The application layer consists of the following blocks:

A surveillance application. This is an application for observation of sensor coverage surfaces, which will conveniently display the maritime situation.

HFSWR network monitoring / control application. This application includes an overview of all monitor points, which should be hierarchically classified.

External NMS application. Due to the fact that the HFSWR network can be a subsystem of a more complex network and because of the popularity of SNMP-based NMS, there is a need to provide an additional SNMP-based interface that would use external NMS applications, such as Centerity Monitor [10], to represent a functional "mirror" of the underlying Web service interface.

Resource management application. This application should be able to configure the software part related to the postprocessing of sensor data, configure the computer hardware and take care of correct device configurations and access parameters.

Cloud Computing Platform. The Cloud Computing (CC) platform is tasked with enabling the implementation of systems in a private cloud. Its physical base consists of several physical servers, data storage, routers and switches.

Private and public middleware. Distribution middleware is software, installed on remote sites and in the C2 center, which interacts with another part installed on the CC platform. This segment represents the private middleware. The second part of the distribution middleware interacts with active, external users of the system. This middleware segment is named public. The more details are provided in the next subsection.

C. *Distributed middleware*

A generalized distributed middleware scheme is given in Fig. 3, on the example of HFSWR site. Distributed private middleware on remote sites and C2 center nodes is a set of proxy gateway components that contain mappers and data handlers and allow access to controllable parameters, monitoring points (probes) and alarm definitions. These components have a role of translating, mapping and packing inputs and outputs according to the communication channel needs The CC platform has the task of implementing the main SOA-based IoT infrastructure, composed of a stack of Web services. It implements a private and public middleware, whose functionality can be divided into 4 groups, and all of these components have their share in both the private and public part of the distributed middleware:

Agentware. All software components that transform the SNMP polling or control requests of external NMS applications, or that customize internal information by transforming the interface of the controlled components into information that is customized to the SNMP interface, are collectively referred to as the agentware.

Device managers. Device managers perform configuration, polling, startup, shutdown, and direct control of individual devices in the HFSWR network.

Notification managers. In the case of one-way sensors that have a limited interface and send measurements and eventual status messages, notification managers are responsible for receiving such messages, processing and responding, in coordination with the agent middleware.

Data managers. They are primarily responsible for implementing interfaces to various data storage. This specifically refers to maritime surveillance databases, system user databases and system monitoring databases, which store information related to the HFSWR network diagnostics.

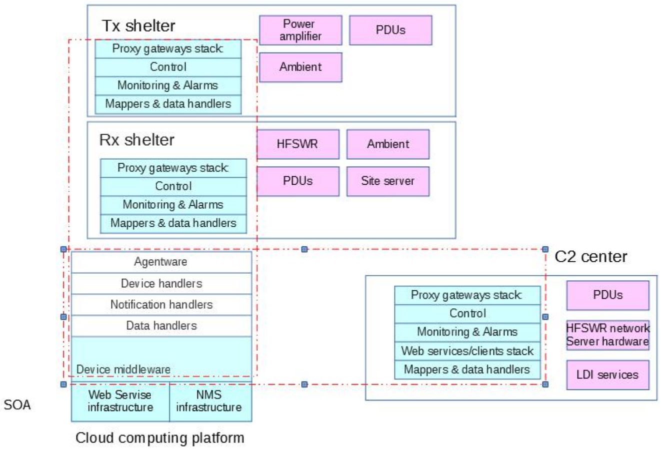


Figure 3. Distributed middleware structure of HFSWR network's IoT architecture

III. Implementation of IoT architecture software infrastructure

The implementation of the IoT architecture software on the CC platform begins with a description of the hardware and software platform configuration. In the logical presentation of the CC platform, it is clear that an application server is required, which will be the carrier of Web service implementations and much of the private and public middleware. Due to database needs, one of the logical units has to be a database server. These two logical servers (without counting their redundancies) form the basis of the CC platform's logical architecture. There are 3 databases in the system:

System user database. The database stores user information, roles, allocated resources and specific user tasks.

Naval observation database. This database stores common operational picture (COP) data in each iteration. In addition to the COP, tables for entering AIS data as well as individual HFSWR outputs were implemented.

Network system database. This database records system configuration and error logs in the middleware, analogous to the role of the middleware historian model in [11].

The application server implements a Web service stack, a major SNMP agent for communication with external NMS infrastructure and part of a private and public middleware, which refers to device managers and data controllers. The software is organized as one multi-component Web application, hosted on Microsoft IIS (Internet Information Services), with the direct connection of SNMP agent and Web service stack. External requests to the SNMP agent are translated by agentware either into calls to the appropriate Web Service stack methods, where further execution takes place, or passed through device handlers to specific devices in network. Notification mechanism delivers response through message queue, where notification handler generates response via initial calling interface. Within the C2 center, the data processing nodes house the servers where the software that performs these tasks is installed. The fusion integration server, which contains a central process for processing sensor data and aggregation monitor component, accesses the web services of the application server mostly through its Web clients. Most of monitoring data originates from sensors with one-way communication style and is collected on this server. Besides monitoring purposes, this data is also used in sensor processing and it is a direct advantage of star-shaped HFSWR network topology. User communication is based on the HTTP REST software architecture style. The data is transmitted in JSON format. This applies to both internal and external nodes, which need to exchange data with the application server. The exception is, of course, the external NMS application. The web service stack was implemented in C# programming language and hosted on IIS. There are 3 main groups of services: control, monitoring and surveillance data services. Control services, represented in Fig. 4 with light green color and described through their service contract names, are dedicated for control of power amplifiers, power distribution units and configuration and process state control. Monitoring services (yellow color on Fig. 4) are dedicated for monitoring of equipment, alarms and current process states data flow, along with error logging, diagnostics and access to middleware historian. Surveillance data services (dark green color on Fig. 4) are dedicated to operational surveillance data exchange between inner and outer HFSWR network nodes.

Typical information flow will be demonstrated on one scenario with one HFSWR data scan, presented on Fig. 5. On new HFSWR data available, proxy gateway component activates its data handler, which packs sensor readings and dispatches them through communication channel, via file transfer protocol and ethernet network. Upon reception of data packet in HFSWR data node, data is processed and passed through fusion/integration node routines, where COP output, possible alarms and other information are generated, via notification mechanism. Notification managers of aggregate monitor component and web client from C2 transport node process and pack messages into JSON format and send it via its Web clients to application server data and monitoring services. Monitoring data is further translated via agentware component into format suitable for SNMP OID data storage, where SNMP traps mechanism generates trap notifications, if necessary. The data from monitoring, surveillance and SNMP OID repositories is then available for external clients, who read it via appropriate service or SNMP calls.

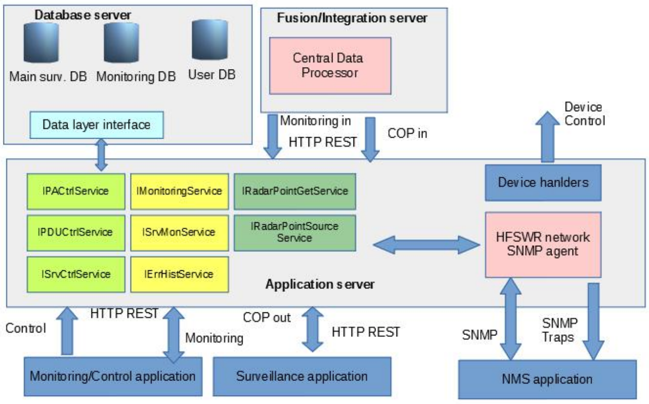


Figure 4. CC platform logical architecture

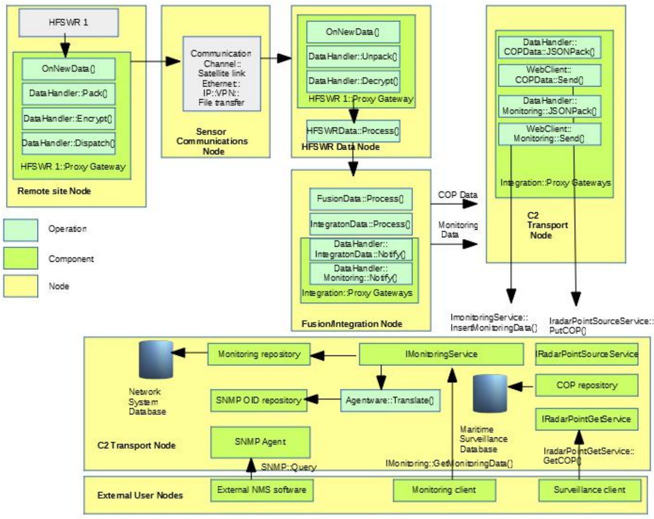
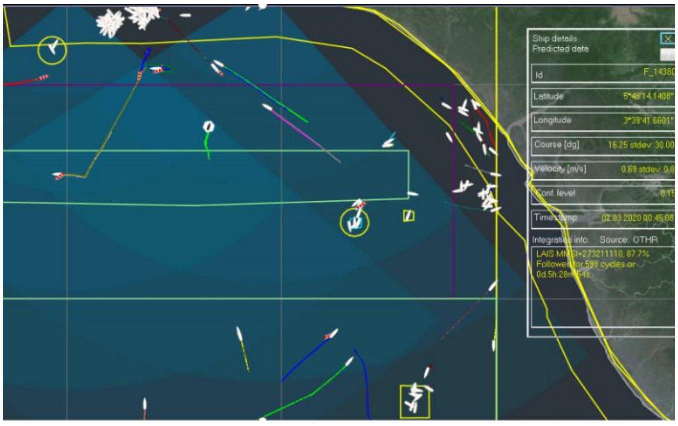


Figure 5. Information flow diagram for one HFSWR data scan scenario

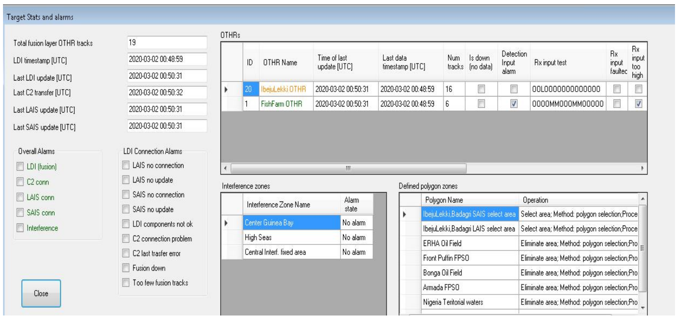
IV. DEMONSTRATION

Current implementation on the CC platform takes up the resources of one physical server with 2 CPUs and a total of 24 CPU cores. IoT architecture of the HFSWR network is demonstrated with screen-shoots from application layer utilities. First, on Fig. 6, a typical view from the maritime surveillance application client is presented. The client presents all possible view layers, including integrated views, and presents selected target details, including integration information. For example, selected target details (white hexagon marker) show that it is a target from HFSWR fusion view layer, integrated with AIS MMSI 27321110, followed for more than 5 hours. Other useful details, including velocity, course and estimated coordinates are presented as well. Monitoring of the equipment and remote site node measurements are read and displayed in appropriate monitoring application. In Fig. 7, one of its windows is presented. On the left side of screen there are general alarms, in charge for general HFSWR network state. On the right side, there are particular alarms and measurements from remote sites, special areas of interest (marked as yellow polygons on Fig. 6) and ionospheric interference zone alarms overview. SNMP interface is tested via simple SNMPB application [12], installed on application server. This application is used as Management Information Base (MIB) file browser and SNMP agent tester. MIB file for the HFSWR network is loaded and main OIDs (Object Identifiers) are displayed on Fig. 8, left. SNMP query is tested on marked OID, named vMsMonitor, and results are shown on the right side of Fig. 8.



Id F_14380
Latitude 5°48'14.1408"
Longitude 3°39'41.6601"
Course [dg] 16.25 stdev: 30.00
Velocity [m/s] 0.69 stdev: 0.8
Conf. level 0.15
Timestamp 02.03.2020 00:45:08
Integration info: Source: OTHR
LAIS MMSI=273211110, 87.7%
Followed for 598 cycles or
0d:5h:28m:54s

Figure 6. Maritime surveillance client application screen.



Total fusion layer OTHR tracks	19
LDI timestamp [UTC]	2020-03-02 00:48:59
Last LDI update [UTC]	2020-03-02 00:50:31
Last C2 transfer [UTC]	2020-03-02 00:50:32
Last LAIS update [UTC]	2020-03-02 00:50:31
Last SAIS update [UTC]	2020-03-02 00:50:31

Overall Alarms
□ LDI (fusion)
□ C2 conn
□ LAIS conn
□ SAIS conn
□ Interference

LDI Connection Alarms
□ LAIS no connection
□ LAIS no update
□ SAIS no connection
□ SAIS no update
□ LDI components not ok
□ C2 connection problem
□ C2 last trasfer error
□ Fusion down
□ Too few fusion tracks

OTHRs

	ID	OTHR Name	Time of last update [UTC]	Last data timestamp [UTC]	Num tracks	Is down (no data)	Detection Input alarm	Rx input test	Rx input faultec	Rx input too high
▸	20	IbejuLekki OTHR	2020-03-02 00:50:31	2020-03-02 00:48:59	16	□	□	00L000000000000	□	□
	1	FishFarm OTHR	2020-03-02 00:50:31	2020-03-02 00:48:59	6	□	☑	0000MM000MM00000	□	☑

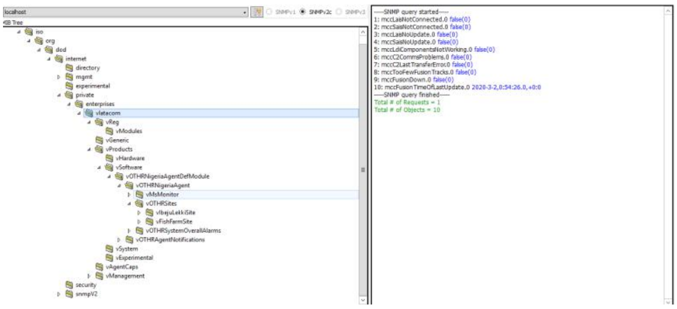
Interference zones

	Interference Zone Name	Alarm state
▸	Center Guinea Bay	No alarm
	High Seas	No alarm
	Central Interf. fixed area	No alarm

Defined polygon zones

	Polygon Name	Operation
▸	IbejuLekki,Badagri SAIS select area	Select area; Method: polygon selection;Proce
	IbejuLekki,Badagri LAIS select area	Select area; Method: polygon selection;Proce
	ERHA Oil Field	Eliminate area; Method: polygon selection;Pro
	Front Puffin FPSO	Eliminate area; Method: polygon selection;Pro
	Bonga Oil Field	Eliminate area; Method: polygon selection;Pro
	Armada FPSO	Eliminate area; Method: polygon selection;Pro
	Nigeria Teritorial waters	Eliminate area; Method: polygon selection;Pro

Figure 7. A window with monitoring alarms from maintenance/monitoring client application



```
iso
  org
    dod
      internet
        directory
        mgmt
        experimental
        private
          enterprises
            vlatacom
              vReg
                vModules
              vGeneric
              vProducts
                vHardware
                vSoftware
                  vOTHRNigeriaAgentDefModule
                    vOTHRNigeriaAgent
                      vMsMonitor
                      vOTHRSites
                        vIbejuLekkiSite
                        vFishFarmSite
                      vOTHRSystemOverallAlarms
                    vOTHRAgentNotifications
                vSystem
                vExperimental
              vAgentCaps
              vManagement
        security
        snmpV2
```

```
-----SNMP query started-----
1: mccLaisNotConnected.0 false(0)
2: mccSaisNotConnected.0 false(0)
3: mccLaisNoUpdate.0 false(0)
4: mccSaisNoUpdate.0 false(0)
5: mccLdiComponentsNotWorking.0 false(0)
6: mccC2CommsProblems.0 false(0)
7: mccC2LastTransferError.0 false(0)
8: mccTooFewFusionTracks.0 false(0)
9: mccFusionDown.0 false(0)
10: mccFusionTimeOfLastUpdate.0 2020-3-2,0:54:26.0,+0:0
-----SNMP query finished-----
Total # of Requests = 1
Total # of Objects = 10
```

Figure 8. SNMP query test of HFSWR network's main SNMP agent in SNMPB utility

V. Conclusion

This paper presents the basis for building the IoT architecture of the HFSWR network in the IMS concept. Exploiting network's topology features, an aggregated surveillance and monitoring solution via Web REST services and popular SNMP protocol has been developed as a Web application, working in private cloud. Such solution allowed direct monitoring and collection of data from one set of nodes, located in C2 center, greatly simplifying distributed middleware, which contains minimal number of intermediate components, thus increasing the reliability and availability of system components. Finally, it can be concluded that an efficient system for remote monitoring of the HFSWR network has been developed, with a rapid response of both the system and the user to unforeseen events, while providing complete insight into all the functionality of the network to its operators. For the future work, further expansion of presented IoT architecture is planned. At first glance, the system topology seems to have a small number of process nodes, but the whole presented architecture is scalable and designed in IoT sense to provide flexibility in the integration of additional process nodes and future more modern and secure solutions, such as more reliable private cloud technology stacks based on the Linux operating system.Smart, autonomous, run-time configurable software agent concepts that will manage remote site-C2 center data exchange will be introduced. Besides on-site sensor and communication channel interfacing, their role will also be the management of uploads of large amount of data, accumulated during remote site's communication offline stages, via narrowband and noisy communication channel, thus supporting implementations of scenarios for communication in harsh environments.

References

[1] L.D. Sevgi, A.M. Ponsford, H.C. Chan, "An integrated maritime surveillance system based on high-frequency surface-wave radars Part 1: Theoretical background and numerical simulations", IEEE Antennas and Propagation Magazine, vol. 43, no. 4, pp. 28-43, Aug. 2001.

[2] L.D. Sevgi, A.M. Ponsford, H.C. Chan, "An integrated maritime surveillance system based on high-frequency surface-wave radars Part 2: Operational status and system performance", IEEE Antennas and Propagation Magazine, vol. 43, no. 5, pp. 52-63, Oct. 2001.

[3] Buckl, C., Sommer, S., Scholz, A., Knoll, A., Kemper, A., Heuer, J., Schmitt, A., 2009. "Services to the field: an approach for resource constrained sensor/actor networks". In: Proceedings of WAINA, Bradford, United Kingdom.

[4] Enji, S., Zhanga, X., Lib, Z., 2012. "The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and prealarm system in mines". Saf. Sci. 50 (4), 811–815.

[5] Drenoyanis, A.; Raad, R.; Wady, I.; Krogh, C. Implementation of an IoT Based Radar Sensor Network for Wastewater Management. Sensors 2019, 19, 254.

[6] H. Nwana, “Software agents: An overview,” Knowl. Eng. Rev. J., vol. 11, no. 3, 1996.

[7] A. Ouaddah, H. Mousannif, A. Abou Elkalam and A. Ait Ouahman, "Access control in IoT: Survey & state of the art," 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2016, pp. 272-277, doi: 10.1109/ICMCS.2016.7905662

[8] Gameiro, A., Castanheira, D., Sanson, J. et al. Research Challenges, Trends and Applications for Future Joint Radar Communications Systems. Wireless Pers Commun 100, 81–96 (2018).

[9] Petrovic R., Simic D., Drajic D., Cica Z., Nikolic D., Peric M. “Designing Laboratory for IoT Communication Infrastructure Environment for Remote Maritime Surveillance in Equatorial Areas Based on the Gulf of Guinea Field Experiences”. Sensors. 2020; 20(5):1349.

[10] Centerity Monitor information page, https://www.centerity.com, available online 17.04.2020

[11] Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., Souza, L., Trifa, V., 2009. “SOA-based integration of the internet of things in enterprise services”. In: Proceedings of IEEE ICWS, Los Angeles, Ca, USA.

[12] SNMPB application download page, https://sourceforge.net/projects/snmpb, available online 27.04.2020