IEEE Standard for Information Technology—

Telecommunications and information exchange between systems

Wireless Regional Area Networks (WRAN)—

Specific requirements

Part 22.3: Spectrum Characterization and Occupancy Sensing

Sponsor

**LAN/MAN Standards Committee**of the  
**IEEE Computer Society**

Approved Date XX

**IEEE-SA Standards Board**

Abstract: This standard specifies the architecture, abstraction layers, interfaces and metadata requirements for Spectrum Characterization and Occupancy Sensing (SCOS) system, a defines performance parameters, units and measures. This SCOS system comprises one or more semi-autonomous Spectrum Sensing Devices which scan electromagnetic spectrum, digitize it and perform processing, transmitting the resultant data with appropriate metadata to a central storage and processing system, according to rules, policies or instructions imposed on the Spectrum Sensing Devices by a management system.

Keywords: radio spectrum sensing, spectrum monitoring, signal characterization, cognitive radio, IEEE 802.22.3, WRAN standards

[[1]](#footnote-1)•

**IEEE Standards** documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854

USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This standard specifies the functional elements, system architecture, abstraction layers, interfaces and metadata requirements for Spectrum Characterization and Occupancy Sensing (SCOS) system, with some limited definition of performance parameters, units and measures. It is intended to incorporate elements of existing standards and technology components to make it fast to implement using “off the shelf” hardware and software modules. The standard is intended to be flexible to make it forward-compatible as both radio sensing hardware and software technology develops, with an emphasis on using shared, virtualized, Internet-connected computing resources. The reference architecture describes one or more semi-autonomous Spectrum Sensing Devices which scan electromagnetic spectrum, digitize it and perform some level of processing, transmitting the resultant data with appropriate metadata to a Spectrum Sensing Management System. This command and control system manages scan requests from users, manages and advertises to users the scanning resources available to it from its connected Sensing Devices, and packages and forwards scan data to specified destinations according to rules, policies or instructions imposed by operator of the SCOS system.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL:   
<http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: [http://standards.ieee.org/reading/ieee/interp/  
index.html](http://standards.ieee.org/reading/ieee/interp/index.html).

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA for approval, the following voting members had participated in the IEEE P802.22.3 Task Group:

**TBC**

Major contributions to this standard were made by the following individuals:

**TBC**

The following members of the balloting committee voted on this **TBC**. Balloters may have voted for approval, disapproval, or abstention.

When the IEEE-SA Standards Board approved this on TBC, it had the following membership:

**Richard H. Hulett,** *Chair*

**John Kulick,** *Vice Chair*

**Robert M. Grow,** *Past Chair*

**Judith Gorman,** *Secretary*

\*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish Aggarwal, *NRC Representative*

Richard DeBlasio, *DOE Representative*

Michael Janezic, *NIST Representative*

Patricia Gerdon

*IEEE Standards Program Manager, Document Development*

Catherine Berger

*IEEE Standards Project Editor*

**Contents**

1. Overview 11

1.1 Scope 11

1.2 Purpose 11

1.3 Application 12

2. Normative References 12

3. Abbreviations and acronyms 12

4. Operational Modes 13

5. System Architecture 13

5.1 Roles 13

5.2 Functions 13

5.3 Entities 14

5.4 Functions 15

5.5 System Model 16

5.6 Spectrum Sensor Manager (SSM) 20

5.7 Data Manager 20

5.8 Topology 20

6. Interfaces, Messaging and Primitives 20

6.1 SCOS Interfaces 21

6.2 SCOS Messaging 23

6.3 SCOS Message exchanges 26

6.4 Primitives 28

7. Procedures 30

7.1 State Diagram 31

7.2 Messaging Chart for State Changes 31

7.3 Operations and Security 31

7.4 Data Ownership 32

7.5 Security Systems 32

Annex A Informative: Reference Applications 33

A.1 White Space device radio operation 33

A.2 National spectrum regulation 33

A.3 Research programmes 33

A.4 Law enforcement and public order 34

A.5 Network Operator Applications 34

Annex B Normative Functional Requirements 35

B.1 Tasking Agent Requirement 35

B.2 Data Quality and Definition 35

B.3 Regulatory requirements 35

B.4 Policy Management and Enforcement Requirements 35

B.5 Sensor Location-Fixing Requirements 36

B.6 Service Level Agreement Requirements 36

B.7 Certification Requirements 36

B.8 Technical Requirements 36

B.9 Security Requirements 37

Annex C Normative - SCOS Metadata Specification 39

C.1 SSD metadata specification 39

7.6 System Units and Parameters (NOTE THESE NEED UNITS, SYNC W TABLES) 44

7.7 Metadata Formats 46

Annex D System Policy Model 48

D.1 SCOS Policy 48

Annex E Informative: Latency Requirements for Scans 55

Annex F Informative: Regulatory Technical requirements 56

Annex G Device and System Security Recommendations 57

Annex H Implementation Guidelines/Notes 58

H.1 Management Reference Architecture 58

Annex I (normative) IEEE 802.22 regulatory domains and regulatory classes requirements 63

I.1 Regulatory domains, regulatory classes, and professional installation 63

I.2 Radio performance requirements 64

Annex J (informative) Sensing 65

J.1 References 65

Annex K (informative) Bibliography 66

IEEE Standard for Information Technology—

Telecommunications and information exchange between systems

Wireless Regional Area Networks (WRAN)—

Specific requirements

Part 22.3: Standard for Spectrum Characterization and Occupancy Sensing

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

***This IEEE document is made available for use subject to important notices and legal disclaimers.   
These notices and disclaimers appear in all publications containing this document and may   
be found under the heading “Important Notice” or “Important Notices and Disclaimers   
Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at*** [***http://standards.ieee.org/IPR/disclaimers.html***](http://standards.ieee.org/IPR/disclaimers.html)***.***

1. Overview
   1. Scope

The purpose of the Spectrum Characterization and Occupancy Sensing (SCOS) system is to acquire and make available data from networks of sensors. It is intended to establish a platform that enables “spectrum sensing as a service” and collective measurement efforts.

The standard leverages interfaces and primitives that are derived from IEEE Std. 802.22-2011, and uses commonly used network transport mechanisms to achieve the control and management of the system. Interfaces and primitives are provided for conveying value-added sensing information to various spectrum sharing database services.

* 1. Purpose

The purpose of the Spectrum Characterization and Occupancy Sensing (SCOS) system is to characterize and assess the occupancy of spectrum resource towards supporting its more efficient and effective use. The intent of the SCOS system is to create a high-level architecture to support different spectrum sensing deployments, technologies and devices being shared to achieve economies of scale, and a broader availability and usage of sensing information from different sources. This will enable clients to acquire and use spectrum sensing information from a multiplicity of predefined independent systems to serve their goals.

* 1. Application

Various national regulators and government authorities are developing regulatory and policy frameworks to allow cooperative spectrum sharing approaches in order to optimize spectrum utilization. There is emphasis on greater spectrum efficiencies, spectrum sharing and spectrum utilization, which requires not only database-driven configuration of the radios, but systems that can provide spectrum occupancy at a particular location and at a particular time.

The IEEE 802.22.3 standard described in this document will help fulfil this need by creating a Spectrum Characterization and Occupancy Sensing (SCOS) system. This will improve knowledge of spectrum utilization and support shared spectrum applications, hence benefitting the regulators and users alike.

The Spectrum Occupancy Sensing (SCOS) System has many applications which include:

1. On-demand spectrum survey and report

2. Collaborative spectrum measurement and calibration

3. Labelling of systems using the spectrum

4. Spectrum planning

5. Spectrum mapping

6. Coverage analysis for wireless deployment

7. Terrain and topology - shadowing and fading analysis

8. Quantification of the available spectrum through spectrum observatories

9. Complement database access for spectrum sharing by adding in-situ awareness and faster decision making

10. Space-Time-Frequency spectrum hole identification and prediction where non-time-sensitive tasks can be performed at certain times and at certain locations, when the spectrum use is sparse or non-existent

11. Identification and geolocation of interference sources.

The Spectrum Characterization Occupancy Sensing (SCOS) systems may be deployed to characterize many bands such as VHF/UHF, L, S, C and X bands.

1. Normative References

Sections of the IEEE P1900.6 standard defining the M-SAPs.

To be completed…

1. Abbreviations and acronyms

Tasking Agent – A human or machine entity that interacts with the SSM to query scan resources or request scans to be scheduled

RF – Radio Frequency

RFI – Radio Frequency Interference

SCOS – Spectrum Characterization and Occupancy Sensing

SD or SSD – Spectrum Sensing Device

SM or SSM – Spectrum Sensing Manager

DM – Data Manager

1. Operational Modes

To allow great system flexibility with ability to meet multiple unknown use cases, but also allow a simplified task-specific operational use, two Operational Models are proposed:

* “Tasking SCOS Mode” which is a full-featured mode suitable for wide application, where the SSM acts as a management device to allow multiple different users (“Tasking Agents”) to do different scans
* “CR Mode” suitable for cognitive radio implementations, where a sensing device is used in a semi-fixed configuration, reporting channel occupancy to the radio management system over heartbeat messages for low overhead, with some capability to perform specific scans as a task to let a radio supervisor system request a detailed scan

CR Mode is a subset of Tasking SCOS Mode, using the same interfaces, primitives and protocols.

A further “Offline Mode” is proposed for further examination and inclusion in later versions of standard. This mode would enable sensing devices to be given a task schedule, and then operate offline from the SCOS management systems, and synch data and tasks later when re-associated to management systems.

1. System Architecture
   1. Roles

To allow the abstraction of system components, as well as the application of policies and similar management functionality, a number of roles are defined:

**Sensor Owner:** The individual or organisation that deploys and has administrative and physical control over the sensing devices (SSD). SSDs are typically physical devices.

**Sensing Data Administrator:** The individual or organisation that deploys and has administrative and physical control over the Data Receive Points consisting of data stores or other consumers of spectrum sensing data delivered by the SCOS system. Data Receive Points are typically software systems on Internet-connected shared or dedicated compute resources.

**SCOS Administrator:** The individual or organisation that deploys and has administrative and physical control over the SCOS System, consisting of the Sensing Management System and Sensing Data Manager. . The SCOS System components are typically software systems on Internet-connected shared or dedicated compute resources.

**Tasking Agent:** The individual or system that authenticates with the SCOS system and causes a scan activity to be scheduled.

* 1. Functions

The functions is based on the design objective of abstracting the layers between user, sensor management, sensor device, and sensed data, to allow a flexible implementation where different areas by be implemented or operated by different organizations, but still allow inter-operation.

* A client of the SCOS system will connect to the tasking function of Sensing Management System (SMS) over a network connection and interact with it through the 802.22.3 defined interface, allowing them to query available sensing resources and schedule a sensing task as permitted by resource availability, authorisation level and system policies. Once a client has scheduled a task, they will become a Tasking Agent.
* Within the SMS, a discovery and task management function will be performed by the Spectrum Sensing Manager (SSM), which will provide to the Tasking Agent an inventory of the sensing resources that are currently being provided by its connected Spectrum Sensing Devices (SSDs), with capabilities and parameters described according to this 802.22.3 standard
* The Tasking Agent will insert a scanning task into a schedule managed by the SSM using the protocol defined in this 802.22.3 standard
* The SSM shall maintain the schedule of tasks and synchronises this schedule of tasks to the SSD using the protocol defined in this 802.22.3 standard
* Within the SSD, radio energy shall be collected by an antenna and transferred through an interconnect to a signal conditioner. Conditioned signal will be then transferred to a signal processing system to produce a baseband signal that can be quantised and passed in digital form to be analysed through whichever sensing technique is offered by the SSD
* The data from this analysis, and the associated metadata that includes the sensing technique and environment, hardware, software and configuration parameters as defined in this standard, can be temporarily stored on the local device before it shall be transmission to an end point. This transmission may be direct from SSD to the Data Receive Point, or should be transmitted indirectly via the DM, but in all cases policy decisions and transmission end point must be mediated via the Spectrum Sensing Management System’s Data Manager (DM).
* The DM shall establish the end point of data package transmissions according to the Tasking Agent’s nominated end point(s), and in accordance with the policies defined in the SSMS, and shall transmit the data packages, reporting the success or otherwise back to the original Tasking Agent.

.

* 1. Entities

Figure 1. Architecture Block Diagram illustrates the functional components within the SCOS system. Note that all arrows in this diagram refer to connections made over a standard network transport (the choice of which is up to the implementer of the SCOS system).

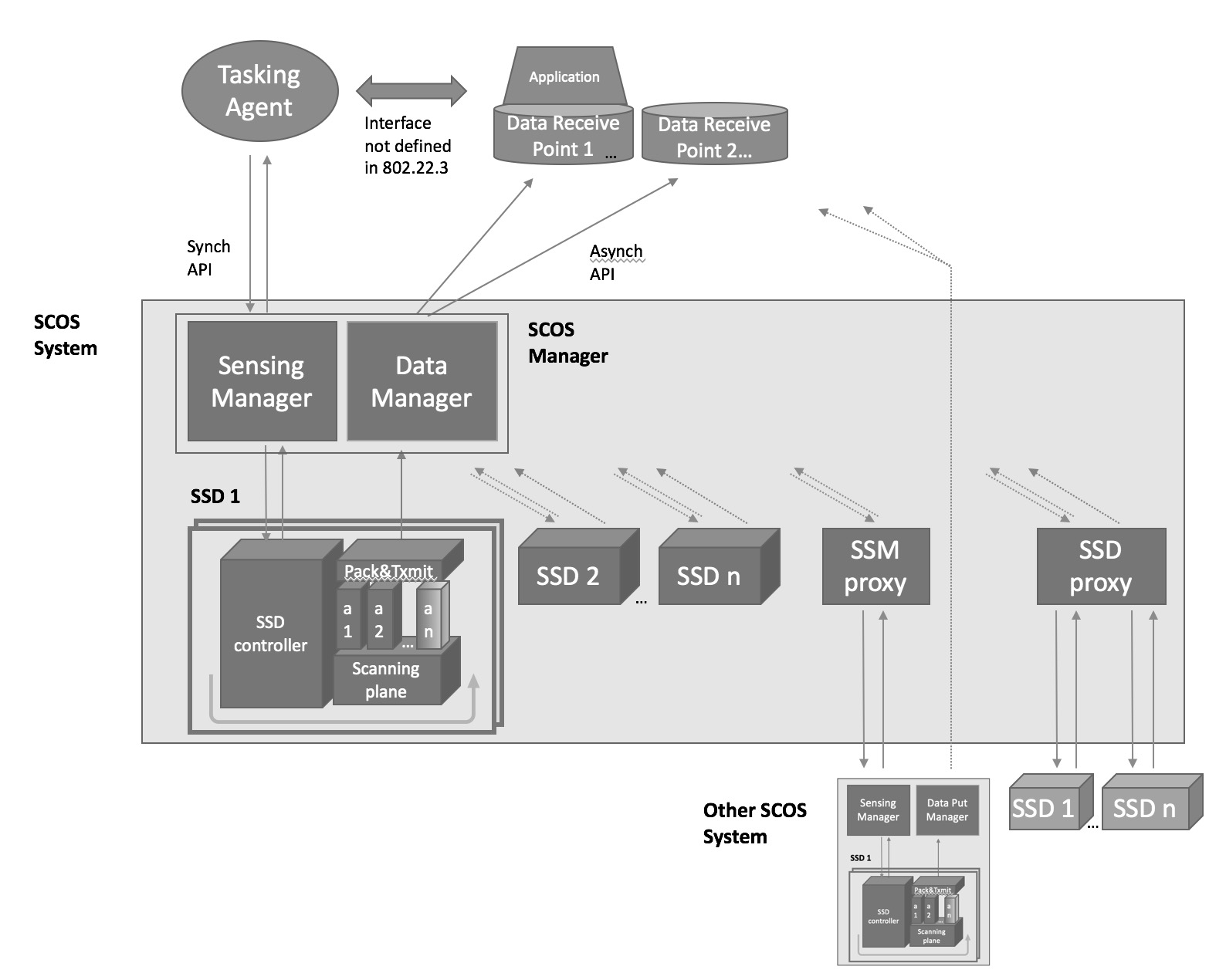


Figure 1. Architecture Block Diagram

* Tasking Agent is the entity that initiates a spectrum monitoring request to one or more Spectrum Sensing Managers (SSM). Tasking Agents can be human or machine, and have various levels of privileges regarding what spectrum information collection can be initiated. Tasking Agents would determine where sensing data is to be transmitted, and authorization to access that data would rest with the owner of that data storage entity. and what spectrum information can be accessed from a Data Receive Point.
  + An Tasking Agent (user of the SCOS system) and SSM (Sensing Manager) communicate by REST API to ask for available resources, and request a scan.
* Data Receive Point is a data store for storing spectrum information collected from the sensing network. There can be multiple DRPs that sensing data is transmitted to by the Data Manager, and these can be, but not necessarily, associated with a specific Tasking Agent.
  + The Data Manager transmits data to the DRP via a Message Queue, and the Tasking Agent interacts with the DRP using their chosen mechanisms (out of scope of this standard)
* Spectrum Sensing Manager (SSM or Sensing Manager) manages a collection of Spectrum Sensing Devices (SSD). Requests for spectrum measurements from Tasking Agents are inserted into a scan schedule on the SSM for all its attached SSDs, as far as possible under a set of slot availability rules. This schedule is synched to the appropriate SSDs associated with the SSM. Data from the SSDs are collected at the Data Manager for transmission to one or more DRPs for long term storage and processing.
  + The SSM is associated with SSDs (Sensing Devices) through a synchronous interface, where the SSM enumerates and holds a list of available resources for each SSD.
  + The SSM stores and manages a schedule of scans against the sensing resources, and synchronizes this schedule with all SSDs both on a change being made and periodically to ensure correct state.
  + Typically (but not necessarily) the SSM and Data Manager would be running on the same physical server.
* Data Manager receives transmissions of packaged scan data from SSDs, and retransmits it to one or more destinations, as defined by the policies associated with each Tasking Agent (the source of scan requests)
  + The “Data Manager” applies any policies and then handles the Store & Forward to one or more DRPs using a Message Queue or Streaming Mechanism
  + Typically (but not necessarily) the SSM and Data Manager would be running on the same physical server.
* The Sensing Manager and Data Manager together form the SCOS Manager, and each can be on the same platform or separate platforms.
* The Spectrum Sensing Device is the sensing hardware that collects the spectrum data requested by the SSM on behalf of each Tasking Agent. The SSDs may exist with various levels of sophistication. The less sophisticated might be capable of measuring only one band, at only one resolution with little on-board processing. Other sensors may incorporate sophisticated antenna techniques, multiple bands, calibration processes, on-board data processing and/or storage and/or be capable of mobile operation.
  + An SSD performs the scans in the schedule, and transmits the data and associated metadata through an asynchronous interface (message queue, or real time stream) to a “Data Manager” that performs system data validation (i.e. that a transmission is received completely, partial scans are consolidated, etc).
* SSM Proxy lets one SSM talk to another, with the downstream SSM appearing as if it were an SSD with a set of resources it provides. This downstream SCOS system would need to be 802.22.3 compliant.
* SSD Proxy lets an SSM talk to any other proprietary sensing hardware, acting as a software translation mechanism that translates between commands/metrics/etc. It would need to be custom written for the particular device it talks to.
  1. Functions

The proposed architecture is composed of five key elements: Tasking Agent(s), Spectrum Sensing Device(s), a SCOS Management System (Sensing Manager + Data Manager) and Data Receive Point(s). The flow of instructions and data is described in Figure 2: SCOS Functional Block Diagram.

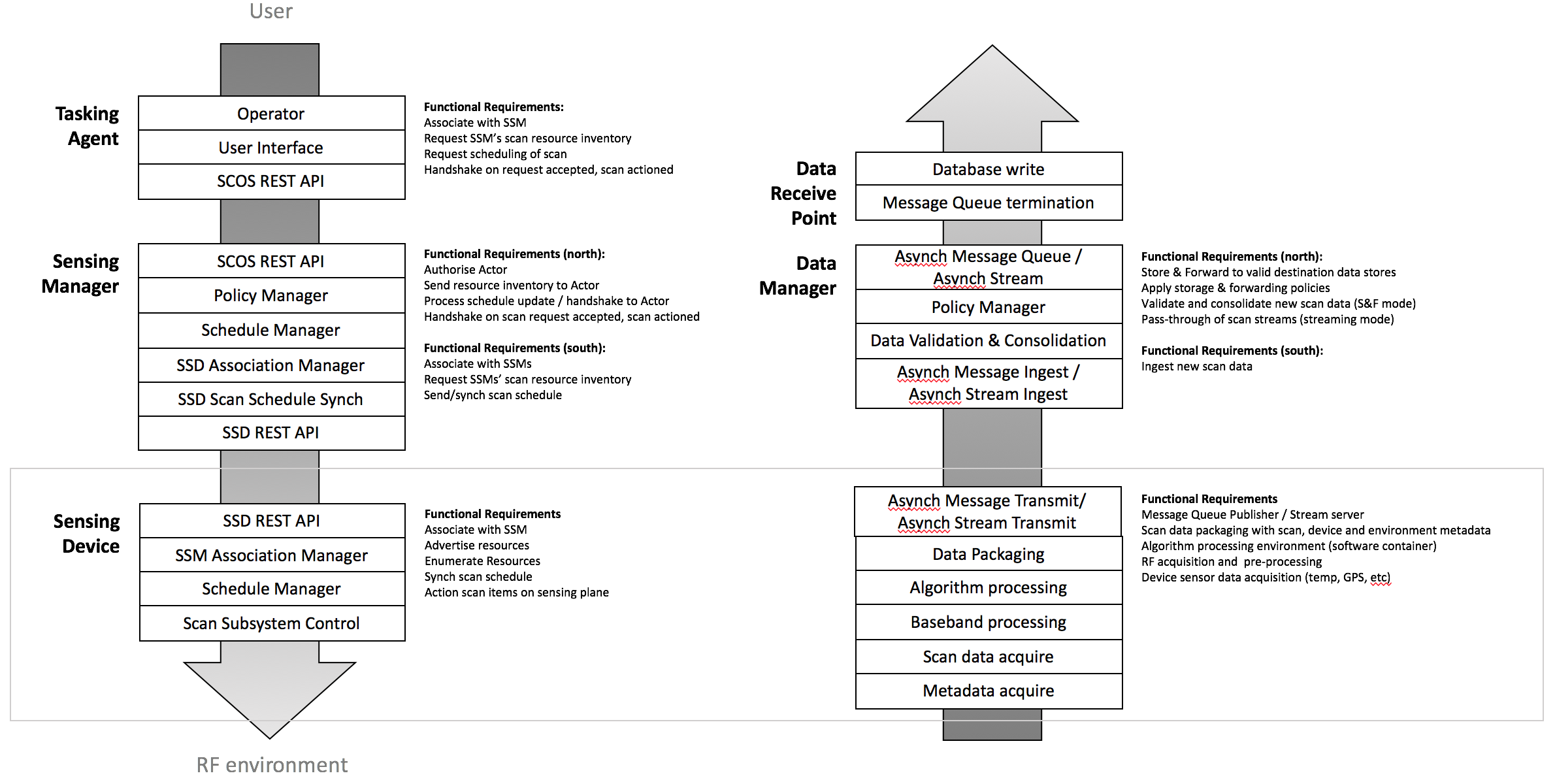


Figure 2: SCOS Functional Block Diagram

This diagram can be extended with the concept of proxying to allow SCOS systems to be cascaded, or the use of non 802.22.3 compliant sensing devices.

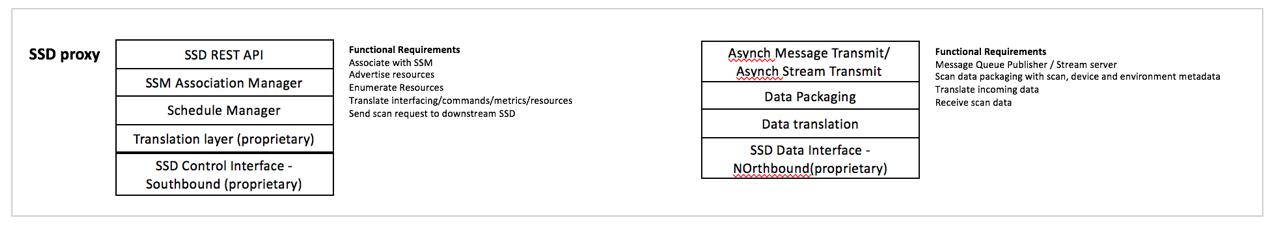


Figure 3: SSD Proxy

****

Figure 4: SSM Proxy

* 1. System Model
     1. Tasking Agent

Tasking Agents are human or machine entities that can query SCOS resources and request scans to be performed.

There are at least three main classes of consumers of spectrum data:

**Type A Agent:** are specifically looking for current sensing information, and request specific scans to obtain specific data (e.g. law enforcement).

**Type B Agent:** have a requirement to keep spectrum information up to date (e.g. spectrum occupancy database operators), and will need to request periodic scans to achieve this.

**Type C Agent:** those that want to read spectrum information from a DRP that is already populated with their required data. These users are not contemplated in this standard.

In general it should be assumed that a Type A Tasking Agent would have higher priority in terms of scan resources, as governed by a Policy expanded on below.

* + 1. Spectrum Sensing Device (SSD)

SSDs convert radiative electromagnetic energy into a voltage, which is then sampled. The samples can then be processed in various ways to provide information on the immediate RF environment, e.g., amplitude statistics versus frequency, amplitude and phase versus time at a given frequency, occupancy statistics, angle of arrival.

* + - 1. Hardware Model

A simplified hardware block diagram of a general SSD model is depicted in Figure 5. SSD hardware designs are not required to have each component shown in the block diagram. Specifics for each component (e.g., presence, model, operational parameters), however, is required metadata when SSD capabilities are queried by the SSM. This SSD definition metadata will also accompany the output data messages.

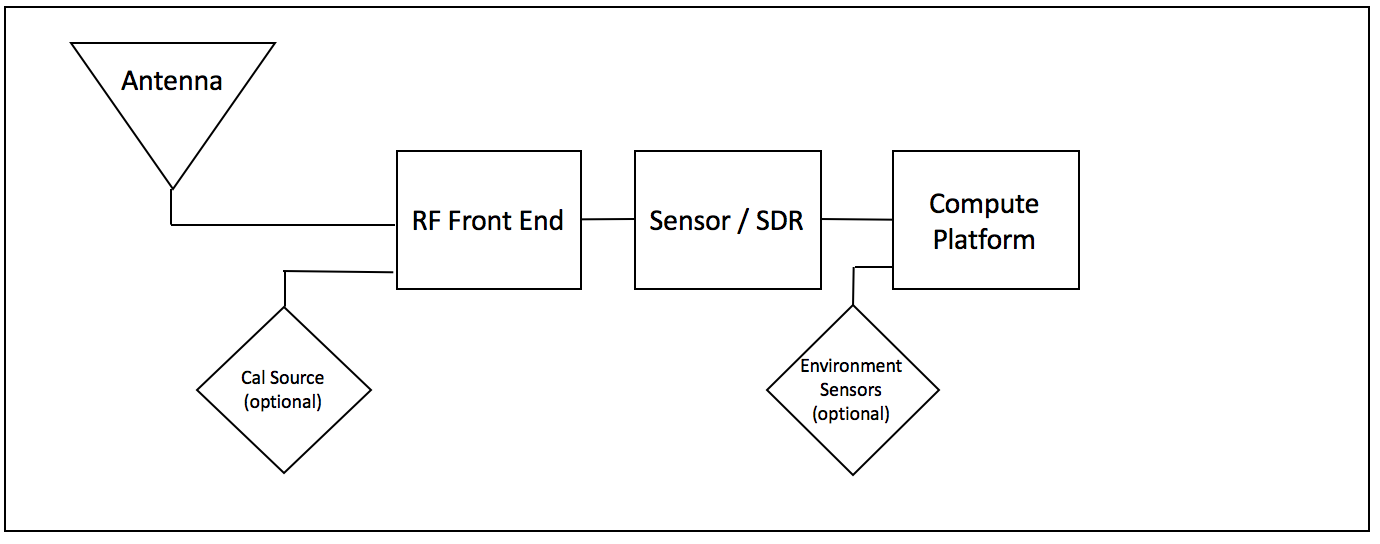


Figure 5: SSD Simplified Hardware Model Block Diagram

The SSD is composed of the following functional elements, as follows:

* Section 1 – Antenna: An antenna used to collect RF energy. This is fed to Section 2 over a hardware interface (interconnect cable)
* Section 2 – Signal Conditioning Unit: An RF front end unit consisting of (all or some of) an RF switch (optional, with the ability to accept an optional calibration signal), filter, Low Noise Amplifier, mixer. This sends the conditioned signal to Section 3 over an analogue hardware interface (interconnect cable/track).
* Section 3 – Signal Extraction Unit: Analogue Digital Converter, spectrum analyser or Software Defined Radio to act as a baseband processor, performing a demodulation of the conditioned signal and acquires the baseband signal. This sends a digitised signal over a digital interface (interconnect)
* Section 4 – Compute Platform: that provides
  + A signal processing function with a signal detection and/or classification algorithm. It sends detection/classification data to metadata consolidation and packaging function over a software interface.
  + A metadata consolidation and data packaging function that combines sensing data with environmental inputs (where implemented), hardware, operating and system-configured metadata. It sends data packages to the transmission system over a software interface.
  + A transmission unit that transmits scan data to the destination system over a best-effort IP connection.

The Compute Platform sends necessary command and control signals to Section 2 (Conditioning Unit) and Section 3 (Extraction Unit). It receives data from the Sensor/SDR, and polls any environment sensor input devices for necessary metadata items, such as GPS location. Interaction of the various elements is described in Figure 6: SSD Functional Elements.

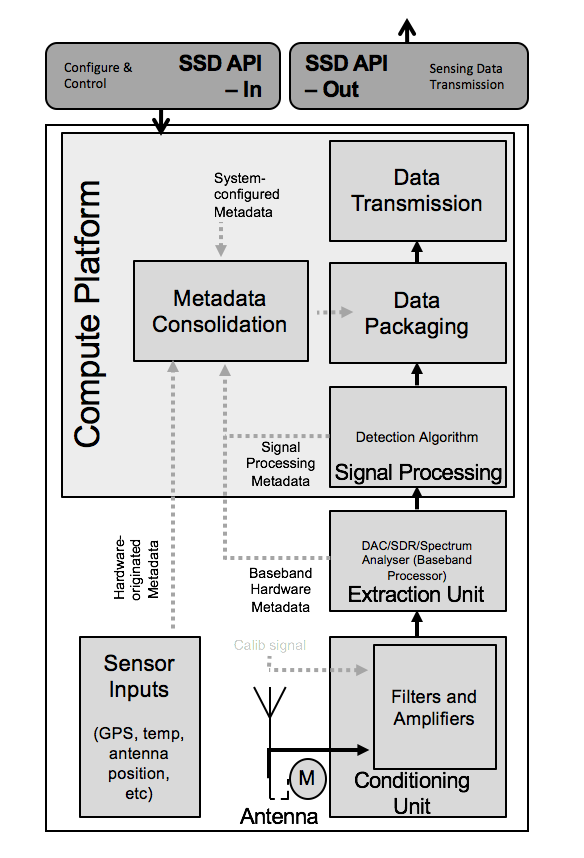


Figure 6: SSD Functional Elements

This block diagram can be split into the hardware layer and the software processes that run alongside. These hardware blocks or software services can/will generate metadata that is associated with each item.

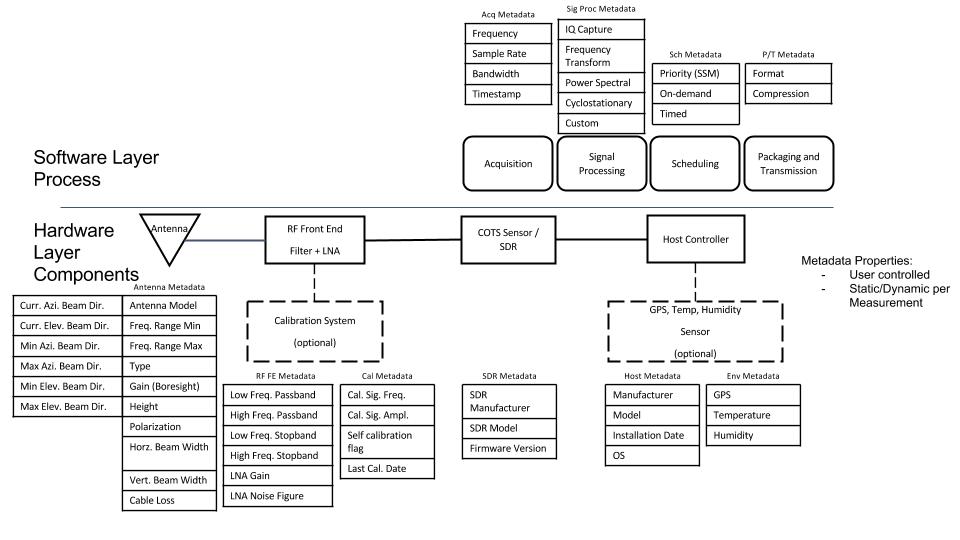


Figure 7: SSD model - Hardware layer components and Software layer processes with relevant metadata

* + - 1. SSD Calibration Model

A calibration can be done in the lab at build/commissioning time, and stored as a calibration file on the SSD.

Further, an SSD with a self-calibration capability can be instructed through an administrative interface (not Tasking Agent request) to perform a calibration using a local calibration source.

* + - 1. SSD Algorithm Model

The Algorithm models shall be described in terms of inputs into black box: the identity of the USER and SSM requesting the scan, the measurement parameters, which algorithm is to be used; and outputs from the black box: the identity of the USER and SSM requesting the scan, the requested scan parameters, the identification of the algorithm model, and the processed results.

<Define use cases>

Normative model: general energy detection algortithm

At least one algorithm model is defined – a general energy detection algorithm.

<Trigger event algorithm>

<DF algorithm>

<Cyclostationary>

It is the responsibility of the SSM operator to publish algorithm definitions externally. Code does not need to be publicly accessible.

Allow for the development of advanced algorithms, e.g., DF.

* 1. Spectrum Sensing Manager (SSM)
     1. SSM Association

SSM’s receive and manage association requests from SSDs

* + 1. SSM Task Scheduling

Scheduling is defined in terms of scan intervals that take up slots in a calendar schedule. These slots will include slots for long scans; and slots for very short scans to ensure fair allocation of scan resources.

Scheduling requests from a USER will be defined in terms of duration, time, repetition, etc, as well as a flag to indicate whether the desired scan slots are “Exact Time” slots or “Nearest Time” slots. The scheduler on the SSM will use this to try meet the USER request (and either confirm the scan schedule is accepted or refused).

* 1. Data Manager
     1. DM Functional Specification
  2. Topology

The SCOS system consists of a single SSM, which communicates over any standard network transport with one or more SSDs. The SSDs shall not communicate with each other, or directly with the user of the SCOS system (Tasking Agent). One or more Tasking Agents may communicate directly with one or more SSMs, but each communication is independent of the others.

The topology downstream is hence N:1:N for Tasking Agent:SSM:SSD, and similarly upstream it is N:1:N for SSD:DM:DataStore.

Provision has been made for an SSM Proxy, where an SSM can communicate with other SSMs as if they were associated SSDs.

Provision has also been made for proxying, which allows a non 802.22.3 compliant SSD to associate with and be controlled by an SSM, as well cascading of systems, where one 802.22.3 compliant SSM to be associated with, and delegate tasks to, another 802.22.3 SCOS system.

1. Interfaces, Messaging and Primitives

Figure 8 illustrates a simplified SCOS interactions model.

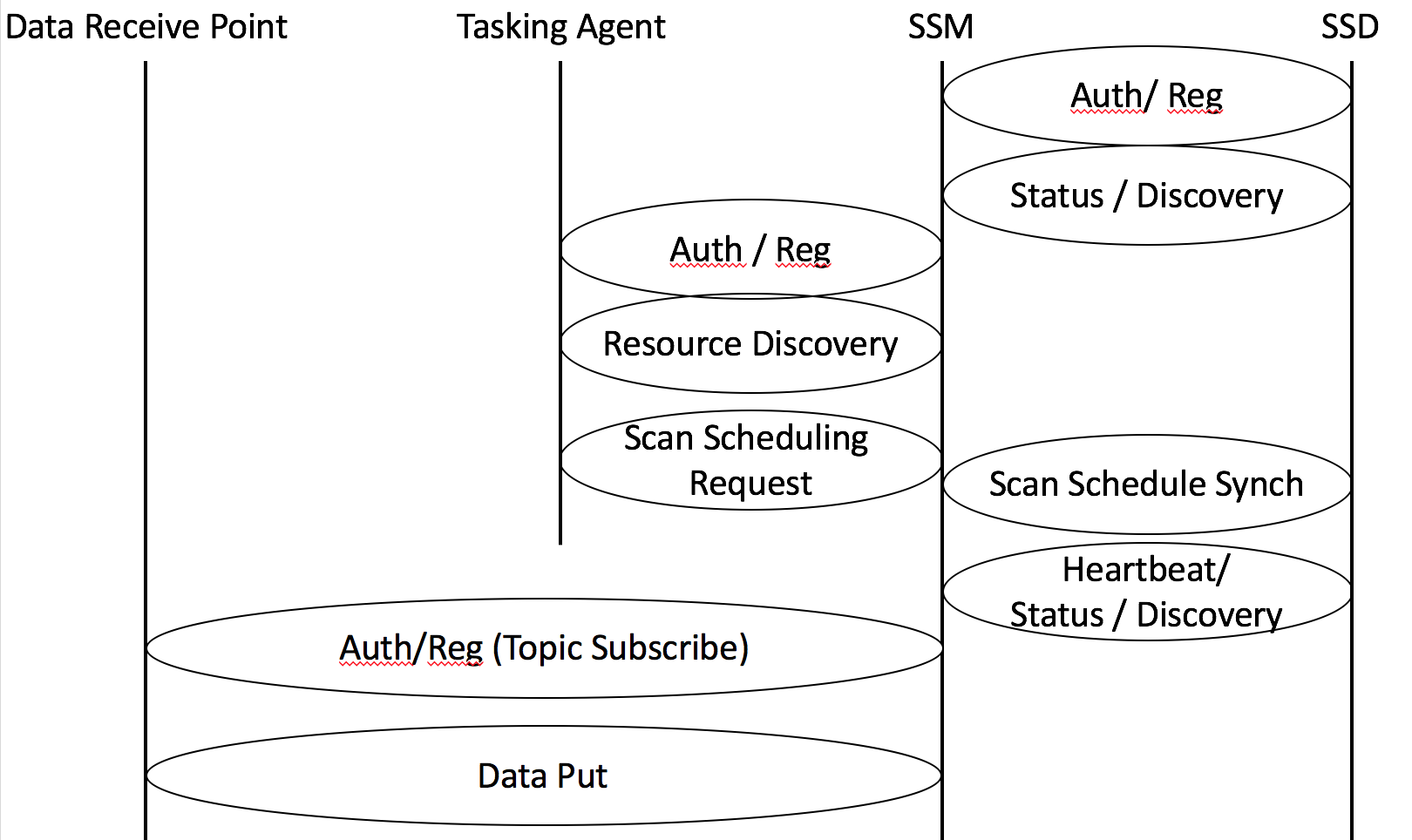


Figure 8. Simplified Interactions Model

* 1. SCOS Interfaces
     1. SCOS communication interfaces

Following are the key SCOS communication interfaces.

* Tasking Agent and SSM Interface
* SSM and SSD Interface
  + The interface between SSM and SSD is required to be synchronous.
* SSD and SDM Interface
* SDM and DRP Interface
  + The interface between SSD and SDM is required to be asynchronous.
    1. Tasking Agent to SSM Interface
       1. Authentication and Registration

These procedures define the association and authentication process for an SSM and Tasking Agent entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSM is authenticated and registered to a Tasking Agent, the Tasking Agent can then discover the capabilities of the SSM and its associated SSD’s. The Tasking Agent may then define and make sensing requests to the SSM, which include a designation of the Data Receive Point(s) to which the data is to be sent. The SSM will notify the Tasking Agent when measurements are successfully completed (or not) and available at the Data Receive Point.

* + - 1. Resource Discovery

Resource Discovery is the process of informing the Tasking Agent of what capabilities that the SSM has with regard to what types of measurements, what bands can be measured and associated measurement parameters that can be specified and controlled and over what locations. This takes the form of a resource/capability descriptor and the current scan schedule per SSD.

* + - 1. Scan Request

The Scan Request message from the Tasking Agent to the SSM includes the parameters of the desired spectrum measurement to be made and any associated processing to be performed by either the SSD or the SSM. This scan request is wrapped in a scheduling task description, defining the time the scan is to be made, the repetition rate (if applicable), the locations, etc. When the scan parameters in their scheduling wrapper are received by the SSM it will be validated as possible to be executed (i.e. the resources requested meet the SSMs schedule of resources available), and either acknowledged as being queue, or a refusal is returned to the Tasking Agent. If a scan schedule is updated for a particular SSD, it is then replicated down to that SSD.

* + 1. SSM to SSD Interface
       1. Authentication and Registration

These procedures define the association and authentication process for an SSD and SSM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once an SSD is authenticated and registered to a SSM, the SSM can then discover the capabilities of the SSD. An SSM will have associated with it at least one SSD. The SSM may then assign sensing requests to the appropriate set of SSDs in order to fulfil the sensing request of the Tasking Agent.

* + - 1. Status and Discovery

The Status and Discovery process serves two functions. The first is to inform the SSM of what capabilities that the SSD has with regard to what types of measurements, what bands can be measured and associated measurement facilities (such calibration, antenna control, mobility, storage, processing) that can be specified and controlled and over what locations. The SSD will transmit a package describing its capabilities and available resources at time of authentication/discovery, and if there is any change in its configuration. The second function is to maintain association with the SSM. It will transmit a period heartbeat to indicate it is still associated with the SSM. If it is to disconnect, it will transmit a disassociation message (e.g. if it is rebooting or about to go into an offline mode).

* + - 1. Scan Request

The Scan Request message originating from the SSM is sent to the appropriate SSDs for execution as a scan schedule. It includes the parameters of the desired spectrum measurement to be made based on knowledge of the SSD’s capabilities. This request will include the time to make the measurement, the repetition rate (if applicable), the locations, etc. and the format of the measured data. In the case of a single, once-off scan, the schedule will indicate no repitition.

* + 1. Data Manager to Data Receive Point Interface
       1. Authentication and Registration

These procedures define the association and authentication process for a Data Receive Point and DM entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a Data Receive Point is authenticated and registered with a DM, the DM is then authorized to cause data to be delivered to the Data Receive Point based on the privileges of the Data Receive Point and the DM. The Data Receive Points can be grouped into Data Receive Point Groups, where a transmission of data from the DM is delivered to multiple Data Receive Points.

* + - 1. Data Manager

These procedures define and enable the storage of data from the DM to the Data Receive Point. The successful reception of this data initiates a notification of the initiating Tasking Agent that requested that data.

* + 1. Tasking Agent to Data Receive Point Interface
       1. Authentication and Registration

These procedures define the association and authentication process for a DRP and Tasking Agent entity to connect and communicate. They include facilities to prevent spoofing based on shared key exchange. Once a DRP is authenticated and registered to an Tasking Agent, the Tasking Agent is then authorized to cause data to be delivered to the DRP, and read that data.

* + - 1. Resource Discovery

Resource Discovery is the process of informing the Tasking Agent of what capabilities that the DRP has with regard to what types of data can be stored, at what rate, at what access level, and in what quantity can be specified. It may also initiate that association of a particular DRP with a specific SSM that will be providing the data.

* 1. SCOS Messaging

The communication between each of the entities defined above can be grouped and defined within the Interface Categories shown in Figure 9. Message Sequence and described below.

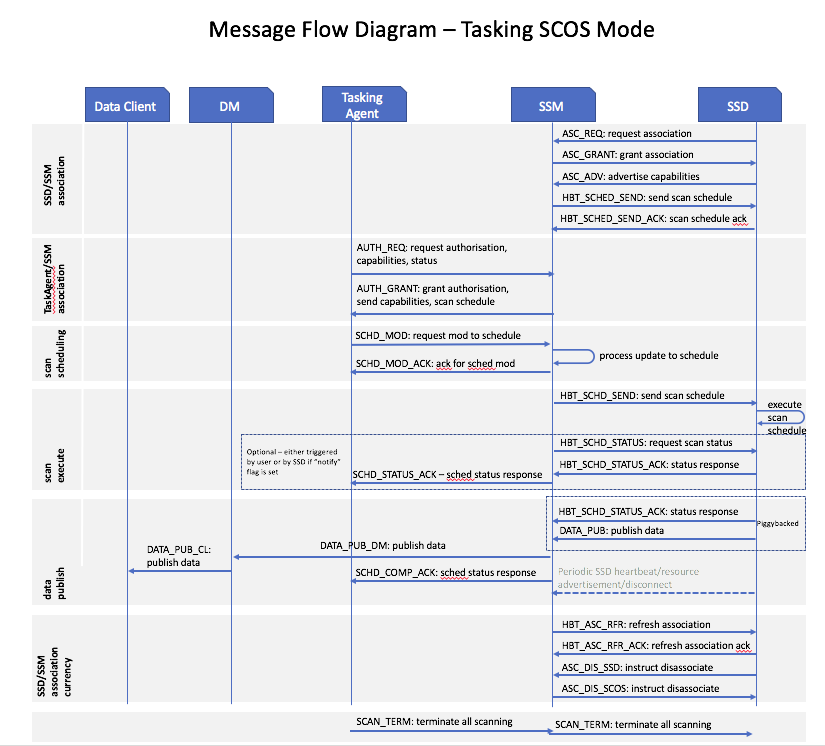


Figure 9. Message Sequence

* + 1. Message Encoding

SCOS messages are encoded in JavaScript Object Notation (JSON). JSON is a language-independent data-interchange format that is easy for humans to read and write. There are code and functions readily available in C, C++, C#, Java, JavaScript, MATLAB, Perl, and Python for parsing and generating JSON. It is a lightweight alternative to XML, commonly used to transmit data between server and browser application.

The first five fields are the same for all messages; they are:

1. Ver = Schema/data transfer version with the major.minor.revision syntax (string)

2. Type = Type of JSON message (string) {“Sys”, ”Loc”, or “Data”}

3. SensorID = Unique identifier of sensor (string of URL unreserved characters)

4. SensorKey = Authentication key given out by MSOD (integer)

5. t = Time [seconds since Jan 1, 1970 UTC] (long integer)

Each message begins with a header comprised of attribute-value pairs in ASCII characters. [#confirm]

If an attribute is not relevant to the sensor implementation, then the value is set to NaN or "NaN".

The following are specific formatting rules to be followed:

* All timestamps, i.e., t (defined above)and t1 (to be defined in Data message description) will be reported as seconds since 1/1/1970 midnight UTC in the UTC time zone.
* String values must only contain URL unreserved characters (i.e., uppercase and lowercase letters, decimal digits, hyphen, period, underscore, and tilde), and
* Field names cannot start with an underscore because that convention is reserved for internal implementation-specific uses.
  + 1. Message Transport protocols

The standard requires reliable transport mechanism, with MQTT and AQMP recommended as well understood protocols. Within MQTT, QOS 1 (AT-LEAST-ONCE) is suggested.

The SSM devices should use MQTT to speak to a MQ server instance (e.g. RabbitMQ). The MQ server instance maps the MQTT topics from the SSM into queues which the SSM ingest layer monitors and processes messages out of.

All traffic from the Tasking Agents to the SSM goes via AMQP queues into the MQ server instance which maps it out to the appropriate MQTT topics. The SSM pick up messages on any topics to which they have subscribed.

The standard recommends MQTT transport for communication between SSM and SSDs [#RecommendedTransport? #AddReference MQTT].

Transport security is ensured using the security protocols and procedures within the transport mechanism.

Example: MQTT messages can be secured using TLS. Please refer to [#Reference] for security mechanism in MQTT.

* + - 1. Message Transport QOS

All messaging on the MQTT side makes use of QOS 1. When using QoS level 1, it is guaranteed that a message will be delivered at least once to the receiver. The message can also be delivered more than once. If a message is delivered more than once it should start a counter and a clock. If the clock/counter exceeds a threshold it should create an alert on the administration console that there is a comms or ingest fault.

The SSM’s use a non clean session when connecting which ensures that messages sent to the client when non connected will be queued and delivered on reconnection. On the RabbitMQ the messages are queued on a topic for a client for up to 30 minutes before being discarded (this threshold for discussion).

The MQ server must use persistent queues for all applicable queues. Messages should survive a restart.

* + - 1. Message Transport security

The MQTT segment has security based on TLS with pre-generated certificates.

* 1. SCOS Message exchanges

Following table identifies messages across different entities.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Operational procedure** | **Message Name** | **Description** | **Transport** | **Section Ref** |
| Tasking Agent association |  | From:  To:  Purpose: |  |  |
| Tasking Agent dis-association |  | From:  To:  Purpose: |  |  |
| SSD association |  | From:  To:  Purpose: |  |  |
| SSD dis-association |  | From:  To:  Purpose: |  |  |
| Spectrum-scan |  | From:  To:  Purpose: |  |  |
| Spectrum-data-dissemination |  | From:  To:  Purpose: |  |  |
| Heartbeat |  | From:  To:  Purpose: |  |  |
| Calibration |  | From:  To:  Purpose: |  |  |
| Configuration |  | From:  To:  Purpose: |  |  |
| Query |  | From:  To:  Purpose: |  |  |
| Reporting |  | From:  To:  Purpose: |  |  |
| Management |  | From:  To:  Purpose:  Note: Platform control message |  |  |

* + 1. Response codes

0: success

100 – 199: error events related to the entity association and disassociation

200 – 299: error events related to the entity configuration and policy enforcement

300 – 399: error events related to the scanning procedures

400 – 499: error events related to the data dissemination procedures

500 – 599: error events related to the heartbeat procedure and SCOS entity/platform health

600 – 699: error events related to the SCOS infrastructure administrative procedures

* + 1. Transmission – from SSD to SM / from Platform Control to SM

Northbound (SSD to platform): The package is transmitted to a remote system that ingests and validates data, and stores for further processing, with ACK back to SSD that packages were received.

Southbound (platform to SSD): Control messages are transmitted to SDD for execution by SSD, with ACK that control messages was received, and response code that instruction was accepted/rejected.

* + 1. DM to Data Receive Point

Package must be reliably, securely and scaleably received and transmitted to Data Receive Point

Messages are processed inside the SSM using an ESB application. The ESB application architecture allows for small discrete message handlers to be written to deal with each type of message. Using a load balanced and multiple instances of the servers the load can be shared out across multiple servers.

Handlers are written for each of the types of messages. These handle unpacking and persistence of the incoming data. In some circumstances messages may be forwarded on to a task processor for further processing or analysis. All messages are persisted in a database.

* + - 1. Data Receive Point move to Storage

Data moved into structured database

* + 1. From Tasking Agent to SSM: Platform Control Messages

HTTP service endpoints are implemented in the ESB application to allow for the triggering of outbound control messages to the SSDs through a southbound interface.

A variety of task requests can be predefined by the SSM policy such as different scan modes of the SSM, defining different timeframes, scan parameters, etc:

- Test Mode: one ping and one raw scan every 15 minutes

- Mobile Mode: one ping and one raw scan every 10 minutes

- Static Mode: one ping and one TV channel scan every 15 minutes. one raw scan every ½ hour.

These messages can be used to trigger SSD scan activity, or for system management.

* + 1. Heartbeat
    2. Configuration
    3. Calibration
    4. Query
    5. Log
    6. Report
    7. Management

SCOS Administration described in this section.

1. Administrative interface
2. SCOS Configuration, Management, and Maintenance
3. Policy
4. Security

Section to be developed further – but note that should not be proscriptive as admin/management can be considered implementation specific

* 1. Primitives

SSD and SSM messages will be in JavaScript Object Notation (JSON). JSON is a language-independent data-interchange format that is easy for humans to read and write. There are code and functions readily available in C, C++, C#, Java, JavaScript, MATLAB, Perl, and Python for parsing and generating JSON. It is a lightweight alternative to XML, commonly used to transmit data between server and browser applications.

The data fields in the JSON message descriptions below are required fields. If an attribute is not relevant to the sensor implementation, then the value is set to NaN or "NaN". Each message (in general) will begin with a header comprised of attribute-value pairs in ASCII characters. The first five fields are the same for all messages; they are:

1. Ver = Schema/data transfer version with the major.minor.revision syntax (string)

2. Type = Type of JSON message (string) {“Sys”, ”Loc”, or “Data”}

3. SensorID = Unique identifier of sensor (string of URL unreserved characters)

4. SensorKey = Authentication key given out by MSOD (integer)

5. t = Time [seconds since Jan 1, 1970 UTC] (long integer)

The following are specific formatting rules to be followed to avoid problems when messages are ingested into MSOD: (1) All timestamps, i.e., t (defined above)and t1 (to be defined in Data message description) will be reported as seconds since 1/1/1970 midnight UTC in the UTC time zone. (2) String values must only contain URL unreserved characters (i.e., uppercase and lowercase letters, decimal digits, hyphen, period, underscore, and tilde), and (3) Field names cannot start with an underscore because that convention is reserved for MSOD internal use.

* + 1. SSD<>SSM Messages
       1. SSD-SSM Association Primitives

|  |  |
| --- | --- |
|  |  |
|  |  |
| SSD Association: |  |
|  |  |
| SSD Send: |  |
| SSD associate { |  |
| Association [request new, request refresh, request disassociate] |  |
| SSD Device ID |  |
| Public Key} | SSM would have all possible SSDs’ public keys that can associate |
|  |  |
| SSM Reply: |  |
| SSM associate { |  |
| SSD Device ID |  |
| Association state granted [new, refresh, disassociate] |  |
| SSD association max TTL | Tells SSD how long before it gets auto disconnected |
| SSD association remaining TTL} | Tells SSD how long left on clock |
|  |  |

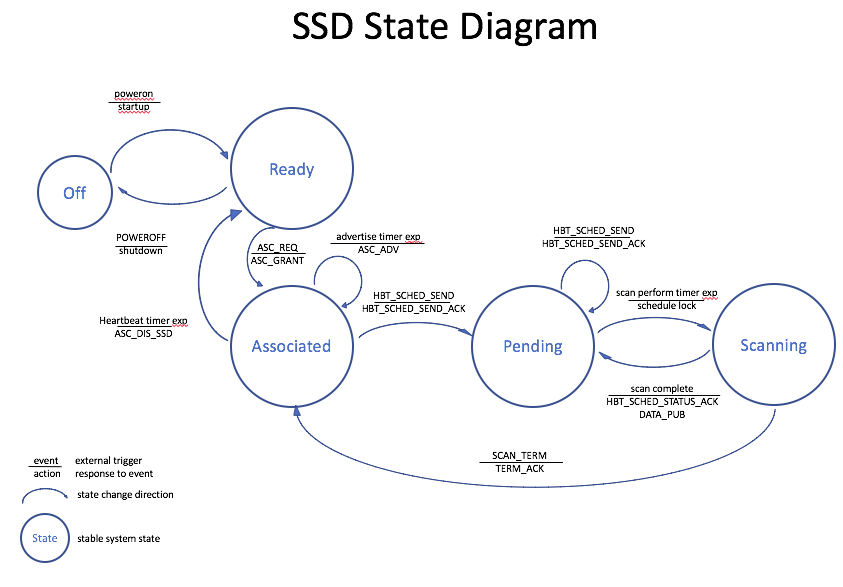
* + - 1. SSD-SSM Scheduling Primitives

|  |  |
| --- | --- |
| SSD Advertise: |  |
|  |  |
| SSD Send: |  |
| SSD spec { |  |
| Fmin |  |
| Fmax |  |
| Resolution |  |
| Algorithm Type 1..n |  |
| Antenna type |  |
| Antenna direction |  |
| GPS available |  |
| GPS location |  |
| …etc } | All standard defined metadata types |
|  |  |
| SSM Reply: |  |
| SSM scan schedule for (SSD Device ID) |  |
| Scan 1 time { |  |
| Scan Schedule Sequence Number | Unique to scan |
| Time Start Offset | Time in minutes from start of week |
| Time Slots | How many minutes to block |
| Repeat start offset | Interval to repeat start |
| Number of repeats | How many repeats (anything outside week window are dropped) |
| Scan 1 spec { |  |
| Fmin | Desired Fmin |
| Fmax | Desired Fmax |
| Resolution | Desired res |
| Algorithm Type | Give desired algorithm type |
| Antenna type | Give expected antenna type |
| Antenna direction | Give expected/desired antenna direction |
| GPS enable | Yes/No |
| GPS location | Give expected GPS location |
| …etc } | All standard defined metadata types |
|  |  |
|  |  |
| Scan 1 destination { |  |
| Tasking Agent public key | Tasking Agent’s public key identifier |
| MQ topic or URL of data destination} | Where data will be published to |
|  |  |
| Etc … Scan n |  |
|  |  |
|  |  |
| SSD reply on scan execute: |  |
| Scan Schedule Sequence Number |  |
| Scan Completion Code | 1 – complete, 2 – incomplete, 3 – rejected |
| Scan Completion Fstart | Freq where scan was to start |
| Scan Completion Fend | Freq that was attained (“0” for invalid) |
| Scan parameter that caused rejection | If Completion Code 3, this gives problem metric |
| Scan Time to Complete |  |
|  |  |
|  |  |
|  |  |

1. Procedures

These sections need considerable attention

* 1. State Diagram



* 1. Messaging Chart for State Changes
  2. Operations and Security
     1. SSM Policy

A policy layer in the SSM at the northbound and southbound API will ensure that the SSM is operated within requirements of a local authority (national regulator, law enforcement, military, etc).

The policy on the southbound interface will determine, based on the Tasking Agent type, (e.g. how a central authority can define what kinds of sensing can be done in what bands, what data governance rules there are, etc, the resource allocation, what kinds of users are authorized to request resources from the sensor network and in which priority (i.e. if a sensing network is resource constrained, who gets first priority on the sensors)

Policy on the northbound interface (SSM>DRP) will have rules for how sensing data may be distibuted, and data storage policies. This would include which scan data takes priority if local storage in the store&forward buffer is running out due to a failed transmission link, and how long certain USER data is allowed to be stored in the local store&forward buffer.

Policy file: It is envisioned in the first version of this standard that the SSM stores a policy file which is installed manually by Sensing Operator (through mechanism such as SSH and update pull, or remote SCP).

Security Considerations

* + 1. SSM Administration

Administrative functions on the SSDs and SSMs are largely assumed to be implementer-specific, and out of scope for the standard, but recommendations are included in the informative annex.

This interface shall have a secure mechanism to administer the system, allowing:

* performing of calibrations
* updating firmware
* changing configuration of SSD, and making associated changes to the SSD configuration file
* triggering reboots and other hardware maintenance functions.

The administration interface must be a secure interface with key exchange, and these keys must not be the same as keys used for TASKING AGENT<>SSM<>SSD authentication.

* 1. Data Ownership

The entity that builds/owns the SCOS owns the data it acquires. It can sell this data. Once that transaction takes place. The client has ownership, which is not necessarily exclusive - i.e., SCOS can sell it to other clients.

* 1. Security Systems
     1. Threat overview
     2. Authorisation, authentication, identity
     3. Security design between each architecture layer
        1. Physical security
        2. Data transmission security
     4. Security and redundancy model for Data Receive Points

# Informative: Reference Applications

## White Space device radio operation

Either the network operator or device operator using spectrum sensing to identify primary or other secondary users of particular channels. Spectrum sensing would either built into the radio devices or in standalone sensing units.

The standard allows a “CR Mode” of operation that would make it suitable for use in radio systems to complement Geolocation Databases (such as a WSDB).

## National spectrum regulation

National radio regulators would use a system comprising spectrum sensing devices to feed into a national spectrum utilization database for assignment management and planning purposes, and generating historical records for compliance monitoring and enforcement.

Devices deployed in various scenarios:

* Fixed devices at key locations and high sites
* Mobile devices on vehicles that travel widely and can create a sample set of spectrum utilization through snapshots at time or location intervals
* Devices either at fixed locations or periodically moved to create location-based spectrum utilization datasets
* Nationally deployed in a swarm of a given device density to create real-time national spectrum utilization maps and for validation of Spectrum Geolocation databases.

When spectrum monitoring is used for automated spectrum usage enforcement, data from a spectrum monitoring system has a critical role in the six basic steps for spectrum enforcement:

1. detecting, 2. identifying and classifying, 3. locating, 4. reporting, 5. mitigating, 6. remediating interference.

It is important to note that each of these six steps may, in general, require a different data type to be collected and stored; ranging from amplitude only information to raw IQ samples. It is possible for the sensing network to process spectrum data at the edge and only report the result of the processing, where conceivably a sensor or set of sensors can identify and locate an emitter without sending the raw spectrum measurements.

For example, the sensing network might report and store only the location information along with the signal classification information. This standard has been made flexible enough to define and enable both the collection of the various data types, along with associated meta-data, as well as the reporting and collection of the results of data analysis performed at the edge.

Spectrum management systems work to accomplish agency missions in geographic area(s) with limited and often shrinking frequency assignments. Monitoring can support spectrum managers in being more efficient by providing real-time and historical information about the RF environment on-base and at-boundary. Further, monitoring information can be used to mitigate and protect government wireless assets from intentional and unintentional interference.

## Research programmes

Scientists using sensitive radio frequency systems (e.g. radio-telescopes) struggle with RF interference. SCOS devices can let them identify RFI and the location of their sources.

## Law enforcement and public order

Law enforcement and other authorities are increasingly dealing with problems stemming from radio-controlled or radio-connected systems.

**Illegal drone use:**  These include people flying radio-controlled unmanned aerial vehicles (drones) in prohibited places. SCOS systems can be used to detect characteristic transmissions of drone operation in areas such as in the airfield flight traffic area.

**Detecting jamming devices:** A problem area for security staff and law enforcement is the use of radio jammers to interfere with remote control devices like vehicle keyless entry systems or radio links for alarm systems. SCOS devices can be used to identify and locate jamming systems.

**Detecting unauthorized mobile phone use:** Controlled and high security areas such as prisons will frequently prohibit the use of cellular phones in certain areas, but may not jam operating frequencies because of other regulations. Identifying and locating transmissions allows direct action to be taken on equipment users.

## Network Operator Applications

Radio planning for fixed radio deployment.

Spectrum forensics for identifying sources of interference.

# Normative Functional Requirements

## Tasking Agent Requirement

Tasking Agents accessing a distributed SCOS system will require access to one or more spectrum sensor devices situated at a remote location through an Internet-connected interface.

This interface must expose all of these functions to the SCOS system user through a defined, standardised interface

* The TA can discover the availability and capability of sensor devices connected to a Sensor Management System
* The TA can request the performance of a scan task according to chosen parameters, or in a more advanced system request a recurring scan to be scheduled that will be executed automatically by the SCOS system
* The TA can define where the data generated in the scan should be transmitted to once complete
* The TA must be given diagnostic or performance information relating to the execution of their scan task

The user must be able to access their scan data and associated metadata describing the scanner’s environment, hardware and software configuration and scan settings.

## Data Quality and Definition

Data acquired must be accompanied by adequate metadata information to allow for duplication of the measurement or assessment of data quality by a subject matter expert. Hardware specification and measurement parameters are to be included in the messaging metadata requirements. Information less amenable to metadata capture should be made available via appropriate and accessible documentation, e.g., algorithm described via written article with source code in Github repository.

## Regulatory requirements

This standard should provide mechanisms to meet the regulatory requirements of national operators that have defined parameters or requirements for spectrum sensing in various applications. These regulatory requirements would take two forms: the first is technical requirements for sensitivity, resolution, etc. The second is limitations on how and where sensing might be done where there are sensitivities around privacy, military use and other national policies and regulations.

## Policy Management and Enforcement Requirements

To allow for granularity in what the SCOS systems can do, but also ensure spectrum occupancy or utilization data is not exposed in contravention of national policy or regulation, it is proposed that the SSM would be able to apply policies to allow or disallow certain functionality in the SSDs, or disallow transmission of the data to third party systems.

These policies would be determined by the SSM operator in accordance with their requirements and that of local authorities (e.g. a national regulator or network operator), and cascaded down to any connected SSDs. These policies would allow sensing only according to allowed metrics (e.g. no hi-resolution raw scans in military radar bands), and limit sensing data transmission to certain classes of third party systems.

## Sensor Location-Fixing Requirements

The SCOS device can convey the location of the sensors to the aggregation entity such as the SSM. The instruction to use available location capabilities on the SSD (e.g. GPS location) will be part of the scan schedule instruction from the Tasking Agent requiring the scan. This feature allows the SSM or the aggregation entity to localize the proximity of the signal source location allowing more efficient spectrum management. This location fixing capability will be implemented by the system operator to be in accordance with local regulatory requirements.

Location can be fixed in three ways:

* At scan-time from lat/long co-ordinates from internal GPS, GLONASS or similar system
* Configured at startup-time from lat/long co-ordinates from internal GPS, GLONASS or similar system
* Configured on SSD by authorised/certified installer at commissioning time with accurate lat/long coordinates
* Configured on SSD by authorised/certified installer at commissioning time with street address/location

The type of location fix would be specified in device metadata (NOTE: ADD REFERENCE).

## Service Level Agreement Requirements

To be completed.

## Certification Requirements

To be completed.

## Technical Requirements

### Device classes and complexity

The following sensing device categories may be considered:

* **Energy Efficient Sensing Devices**: This standard should provide mechanisms of energy efficient operations, eg. solar powered or battery operated spectrum sensors for monitoring applications.
* **Small form factor devices**: Devices that can fit the spectrum sensing function within a small form factor (e. g. a USB dongle, cell phone etc.)
* **Advanced Spectrum Sensing Devices**: Advanced Spectrum Sensing Devices with capable Radio Frequency Front Ends (RFFE) and dedicated resources for spectrum sensing may be considered.
* **Non-dedicated Devices with Sensing Capability:** A number of consumer and professional radio devices contain radio receivers that can be used as sensing devices, including mobile phone handsets, Wi-Fi access points (from 802.11ac) and Dynamic Spectrum Access radio systems (including 802.22).

### Number of devices

This standard shall support at least one Spectrum Sensing Device to cover a location or area, communicating with a back-end Spectrum Sensing Management System (SSM), but will extend to describing an architecture and interfaces for multiple SSDs potentially communicating with multiple SSM instances.

### Real-time applications

The sensing devices will be performing spectrum sensing functions according to its scheduler (which is managed by its SSM), which can be updated in near-real time (dependant on speed of communication between Tasking Agent, SSM and SSD), or perform scans at scheduled intervals based on pre-configured schedules. However, the spectrum sensing reporting of data is out on a Best Effort basis, since the SCOS System uses the chosen available transport mechanism (e. g. 802.11, 802.22, Ethernet, Cable, Cellular etc.).

The SCOS system will benefit if sensing reports from various sensors are provided on a reasonable time-scales (e. g. minutes) so that the information is not stale. However, this is not a mandatory requirement. Also, the messaging format may be defined such that it does not produce excessive overhead penalty on the transport layer being used.

It is envisioned that real-time streaming will be provided for in future drafts of 802.22.3.

### Channelization

This standard may specify a Spectrum Manager entity that can command various sensors to go and sense in certain bands, or it may even specify the spectrum sensors to ignore certain bands from sensing, and impose channelization maps for sensors to meet local regulations or technical requirements.

Specific channelization maps may be provided in future drafts of 802.22.3.

## Security Requirements

This standard mandates secure authentication and authorisation between Tasking Agent and SSM, SSD and SSM, SSM and Data Manager, and Data Manager and DRP. Traffic between these components must also be encrypted. The specific security technology to be used is not mandated in this standard, but recommended best practices are described in Annex B. Note that the security model does not extend past transmission to the DRP. Responsibility for securing the spectrum data at destination remains the responsibility of the operator of that store.

The technology model is designed to ensure that data derived from SCOS devices and SSM are not used as an attack vector against White Space Databases, regulator spectrum management databases, etc. It is also designed to ensure that only authorised Tasking Agents can make use of the SCOS resources, and that they are correctly identified to enable correct application of the relevant system policies.

In each case, the security model must address:

(1) Data categorization (i.e. sensitivity/confidentiality of scan data)

(2) Access control - authorization and authentication (of each element when interacting with another)

(3) Logging and auditing (of instructions, tasks, access control)

(4) Data encryption (within devices and in transmission)

(5) System and information integrity (validation of device configuration, storage system)

(NOTE: Section to be developed further)

### Intra-device Layer Security (physical interfaces)

This standard defines security mechanisms to ensure integrity of sensing chain from antenna to DRP.

* Antenna to amplifier/filters: physical security of device in terms of cable/connectors (tampering such as substituting antenna, physical such as connector corrosion)
* Amplifier to SDR: cable connectors or PCB connections
* SDR to processing unit: cable connectors or PCB connections
* Enclosure for active elements: Protection against moisture, dust ingress. Screening against RFI from external sources. Screening to protect antenna elements against RFI from active elements.

(NOTE – this section needs considerable attention)

### Inter-Layer Security

#### Network Layer

Since this standard uses any available transport mechanism for data transmission, it will not recommend its own security mechanisms, but will use the existing security mechanisms of the transport mechanism being used (e.g. network 802.11 using Transport Layer Security,

#### Application Layer

Data transmissions should be secured on the application layer using mechanisms to guarantee the integrity and confidentiality of sensing and control data transmissions. This standard does not specify the technology used, but recommended implementation practices are noted in Annex B: Device and System Security Recommendations.

### Security of sensed data

This Standard shall not support mechanisms that expose data of radio system users that are modulated onto signals that are examined by the 802.22.3 SCOS System. For example, any kind of demodulation of the signals that may interfere with the privacy of the radio system users shall not be not be supported. However, the SCOS system shall support sophisticated spectrum sensing methods such as cyclostationary processing that can detect signals and characterize their modulation type.

### Security of analyzed or characterized spectrum data

This Standard shall support security mechanisms to ensure that spectrum characterization data is transmitted to the destination DRP in a secure way. This Standard shall not specify the security mechanisms used to protect this data once received by the DRP – this is implementation and system user specific.

# Normative - SCOS Metadata Specification

According to SCOS architecture and components, there is the need to add additional pieces of data, i.e. metadata, able to identify a peripheral node, SSD, on the basis of its own capabilities, and to tag occupancy results with information such as location, swept frequency, sensing algorithm etc. (proper definition and detailed explanation of employed metadata is given in sections C.1 and C.1.7).

It is necessary to classify such information in order to give them a priority order and to reduce the amount of exchanged data for each scanning request.

Metadata can be categorized into Classes, having different purposes:

* Class A (System Metadata) includes all pieces of data that are related to factory information and remain constant for the entire lifespan of the component (SSD);
* Class B (Current Status Metadata) includes data describing the actual configuration of the device, in terms of hardware (positioning, antenna configuration, battery level) and software (frequency settings, sampling rate, sensing algorithm, available local memory etc.);
* Class C (data related metadata), specifying parameters strictly related to performed sensing action (scanned time, timestamp, atmosphere conditions, amount of data to be read, estimated noise level);

Class A and Class C metadata are not subjected to any change since they are offered as a response to a specific query (in SSD association process and Sensing request, respectively).

Class B metadata are provided to SSM, after a specific user request, and can be subjected to modification and special settings by the Tasking Agent. They must be provided to the SSM before a scanning section starts, and they must be accompanied by an additional information bit, indicating their editing property (0, non-editable parameter; 1, editable parameter).

Each metadata must respect JSON message syntax and each message must contain the following fields:

* Name
  + This is a text field that contains the metadata name;
* Type
  + This field contain the data type [string|float|int|boolean];
* Editable
  + This field contain a boolean information. In particular it indicates the status of being editable of a specific piece of metadata (set to 0 for Class A and C, settable to 0 or 1 for Class B);
* Content
  + This field contain the content of the metadata.

## SSD metadata specification

#### Top level hardware metadata

|  |  |  |
| --- | --- | --- |
| Parameter | Values | Description |
| Antenna | 0 | Number of antennas |
| Calibration source |  | Present/absent |
| RF switch |  | Present/absent |
| RFFilter |  | Present/absent |
| LNA |  |  |
| Sensor |  | COTS/SDR |

#### Antenna Metadata

Antenna metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Antenna Model | Class A |
| Freq. Range Min | Class A |
| Freq. Range Max | Class A |
| Type | Class A |
| Gain (Boresight) | Class A |
| Polarization | Class A |
| Height | Class A |
| Horz. Beam Width | Class A |
| Vert. Beam Width | Class A |
| Min Azi. Beam Dir. | Class A |
| Max Azi. Beam Dir. | Class A |
| Min Elev. Beam Dir. | Class A |
| Max Elev. Beam Dir. | Class A |
| Curr. Azi. Beam Dir. | Class B |
| Curr. Elev. Beam Dir. | Class B |
| Cable loss | Class A |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Antenna Model | string | “0” | It contains a string with the model of the antenna that is installed. |
| Freq. Range Min | float | “0” | Min frequency value expressed in Hz |
| Freq. Range Max | float | “0” | Max frequency value expressed in Hz |
| Type | string | “0” | Antenna type |
| Gain (Boresight) | float | “0” | Antenna gain expressed in dBi |
| Polarization | string | “0” | Antenna polarization [“VL”|“HL”|“LHC”|“RHC”|“Slant”] |
| Height | float | “0” | Antenna heigh in m. |
| Horz. Beam Width | float | “0” | Horizontal 3-dB beamwidth expressed in degrees |
| Vert. Beam Width | float | “0” | Vertical 3-dB beamwidth expressed in degrees |
| Min Azi. Beam Dir. | float | “0” | minimum direction of main beam in azimuthal plane expressed in degrees from N |
| Max Azi. Beam Dir. | float | “0” | maximum direction of main beam in azimuthal plane expressed in degrees from N |
| Min Elev. Beam Dir. | float | “0” | minimum direction of main beam in elevation plane expressed in degrees from horizontal plane |
| Max Elev. Beam Dir. | float | “0” | maximum direction of main beam in elevation plane expressed in degrees from horizontal plane |
| Curr. Azi. Beam Dir. | float | “0” if fixed antenna is used  “1” if an antenna with beam steering capability is used. | Current direction of main beam in azimuthal plane expressed in degrees from N |
| Curr. Elev. Beam Dir. | float | “0” if fixed antenna is used  “1” if an antenna with beam steering capability is used. | Current direction of main beam in elevation plane expressed in degrees from horizontal plane |
| Cable loss | float | “0” | Cable loss expressed in dB of the cable connecting the antenna with the RF front-end |

### RF Front-end metadata

RF Front-end metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Low Freq Passband | Class A |
| High Freq Passband | Class A |
| Low Freq Stopband | Class A |
| High Freq Stopband | Class A |
| LNA Gain | Class A |
| LNA Noise Figure | Class A |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Low Freq Passband | float | “0” | Low passband frequency evaluated at -1 dB and expressed in Hz |
| High Freq Passband | float | “0” | High passband frequency evaluated at -1 dB and expressed in Hz |
| Low Freq Stopband | float | “0” | Low stopband frequency evaluated at -60 dB and expressed in Hz |
| High Freq Stopband | string | “0” | High stopband frequency evaluated at -60 dB and expressed in Hz |
| LNA Gain | float | “0” | Low Noise Amplifier Gain expressed in dB |
| LNA Noise Figure | float | “0” | Noise Figure of LNA expressed in dB |

### Calibration Metadata

Calibration metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Cal. Sig. Freq. | Class A |
| Cal. Sig. Ampl. | Class A |
| Self Calibration flag | Class A |
| Last Cal. Date | Class A |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Cal. Sig. Freq. | float | “0” | Frequency of the internal calibration source expressed in Hz |
| Cal. Sig. Ampl. | float | “0” | Amplitude of the internal calibration source expressed in dB |
| Self Calibration flag | boolean | “0” | This is set to “1” if the sensor performs a periodical self calibration procedure. Otherwise it is set to “0” if the self calibration is performed after a user request |
| Last Cal. Date | string | “0” | The time stamp of the last calibration expressed as HH:MM:SS YYYY/MM/DD |

### SDR Metadata

SDR metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| SDR Manufacturer | Class A |
| SDR Model | Class A |
| Firmware version | Class A |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| SDR Manufacturer | string | “0” | Manufacturer of the sensor used |
| SDR Model | string | “0” | Model of the sensor used |
| Firmware version | string | “0” | Current firmware version |

### SSD Host Metadata

Host metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Manufacturer | Class A |
| Model | Class A |
| Installation Date | Class A |
| OS | Class A |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Manufacturer | string | “0” | Manufacturer of the host |
| Model | string | “0” | Model of the host |
| Installation Date | string | “0” | The date when SSD has been installed expressed as YYYY/MM/DD |
| OS | string | “0” | Operating System installed on the host |

### Environmental Metadata

Environment metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| GPS | Class C |
| Temperature | Class C |
| Humidity | Class C |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| GPS | Array of float | “0” | [Latitude expressed in decimal degrees (-90°-90°)  Longitude expressed in decimal degrees (-180°-180°) |
| Temperature | float | “0” | Environment temperature expressed in K |
| Humidity | float | “0” | Environment relative humidity expressed in percentage |

### SSD Software configuration metadata

#### Acquisition Metadata

Acquisition metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Frequency | Class B |
| Sample Rate | Class B |
| Bandwidth | Class B |
| Timestamp | Class C |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Frequency | float | “1” | Center frequency of the channel where the SSD is currently tuned expressed in MHz |
| Sample Rate | float | “1” | Current sampling rate expressed in MS/s |
| Bandwidth | boolean | “1” | Bandwidth of the channel where the SSD is currently tuned expressed in MHz |
| Timestamp | string | “0” | The time information when the data has been acquired expressed as HH:MM:SS.mmm YYYY/MM/DD |

#### Signal processing Metadata

Signal processing metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Data Typology | Class B |
| Sensing Technique | Class B |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Editable** | **Content** |
| Data Typology | String | “0” | Description of the received data domain. Possibilities are:   * I/Q capture * Frequency transform * Power spectral density |
| Sensing Technique | String | “0” | Sensing processing algorithm used by SDR. Possibilities are:   * Cyclostationarity * Energy Detection * Custom |

#### Scheduling Metadata

Scheduling metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Priority | Class B |
| Timing | Class B |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Priority | String | “0” | Scheduling Scheme used for incoming request.  Possibilities are:   * (FCFS) First Come First Served * (RR) Round Robin * Custom |
| Timing | String | “0” | Types of requests to be managed:   * On demand * Timed with periodicity |

#### Packaging and transmission Metadata

Packaging and transmission metadata is reported in the table below. In the second column of the table the class of the metadata is specified.

|  |  |
| --- | --- |
| **Metadata Name** | **Metadata class** |
| Format | Class C |
| Compression | Class C |

A detailed description of the field of each metadata is reported in the table below

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Type | Editable | Content |
| Format | string | “0” |  |
| Compression | string | “0” |  |



### SSD Task Control metadata

#### Scheduler Specification

|  |  |  |
| --- | --- | --- |
| Algorithm | Value | Notes |
| Unspecified | 0 |  |
| Host Controller | 1 |  |
| Embedded Job Controller | 2 |  |
| Multilevel | 3 |  |

#### SSD Output Specification

|  |  |  |
| --- | --- | --- |
| Algorithm | Value | Notes |
| Unspecified | 0 | Invalid |
| Time domain IQ | 1 | Default |
| Freq. domain IQ | 2 |  |
| Time domain Amp, Phase | 3 |  |
| Freq. domain Amp, Phase | 4 |  |

#### System Definitions and Interfaces

#### (NOTE THAT THIS SECTION BELOW OVERLAPS WITH MATERIAL ABOVE, TO BE RESOLVED)

Definitions of units, measurements for each defined parameter in the standard

The parameters defined in the previous section need a detailed definition. In the following, they will be defined in detail, a priority grid (paradigm MoSCoW adopted) will be provided and canonical measurement units will be given.

According to MoSCoW paradigm, used in software engineering requisite classification, a parameter can belong to the following categories:

M (MUST HAVE): very high priority parameter, it cannot be missed in the data exchange process;

S (SHOULD HAVE): medium priority parameter, it is requested to be present but in rarely cases he could be skipped.

C (COULD HAVE): low priority parameter, it could be useful if present but its absence would not affect negatively the system;

W (WISH LIST): optional parameter, to be used if room: not actually needed.

* 1. System Units and Parameters (NOTE THESE NEED UNITS, SYNC W TABLES)

**Stage 1 parameters:**

**Antenna gain (M):** the ratio of the power received by the antenna and the power received by a hypothetical lossless isotropic antenna.

**Antenna type (M):** according to its shape and radiation pattern, different antenna types can be used for SCOS purposes, if they can provide requested accuracy results.

**Antenna bandwidth (M):** the frequency range over which an antenna can work well.

**Amplifier gain (M):** it is the difference (in dB) or the ratio between the power at the exit stage and that one at the input stage of the amplifier.

**Antenna orientation and polarization (if non omnidirectional antenna is used) (S):** The polarization of an antenna is intended the orientation of the electric field (E-plane) of the radio wave wrt the Earth's surface. It depends of the physical structure of the antenna and its orientation.

**Insertion loss (into amp) (S):** it refers to the attenuation the received field experiences passing through the wire connecting the antenna to the amplifier.

**Return loss (S):** it is defined as the power loss of the signal due to the reflections in correspondence with impedance discontinuity along the transmission line.

Analytically, it is defined as: , where *Pi* is the incident power, *Pr* the reflected power.

**Noise figure (S):** noise level estimation through the analysis of a surely vacant channel.

**Filter parameters (C):** filter defined by typology (LPF, HPF, BPF, RBF) and cut-off frequencies.

**Antenna impedance (C):** the output impedance of the antenna.

**Stage 2 parameters:**

Input parameters:

**Channel to be sensed (M)**: frequency interval to be scanned, it can be provided through starting and stop frequency, or by using a LUT (look-up table), where a correspondence between a unique code and channel features is provided, in order to minimize data exchange communication overhead.

**Max Scan time (S)**: it is the amount of time a SSD must spend in order to acquire the signal and perform sensing. No data packaging time included.

**Resolution bandwidth setting (S):** it is actually defined as the ratio between the frequency interval under analysis and the number of frequency bins of the FFT process. Higher the RBW, higher the probability to detect very narrowband signals, such as wireless microphones.

**Sensing method to be adopted (C):** if more than one sensing method is loaded into SSD, the SSM could send a code corresponding to one of those methods, especially if different performance is ensured by different sensing methods.

Output Metadata:

**SSD hardware ID/key (M):** alphanumeric code indicating the specific SSD, for fixed stations it could be related to the sensor position.

**Scan parameters (S)** (channel, scan time, sensing method, resolution bandwidth): definition corresponds to input parameters but they are provided back to the SSM in order to ack the system that requested parameters have been correctly set and used.

**Temperature/humidity (S)** (in order to evaluate if the SSD hardware is working in normal operating condition): in some atypical conditions (extremely hot or extremely cold) the SSD hardware may provide inaccurate results or they could be corrected by a correcting factor depending on the temperature/humidity pair.

**Battery level (C)** (if the SSD is battery powered): indicated as the percentage wrt the full charge value, under a threshold sensing could be considered not reliable and recharging could be enabled by SSM.

**Sensor location coordinates (M for mobile devices, C for fixed stations):** latitude and longitude or distance from a reference point or node. Values can be provided by a GPS sensor embedded in SSD.

* + 1. Key minimum sensing parameters

In order to be compliant with SCOS framework, every SSDs must show, on testing scenario, performance in terms of two figures of merit:

1. Detection Probability (Pd):
2. False Alarm Probability (Pfa):

Where *Bo,i , Bo,tot , Bf,i* and *Bf,tot* represent the *ith* detected occupied bandwidth inside the actually occupied frequency interval, the total occupied bandwidth, the *ith* detected occupied bandwidth inside the free frequency interval, the total free frequency bandwidth, respectively.

According to SCOS purposes, Pd must be greater than 90% and Pfa less than 10% for every operating conditions, down to the minimum sensitivity level, defined in Section **Error! Reference source not found.**.

* + 1. Standard system units

|  |  |
| --- | --- |
| Parameter | Unit of measurement |
| Antenna gain | dBi |
| Antenna bandwidth | MHz |
| Antenna Impedance | Ω |
| Insertion loss | dB/m |
| Return loss | dB |
| Amplifier gain | dB |
| Scan time | ms |
| Resolution bandwidth | kHz |
| Temperature | K |
| Humidity | %rh |
| Battery level | % |
| Sensor Location coordinates | DD°MM’SS’’ N/S (latitude)  DD°MM’SS’’ W/E (longitude) |

* 1. Metadata Formats

Definition of metadata to be captured at each layer

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Data type** | **Format** |
| Antenna gain | Numerical | integer |
| Antenna type | enumerator | 1. Dipole antenna 2. Half-wave dipole antenna 3. Monopole antenna 4. Etc. |
| Antenna bandwidth | Numerical | Double (two digits after decimal mark) |
| Antenna impedance | Numerical | Integer |
| Antenna orientation | Numerical | Roll |
| Antenna polarization | Enumerator | 1. Horizontal 2. Vertical 3. Circular 4. Elliptical   Etc. |
| Insertion loss | Numerical | Double (two digits after decimal mark) |
| Return loss | Numerical | Double (two digits after decimal mark) |
| Amplifier gain | Numerical | Double (two digits after decimal mark) |
| Filter parameter: |  |  |
| Filter type | Enumerator | 1. LPF 2. HPF 3. BPF 4. Etc |
| Cut-off frequencies | Numerical | Double (two digits after decimal mark) |
| Channel to be sensed | Numerical | Double (two digits after decimal mark) |
| Channel to be sensed | Enumerator | List of channel |
| Max scan time | Numerical | Integer |
| Sensing method to be adopted | Enumerator | 1. Energy detection 2. cyclostationarity 3. matched filter 4. Etc |
| Resolution bandwidth setting | Numerical | Integer |
| SSD hardware ID/key | Alphanumeric |  |
| Battery level | Numerical | integer |
| Temperature | numerical | Double (one digit after decimal mark) |
| Humidity | Numerical | Integer |
| Sensor Location coordinates | alphanumeric | DD°MM’SS’’ N/S (latitude)  DD°MM’SS’’ W/E (longitude) |

# System Policy Model

## SCOS Policy

A policy layer in the SSM at the northbound and southbound API will ensure that the SSM is operated within requirements of a local authority (national regulator, law enforcement, military, etc).

The policy on the southbound interface will determine, based on the USER type, (e.g. how a central authority can define what kinds of sensing can be done in what bands, what data governance rules there are, etc

-- resource allocation – what kinds of users are authorized to request resources from the sensor network and in which priority (i.e. if a sensing network is resource constrained, who gets first dibs on the sensors)

Policy on the northbound interface (SSM>DBstore) will have rules for how sensing data may be distibuted, and data storage policies. This would include which scan data takes priority if local storage in the store & forward buffer is running out due to a failed transmission link, and how long certain USER data is allowed to be stored in the local store & forward buffer.

Based on SCOS platform architecture, the SCOS policy is categorized based into following categories:

* Spectrum Sensing Manager (SSM) Policy
* Spectrum Sensing Device (SSD) Policy
* Sensing Data Manager (SDM) Policy \*\*SDM=Data-Put-manager
* SCOS Platform Administration (SPA) Policy \*\*Names/Acronyms temporary
* SCOS Platform User (SPU) Policy \*\*Names/Acronyms temporary

The SCOS policy is expressed using JSON. Following subsection provides details about the schema of SCOS policy.

### The SCOS policy schema:

Each SCOS policy is associated with a policy-name, policy-namespace, policy-category, policy-scope, optional policy-description, and one or more statement(s).

Following figure shows the structure of a SCOS policy.

**SCOS Policy**

Top-level attributes

Statement

Statement

**Statement**

StatementId

Policy-Action

Actor

Resource

SCOS-Task

Condition-Block

Figure XXX. High-level structure of the SCOS Policy

Example:

{

# "Version": "2017-02-15",

"Policy": {

"namespace": "OperatorFoo",

"name": "Calibration-access-control",

"description": "This policy added by FooAdmin On this date."

"Policy-type": "SPA-Policy",

"Policy-Action": "permit",

"Resource": "Foo:Sensors::\*"

"SCOS-Task": "Calibration-operation"

"Scope": "Sensor-management:"

"Condition": {

"equals" : {

"Actor" : "FooAdminRole"

}

}

}

The default namespace is global. Specific-Namespaces could be used to restrict the application of policy within a certain context. Namespaces avoids name collisions and enables to identify actors or resources uniquely (when the names have been reused across namespaces).

**SCOS Policy Statement**

Each statement specifies certain action. Different categories of SCOS-Policies are associated with different actions.

A statement may also have optional attributes that identify the context of applying the policy. These attributes allow specifying a fine-grained policy. Example context-attributes are Actor, Resource, SCOS-Task, time, frequency, and location.

A statement has an optional condition-block. The action is performed only when the condition(s) are matched.

**Tasking Agent**

A Tasking Agent is an entity that wishes to use the SCOS platform. A Taskin Agent could be specified in terms of role, user, or a user-group.

**User**

An user is an individual Tasking Agent with specified name and access-credentials.

**User-group**

A user-group is a logical collection of users. A user-group is specified with name and access-credentials.

**Role**

A role is specified with a name. The role could be associated with specific SCOS services/functionality. A role could also be associated with privilege of various users of SCOS platform.

An user (or a user-group) is associated a role.

**Resource**

SSD and Sensing data are two prime resources within SCOS platform.

**Resource-group**

Multiple SSDs could be grouped together to jointly specify policies for using the SSDs. SSDs could possibly be grouped based on various attributes such as location, SSD-hardware-type, SSD-software-type.

**Namespace**

Actors or resources are associated with a namespace. This avoids name collisions and enables to identify actors or resources uniquely (when the names have been reused across namespaces).

**SCOS-Task**

An SCOS-task represents a specific sensing-task within SCOS platform issued by a particular Actor on particular resources. Additionally, a policy may specify pre-defined SCOS operations in the SCOS-Task. These predefined SCOS-Tasks include: Scanning, Calibration, Storage, and Transmission.

**Task-group**

Multiple tasks could be grouped together for convenience in specifying policies. For example, various tasks that can be performed towards sensor-management for a particular SSD operator could be grouped together and referred to in the SCOS policy. Similarly, sensing data management related tasks could be grouped together for precisely and conveniently specifying sensing-data-management related policies.

**Conditions**

A condition is specified with a triplet of field(key), conditional-operator, and value. Condition is optional within a statement.

A condition evaluates whether a field meets certain criteria. Following table identifies various conditional operators.

|  |  |
| --- | --- |
| **Conditional-operator Name** | **Syntax** |
| equals | "equals" : "<value>" |
| Like | "like" : "<value>" |
| Contains | "contains" : "<value>" |
| In | "in" : [ "<value1>","<value2>" ] |
| Exists | "exists" : "<bool>" |
| LessThan | "lessthan" : "<value>" |
| GreaterThan | "greaterthan" : "<value>" |
| LessThanEquals | "lessthanequals" : "<value>" |
| GreaterThanEquals | "greaterthanequals" : "<value>" |

**Logical Operators**

Logical operators enable to manipulate or combine multiple conditions. Following table specifies the logical operators.

|  |  |
| --- | --- |
| **Logical operator** | **Syntax** |
| Not | “not”: {<condition>} |
| AllOf | "allOf" : [ {<condition>},{<condition>}] |
| AnyOf | "anyOf" : [ {<condition>},{<condition>}] |

**Aliases**

Aliases add convenience. Using aliases, multiple users can be combined together or multiple resources can be combined together to be referred in the SCOS policy . Furthermore, multiple tasks can be combined using task-groups.

Furthermore, locations could be specified using aliases to capture latitude, longitude, and altitude. A group of frequencies could also be combined using aliases. A group of time-slots also could be combined using aliases.

#### SSM Policy Schema

Each SSM policy has following required fields: PolicyName, PolicyScope, PolicyType, and PolicyAction.

Optional fields include: Policy-Description, condition-block, Actor, Resource, and SCOS-Task.

With Policy-Action ‘set’, SSM attribute and value(s) could be specified.

#### SSD Policy Schema

Each SSD policy has following required fields: PolicyName, PolicyScope, PolicyType, PolicyAction, and Resource.

Optional fields include: Policy-Description, condition-block, Actor and SCOS-Task.

Policy-Actions: Set, Permit, Deny, Calibrate, Scan,

With Policy-Action ‘set’, SSD attribute and value(s) could be specified.

#### SDM Policy Schema

Each SDM policy has following required fields: PolicyName, PolicyScope, PolicyType, and PolicyAction, and SCOS-Task.

Optional fields include: Policy-Description, condition-block, Actor and Resource.

Policy-Actions: Set, Permit, Deny, Transmit-Sensing-Data, Store-Sensing-data, Discard-Sensing-data

With Policy-Action ‘set’, SDM attribute and value(s) could be specified.

#### SPU Policy Schema

Each SPU policy has following required fields: PolicyName, PolicyScope, PolicyType, PolicyAction, and Actor.

Optional fields include: Policy-Description, condition-block, SCOS-Task, and Resource.

Policy-Actions: Set, Permit, Deny

With Policy-Action ‘set’, SPU attribute and value(s) could be specified.

#### SPA Policy Schema

Each SPA policy has following required fields: PolicyName, PolicyScope, PolicyType, and PolicyAction.

Optional fields include: Policy-Description, condition-block, SCOS-Task, Actor, and Resource.

Policy-Actions: Set, Permit, Deny,

With Policy-Action ‘set’, SPA attribute and value(s) could be specified.

Policy file: It is envisioned in the first version of this standard that the SSM stores a policy file which is installed manually by Sensing Operator (through mechanism such as SSH and update pull, or remote SCP).

### Policy Evaluation

Whenever an SCOS API needs to be executed, SSM needs to confirm if the action is permitted by evaluating related policies.

There exist three scopes for SCOS policies: Sensing management scope, Sensing-data management scope, and Sensor-management scope. Depending on the API, policies in the appropriate scope are looked up.

The second step is ensure that the actor is authorized to perform tasks on the resource. A specific accept policy or default-accept policy should be match for the user, user-group, or role.

The final step is ensure if the resource permits the intended task. A specific accept policy or default-accept policy should be match for the resource, or resource-group.

### Security Considerations

<Nilesh input>

### SCOS Policy Examples

#### SSD Policy

Set sensitivity to -114 dBm task frequency UHFBand

PolicyID: <generated>

PolicyName: SCOSMinSensitivityRule

Policy-Category: SSD-Policy

PolicyDescription: It applies to all SSDs within the SCOS operational region.

Policy-Action: Set

Sensitivity: Value

Frequency: value

Discuss: Should frequency be within the context-block or condition-block?

#### SSM Policy

Set scheduling minimum slot duration

PolicyID: <generated>

PolicyName: SSMMinSensingSlotDuration

Policy-Category: SSM-Policy

PolicyDescription: It specifies the minimum slot duration for sensing task. The value is in seconds.

Policy-Action: Set

Min-sensing-slot-duration: Value (seconds)

Note: Fine-grained policy could be specified for a particular resource (SSDs) or sensing-tasks.

Set sensing behavior for prioritized scan

PolicyID: <generated>

PolicyName: SSM-Prioritized-Scan-Behavior

Policy-Category: SSM-Policy

PolicyDescription: It specifies whether existing scan should be suspended if a prioritized scan-request is received.

Policy-Action: Set

Prioritized-scan-enabled: true

Condition-block: if wait-time greaterthan value (in seconds)

Note: Condition-block is optional. Condition-block can be used to specify a condition when existing scans can be suspended.

#### SDM Policy

Set max-data-storage-duration at SDM

PolicyID: <generated>

PolicyName: SDMMaxStorageConfig

Policy-Category: SDM-Policy

PolicyDescription: It specifies how long SDM can hold the sensing data.

Policy-Action: Set

Max-data-storage-duration: Value (seconds)

Note: Optionally specify task or SSDs or SDS. The value is in seconds.

Discard sensing-data for <scan-task-L-band-User-Jim> if sensing-data is unqualified.

PolicyID: <generated>

PolicyName: User-Jim-L-Band-Discard-Data-Policy

PolicyDescription: If sensing data does not meet the criteria specified in the sensing task, discard the data.

Policy-Category: SDM-Policy

Policy-Action: discard-data

SCOS-Task: scan-task-L-band-User-Jim

Condition-block: sensing-data-quality is ‘unqualified’.

Note: The condition-block identifies when the operation is performed. Here, sensing-data has attribute sensing-data-quality. The condition is satisfied when the attribute’s value is unqualified. The sensing-task is identified pre-defined using name-alias. Optionally, the policy could be made more specific for certain time, and location attributes.

#### SPA Policy

Enable SSM-Proxy device usage in SCOS system.

PolicyID: <generated>

PolicyName: Enable-SSD-Proxy-Config

Policy-Category: SPA-Policy

PolicyDescription: Enable SSM-Proxy devices in the SCOS platform.

Policy-Action: Set

SSM-Proxy-Enabled: Boolean-Value

Note: Optionally, the policy could be made more specific for certain frequency, time, and location attributes.

#### SPU Policy

Deny scan operation for User-Foo in the military bands

PolicyID: <generated>

PolicyName: MilitaryBandScanRestrictionPolicy

Policy-Category: SPU-Policy

PolicyDescription: Deny certain users/roles/groups to scan in certain bands.

SCOS-Task: scan

Actor: User-Foo

Policy-Action: Deny

frequency: X-band

Note: The actors could be specified with user/role/user-group. The frequency bands could be pre-defined using name-aliases. Optionally, the policy could be made more specific for certain time, and location attributes.

#### SDS Policy

Send sensing-data for <scan-task-L-band-User-Jim> to data-store <FooStore3>

PolicyID: <generated>

PolicyName: User-Jim-L-Band-DataStorePolicy

Policy-Category: SDS-Policy

PolicyDescription: Configure data store for a scan request.

Policy-Action: Transmit-sensing-data

SCOS-Task: scan-task-L-band-User-Jim

Resource: FooStore3

*Note: The data-store is specified with resource on which operation is done. The sensing-task is identified pre-defined using name-alias. Optionally, the policy could be made more specific for certain time, and location attributes.*

# Informative: Latency Requirements for Scans

The latency requirement for performing a sensing task and transmitting metadata from SSD to SDM is a critical metric for certain use cases.

The maximum allowed latency depends on signal type and frequencies that need to be scanned, and are determined by the application. As such, a number of reference applications are given, with recommended latencies. In each case, to meet the specified latency, the SCOS system design and particular implementation would need to be capable.

Maximum Latency would be the sum of:

* Task Request Latency: Time from scan request to scan start
* Scan Time Latency: Time from scan start to scan complete
* Spectrum Characterisation Latency: Time from scan complete to algorithmic processing
* Sensing Data Delivery Latency: Time from processing to delivery to Data Receive Point

|  |  |  |
| --- | --- | --- |
| **Reference Application** | **Band Swept** | **Maximum Latency** |
| TVWS Base Station Device | 460-760MHz |  |
| CBRS Base Station Device | 3.5GHz-3.8GHz |  |
| TVWS CPE Device | 460-760MHz |  |
| CBRS CPE Device | 3.5GHz-3.8GHz |  |
| Etc | 460-760MHz |  |
|  |  |  |

# Informative: Regulatory Technical requirements

Various countries will have differing requirements here, but a few countries already have definitions in place that should be observed. For example, in the FCC rules for the VHF/UHF TV bands, the FCC requires a spectrum sensing detection accuracy as specified by the Table 1: FCC Sensing sensitivity requirements.

Table 1: FCC Sensing sensitivity requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Regulatory domain** | **Type of signal** | **Sensing detection threshold**  **(in dBm)** | **Data fusion rule for distributed sensinga** | **Monitoring requirements** |
| USA | ATSC | –114  (averaged over 6 MHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |
| USA | NTSC | –114  (averaged over 100 kHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |
| USA | Wireless microphone | –107  (averaged over 200 kHz) | “OR” rule | Detection threshold referenced to an omni-directional receive antenna with a gain of 0 dBi |

aThe value “1” indicates detection.

Other requirements for the 2.7 GHz to 3.7 GHz band shall be defined based on the evolving regulations. For example, the spectrum sensing devices in the 2.7 GHz to 3.7 GHz can sense for Radar Signals and provide that information to the Spectrum Access System (SAS) that is being defined in these bands.

# Device and System Security Recommendations

\* Remote access to SSD hardware through remote secure shell (SSH) and similar technologies must not use the same keys as SSM/SSD interface keys

\* Devices’ physical characteristics must be evaluated and enumerated at build validation and testing, with hardware and configuration parameters written to file /DEVICEHARDWAREPARAMETERS.CONFIGFILE (placeholder) and stored in non-writable file

\* Any changes to hardware configuration (e.g. change of antenna) must be recorded in DEVICEHARDWARECONFIGCHANGES.LOGILE and changes made to relevant parameters in D..H...P...CONFIGFILE, either through manual editing of config file or through a secure remote update mechanism (e.g. scripted SCP file revision).

# Implementation Guidelines/Notes

<Currently this section contains miscellaneous notes>

Tasking API, Mission API and Data Request API: The Mission API would be the equivalent of the SCOS API (i.e. where the Tasking Agent requests a scan schedule); the Task API would be the SSD API (i.e. the SSM sending an schedule update to a specific SSD). The Data Request API would not be included in the current design, as the retrieval of scan data would be between the Tasking Agent and the Data Receive Point, which is implementation dependent.

## Management Reference Architecture

### Spectrum Sensing Platform – Sensing Service Control

#### Spectrum sensing API

The spectrum sensing platform provides spectrum sensing as a service using Spectrum sensing API. This is the northbound interface from the block diagram.

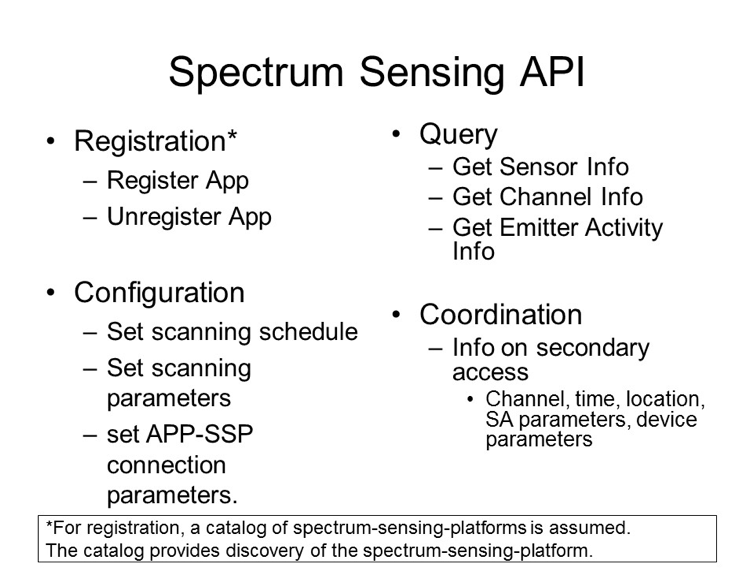
We identify following four types of API

1. Registration (ID, key exchange, authorisation)
2. Query (sensor model, signal processing capability (occupancy, characterisation, calibration, df), health, availability, location)
3. Configuration (sensing config, scheduling config, calibration, [operational])
4. Notification of Change (reverse Query)
5. Notification of Busy (TBC?)

With the Registration API, an SSA can enable/disable usage of the API. Configuration API enables an SSA to configure the SSP for desired purpose. Using Query API, an SSA can request real-time data or past data. (*Inference regarding secondary spectrum-access is purposefully excluded from the SSP API. For example, Is it safe to transmit? This spectrum-access inference logic is considered to be in the apps that are using the spectrum-sensing platform*.)

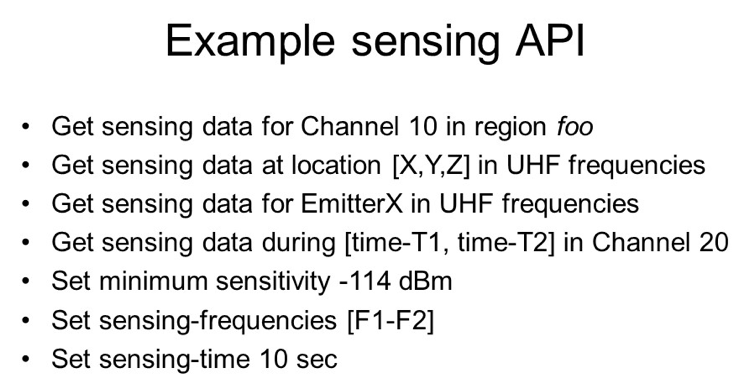
The coordination API is optional. It can be used in circumstances wherein the Apps wants to provide information about secondary spectrum-access. For example, an SSA may use the real-time sensing data and infer feasibility of secondary spectrum-access. This SSA would grant spectrum-access parameters to secondary user radios and use the coordination API to notify the secondary spectrum access to SSP.

Following diagram captures the high-level summary of the SSP API.



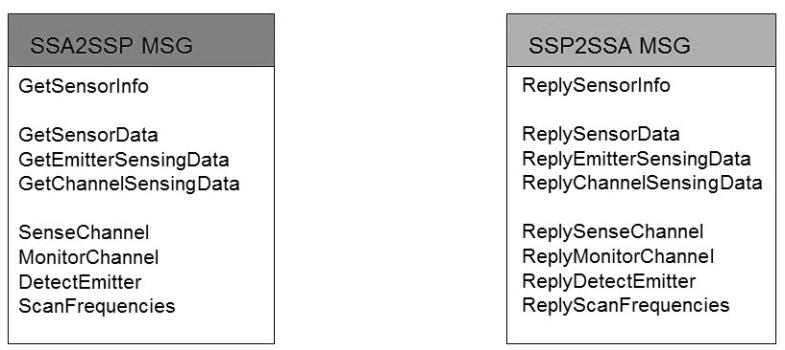
#### Example spectrum sensing API design

The spectrum sensing requirements vary significantly in terms of geographies (different countries have different regulations) and they have been evolving over time. The requirements also vary depending on frequency-bands. Thus, there is a need for configurability and extensibility for SSP API. In this regard, policy-based interface is very much appealing. Furthermore, we may consider developing semantics for sensing-data and ontology-driven sensing policy (OWL). Following diagram shows some examples of possible SSP API.

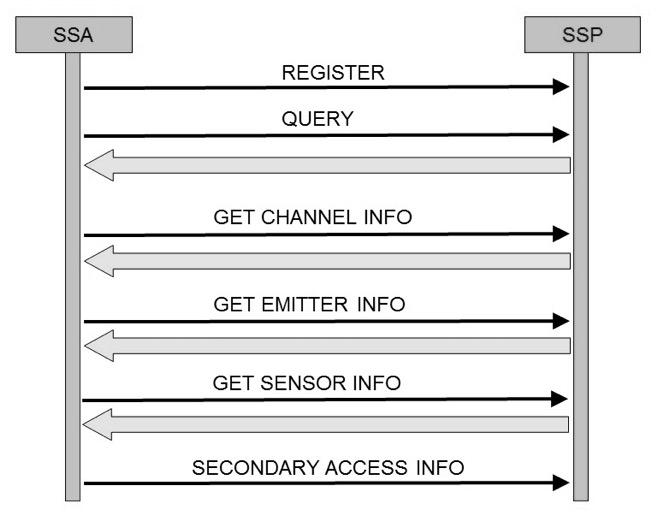


#### Message Exchange

SSA API requests and SSP API response are encapsulated in messages. Each message has a message-ID, message-Type, and the message body. Following diagram identifies various message types.



Following sequence diagram illustrates message exchange between SSA and SSP.



### Spectrum Sensing Control

The spectrum sensing platform provides spectrum sensing service by controlling the spectrum sensing devices (SSD) with southbound interface. There are following 3 types of API

1. Registration: Allows to add/remove an SSD to SSP
2. Control: Controlling the sensing function and schedule of an SSD
3. Query: Requesting sensing data from an SSD

#### Sensing Functions

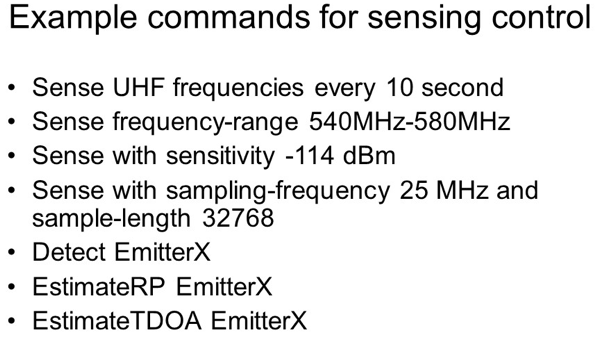
There exist multiple sensing techniques/algorithms from energy detection to exploiting cyclostationarity and signal statistics. Some sensors may be able to report occupancy in terms of aggregate RF-power received at the sensor location while higher end sensors may be able to estimate location and received power (RP) in the presence of cochannel interface and noise.

#### Sensing Schedule

The SSP may need to scan a wide range of frequencies at a specific periodicity. Thus, SSP may in tur define a sensing schedule for each of SSDs. The schedule may be adapted in response to certain events or policies from the SSAs.

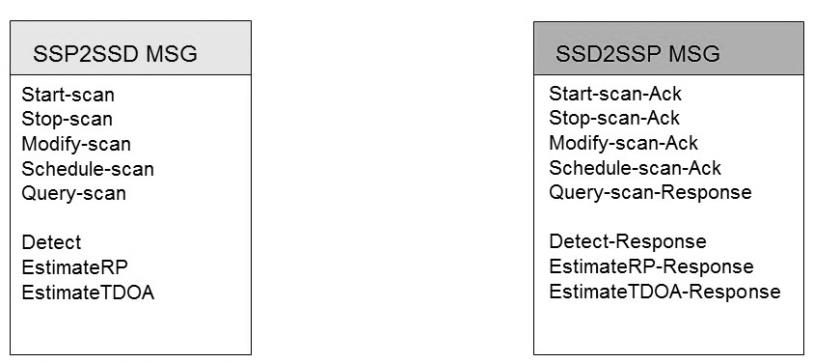
Examples

Following are a few examples of the interface between the SSP and SSD.

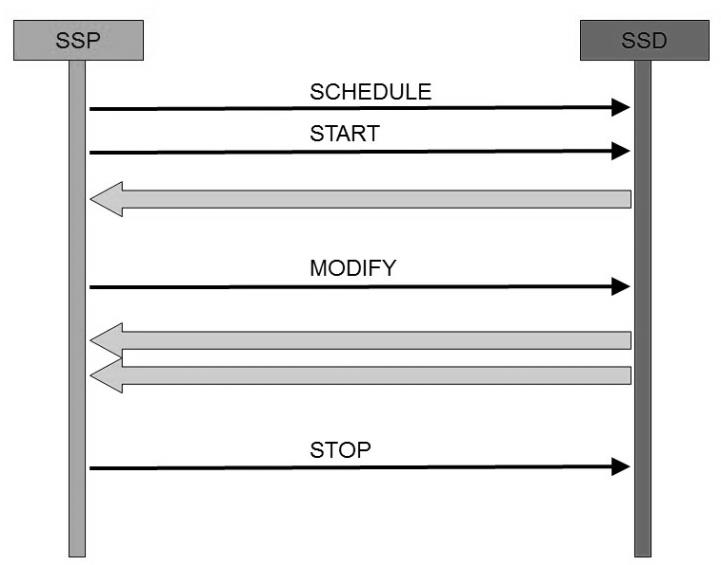


#### Message Exchange

The message from SSP to SSD is formatted in the similar way (has message-ID, message-type, and actual message). Following diagram shows some of the message types.

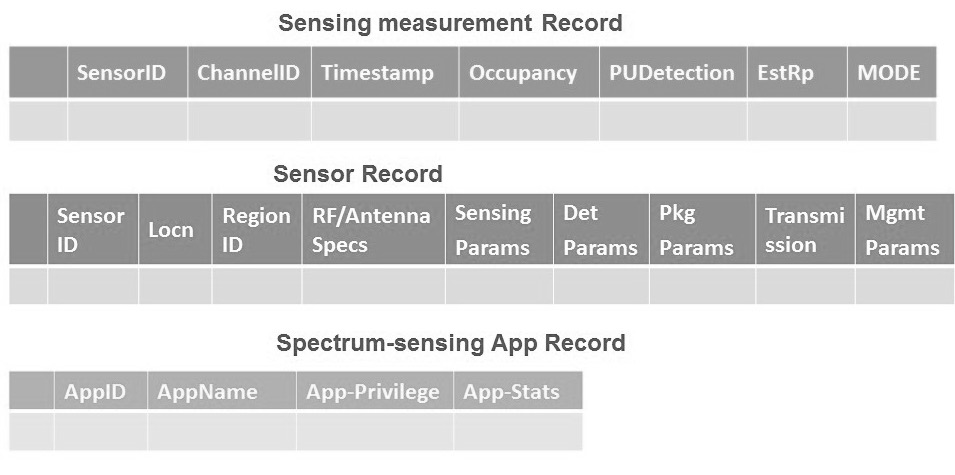


Following sequence diagram illustrates the message exchange between SSP and SSD.



#### Data Receive Point

SSP collects and stores the sensing data to provide the services defined under the SSP APi. One of the popular approaches is to use relational database. Following diagram illustrates records for (a) sensing measurement, (b) SSD (c) SSA.



Alternate approach could be to develop spectrum sensing semantics based data-store.

#### Management and Maintenance

The back-end management system exchanges control information with SSDs

Manage them

* Device health reports – power, temperature, location, GPS health, OS/environment health, network health, storage health, scheduled and by query
* Manage by device, group, Class of device

Validate their operation

* Run test scans against known data points (e.g. from WSDB)

Verify integrity of information chain

* Software tools to validate process chain

Perform maintenance

* Push updates to devices (software, OS, firmware, certifications)
* Perform remote reboots, resets
* Shell into device to do diagnostics

# (normative) IEEE 802.22 regulatory domains and regulatory classes requirements

This annex describes the various technical parameters and specifications required by the various regulatory domains for operation of the IEEE Std 802.22 in the TV bands.

## Regulatory domains, regulatory classes, and professional installation

Table F.1 specifies the regulatory domains and licensing regime where the IEEE 802.22 systems are planned to be authorized to operate in the TV bands.

Table F.1—Regulatory domains

|  |  |  |  |
| --- | --- | --- | --- |
| **Geographic**  **area** | **Regulatory domain ISO 3166 (3 Bytes)** | **Licensing regime** | **Approval**  **authority** |
| United States | USA | Unlicensed | FCC |
| Canada | CAN | Licensed | IC |
| United Kingdom | GBR | — | OFCOM |
| — | — | — | — |

1921HTable F.2 specifies the authorized regulatory classes under their respective regulatory domains.

Table F.2—Regulatory classes

|  |  |  |
| --- | --- | --- |
| **Regulatory domain** | **Regulatory class and profile** | |
| **Fixed** | **Personal portable** |
| USA | Stationary fixed | Mode I & IIa |
| CAN | Stationary fixed | N/A |
| — | — | — |

aThe behavioral limits sets for Modes I and II are defined in the FCC Report and Order. However, IEEE Std 802.22 will only operate in portable nomadic Mode II.

Table F.3 specifies the requirement for professional installation of the WRAN BS and CPEs.

Table F.3—Professional installation requirement

|  |  |  |  |
| --- | --- | --- | --- |
| **Regulatory domain** | **Type of terminal** | | **Definition of professional installer** |
| **BS** | **CPE** |
| USA | Professionally installed | Professionally installed | A professional installer is a competent individual or team of individuals with experience in installing radio communications equipment and who normally provides service on a fee basis—such an individual or team can generally be expected to be capable of ascertaining the geographic coordinates of a site and entering them into the device for communication to a database. |
| CAN | Professionally installed | N/A | Same as for USA. |
| — | — | — | — |

## Radio performance requirements

### Sensitivity and Noise

# (informative) Sensing

This annex contains descriptions of a number of sensing techniques. A sensing technique is an implementation of the spectrum sensing function.

## References

# (informative) Bibliography

At the time of publication, the editions indicated were valid. All standards and specifications are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the references listed below.

1. The Institute of Electrical and Electronics Engineers, Inc.

   3 Park Avenue, New York, NY 10016-5997, USA

   Copyright © 2011 by the Institute of Electrical and Electronics Engineers, Inc.

   All rights reserved. Published 1 July 2011. Printed in the United States of America.

   IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics   
   Engineers, Incorporated.

   **PDF: ISBN 978-0-7381-6723-7 STD97146**

   **Print: ISBN 978-0-7381-6724-4 STDPD97146**

   *IEEE prohibits discrimination, harassment and bullying. For more information, visit* [*http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html*](http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html)*.*

   *No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*  [↑](#footnote-ref-1)