 Input paper: [[1]](#footnote-1) ENAV15-14.2.31

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**□** ARM **□** ENG **□** PAP **X** Input

**X** ENAV **□** VTS **□** Information

Agenda item [[2]](#footnote-2) 10

Technical Domain / Task Number 2 Shore side communications

Author(s) / Submitter(s)… Fred W. Pot, Marine Management Consulting

Proposal for a Standard for

Interfaces among Shore-side Systems

# Summary

The ENAV Committee is invited to consider Universal Plug-n-Play (IEC 29341-x) as a readily available and well proven standard for the interface between shore-based devices, systems and services. This paper describes how UPnP fits in the Common Shore-side System Architecture (CSSA), the requirements for the interface and how UPnP fulfils these requirements, what UPnP is, how it works and what vendors would need to do to make their products compatible.

## Purpose of the document

The purpose of this document is to present to the ENAV Committee how UPnP could be implemented as a practical standard for machine-to-machine (M2M) interfaces between the devices, systems and services that, together, form a shore-based system.

The Committee is invited to consider adoption of UPnP as the IALA Guideline for such interfaces.

## Related documents

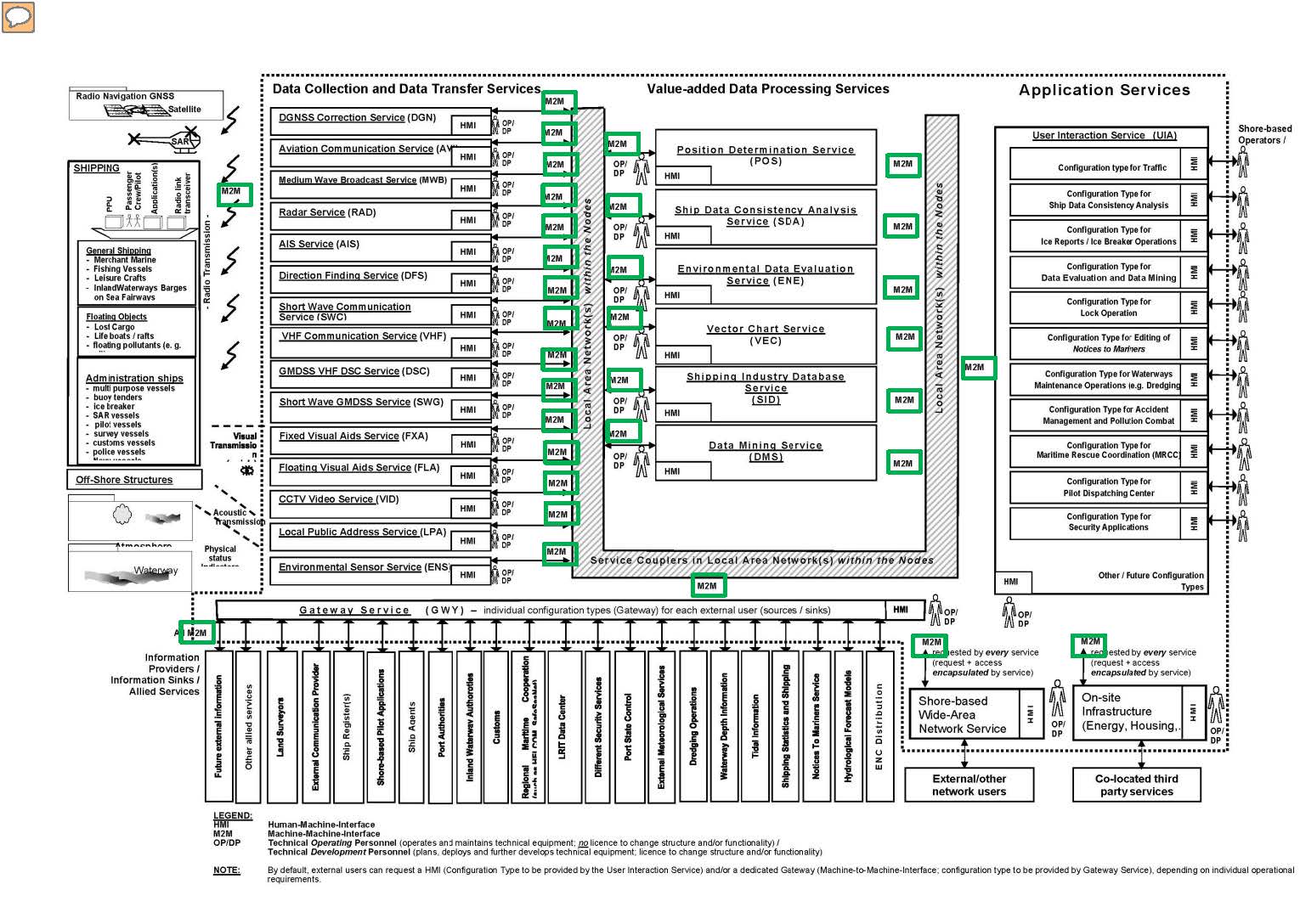
Documents related to this input paper are:

### CSSA1-2.2 Main Draft IALA Recommendation on Generic Service Engineering Model V0-07 20140813

### Appendix05 Interfacing Model Rec Generic Service Eng Model V0 06 20140812

# Background

The Generic Service Engineering Model is depicted below.



It shows a large number of machine-to-machine (M2M) connections. I counted 33 M2M connections in the layout and that assumes there only is one that connects all user interface services with all other services.

Each machine-to-machine connection is between a specific application service and another service or between a specific value added service and another service. As you can see, the number of unique M2M connections is very high and inter-vendor operability is required, meaning that services provided by one vendor will need to be integrated with the services of other vendors.

To me this looks like chaos. To solve this problem we need a standard for M2M communications. The standard we choose should comply with the overall CSS requirements.

# Discussion

## Requirements

IALA’s e-Navigation Committee identified categories of requirements for the CSS and its components. Not all of these apply to the requirements of M2M communications. The ones that do are listed here.

|  |  |
| --- | --- |
| * Scalability | * Security |
| * Interoperability | * Integrity |
| * Flexibility | * Survivability/robustness |
| * Modularity | * Seamlessness |
| * Latency | * Extensibility |
| * Maintainability |  |

## Origin of UPnP

The need to interface devices, systems and services from different vendors is not a new problem. It has been around for a while. Major electronics companies have had to address inter-vendor operability of their products.

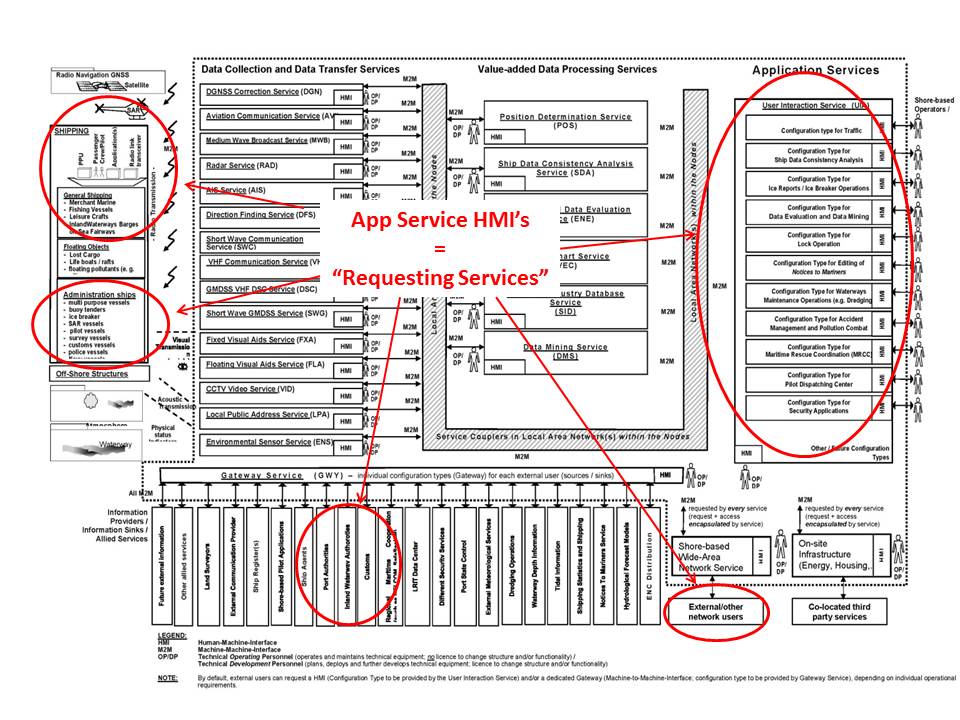
Among them are Intel, Cisco, Samsung, LG Electronics, Alcatel-Lucent, Nokia, Microsoft, HP, Sony, HTC, RIM, Motorola, QualComm, NEC, Toshiba, Sharp, Pioneer, Philips, Mitsubishi, Seagate, Lenovo, Hitachi, Fijutsu and many others.

In 1999 a number of them formed the UPnP Forum ([www.UPnP.org](http://www.UPnP.org)). Its membership has grown to 1018 companies from all over the world.

Their requirements for an inter-vendor operability standard are completely congruent with the ones that IALA identified.

## How does UPnP Work?

To understand how UPnP works I need to make a distinction between application services and other services. User use application services (circled in red below) to interact with the other services. These application services are the “Requesting Services” that interact with other “Services”. In the parlance of Universal Plug-n-Play these are called “Control Points”.

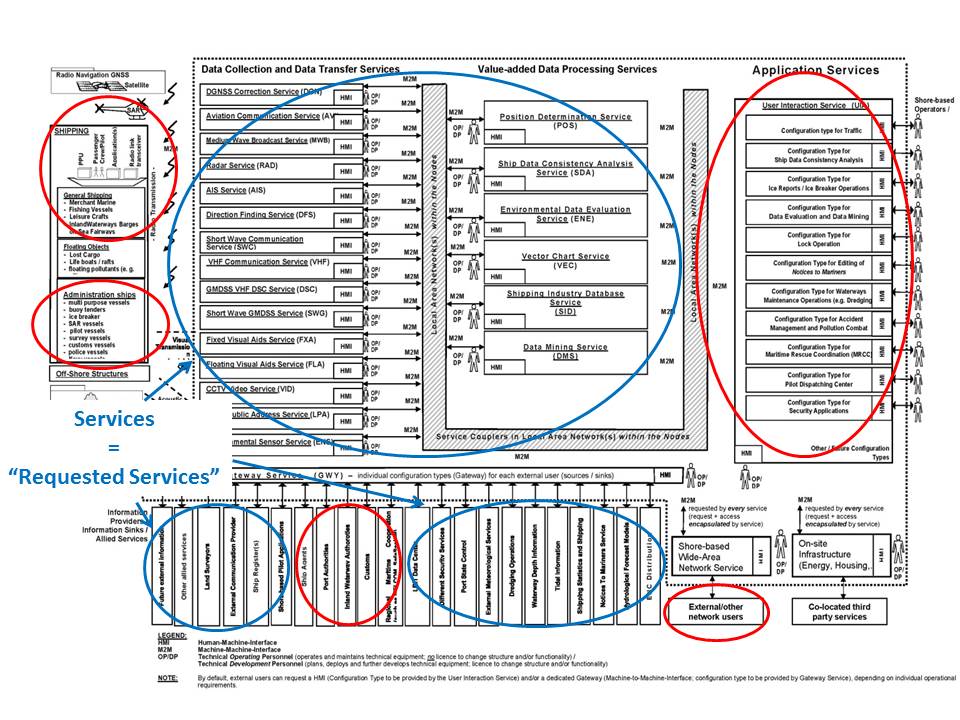


Requesting Services interact with other services (“Requested Services”):

* Data Collection and Data Transfer Services
* Value Added Data Processing Services
* Gateway Services

These Requested Services are highlighted in blue below.

In UPnP parlance these are called “Devices”. Actually Devices should be interpreted to stand for more than just physical devices. They include devices, systems, services as well as actuators.



So how does the UPnP interface work?

It starts with connecting a service (or a system or a device) to the network. The service then gets an IP address from the network router Dynamic Host Configuration Protocol or DHCP host.

**Universal Plug-n-Play Phases**

**in connecting a “Requesting Service” with a “Requested Service”**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  | **7. Subscribe to Service** | **8. Stream Service data** | **9. Change Service**  **configuration\*** | **10. Update Service software\*** |
|  |  |  |  |  |  | **6. Allocate bandwidth to the Requested Service’s data stream (**[**QoS**](http://upnp.org/specs/qos/UPnP-qos-Architecture-v3.pdf)**)** | | | | |
|  |  |  |  |  | **5. Learn about the details of the Requested Service from its** [**S-100 XML**](http://www.iho.int/iho_pubs/standard/S-100/S-100_Info.htm) **description file** | | | | | |
|  |  |  |  | **4. Encrypt inter-service communications using** [**TLS**](http://en.wikipedia.org/wiki/Transport_Layer_Security) **(optional)** | | | | | | |
|  |  |  | **3. Assign a role to the Requesting Service as specified in the** [**ACL**](http://en.wikipedia.org/wiki/Access_control_list) **of the Requested Service** | | | | | | | |
|  |  | **2. Authenticate Requesting** [**Service’s Security Certificate**](http://en.wikipedia.org/wiki/X.509) **using the** [**ACL**](http://www.google.com/url?q=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FAccess_control_list&amp;sa=D&amp;sntz=1&amp;usg=AFQjCNHtQLO_JPHAvD1tdtHcwLGCEMr4CQ) **of the Requested Service** | | | | | | | | |
|  | **1. Advertise / Discover Service using** [**UDP**](http://en.wikipedia.org/wiki/User_Datagram_Protocol) **and** [**SSDP**](http://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol) | | | | | | | | | |
| **0. Obtain an IP Address for the Service using** [**DHCP**](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) | | | | | | | | | | |

\* If the Requesting Service’s Role permits it to change a Service’s configuration and/or update its software

Then the service, using UDP, starts to advertise itself on the network using the Simple Service Discovery Protocol or SSDP. SSDP doesn’t provide a lot of detail about the service but just enough for Requesting Services to determine whether it is relevant for them.

If a Requesting Service wants to connect to the service (i.e. to subscribe to the device), then it first authenticates itself to the service using its security certificate. If the Requested Service has the Requesting Service in its Access Control List then it (optionally) established a secure Transport Level Security connection with the Requesting Service and assigns a role to the Requesting Service that depends on the level of trust. Typical roles are “Public”, “Basic” and “Admin”.

Next the Requesting Service finds out the details of the service. It reads an (S-100) XML file that provides general information, details about how it can be controlled and details about the information the service either generates or expects to receive.

Then the Requesting Service sets up a subscription to the provided. In UPnP parlance services are rendered by “Eventing”. An event is a change in the value of one of the variables that the service provides. Variables may be IEC 61162-1 (NMEA) sentences or proprietary variables that are described in the S-100 XML file.

Next, if the Requesting Service has a role that allows it to control the service, then it issues Simple Object Access Protocol (SOAP) commands to control it.

## Implementation Requirements

UPnP requires vendors to run UPnP protocols on their devices, systems or services. These protocols are independent of the programming language or the operating system that the device uses.

The UPnP Forum publishes and maintains several publicly available protocols. I have listed the most important ones below:

* [Basic Device Control](http://upnp.org/specs/basic/UPnP-basic-Basic-v1-Device.pdf)
* [Sensor Control](http://upnp.org/specs/smgt/UPnP-smgt-SensorManagement-v1-Device.pdf)
* [Protection for individual devices, systems and services](http://upnp.org/specs/gw/UPnP-gw-DeviceProtection-v1-Service.pdf)
* Remote maintenance
  + [Configuration Management](http://upnp.org/specs/dm/UPnP-dm-ConfigurationManagement-v2-Service.pdf)
  + [Software Management](http://upnp.org/specs/dm/UPnP-dm-SoftwareManagement-v2-Service.pdf)
* [Controlled allocation of available bandwidth to data item streams (aka Quality of Service or QoS)](http://upnp.org/specs/qos/UPnP-qos-Architecture-v3.pdf)

The protocols that the UPnP Forum publishes and maintains can be used on a Local Area Network (LAN) and on a Wide Area Network (WAN). On a LAN the Hypertext Transfer Protocol (HTTP) must be used to support the operation of UPnP Protocols. On a WAN the Extensible Messaging and Presence Protocol (XMPP) must be used to support the operation of UPnP protocols.

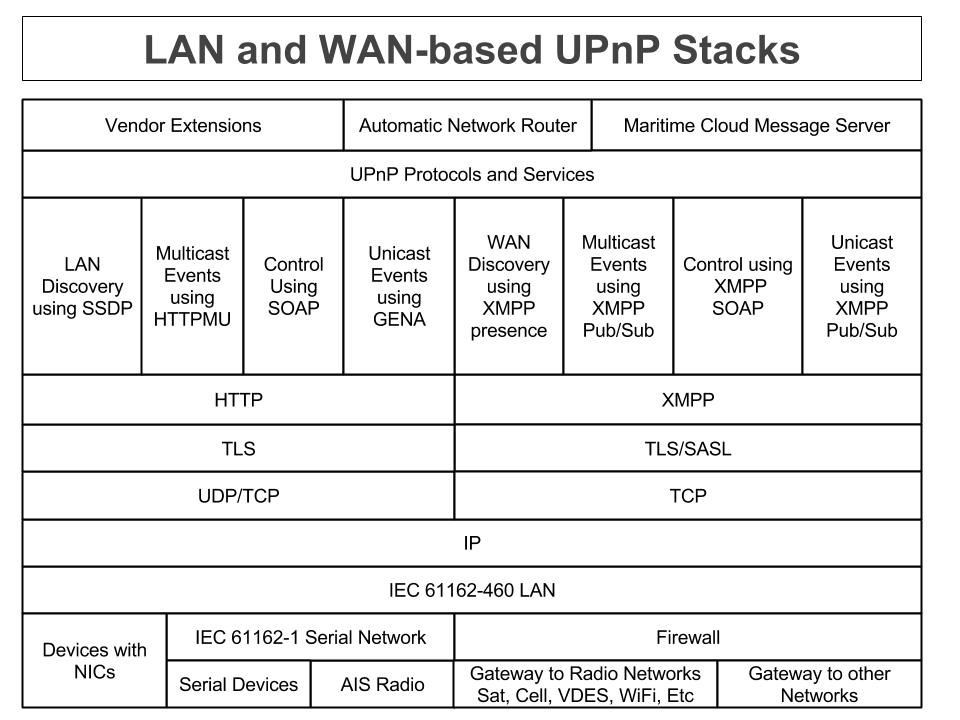
The UPnP Protocols are congruent with evolving standards for the Maritime Cloud Messaging System, the S-100 XML encoding system and the standard for a secure LAN (IEC 61162-460).

Certification of compliance with UPnP protocols is inexpensive and quick. The UPnP Forum makes self-certification software available and it takes the Forum typically less than a week to certify test software results.

Membership to the UPnP Forum is required to get access to the test software but only costs US$5000 per vendor per year, irrespective of the number of devices that are certified.

Most UPnP Protocols are recognized by IEC, specifically the IEC 29341-x series of standards.

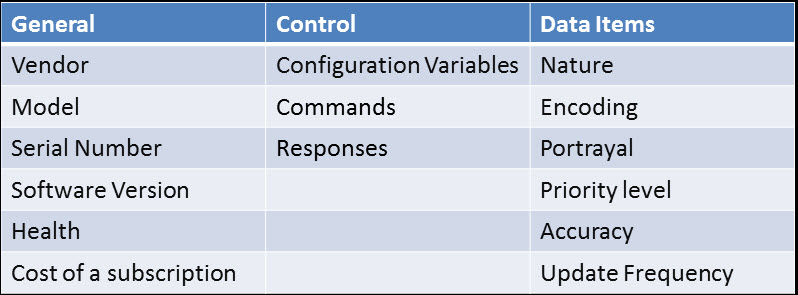
UPnP Protocols are future proof because they are independent of the operating system and the programming language. The UPnP Protocols also are being extended to support the evolving standards for the “Internet of Things” or IoT.



This diagram shows the UPnP Stack that a vendor would need to implement on his products. On the left side is the stack for a LAN and on the right side is the stack for a WAN. Both stacks are based on standard internet technology that most (embedded) processors and operating systems already support.

I won’t go into the details of this diagram but wanted you to note that I show the LAN to comply with the new IEC 61162-460 standard that integrates well with legacy IEC 61162-1 serial networks.

**Service Description**



To support UPnP Protocols vendors will also need to describe their products in an S-100 XML file. Such a description will need to include general information such as the vendor name, the model, the serial number, the software version, the health of the product and the cost of a subscription to its services (if any). The device description will also need to include a list of variables, the commands it responds to and how it will respond to these commands.

The description will furthermore need to include details of each of the data item variables, their nature, their encoding, their portrayal, their level of priority, their accuracy and how often they are updated.

# Conclusion

UPnP Protocols provide readily available implementations for inter-vendor operability between devices, systems and services from different vendors

They are secure, extensible and future proof. They allow for seamless zero configuration set-up of M2M communications. They are modular allowing mixing and matching of best in class devices, systems and services thus avoiding vendor lock-in.

UPnP protocols can be used to remotely trouble shoot and fix issues without requiring down-time of the network and they are congruent with evolving standards for the Maritime Cloud Messaging System, S-100 XML, IEC 61162-460 Secure LAN and for the Internet of Things (IoT).

Adoption of UPnP protocols for CSSA M2M Communications should be considered.

# References

1. The UPnP Forum (<www.upnp.com>)

# Action requested of the Committee

The Committee is requested to:

1. Consider adoption of UPnP protocols as the standard for machine-to-machine communications in the Common Shore-based System

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)