SWAN
THE SMART WATER NETWORKS FORUM

Communication in Smart Water Networks

SWAN Forum Interoperability Workgroup

June 2016

Authors:
Dr Andreas Hauser, TUV SUD, Chair
Nicolas Foret, Schneider Electric
Stuart Combellack, Technolog
Jonathan Coome, Syrinix
Quintilia Lopez, Indra
Elkin Hernandez, DC Water
Salil M Kharkar, DC Water
Amin Rasekh, Sensus
Michal Koenig, Qualcomm
Remy Marcotorchino, Sierrawireless
Nicolas Damour, Sierrawireless

Abstract

In smart water network applications, communication protocols are used to communicate with different system components. Smart water network applications may, for example, be systems for Leakage Detection, Pressure Management, Water Quality Monitoring or Asset Management. Smart water network system components could be field devices, automation systems or various software tools. Many different communication protocols are currently used which do not allow interoperable communication. However, a seamless and interoperable communication and operation is needed, in order to foster the deployment and acceptance of smart water applications. This in turn requires generally accepted communication protocols.

This SWAN Interoperability Workgroup is dedicated to fostering the interoperability of smart water applications. In this particular project, we have set the goal to list generally applied communication protocols in smart water networks applications, and to define the communication-related requirements of the involved components. It represents a first step towards the broad field of interoperability.

Introduction

Interoperability refers to the capability of units of a smart water system to exchange and use information and services with one another and interfaced external units to enable an effective, secure system operation with little or no need for manual intervention. The three types of interoperability, i.e., technical, semantic, and process interoperability, ensure effective exchange of data, common understanding of the data exchanged, and coordination of different work processes.

Current smart water applications are all necessarily based on existing/legacy network management systems; SCADA managed systems are the most prominent ones in this context. The main cause of interoperability problems with existing systems are that solutions often have data silos and are closely vertically integrated. The addition of smart applications such as leakage detection to these legacy systems is designed inevitably from the point of view of the individual smart technology provider, rather than from an overall network design perspective. This has led to a diverse communication landscape with numerous proprietary technologies and protocols resulting in non-interoperable systems and subsystems.

Interoperability has been a key subject in the power sector for many years with tangible outcomes, such as architectures and reference models. This WG seeks to adopt existing approaches and methodologies as much as possible rather than reinventing the wheel for the water sector. For the description of the interoperability requirements and concepts with reference to Smart Grids [2], we follow the approach of the Smart Interoperability Panel. Other descriptions adopted from the Smart Grid mapped to water networks can be found in e.g. [1]. In principle, large, integrated, complex systems require different layers of interoperability, from a plug or wireless connection to compatible processes and procedures for participating in distributed business transactions. In Figure 1 three different layers are distinguished according to different requirements:

- Technical: Emphasizes the syntax or format of the information, focusing on how information is represented on the communication medium.
- Informational: Emphasizes the semantic aspects of interoperation, focusing on what information is exchanged and its meaning.

- Organizational: Emphasizes the pragmatic (business and policy) aspects of interoperation, especially those pertaining to the management of the network.

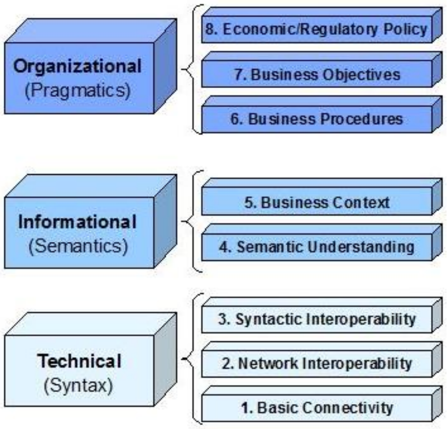

Figure 1: The GridWise Architecture Council GWAC Stack [2].

The architecture shown above is a concept for how a complex system can be designed in order to gain full interoperability. Reality shows however, that systems are upgraded gradually and new features are added on top of legacy/proprietary systems; they are not built from scratch. Therefore, the transformation (migration) from legacy systems to interoperable, efficient smart systems will be accomplished in a step-by-step manner in the coming years.

Big Data and IoT, i.e. the fusion of IT (Information Technology) and OT (Operations Technology), is having a big impact on water networks and is driving many changes to technology and policy. IoT has been boosted by the following trends, which have direct relevance to smart water applications:

- Big data
- Real time
- Sensors spread
- New communications
- Event-driven architecture

But the IoT paradigm will not imply the obsolescence of legacy systems rather it will merge old and new data to make the systems more interoperable and to reduce uncertainty for decision makers.

It is the defined goal of this project within the SWAN WG Interoperability to list and understand currently used communication protocols. To meet this end, in this white paper we focus on communication protocols only, which are part of the technical (syntax) level.

This paper is structured as follows: Firstly, the methodology for describing the existing communication architecture will be given. Secondly, currently used communication protocols are presented. Thirdly, an approach for identifying the appropriate communication protocols for smart water networks is provided from the perspective of current practice (a vertically integrated automation control system approach). This paper finishes with a conclusion.

Methodology

For the collection of currently used communication protocols, the following three smart water applications were considered: Leakage Detection, Pressure Management and Water Quality Monitoring. The reasons for this selection were the relevance of the applications in the market and the different technical requirements in terms of components and unidirectional (Leakage Detection, Water Quality Monitoring) versus bidirectional (Pressure Management) communication.

In order to normalize the representation of the protocols, the communication channels/connections between the different components/objects are identified; the corresponding protocols are listed and their requirements briefly described. Because many objects (and hence communication channels) are the same for the different Smart Water applications, the representation is independent of the actual application.

Communication Protocols

Identification of Communication Channels

A Smart Water architecture, as it is currently known, can be characterized by five layers: physical layer, sensing and control layer, collection and communication layer, data management and display layer, and data fusion and analysis layer. Each layer covers a distinct function in the network [3]. In Figure 2, the SWAN architecture for pressure management is shown as an example.

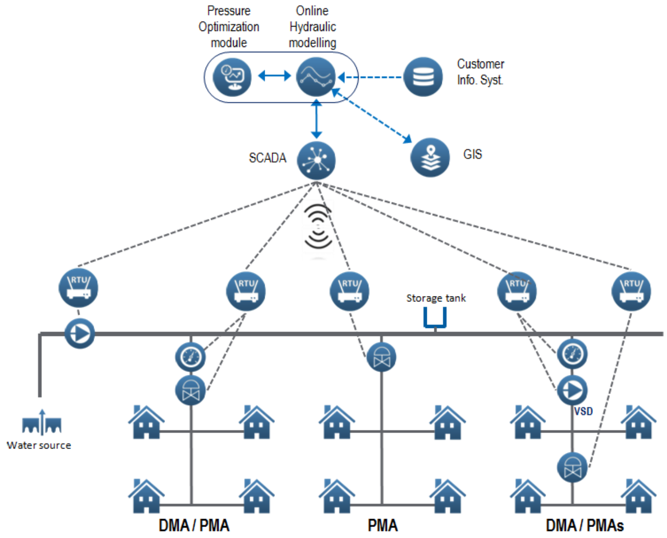

Figure 2: SWAN Architecture pressure management[1]

Table 1: Description of the components in smart water applications

Figure 3 shows the simplification of such an architecture in terms of its communication. It highlights the relevant components and communication channels within a smart water network application. In Table 1 the components are then briefly explained.

[1] SWAN WG Architecture

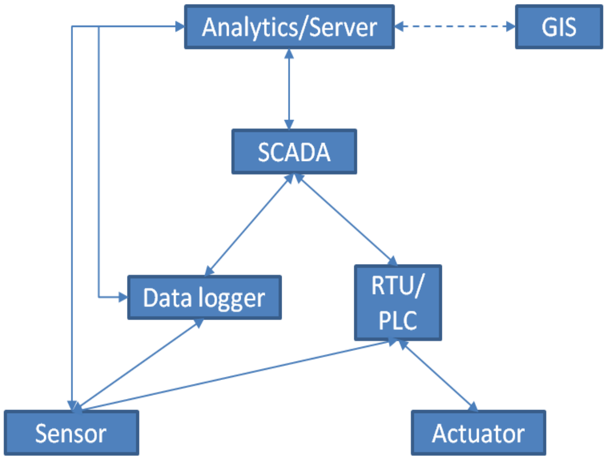

Figure 3: Diagram of all potential communication channels

Sensor	Measure continuously acoustic signals, pressure, flow or other data at a single point of a pipe network.
RTU	Able to read data from local sensor and actuator sending it to SCADA periodically. Additionally, it can provide local control of pumps and valves.
Data logger	Read data from sensor (flow, pressure, etc.), stores them at regular intervals, and transmits it to the SCADA system.
SCADA	Receives and aggregates data from multiple installations to monitor and control the network in near/real time. It may store historical data for later viewing.
Analytics/ Server	Analysis of data and Big data: Able to process massive and heterogeneous data. It can process structured and non structured information

Table 1: Description of the components in smart water applications

Protocols for Communication Channels and Requirements

Table 2 displays the identified communication segments within the Smart Water network applications derived from Figure 3.The protocols are just compiled without any prioritization or assessment.

For the sake of clarity, we have chosen a layered approach to describe/classify protocols. We have simplified the seven layers Open System Innterconnection (OSI) model into three layers as shown in Table 2: Application layer (correspondent to Application, Presentation and Session in OSI model), Network layer (corresponding to Transport and Network in OSI model) and Physical Layer (corresponding to Data Lynk and Physical layers in OSI model).

	Requirements	Application Presentation Session	Transport Network	Data Link Physical
Sensor – Data logger	Fault tolerant; command transmission (bidirectional communication); standard interface: 4-20 mA, counter inputs, or serial link (modbus,….); low power consumption	Modbus M-Bus (EN1434-3)		RS232, RS485, M-Bus SPI Digital I/O, pulse counting, 4-20mA, 0-10V
Data logger – SCADA	GSM/GPRS coverage; secure communication, resilient to failure, some applications require diversity[2], interoperability	DNP3, WITS-DNP3, proprietary SMS-based protocols	TCP, UDP, DNP3, IP Radio, IPv6, IPv4, Cellular IoT Small Data	DNP3, Cellular RF, LORA, SIGFOX
SCADA – Server/Analytics	Web services tend to be proprietary interfaces but can have automatic discovery; secure communication, security, backfill, redundancy, interoperability	OPC DA, JSON, RDF, OWL, HTTP/COAP, RESTful web services SOAP, WSDL, XML, CSV, ODBC, OGC, SensorML, WaterML2.0, OpenMI,	IPv6, IPv4, TCP, UDP	Diverse (Ethernet, x21, ppp, fiber)

[2] Connected to more objects with different protocols

Data logger – Server/Analytics	Secure data exchange; fault tolerant; command transmission (bidirectional communication);	MQTT, HTTP, LWM2M, COAP	IPv6, IPv4, TCP, UDP, Cellular IoT small data	Cellular RF, LORA, SIGFOX, PSTN
SCADA – RTU	Backfilling capable data exchange (SCADA backfill its historical database, following loss with RTU), secure communication, resilient to failure, some applications require diversity	Modbus, DNP3, WITS-DNP3, Medina, IEC 60870-5 101/104 MQTT, HTTP, LWM2M, COAP	TCP, UDP, DNP3, IPv6, IPv4	Cellular RF, PSTN, Scanning Radio, Licensed and license-free data radios
RTU – Valve	Wired, bidirectional	Modbus, Profibus HART,		RS485, HART Digital I/O 4-20mA, 0-10V
Sensor – RTU/PLC	Fault tolerant, secure, wired and wireless, bidirectional	Modbus, Profibus HART,WirelessHART	6LoWPAN	RS485, HART, IEEE 802.15.4 Digital I/O, pulse counting, 4-20mA, 0-10V
GIS – Analytics	Secure data exchange, usability	OGC web services, GML, ISO19139	IPv6, IPv4, TCP, UDP	Diverse (Ethernet, x21, ppp, fiber)
Sensor – Server	Secure data exchange, uni/bidirectional, wireless	MQTT, XMPP, LWM2M, COAP	6LoWPAN, Cellular IoT small data, IP, UDP	IEEE 802.15.4, Cellular RF

Table 2: List of protocols structured in three layers

Identifying the Appropriate Protocols for SWANs

As can be seen from Table 2, there are many different commonly used protocols. As well as those listed, there are a plethora of proprietary single-manufacturer protocols which do not allow for an interoperable exchange of data. The reason for this shortcoming is mainly the addition of smart features on top of legacy systems, rather than designing the network topology from a communication technology point of view.

In order for Analytics modules to provide new business insights, systems need to be capable of storing and processing heterogeneous and massive quantities of data. IoT systems and the corresponding IoT platforms are being designed to meet these requirements.

Given the different requirements in terms of range, throughput, power consumption, and the lack of accepted best practices for interoperability, there is not one best protocol. All protocols have their pros and cons and it depends on the specific requirements whether one protocol is preferable or not.

Within the context of the rapid development of the Internet of Things and its implied communication requirements, a convergence towards certain protocols can be observed. By using the examples of the popular protocols (Wi-Fi, Bluetooth, ZigBee, 6LoWPAN, and Sub-1GHz protocols), a pragmatic approach can be used to map protocols into the parametric dimensions range, throughput, power consumption and topology [4].

As an example for protocol comparison, we consider only the communication between sensors, data loggers, PLCs and RTUs. Using the topological possibilities of the smart elements, we focus on the requirements in terms of range, throughput, power consumption and topology as shown in Figure 4.

According to this representation, each communication channel within a smart water application should be evaluated in alignment with range, throughput, power consumption and topology requirements.

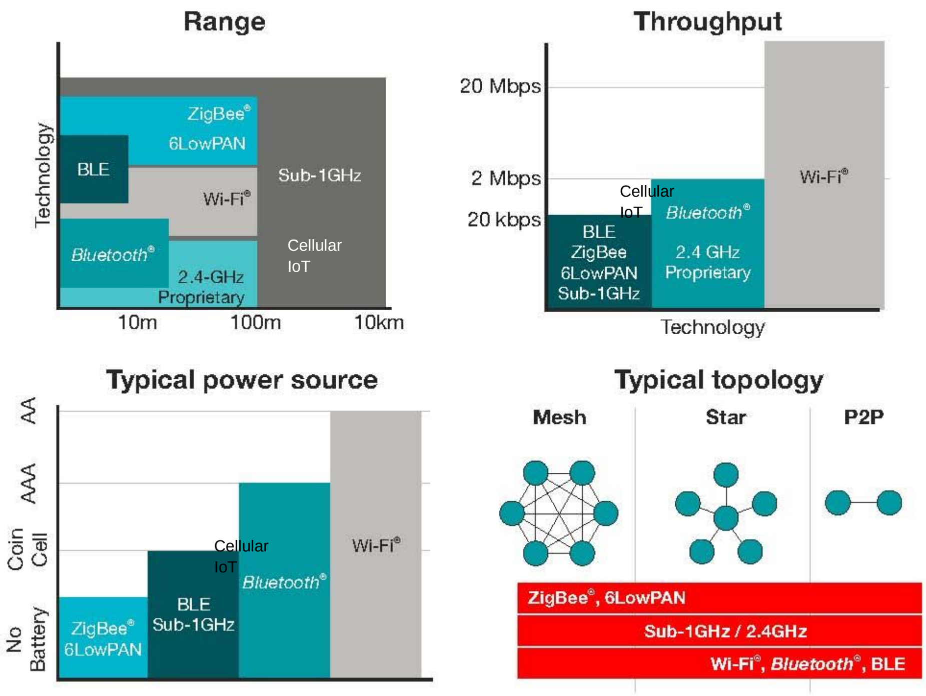

Figure 4: Wireless technology parameters [4]

A practical solution to today's connectivity challenges is the ongoing introduction to the market of multi-protocol handling devices that can be used to interconnect valves, sensors, RTUs, PLCs, servers and the cloud; these devices provide a migration path by facilitating communications using the most popular existing and emerging protocols and also allowing open programmable interfaces that can be customized for applications using less common protocols. This approach can be part of a solid migration strategy and future safe roadmap towards a fully scalable smart water architecture.

SWAN Outlook for Interoperability

There is no single protocol that best suits all the applications and communication infrastructure. Rather, communication protocols are strongly influenced by the environment, the price of transmissions, powered vs battery devices, security, etc.

The Application layer is dependent on the purpose for the data acquisition. Therefore there must be a variety of application protocols for specific purposes. A general application protocol would be too complex to support efficient business processes.

The Physical layer is dependent on the topology, costs and environment in which the infrastructure is deployed, as well as the capabilities of the devices. It is hardly possible to find a generalized physical layer that covers most of the applications. Nevertheless, a trend towards radio and cabled networks can be observed.

The Network layer is currently in the process of convergence/extension to IP based protocols that can operate in all the nine segments abovementioned. Moreover, all emerging physical protocols are in the process of supporting IP based protocols. Therefore, at the network level we can safely say that the communication is in the process of finding an interoperable family of IP protocols that is able to support most of the typical applications.

The Network layer is crucial to secure the information exchange both from a reliability and information security standpoint. Because of this it is an advisable approach to establish interoperability at the Network layer as first step by using IP based protocols in all communication channels.

Depending on the application, it could be possible to extend the IP network from the server all the way to a smart sensor. In this ideal situation, intermediate nodes may not need to decode the sensor data and hence cryptographic keys are only needed on the sensor and server. This improves the security of the overall infrastructure. Furthermore, maintenance, monitoring and troubleshooting of the network can benefit from the available network management tools and the end-to-end communication established by the Network layer.

The current limitation of IP protocols (specially IPv6) is that they are not very well suited for low band width or low speed networks. IP is therefore being adapted to enable its use in low band width segments. For example, 6LowPAN is a development that enables the use of a simplified and compressed IP protocol over these networks. It is probable that there will be other extensions for particular segments and physical layers.

Our recommended approach would be to select between the IP based standards i.e. IPv6 and 6LowPAN is shown in Figure 5.

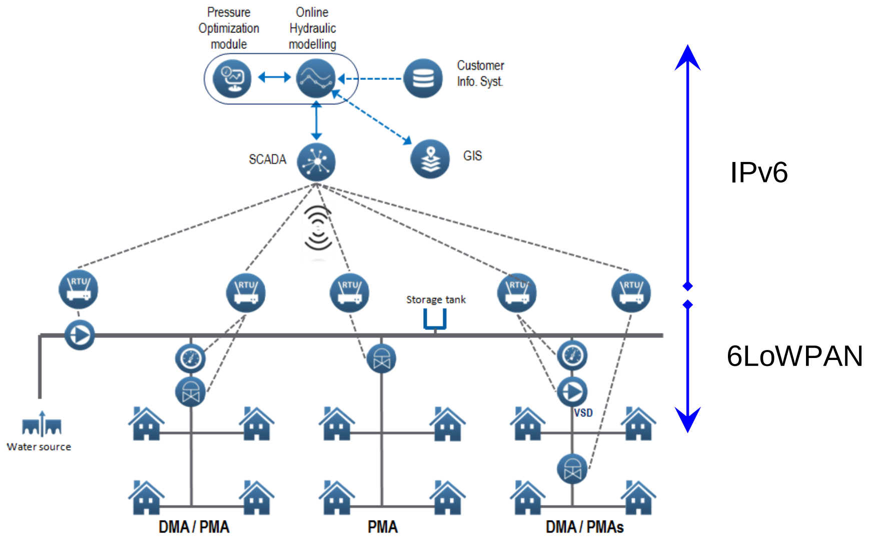

Figure 5: Suitable IP-based protocols in the SWAN Architecture pressure management[3]

[3] SWAN WG Architecture

Conclusion

Currently there are many different communication protocols being used in smart water applications. This makes an interoperable and seamless exchange of data very difficult. This situation is primarily caused by the retro-fitting of new smart applications on top of existing/proprietary network management systems, which were designed from an automation/vertically integrated point of view. The rapid development of the Internet of Things and Data Analytics brings more pressure for horizontal integration with again different requirements in terms of range and throughput, power consumption and topology.

There is not one single protocol that meets all the different requirements in smart water network applications. However, it can be stated that where practicable, protocols for most of the communication channels are converging towards IP-based protocols.

The shake-up in the communication space forces utilities and technology vendors to continuously observe this trend and to adapt accordingly. Consequently, migration and planning for change will play a key part for an interoperable, efficient and reliable smart water network for the near future.

The next project of this WG will be the definition and implementation of scalable pilots in the area of asset management. The pilot will be designed from an interoperability and scalability point of view, which should avoid the current practice of excessive, non-scalable pilots resulting in costly engineered solutions. This project should enable its seamless scalability to large applications and its replication into other areas of smart applications.

Future efforts may additionaly aim at the development and standardization of cyber security, including confidentiality, integrity, and availability in the smart water networks.

Bibliography

[1] A. Hauser and F. Roedler, "Interoperability: the key for smart water management," *Water Science & Technology: Water Supply,* 2015.

[2] SGIP, Smart Group Interoperability Panel, 2015. [Online]. Available: http://sgip.org/Interoperability-and-the-GWAC-Stack.

[3] Workgroup I - Smart Water Network Architecture, SWAN Forum.

[4] R. Gil, "Wireless connectivity for the Internet of Things - One size does not fit all," 2014.