**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **ISA100 Common Network Management** Brief Overview |
| Date Submitted | [18 Sep 2014] |
| Source | [Kinney Consulting][Kinney Consulting][Chicago, IL] | Voice: [+1.847.960.3715]Fax: [+1.847.790.3805]E-mail: [pat.kinney@ieee.org] |
| Re: | [802.15 Interim Meeting in Athens, Greece] |
| Abstract | [Common Network Manager and its reliance on Frequency Coordination] |
| Purpose | [Official minutes of the Working Group Session] |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

**ISA100.20: Common Network Management**

**Part 1: Concepts and Terminology**

# Introduction

## Scope of ISA100.20

This project will present a Common Network Management [[1]](#footnote-2)(CNM) framework to monitor and provide actionable information to various and disparate wireless networks commonly found in wireless network environments for industrial automation and control systems.  The CNM framework will be scalable to address various network sizes and device populations and extensible to adapt to changing technologies, applications, and user requirements.

## Macintosh HD:Users:patrickkinney:MyDocuments:ISA:WG20 (CNM):0-1.emf

Figure 0‑1 Example of a Common Network Management scenario

## Goals of ISA100.20

Define the conceptual interfaces and protocols necessary to provide for interoperable network management functions that may be performed to installed networks (see Figure 0‑1), and may be performed reliably and securely by a CNM infrastructure. This project will utilize existing standards as much as possible and will create new standard(s) (i.e. normative documents) only when necessary to fill gaps or to make a more cohesive or comprehensive solution set.

## Need of ISA100.20

There are a multitude of unique wireless networks for industrial facilities that fulfill specific automation needs, and it is apparent that the numbers of unique wireless networks and numbers of network devices are growing. Any one industrial user may employ many of these networks, sharing the same spectrum and other resources for various automation and IT functions.  Each of these wireless networks typically has unique wireless network management (WNM) devices, protocols, and metrics. As the number of networks and the size of those networks grow, the complexities of managing all of these networks will overstrain existing network management staffing and will often tend to favor one network over another for given shared resources.  A CNM approach would allow an industrial user (or service provider) to monitor and provide actionable information to all of its CNM compatible wireless networks by using consistent policies and standard protocols.

# Scope and Purpose of the Concepts and Terminology Technical Report (C&TTR)

## Overview

Wireless field devices provide extra function beyond the device’s basic function by exchanging information in a network environment without requiring additional wires, have potential to transform maintenance practices so that devices with problems could be identified sooner and remotely. No longer would field technicians have to go to the device itself to get relevant information. Instead, information would be provided directly to the process automation system, plant asset management system, or indeed any other systems or software in the plant that required it.

However, in many cases, this promise of wireless field devices in the plant remains unrealized. This is not so much a technology issue as it is due to resource and work process issues; or concerns about which standard will dominate issue. Too many users are employing old maintenance work processes with new technologies. The new devices and applications are installed, but the operators and technicians stick to their old way of doing things, their old preventive or routine maintenance practices, and never really take advantage of the huge amount of information that is available to them. Finally, there is a concept that one wireless technology in the industrial environment will replace all other wireless networks, despite what we have seen in the past of a quilt work of multiple networks.

The process industries would benefit from a standard set of work processes and best practices for intelligent device management. This would give end users an effective blueprint for achieving the significant economic lifecycle benefits associated with intelligent devices. The process industries would also benefit from a CNM that extends over all other network managers in the facility, providing a platform for common interfaces.

## Current situation

As mentioned earlier, today many industrial facilities have a multitude of wireless networks, both proprietary and standards based, working autonomously to fulfill specific automation needs. It is expected that the numbers of unique wireless networks and the numbers of network devices will continue to grow; however since the spectrum is not growing these networks will increasingly compete for a common frequency band. Each of these networks typically has unique network management devices, protocols, and metrics.

As the number of networks and the size of those networks grow, the complexities of managing all of these networks will overstrain existing network management staffing and will often tend to favor one network over another for given shared resources.

Additionally, the guidance from each of the wireless network vendors seldom takes into account the characteristics of the other wireless networks in use. The method to resolve conflicts would typically be to turn off the other wireless network or move it out of range rather that a deeper understanding of how to modify the characteristics of all wireless networks to coexist in a coordinated manner.

Finally, the security of each wireless network must be handled uniquely, requiring the operators to understand all security procedures of each network. Mobile devices cannot participate in multiple networks due to lack of shared concepts of authority, authenticity, etc.

## Challenges

### General Challenges to Industry

### In today’s process plants, operators, engineers and technicians must navigate an already complex landscape of applications and communication pathways that can often make the problem of accessing data from intelligent devices a herculean task. Multiple databases and interfaces permeate the industry. Digital field devices must interface with a host system, which in turn communicates with a data historian, configuration database, alarm management systems, plant asset management systems, and higher-level computerized maintenance management systems. Enterprise connectivity is a must, since work orders are typically generated through systems like enterprise asset management (EAM), computerized maintenance management system (CMMS) or enterprise resource planning (ERP). Many users get stymied when it comes to integrating all these disparate elements together. Workers at multiple levels in the enterprise (in multiple disciplines) must be informed, and coordinating communication between these workers creates a problem in itself.

End user companies and owner operators want to adopt new technologies and be considered world-class manufacturers, but they do not want to invest in the training and time it takes to use those technologies effectively. There are exceptions to this rule. Leading edge end user companies exist in this industry and are setting an example. Training does not have to be a big investment either.

Many of the fieldbus projects today are green-field projects. However, we are seeing an increase in fieldbus for modernization applications. There is a large amount of diagnostic data that is stranded in these plants and cannot be put to good use. In this case, the existing maintenance and operations personnel need to be convinced that the new work process makes their jobs better, that it improves their performance as employees, and that it gives them a better understanding of their plant.

### Challenges specific to CNM

* CNM’s ability to exchange data and diagnostics with network managers
* CNM’s ability to manage network managers (that weren’t intended to be managed)
* Commonality of MIBs/managed attributes among network managers
* Security issues like shared keys, authenticity, secure communication links with network managers
* CNM’s ability to set up networks and network managers

## Benefit of CNM

A CNM approach would:

* Allow an industrial user (or service provider) to monitor and provide actionable information to all of its CNM compatible wireless networks by using consistent policies and standard protocols.
* Increase the adoption of wireless devices due to reduced focus on only one network
* Provide the ability to maximize use of spectrum
* Enhance communications reliability by providing connectivity between disparate wireless networks
* Provide the ability to monitor wireless networks to report timely network status, individual route status, interference, quality of service (QoS), latencies, instances of possible cyber attacks, network statistics
* Provide actionable information for the avoidance and/or mitigation of wireless network issues
* Assist in the set-up of wireless networks including coordination of local addresses such as PAN IDs, SSIDs, short (hence ambiguous) MAC addresses, frequency usage, codes for CDMA, priorities, security levels, etc.

# Industrial Networks

Industrial networks have significantly evolved since the 1950s, and their rate of evolution is increasing. The following is a illustration of the development progress of industrial networks.

## Historical Perspective

Industrial communication has evolved from pneumatics in the 1940s to analog current loops in the 1960s to serial based in the 1980s. Figure 4‑1 shows major industrial networking milestones over the last fifty years.

Networking for process control began in the 1970’s when control system designers conceived of ways to connect remote/distant devices using “serial communications.” Gradually the technology developed to gain higher speeds, reduce cost, and improve reliability giving rise to token passing protocols, however the dominant network protocol remained master/slave between computer and microprocessor-based devices, but always analog 4-20mA current signal to send the primary measurement data from field instruments to the digital controller.

In the 1980’s the HART protocol was created to enable smart field instruments to send secondary data to control systems, and to enable field calibration and range adjustments using either the control system or local terminals. By the 1990’s it was finally acknowledged that process control networks were often using the same types of data communications as used for information technology networks. Except for FOUNDATION Fieldbus H1, that was purpose-built for both the environmental demands, electrical noise, and reliability requirements for process control data transfers between very smart digital field instruments and control systems. Unlike other network protocols, FOUNDATION Fieldbus was designed to allow peer-to-peer (now called mesh topology) direct communications between nodes on the same network. The purpose was to allow control loop strategies to execute in reliable field devices without requiring a host system. By the end of 2000, there was also an equivalent network designed by the Fieldbus Foundation called HSE, that provides identically the same Application Layer protocol as H1, but uses a full duplex, switched, IEEE 802.3 (Ethernet) network with UDP/IP protocol at the Network and Transport Layers.

By 2008, it was widely recognized that there was a future need for wireless networks in process control. An ISA standards committee was quickly formed to investigate standards for the process control application from the available wireless protocols: IEEE 802.11 (Wi-Fi), Bluetooth (IEEE 802.15.1), and ZigBee (based on IEEE 802.15.4.) All of these were found to be deficient for many reasons. In examining alternatives to these networks, the committee had presentations made by many wireless chip suppliers one of which influenced the ISA100 standards committee to strengthen the IEEE 802.15.4 standard by using a channel hopping pattern in addition to the Direct Sequence Spread Spectrum used in the base chip. A major telecommunications company influenced the committee to use IETF standards for the Network and Transport Layer protocols. A technology leading security company influenced the committee to use an Elliptical Public/Private key exchange during over the air network provisioning. All of this has now been included into ISA100.11a that is now being finally approved as IEC 62734, and is commercially referred to as ISA100 Wireless. Products conforming to these standards are now being sold.

In order to speed wireless products to market, the HART Communications Foundation adopted the protocol being sold by a vendor of wireless chips offering the channel hopping already adopted by ISA100. This protocol was formally written as an HART Communications Foundation standard and submitted to become IEC 62591, commercially referred to as WirelessHART. Although quite similar in cost and implementation, ISA100 Wireless and WirelessHART are not interoperable.

The following summarizes the legacy technologies:

* Copper wire, point to point, typically dedicated to one application, not interoperable with other networks
* Limited amount of devices allowed to participate In the network
* Significant reliance on analog technology
* Low data rate communications, albeit at longer ranges
* Networks faults were analyzed with a volt-ohm meter



Figure 4‑1 Industrial Network Timeline

## Networking today

Today’s industrial networks being deployed contain vestiges of their heritage but are evolving into new and more complicated infrastructures as they adapt to new applications. The following summarizes the today’s technologies:

* Networks are typically digital, even networks dedicated to voice communications
* Wireless networks have taken on tasks and applications that wired networks cannot address
* Wired networks are increasingly using IETF IPv4 over Ethernet (IEEE 802.3) as a transport for an application’s protocol
* Wired and wireless networks that are not based upon IETF IP are not interoperable
* Low cost high speed processors with vast high speed memory are allowing communications to be optimized for special environments
* Security protocols and policies are being developed to handle critical infrastructure needs
* Network standards are being developed to deal with extremely time sensitive applications allowing remote, high speed control of equipment
* Networks faults are analyzed by an array of analyzers such as sniffers, protocol analyzers, etc.

## Future trends in networking

Network standards are being amended with greater capabilities and new network standards are being developed for applications that cannot be serviced with existing network standards. Additionally, future network devices will have much greater capabilities in areas such as computing power, memory, battery life.

The current efforts in IETF are not only to further enhance the capabilities of existing standards but to also address devices that are considered “constrained” in areas such as computing power, memory, and available energy. The IEEE has development efforts underway for both wired and wireless networks. Wired standards are being developed for higher data rates and for Time Sensitive Networks (TSN) yielding networks that can be applied to very high speed industrial environments such as robotics. Wireless standards are being developed to add new frequency bands below 1 GHz in ISM bands and the “TV white space” frequencies that used to be occupied by old analog TV stations which can result in longer ranges for wireless networks. The following summarizes the future technologies:

* Higher data rates available to both wired and wireless networks increasing network capacity
* Wireless networks have additional sub-GHz spectrum from unused TV bands and other low usage bands yielding longer link ranges and reduced interference
* IPv6 will be the ubiquitous networking layer with many different types of lower layer modems
* Industrial Internet of Things (I2oT) allows even simple devices to be networked
* Multiple applications running on a single network
* Increased security isolates virtual networks sharing a common media
* Multiple networks (PAN, LAN, MAN, and WAN) are agnostic to applications and capable of handling most if not all application communication needs
* Increased capabilities to include the use of hand held devices like cell phones and tablets
* Networks faults will be analyzed with dedicated built-in test equipment both locally and remotely administered
* Wireless networks will increasingly support mobile workers and devices. Future trends in mobility will be to cover larger physical areas, higher motion speeds while in operation, larger numbers of devices or workers, and increased complexity of access control.

# Wireless Network Overview

## Introduction

Wireless networks share the major component functions of wired networks, although the lower communication layer protocols (i.e. the physical layer - PHY and the data link layer - DLL) are significantly different due to the lossy aspect of electromagnetic radiation and high probability of interference.

Figure 5‑1 shows two major logical types of communications in a wireless (or wired) network: application data and management data. Application data consists of that information coming from sensors or to actuators. Field device data flow is communicated to and from the gateway which may translate the application data and sends it onward to the application(s). Management data consists of operational commands and status. Communication status, generated by the network device, is communicated to the WNM, which then communicates to the CNM.

Figure 5‑2 depicts a typical scenario of a field device mesh network consisting of the two logical types of data flows, application and management.

This section sets the background for this paper by describing common aspects of industrial wireless networks. The CNM project will focus on four major industrial WNMs: IEC62591, IEC 62734 , IEEE 802.11, and ISA100.15 Backhauls. These WNMs are described in the annexes of this document.

### Macintosh HD:Users:patrickkinney:MyDocuments:ISA:WG20 (CNM):5-2.png

Figure 5‑1 Application and Data Communication Types

## Macintosh HD:Users:patrickkinney:MyDocuments:ISA:WG20 (CNM):5-3.png

Figure 5‑2 Mesh Network Data Flows

# Network Manager Functions

This section describes common functions shared among most wireless network managers.

## Initialization/Configuration

### Network Formation

The WNM needs to initialize and set up its network with parameters such as frequency band, data rates, number of retries, etc.

### Joining

The WNM needs to validate all devices that try to join the network. Upon authenticating a device, the WNM provides the joining device with keys such as a network key, and session keys such as network manager session keys, and gateway session keys,

### Device Address assignment

Some network protocols allow the WNM to assign “short” addresses to save transmission time and energy. Since these short addresses are ambiguous outside of the network, the WNM will store these addresses and not reassign them to any other device, unless the original device is no longer joined to the network.

### Network/Subnet address assignment

Devices need to be configured with the network ID before they attempt to join the network, enabling them to find the right network to join.

#### Address lease renewal

Method to periodically renew addresses to prevent address leakage

## Scheduling

Scheduling allows a service to occur at a known time, i.e. it provides deterministic behavior. Scheduling requires a well known clock along with specified times and participating devices. Protocols based upon scheduling include reservations (RSVP) specified in RFC2205, time schedule channel hopping (TSCH) used in IEC 62591 and IEC 62734, and guaranteed time slots (GTS) used in IEC 62601.

### Creating slotframes

Superframes and slotframes are the periodic concatenation of timeslots, large networks often require large amounts of timeslots resulting in a low periodicity. Assigning a device multiple time slots within a slotframe or creating multiple overlapping slotframes are ways to provide shorter latencies

### Time slot assignments

As noted in 6.2.1, time slot assignments to a network device is critical to the latency of its communications, however, providing too many time slots to a device could negatively impact energy consumption and hence battery life

### Setting up links

All network devices wishing to participate in a data link must be set up on the same timeslot, when multiple hops are required to increase the communication distance, the relaying devices must be included in appropriately sequenced links.

## Routing

### Source routing

While source routing is often defined as when the sender of a message either partially or completely specifies the route the packet takes through the network, in this paper source routing is when the network managers define the route that is followed with no exceptions. Source routing allows a network manager to detect flaws in the network by noting when a source route drops the message, since individual devices cannot deviate from the specified path.

### Graph routing

Graph routing is similar to source routing, 6.3.1, except that exceptions are allowed to avoid dropped messages. When sending a message, the source device writes a graph ID in the network header. The paths in each graph are supplied to by the network manager to each network device, in other words the graph ID specifies the end node and therefore allows all connecting devices to work around flaws in the requested route. Graph routing provides a more reliable transmission.

## Channel management

### Allocation of communication resources as per device needs

Communication needs often change with time, therefore communication resources such as slotframes, timeslots, and links also need to be changed to accommodate the communication needs.

### Keeping track of black and white channels

#### Black channels are those that are to be avoided for a number of reasons such as poor performance or that they cause interference to other devices or networks

White channels are those that are preferred due to better performance and causing less interference.

### Maintenance of Channel hopping sequence

Over time a specific channel hopping sequence may encounter increased interference, the network manager may be able to alter the hop sequence in an effort to increase transmission success. This operation requires the network manager to log paths encountering interference.

## Security

### Proxy for the security manager

In industrial networks the network manager often provides the only interface to the security manager, i.e. the security manager interface is not exposed.

### Policy enforcement

Networks have numerous policies that essential for deterministic behavior, security, network device battery life, and good coexistence with other networks. The network manager implements these policies via device configuration, topology, and routing,

## Diagnostics

### Address collision

As per 6.1.3, the WNM will assign a short address if the network protocol allows it to do so, unique within the network, to a device. The network manager is responsible for making sure there are no duplicate addresses used. When a device detects an address collision (i.e. frames using duplicate addresses) the network manager must resolve the address issue.

### Frame collisions

In wireless networks, network devices are verified to have a sufficient signal to correctly receive frames from its neighbors. Hence, when a frame is not received correctly, a collision with another packet is assumed. Collisions may occur due to many circumstances such as not detecting any node is transmitting (i.e. hidden node), or improper backoff protocols.

### Excessive interference

The network manager may monitor the network behavior to detect any anomalies caused by excessive interference. Once detected, the network manager may implement mitigation strategies.

## Management

### Priority

Wireless networks are often resource constrained, i.e. their performance and capabilities are limited by resources such as bandwidth, device range, device energy, interference from other devices, etc. Due to these constraints, networks cannot perform all tasks at the same time. Priorities allow the network manager to determine which message should be sent first, which devices are given preferential distribution of resources, etc.

### Topology logging

The network manager will maintain a log of the network topology to be able to provide routing (either source or graph) and to provide such information to the network administrator

### Failure events logging

Any failure event is logged to provide the administrator with the details and time of the failure

### Device monitoring, maintain database on each device’s health

The network manager may monitor device behavior, i.e. key performance indicators (KPI) such as latency, and maintain a database noting this behavior to allow more robust routing and to advise the network administrator of possible problems.

# CNM Concept

## Introduction

As per the WG20 charter noted in 0.1, the CNM is not intended to replace network managers, rather it is intended to aid the network administrators’ efforts to manage the various networks being deployed. For instance, often networks in a facility share many settings or configurations in areas such as security, priorities, and frequency band operation. The network operations may be set up to allow the CNM to provide this common information, thus saving the network administrators time and eliminating errors common in re-entry of data.

## CNM Concept Architecture

WG20 has based the CNM concept on an open version (i.e. vendor independent) of the hierarchical distributed management for multiple networks, as shown in Figure 8‑1. In this concept the CNM serves as a central server that will communicate to multiple heterogeneous network managers from various vendors. It is envisioned that, since the various WNM interface communication protocols will typically be unique to each vendor, the CNM will define a “native” protocol (9.3.2) that can be converted to a vendor’s proprietary interface. As shown in Figure 8‑1, WNM B has a proprietary interfaces while WNM C uses the CNM native interface protocol and therefore needs no adapter. WNM A has no exposed interface, hence the CNM must communicate to WNM A via the Gateway V interface, which in this case is also proprietary, hence the need for an adaptor.

The CNM is also intended to handle hierarchical WNMs that may contain multiple networks and their WNMs.



Figure 8‑1 CNM Concept Architecture

1. Common Network Manager: manager hierarchically various network managers, collecting operational information from those network managers and providing actionable information to them [↑](#footnote-ref-2)