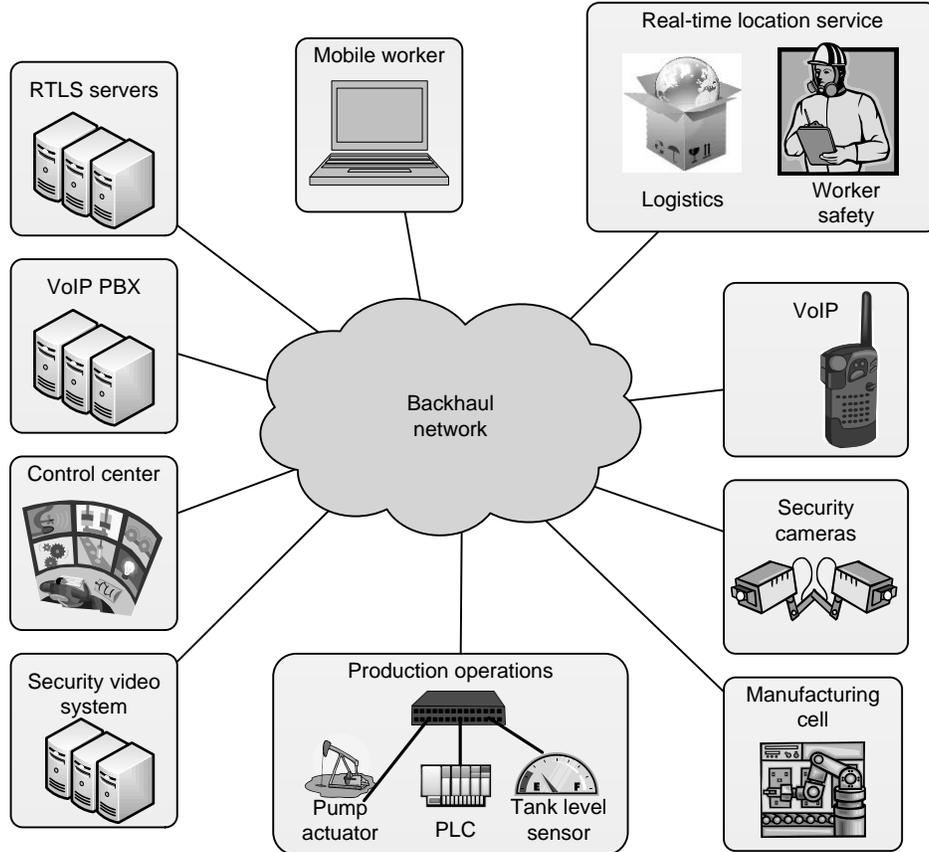


# 1 Scope

## 1.1 General

This document presents an architecture model for interconnecting automation system elements over untrusted backhaul networks. The focus is on wireless physical layer but is not limited to wireless.



**Figure 1 — Example applications using a shared backhaul network**

Figure 1 provides an example of the variety of (potentially simultaneous) uses for backhaul networks. In this example, the “Backhaul Network” cloud could represent a short-distance network such as the user-owned network within a building or site, or it could represent a potentially heterogeneous long-distance network (for example, satellite or cellular communication networks) that are provided as a service effectively by multiple third parties. These backhaul links may be provided by one or more commercial providers such as satellite communications providers, cellular, LTE (see Clause 3), WiMax data services, etc. Alternatively, the backhaul may also be provided by the user—for example, Wi-Fi services, point-to-point microwave links, etc.

## 1.2 Wireless vs. wired backhaul networks

There is nothing in this architecture that precludes the use of wired network technologies (for example, Ethernet) for backhaul networks.

### **1.3 Specific goals**

#### **1.3.1 Provide an architecture model**

One of the primary goals of this document is to create an architecture model that insulates the industrial control system elements from the variety of protocols and interfaces associated with various backhaul technologies and providers. Conversely, this architecture model is also intended to insulate the backhaul providers from many of the technical issues associated with specific industrial control systems vendors, protocols, and interfaces.

#### **1.3.2 Define a common vocabulary**

This generalized architecture model describes elements and interfaces associated with using backhaul services; the resulting model and vocabulary provide a common framework by which industrial control system vendor, user, and backhaul provider communities can better communicate and collaborate in this rapidly evolving space.

#### **1.3.3 Anticipate backhaul technology evolution**

Backhaul network technologies continue to evolve rapidly. For example, new protocols and capabilities for cellular data backhauls continue to emerge—as evidenced by the recent introduction of WiMax and LTE service offerings. Similarly for Wi-Fi, a succession of technologies and standards has emerged over time (for example, IEEE 802.11b, 802.11g, 802.11a, 802.11n, etc.).

#### **1.3.4 Allow for mixed use of a shared backhaul**

In collecting backhaul network use cases, the authors documented a strong demand from the automation user community for general-purpose backhaul utilization beyond that of just transporting industrial control system data. Specifically, as illustrated in Figure 1, many of the use cases drive the need to use the backhaul to support general data services such as security cameras, voice over internet protocol (VoIP) telephony, emergency first responders, and real-time location services. These use cases also drive the need to support industrial application data service models such as client/server, event multicast, and publish/subscribe. This mixed use of the backhaul network means this model also needs to address automation needs regarding backhaul security, backhaul management, backhaul flow control, backhaul user mobility, etc.

#### **1.3.5 Provide a framework for future profile specifications**

As a non-normative document, this architecture has insufficient authoritative detail to enable separate implementers to create products that interoperate.

## **2 Normative references**

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 7498-1, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

ISO/IEC 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IETF RFC 2205, *Resource reservation protocol (RSVP) – Version 1 functional specification*

IETF RFC 2474, *Definition of the differentiated services field*

IETF RFC 2475, *An architecture for differentiated services*