|  |
| --- |
| Ch 6.9 amendment: Industrial network |
| Date: 2018-03-04 |
| **Authors:**  |
| Name  | Affiliation  | Phone  | Email  |
| Max Riegel | Nokia Bell Labs |  | maximilian.riegel@nokia.com |
|  |  |  |  |
|  |  |  |  |
| **Notice:**This document does not represent the agreed view of the OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document provides the concrete amendment proposal according to comment #10 of p802-1cf-d1-0-comments-maxriegel.xls

The revision -01 addresses revised figure following conventions used in other figures mapping to NRM (dotted lines) as well as edits to correct reference to figure and explain virtual servers.

# Chapter

## Deployment scenarios

### Industrial network

Industrial networks connect IoT devices, control processes of machineries and robots, surveillance equipment and building control gear among themselves or to central control processes. Often industrial networks in factory floors and power plants provide connectivity to virtual servers residing in a local datacenter or in the cloud. It is quite common that the local area part of industrial networks are based on Ethernet, in particular due to its multiplexing capability of multiple networks and services within a single infrastructure, and its support for guaranteed packet delivery through Time Sensitive Networking features. Industrial networks are used as well to allow mobile terminals to connect through IEEE 802 wireless technologies to gateways, local servers, or even to the Internet.



Figure (x): Industrial (access) network

The figure x above shows a schematic network of a factory floor with three robots at an assembly line, supervised through surveillance cameras forwarding live video to a central control room not depicted here. A Wi-Fi network throughout the factory floor allows the operators to remotely access the control processes of the robots and live video streams and other information while walking along the assembly line. Virtual servers in the cloud are used for controlling the environment, running the applications accessed by the mobile terminals, and to process various measurements delivered as well to the central control room.

Control processes of robots require highest reliability and immediate response to their messaging. Video streaming is not as critical as robot control, but sufficient bandwidth has to be reserved on the network to ensure that the control center has latest insights into the factory hall. The applications running on smartphones, tablets and notebook computers allowing operators to access control information while walking around in the factory hall may be able to deal with packet losses and higher delays as usual when accessing services over the Internet. However, the network has to ensure through scheduling and prioritization that bulk data transferred to wireless devices does not impact the transmission of the low-delay real-time messaging and streaming data.

The industrial network scenario can be mapped to the NRM as depicted in figure x+1 below.



Figure (x+1) : Mapping of industrial network to NRM

The access switch connecting the robots as well as the surveillance cameras to the Ethernet backbone represents the NA for the wired connections of terminals, while the access point represents the NA for wireless terminals. BH is mapped to the second level aggregation switch with the uplink to the gateway to the local datacenter fitting to the interface between access network and the access router. The router functionality is located in the gateway to the local datacenter where multiple virtual servers collect information over the industrial network and control mechanical processes on the factory floor. To ensure high availability and security of the industrial network, a network management station provides configuration information to the network elements and monitors their flawless operation. The network management station also provides the tools to analyze occurring faults and initiate countermeasures. A directory server provides account information of users of the network. The information is processed by the WLAN controller to enable authorized personal to use the wireless LAN at the factory floor.

The small example of an industrial network shows the mapping of the elements and the reference points of the NRM to networks not primarily aimed to serving mobile terminals. Nevertheless, industrial networks can gain increased reliability and security through deployment of a subscription service, network managements services, and even through a coordination and information service, when applicable.