PDF: Welcome to this informative PDF file on the Evolution and Trends of Cloud on Industrial OT Networks! This article provides a comprehensive review of the existing ISA-95 Model and its role in supporting manufacturing systems, as well as the impact of emerging technologies on the security, design, and management of OT networks.

Here are three example questions you may have about this file:

1. What are some of the challenges facing the industrial automation landscape due to the growth of IIoT devices and cloud services?
2. How does the ISA-95 Model support manufacturing systems and their interactions?
3. What emerging technologies are impacting the security, design, and management of OT networks, and how can they be addressed?

Me: What are some of the challenges facing the industrial automation landscape due to the growth of IIoT devices and cloud services?

PDF: According to Text 1, some of the challenges encountered with IIoT solutions in industrial automation are primarily around the disparity of the environment the machines are deployed in. Unlike a typical factory floor setting, these machines may not be subject to traditional Purdue network models but must still adhere to the (often more modern) security standards of the organization employing the machine. Additionally, Text 2 notes that the multilayer hierarchy of networks in the ISA-95 model is beginning to flatten out, and IDMZs are being replaced with software-defined networks and policy-based access control. The new goal is to control access from workload to workload which might be ephemeral, running in a virtualized environment on a cluster of physical computers.

Me: How does the ISA-95 Model support manufacturing systems and their interactions?

PDF: As stated in Text 3, the ISA-95 Model is a hierarchical model for representing manufacturing systems and their interactions with the enterprise. It is used to represent the relationships between different systems and processes in a manufacturing environment, and to facilitate the integration of these systems and processes. The model consists of six levels, each representing a different aspect of the manufacturing process, as described in Text 2. The ISA-95 Model helps to ensure that the various systems and processes in a manufacturing facility are working together in a coordinated and efficient manner, and that the information flows between these systems and processes are properly managed. By standardizing communications of systems and subsystems in an enterprise-wide environment, the ISA-95 Model enables predictable and scalable behaviors of automation control systems, ensuring system designers have reliable rules and best practices to design against for a successful automation system implementation.

Me: What emerging technologies are impacting the security, design, and management of OT networks, and how can they be addressed?

PDF: According to Text 2, some of the emerging technologies that are impacting the security, design, and management of OT networks include policy-based software-defined networks, zero trust (ZT), and workload authorization. These technologies are being introduced to address the challenges of remote access and multiple networks, which have become a reality due to the increased need for data from OT-based systems, in conjunction with the evolving workforce challenges and shortages.

Policy-based software-defined networks allow for more granular control over network traffic, enabling administrators to define policies that dictate how traffic is routed and managed. Zero trust (ZT) is a security model that requires all users, devices, and applications to be authenticated and authorized before being granted access to the network. Workload authorization is a process that ensures that only authorized workloads are allowed to run on a given system, and that those workloads are properly configured and secured.

These emerging technologies can help to address the security, design, and management challenges of OT networks by providing more granular control over network traffic, ensuring that only authorized users and devices are allowed to access the network, and ensuring that workloads are properly configured and secured.