Quality of Service Aware Configuration of Network Equipment in Industrial Environments

György Kálmán
ABB Corporate Research
Norway
gyorgy.kalman@no.abb.com

Abstract—**Industrial Ethernet offers greater flexibility and potentially lower deployment costs than traditional fieldbuses. Ethernet is already the preferred communication technology from the controller and is expected to penetrate the instrument area also. Engineering and operation of these networks is introducing new challenges in the industrial automation field, including the lack of appropriate Quality of Service (QoS) metrics for these applications. This paper presents an overview of the industrial Ethernet landscape, shows the challenges around QoS parameters and shows an example engineering support function. Through this example, it presents different approaches and decisions taken for the proof of concept implementation. An overview about the issues related to representation and generation of configuration data, support of multiple vendors in the engineering phase and also during operation. The paper concludes with showing the differences between QoS metrics in industrial and office networks. The implemented proof-of-concept tool shows that bulk configuration of devices opens a QoS aware deployment process.**

Keywords*—*industrial Ethernet, QoS, metrics, engineering, infrastructure, switch, configuration, life cycle, multi vendor

I. Introduction

This paper is an extended version of [1], Mass Configuration of Network Devices in Industrial Environments presented at ICN2013. In addition to the original, the scope of the paper is extended with industrial QoS aspects to show, why automated or aided configuration of network devices is crucial in industrial environments.

A modern industrial communication system contains a considerable amount of nodes interconnected with Ethernet and current trends point towards moving the Ethernet connectivity down to instrument level. Having an all-Ethernet infrastructure offers several advantages over traditional fieldbus-based or Ethernet-fieldbus mixed networks. These include simpler deployment by using the same connectors and wires over the whole network, ample bandwidth, wide range of communication hardware and easy connectivity towards office networks or the internet.

One of the main drawbacks is a result of the inherently different network topology compared to office environments. In industry, the bus-like structure has proven to reduce costs with cutting cabling need. In these scenarios, the backbone is usually composed as a ring and the devices, sub networks or other devices are connected to this with small switches (up to approx. 10 ports).

In such structures, switched Ethernet is still operational but not at it's optimal parameters, as, e.g., collisions are eliminated

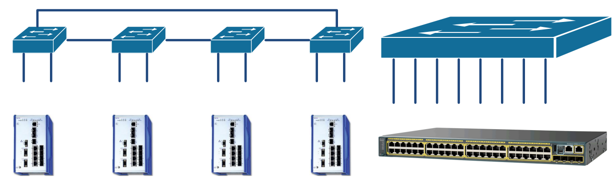

Fig. 1. Comparison of typical switch sizes in industry and other fields

but the traffic aggregation on the ring interfaces can lead to queueing. Important QoS parameters, e.g., convergence time and jitter are both negatively affected by the typical industrial topologies.

The use of small switches lead also to deep and sparse spanning trees which limit the performance of the Rapid Spanning Tree Protocol (RSTP) and have a negative impact on the reconfiguration time in case of link failure. Time synchronization of devices also suffers from the long distance between different part of the networks and has been mitigated by introducing the more precise IEEE 1588 Precision Time Protocol (PTP).

To mitigate the issues associated with the deep spanning trees and the growing RSTP convergence time, several industrial redundancy protocols were introduced from special versions of RSTP through proprietary ring protocols, doubled networks to overlay networks.

Engineering of networks composed from small switches results in typically a magnitude more devices than a comparable office network (e.g., a bigger refinery can have several hundreds of switches with a typical branching factor of 4-7) as shown on Figure 1. During engineering and Factory Acceptance Test (FAT), the effort of configuring these devices is high and severely influences the competitiveness. In the majority of cases, the actual configuration of the devices can be described with setting port-VLAN allocations, RSTP priorities, Simple Network Management Protocol (SNMP) parameters and performance monitoring. These steps currently require manual work, which is increasing cost during engineering and also leads to increased resource usage during FAT as configuration errors may happen.

QoS parameters are often evaluated at the end of the engineering process as part of the FAT which might result in an iterative process with changing structures. The main showstopper as the author can see, is that the QoS metrics used in office or telecommunication networks cannot be used directly in industrial networks.

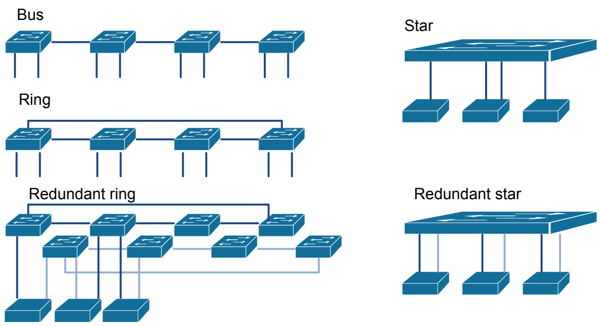

Fig. 2. Typical industrial Ethernet topologies

The primary aspects, which cause differences in the operation and hence the QoS metrics to be used are described in the following sections.

A. Topology

A key area, where industrial networks do differ considerably from their office counterparts is the topology used. In an office environment, the network is structured to resemble an equalized tree as much as possible. Also, high port density switches are used to lower the hierarchy levels in the network.

The industrial environment, as stated earlier, resembles more a bus-like topology. Ring-based redundancy solutions [2], traditional planning and cabling cost both force network engineering towards the use of rings as backbone and small switches to connect the few nodes which are located close.

Ring structures are beneficial for redundancy, but are problematic for traffic engineering. These rings aggregate traffic and force longer paths in the network than in a comparable office counterpart.

Ring mitigates the main risk of a bus topology by allowing the failure of one link and still keeping the network in operation. The long paths introduced by a bus however are still present. Where the constraints allow, it is beneficial to use a redundant star network [3].

B. Network segmentation

The traffic aggregation of rings do cause other issues too, especially if multi- or broadcast traffic is involved. In a typical installation, several industrial protocols are in use. In order to reach a more stable network and avoid that nodes are receiving unnecessary traffic, these networks are often segmented into several Virtual LANs (VLANs). The convergence of different networks on the same physical media also makes network management different compared to legacy systems.

C. Configuration and Maintenance

Current industry practice builds on a detailed network drawing and unit-to-unit configuration of the network devices as part of the deployment. Here, in most cases, the built-in web configuration solutions of the different vendors are used, although some provide their tools for own product lines which enable configuration of multiple units.

From the engineering viewpoint, setting up these devices one-by-one is a great risk, as the chance of human error is high. This risk is mitigated with additional resources, meaning more work hours to check the actual setup [4].

From maintenance viewpoint, this situation is even worse. Most installations have a long life expectancy and, therefore future maintenance engineers will either face 10-15 year old web interfaces if they have to modify something or the the problems associated with replacing the old device and migrating the configuration to a new one.

The purpose of this paper is to give an overview of the issues with the use of Ethernet in the industry-typical engineering practices and scenarios. These include network layout, QoS requirements, e.g., redundancy, time synchronization or maintenance and bulk configuration.

II. Quality of Service in Industrial Ethernet

Ethernet is expected to overtake the role as first choice for communication in industry installations for the majority of the cases. Although it is superior in bandwidth compared to any fieldbus used before, the past history of lacking determinism has raised concerns in the industry. The problems associated with traffic scheduling, prioritization and loss have been explored since both in industrial and other networks, mainly related to audio and video (AV) applications.

QoS is an objective measure of the network performance based on a defined set of metrics. For the AV applications the defined metrics include bandwidth, jitter, delay and loss. These are all relevant to the industrial applications, however, the weights cannot be mapped directly and in some cases the requirements are more strict in an industrial environment. An example would be the tolerance for jitter in industrial applications, in motion control (typically less than 1 ms) or factory automation (typically up to 10 ms). Since data in these examples are used in machine to machine communication, failing under delivery might lead to production stop resulting in direct economic loss instead of reduced user experience.

QoS solutions can be categorized into the two classes defined by IntServ and DiffServ.

A. IntServ

IntServ aims to implement QoS features that can enable to implement circuit switched like services on a packet switched network. It offers a fine grained system, where all nodes in the core network run IntServ and by using the Resource Reservation Protocol (RSVP) to create communication channels with end-to-end QoS. Resources along the whole path are reserved for the specific stream fulfilling absolute timing and bandwidth requirements.

B. DiffServ

DiffServ provides relative traffic prioritization and thus no absolute QoS parameters. Guarantees are not given and the traffic classification is only valid for the specific device. No end-to-end guarantees are given, also not for the insertion into a specific priority queue. The solution is more scalable, as the intermediate nodes do not need to keep track of all streams, there is no end-to-end resource reservation and only a few priority queues are used.

The two classes show the fundamental difference between absolute and relative QoS guarantees.

Currently, DiffServ is the preferred solution for internet traffic as this solution is scalable and offers good enough service quality assuming appropriate over provisioning of resources. The relative traffic priorities given by DiffServ however are not a perfect match for industrial applications. What industry expects is much closer to the granularity of what Asynchronous Transfer Mode (ATM) provided in the QoS field, or if some of the most critical applications are covered by technologies with intrinsic QoS (e.g., EtherCAT), by IntServ. Although not scalable, IntServ-like QoS can still be a valid solution for industry as critical traffic is either used only inside LANs or is transmitted over Synchronous Digital Hierarchy (SDH) or Multiprotocol Label Switching (MPLS) links with strict Service Level Agreements (SLAs). The implementation of an IntServ-like absolute traffic prioritization is however at the moment not a prime objective in industrial environments. The over provisioning of resources and the possibility to take demanding processes into a segment with intrinsic QoS allows the use of standard Ethernet with the existing, relative traffic prioritization and store-and-forward switching. If ample bandwidth is provided, a probabilistic upper bound with good confidence can be given on transmission parameters.

In addition to the AV-typical metrics, there are some network properties, which have to be taken into account in an industrial environment and can be addressed in the engineering phase. These are mostly caused by the specific structures and processes used. An example is the low branching factor. During engineering it is possible to aim for shorter paths in the network between critical nodes or to try to equalize at least parts of the network (e.g., using an AVL-tree [5]).

C. Industrial Ethernet overview

Industrial Ethernet is already the communication technology expected to be present from the controller to the operator workstations and beyond. In the field level, there are still some applications preferring fieldbuses but the trend here also shows the growing market share of Ethernet. In the following, industrial Ethernet is used to reference the use of Ethernet technology in industrial environments (on OSI Layer 2) despite that several of the industrial Ethernet protocols are in fact on upper layers.

Using switched Ethernet offers several benefits in the industrial field, including:

- high bandwidth,
- off the shelf, low cost technology,
- seamless integration with office and telecommunication networks,
- network convergence incorporating automation, security and safety.

In [3], the traditional split of three different networks used in the industrial field is shown. The structure shows a heritage

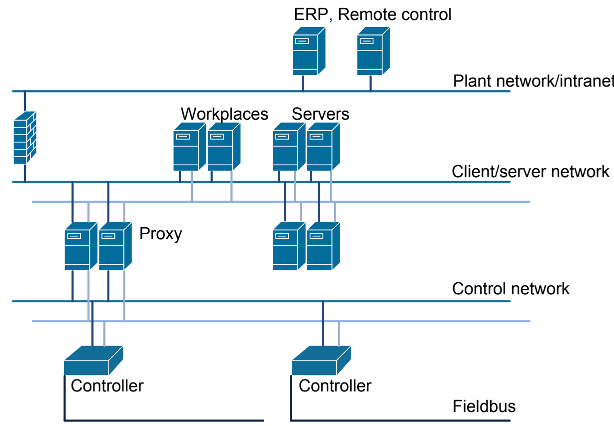

Fig. 3. Automation network hierarchy

of the field buses what explains the frequently used bus and ring topologies.

Considerable efforts in industrial network research are spent on the fields of QoS, time synchronization, redundancy and network convergence.

One of the main assumed drawbacks of Ethernet in automation was the CSMA/CD algorithm used for multiple access. Although the problem of collisions is not present any more (as all networks are implemented as switched, full-duplex Ethernet and thus CSMA/CD is not being run), the probabilistic nature of Ethernet has raised severe concerns on Ethernet's capability to replace strictly scheduled fieldbuses despite the much higher available bandwidth [7]. Industrial applications are now shifting towards the use of 1G links also for the field and control network level, thus traffic, except high frequency control and sampling, can be carried with standard Ethernet equipment.

Data refresh rates differ depending on the field and usage of the industrial network.

Class	Grace time	Desciption
Uncritical	<10 s	ERP, Manufacturing
Automation	<1 s	human interface
Benign	<100 ms	process, manufacturing
Critical	<10 ms	synchronized drives

For high refresh rates and hard-real time applications several technologies have been developed, where EtherCAT is one of the most popular solutions.

EtherCAT implements a ring with a master device connected to both ends and slaves chained on the ring. The master sends out the frames on the network and the slaves, while the signals are passing through the network interface, are exchanging information (Figure 4). The frame is not stored in any way on the slaves and the latency in crossing the EtherCAT ring is fixed. EtherCAT is offering intrinsic QoS, as the jitter is practically 0, the cycle times can be calculated prior to deployment and time synchronization is provided through a distributed clock synchronization algorithm.

The master can be connected to the rest of the industrial network with an additional network interface.

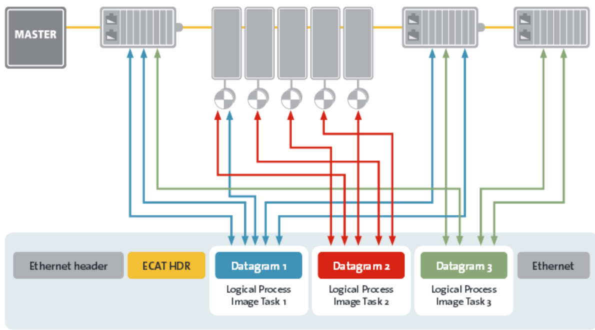

Fig. 4. Structure of the EtherCAT frame [8]

D. Time synchronization

The need for synchronized operation throughout the network is required by most applications, although the precision need and the impact of keeping the limit differs. In a typical non-industrial example system, like a stock exchange system or Enterprise Resource Planning (ERP) the precision limit is more relaxed than, e.g., controlling a surveyor belt, where the high-speed belt is driven by hundreds of electric motors which need to operate synchronous to change the overall speed. The required degree of accuracy also depends on the specific application.

In non-industrial applications, typically the precision reached by Network Time Protocol (NTP) is adequate, while industrial efforts and lately also audio-video standardization is expecting IEEE 1588 Precision Time Protocol (PTP) to serve as synchronization protocol. The combined effort of industry and AV fields are also shown in, that the original IEEE Audio-Video Bridging task group has changed name to Time-Sensitive Networking incorporating also automation.

The synchronization of the local and the system clock is achieved by periodic exchange of messages. Both SNTP and PTP offer by default a system-wide relative clock synchronization which is enabling the operation of the process. In case absolute time synchronization is required (e.g., logging of events also between different networks), a suitable external time source is required. As an example, the GPS service or a land-based clock signal can serve as a high precision time source. Synchronization to a global time reference is also required if the system is composed from different installations where there is no possibility of a direct network-wide time synchronization solution.

1) Network Time Protocol: NTP can provide a satisfactory synchronization service [9] if the required precision is in the 10s of milliseconds range or millisecond range if SNTP is used [10]. The protocol is implemented as a software-only component [11] and is widely supported. Despite the relative precision of the protocol, in most cases the precision requirement of industrial Ethernet networks does require higher precision, which requires the use of PTP.

2) Precision Time Protocol: PTP was defined to allow much more precise time synchronization [12] and as such allow the use of Ethernet for applications where the time precision throughout the network needs to read nanosecond range. To reach the required precision, PTP is using hardware support, a timestamping mechanism integrated into the network adapter of the nodes. The close connection to the NIC is also a limitation, as currently it can only be used on Ethernet networks [13]. The upcoming v3 splits the protocol into a hardware dependent and independent part and opens for different physical bearers.

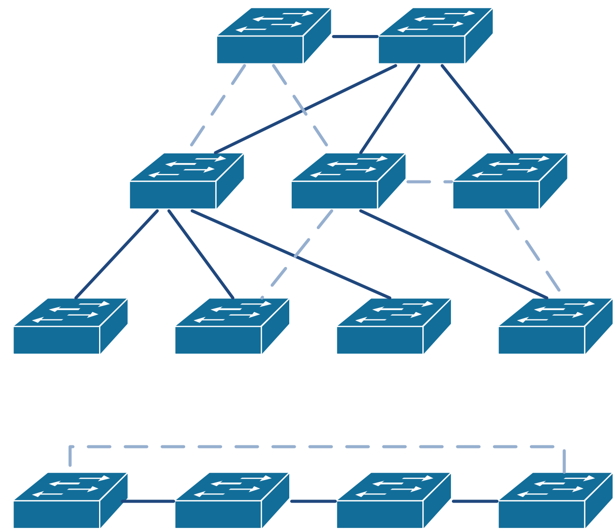

Fig. 5. RSTP redundancy is provided by stand-by links

3) IEEE 802.1AS: The protocol implements a strictly-defined subset of PTP while extending the usage area towards wireless LANs and other physical media than wired Ethernet. The objective was to provide a precision timing solution for AV purposes. As the split of the protocol between hardware dependent and independent layers was successful, in PTP v3, a similar approach is suggested.

III. Redundancy

Network redundancy is an important availability requirement for industrial applications. In upper network levels, the controller and the client/server network, dual-homed devices are common. The actual network redundancy protocol is however dependent on the application area and the supplier.

The simplest solutions offer the use of RSTP and implement stand-by redundancy by offering backup links, which can be enabled in case the primary fails. Typical physical topologies include bus, ring and tree structures.

The bus structure is not preferred as one failure might render large parts of the network inaccessible, but it might be used as one segment of a redundant network.

The reconfiguration time is a decisive QoS parameter for selecting the correct redundancy protocol.

A. Rapid Spanning Tree

RSTP is calculating a minimal-cost spanning tree of an Ethernet network. It is an IEEE protocol incorporated into the IEEE 802.1D standard. While RSTP was designed primarily for loop-avoidance, it is the primary choice for network redundancy in cases where a moderate but not bumpless

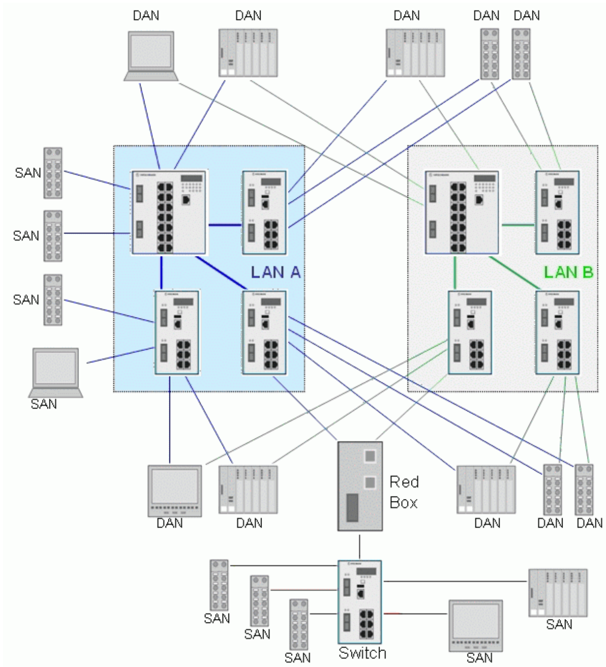

Fig. 6. PRP redundancy [14]

reconfiguration of the network path is acceptable (e.g., process automation).

Extensive research has been executed for evaluation RSTP performance and many automation network equipment suppliers have developed their own flavor of RSTP. The biggest advantage using RSTP is, that it does not require special support in the core network or at the end nodes. The default performance is acceptable where grace periods of several seconds are allowed, which is extended to a part of the factory automation field by the vendor-specific enhancements.

B. IEC 62439

As RSTP was unable to meet some redundancy requirements, a wide range of proprietary redundancy protocols were introduced for industrial Ethernet. IEC has initiated a standardization effort for high availability automation network redundancy, which resulted in the IEC 62439 family of standards. The standard describes several protocols and also references RSTP. From the availability viewpoint, in addition to the standby redundancy provided by, e.g., RSTP, IEC 62439-3 defines two seamless redundancy protocols, Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR). These two protocols provide zero switchover time, as the data is sent always on two networks in the same time.

1) PRP: is one of the two bumpless protocols defined in IEC 62439 and as such offer the highest QoS for redundancy with the deployment of a full reserve network. The two networks are in parallel operation and data is transmitted continuously over the two interfaces. A merge layer is included between the link and network layer to suppress duplicate frames at the receiver. The topology of the network is a tree with double-homed nodes. Single-attached nodes (without redundancy) are also supported.

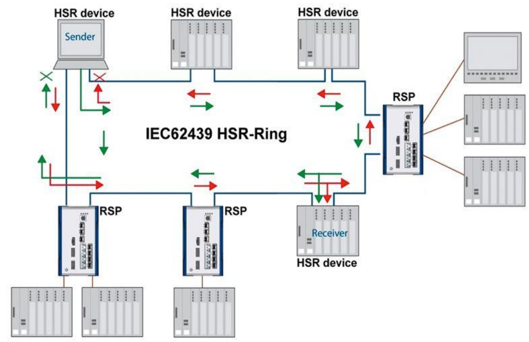

Fig. 7. HSR redundancy [14]

2) HSR: implements a two-directional ring and is sending traffic in both directions simultaneously. This solution does not require a double network infrastructure, but is using more bandwidth, as the core has to be able to carry all traffic aggregated and doubled. Special hardware for all nodes is required, single-attached nodes are supported through the use of a redundant coupler module (RedBox).

C. Convergence in Industrial Ethernet

Ethernet offers a key feature for further optimization of networks, the possibility to use it as a single communication solution which carries both automation, safety, security, communication and other network traffic. The available bandwidth and prioritization solutions allow effective use the network without compromising service quality [3]. An example for safety integrated systems is Safety over EtherCAT [8].

The use of shared infrastructure is still seen as problematic from the QoS viewpoint. It is accepted that in a typical case Ethernet can provide the necessary QoS levels but the lack of composite traffic models and scepticism for shared links is limiting the spread of using the same physical links for different classes of traffic. Most of the issues are raised in connection with Safety Integrated Systems (SIS), where the safety function is using the same communication medium as other parts of the automation network. Stakeholders are concerned about that the probabilistic transmission or network failure will stop the safety function. In contrast, the operation principle used in SIS is that if the safety message is not arriving in time, the system is going into safe state, thus the safety function is intact, but the uptime of the process suffers. From the QoS viewpoint this behavior results in both delay and loss requirements, but probabilistic QoS might be acceptable as only the process uptime is threatened but not the safety in case of the network is failing to meet the QoS parameters.

Using QoS aware planning and appropriate traffic models can however change the scepticism and result in better overall performance. To prove that engineering can be supported with tooling to achieve better QoS a proof-of-concept tool was implemented. The tool shows that engineering aspects can be used to ensure the use of available prioritization solutions, time synchronization and redundancy solutions.

IV. PROOF OF CONCEPT

The motivation behind this work was to reduce engineering costs and to explore possible solutions for providerindependent configuration representation and setup of multiple devices in the same time [15], [16]. The potential cost reduction in the engineering phase is expected to reach 20-25% of the total cost, not counting the life cycle support.

The review of a project portfolio revealed that in most installations 2-3 vendors are involved in supplying network infrastructure based on various preferences. Although the planning of the network is done independently from the actual manufacturers, the configuration and acceptance checks do depend on per vendor knowledge and tools.

The expected result of the research task was in addition to explore possible solutions, to create a proof-of-concept tool, which can compose, deploy and modify configuration of one or multiple Ethernet switches in the same work session.

In long-term, the vision of a common configuration and management tool was defined, where planning, configuration, as-planned checking, monitoring and life cycle management was provided. Such a tool could offer a common interface to plan a network with defining the segmentation and port distribution (this covers the current network drawing step), generate configuration for the devices (which is done typically by engineers), deploy and then through discovery, check that the network has the same structure as planned (for example the VLANs are set up correctly). During operation, the tool could read out the current configuration from a device and upload it to a replacement unit, even if these are from different manufacturers.

V. Hardware

To explore configuration possibilities, remote configuration features of selected product lines were reviewed:

- *RuggedCom RS9xx* [17]: This switch line supports configuration update using a built-in Trivial FTP (TFTP) client or server, depending on requirements. In addition, Secure Copy (SCP), terminal with Command Line Interface (CLI) and SNMP is supported for file and configuration manipulation. As all of the reviewed managed switches, this unit offers a web interface. A vendor-specific tool for monitoring is available.
- *Hirschmann RSRxx* [18]: This switch line offers a TFTP Client, CLI access through telnet or the web interface, a java-based web interface, SCP file transfers and a proprietary Automatic Configuration Adapter. This adapter, if physically connected to the device, uploads or downloads configuration enabling easy replacement from the same vendor.
- *Moxa EDS-508* [19]: Has TFTP server and client, CLI, SCP transfers and offers a web interface. A proprietary Auto-Backup Configurator is offered for backup and restore, allowing easy replacement from the same vendor.

The research also showed that SNMP is supported on all units, although the features were focused on monitoring and not on configuration.

The review showed considerable differences between web interface structures and the available options. The differences were big enough to limit reuse of configuration knowledge and proved to support the initial assumption about cost reduction potential.

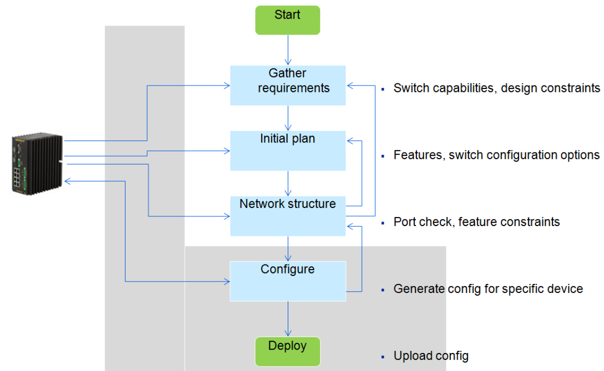

Fig. 8. Proof of concept coverage

Configuration data was accessible on all devices as structured text files, which were human readable and could be a base for the configuration tool design. In Figure 8, the expected coverage of a configuration tool is shown. The objective was to allow up- and downloading, manipulation and storage of configuration information.

A. Multiple unit configuration

One of the most important features was to check the feasibility of configuring multiple units in the same time and to explore the possible issues.

As part of the planning, a feature set was identified, which were set the same on all devices or could be calculated automatically. An example is the selection of the RSTP root bridge.

Other questions were risen in connection with the long paths and rings used in these networks. It was assumed, that depending on the behavior of the devices, the configuration might need to be topology aware.

The user interface was also a crucial point, as the objective was to reduce engineering cost, which pointed towards a simpler interface than most of the switches offered. This request was supported by, that only a handful of features needed to be set and most of the parameters were left at factory defaults.

VI. Engineering tool example

The implementation was focused on a subset of the possible features. Based on feedback from engineering, configuration of multiple devices and support of multiple vendors were selected as key features, which should be supported by a simple user interface. In Figures 9 and 10, the test user interface is shown for single- and multi-unit mode.

The planned system was designed to cover tasks associated with configuration and deployment stages of the engineering process. To ensure, that options, which are not being used by the system are preserved, the tool only replaces relevant parts of the original configuration files with new data 11.

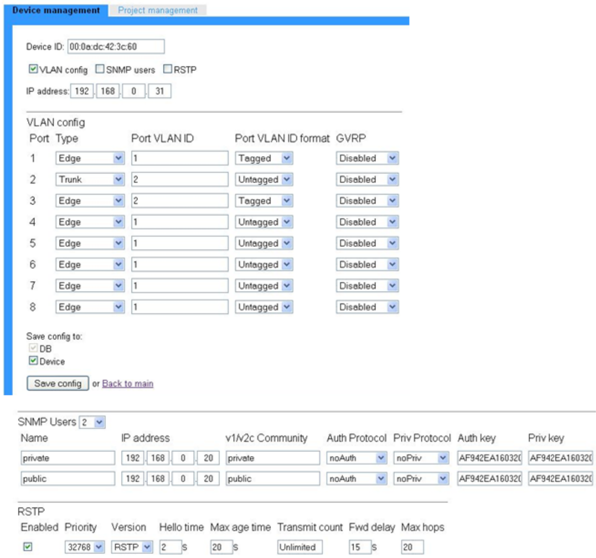

Fig. 9. Single unit configuration

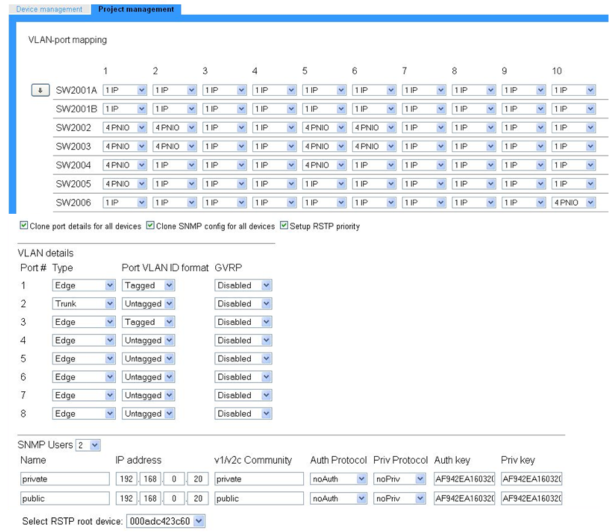

Fig. 10. Multiple unit configuration

A. Requirements

- vendor independent, simple user interface
- remote configuration of one or multiple devices
- life cycle support with configuration versioning and cloning
- configure selected features

B. Features

A subset of available features on the switches was selected based on experiences from engineering. This set was planned to cover most of the engineering needs without resulting in a complex interface.

The feature set was defined for both single and multi mode as:

- *Host IP*: to be able to set the device's IP
- *Port-based VLAN*: allow the setup of per-port VLANs
- *SNMP setup*: configure SNMP access rights and community memberships
- *Spanning Tree*: select STP protocol and allow changes in bridge priority

To support documentation, an automatic network documentation generator function was also included.

A single unit configuration section was included for practical purposes and served also as a testbed for checking the configuration generation capabilities.

The system was designed so, that it would preserve changes made outside the configuration tool (thus allowing device specific configuration for features not covered by the tool), so the composition of the configuration data was implemented in a way, that it is only changing the relevant part and keeps the rest of the data untouched (Figure 11.

C. Multiple vendor support

Enabling support for multiple vendors has risen several issues, which were not foreseen. Even if all the switches covered were complying the same IEEE standards, the actual implementation and availability of features depends on the vendor.

As a result, a vendor independent representation of the configuration data was needed and the configuration generation process had to be split into storage, representation and actual configuration data.

D. Multiple device support

Configuring multiple devices in one session was considered as the most important feature, as this would result in the highest cost cut. Covering multiple devices also meant that the difference between the per unit web interfaces and the configuration tool might be the most emphasized.

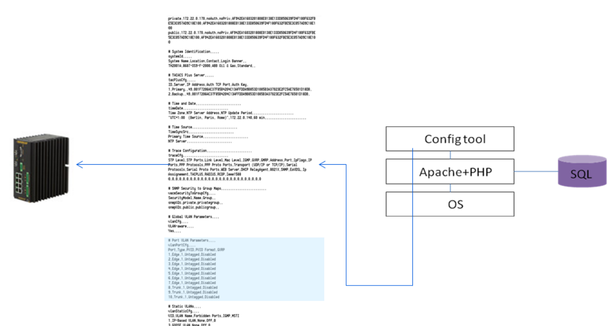

Fig. 11. Composition of the configuration

For the IP configuration and VLAN settings, a matrix of switches and VLANs was generated. This offers a single-screen overview of a typical network in the evaluated projects. The drawback of this representation is, that if a large number of ports and switches are used, the size of the matrix is getting large. This limitation was found acceptable in this case, as in a typical industrial environment low port count switches are used, so adding more switches will result in a longer matrix, but the width will stay limited.

The tool offers cloning of the port and SNMP settings to all devices and setting the root RSTP bridge.

E. Connectivity

The review of connectivity methods has shown that it is problematic to choose one specific solution. Even in case of just the three product lines reviewed, different protocols turned out to be easier to use.

For the proof of concept, for one vendor (RuggedCom) TFTP was chosen for up- and downloading configuration data. For the other vendor (Hirschmann), CLI-based configuration and telnet. While being aware, that none of these protocols provide secure transfers, this requirement was relaxed for the current version. This decision was supported by that the tool is intended to be used during engineering, where these networks operate as isolated islands.

VII. Lessons learned

There are several important issues that were identified during the evaluation and development of the configuration tool.

A. Vendor independent configuration data

In order to support multiple vendors, the configuration data needs to be stored in an independent format. Generation of the appropriate configuration file or script depends on the vendor's implementation and there might be considerable differences.

Changes between vendors in most of the cases results in information loss about the configuration of the device. An example is the support of vendor specific spanning tree protocols. The use of these proprietary protocols is beneficial if the network is homogeneous, but might cause problems if multiple vendors are present. If the original configuration was set up, e.g., to use RuggedCom's eRSTP and the device is replaced with another manufacturer's switch, the configuration tool has to fall back on, e.g., RSTP, as that is the nearest standard protocol which is supported by the new device.

If later the device is changed back (e.g., a device needed to be taken out from the network and was temporarily replaced by another), if the configuration storage depends on the vendor, then only RSTP will be used even if eRSTP is available, as the migration process will only create a representation of the current configuration in the new device.

B. Topology-awareness

An interesting issue with configuration was raised while the tests of the multiple unit configuration were executed. In single unit mode, there were no problems, the configuration was updated, the device was reset and after some seconds, network operation was restored. The same happened if multiple units were configured in an office-like topology (equalized tree), where only a few levels of switches were involved and the longest path was 3-4 hops. In case of industry-typical rings, anomalies and connectivity errors happened.

The investigation showed that while the update operation itself is done in a fraction of a second and it takes approximately 2-3 seconds for a device to reset, this was too short to update all members of the ring. In the tree topology, the devices were updated before the first unit decided to reset. In the ring, however, these resets happened before all members were updated. The result was that the network was falling into fractions and in some cases one had to approach each *lost* device separately.

As a result, it was identified that it would be beneficial if in case of multiple unit configuration, the update would be done with respect to the topology, starting from the leaves and progressing upwards in the tree. The same approach can be used in rings, as these will be represented as a long unbalanced tree (in normal operation RSTP is disabling the redundant link to avoid a loop).

C. Identical configurations

Although the switches used in this work were not the most complex units available, it turned out to be a complicated task to reach exactly the same configuration on devices from different vendors.

A typical example is the configuration of a trunk port. In one case, this option was available directly on the web interface and in the configuration file, but on a different switch at least 6 commands in the CLI were required.

Another example is the above mentioned case of RSTP. In practice, all major vendors have their own enhancements to RSTP to achieve better convergence times. This also means, that these proprietary solutions can only used on homogeneous fractions of the network. If a device is replaced by a device from a different vendor can result in weaker performance, as all the units have to fall back on the first standard solution, which in most cases will be RSTP.

VIII. Applying QoS functions in engineering

Using the proof-of-concept as starting point, possible extensions towards QoS aware design were explored. The objective was to support more of the typical engineering tasks while optimizing the use of available QoS functions. These include traffic prioritization, optimization, topology optimization and time synchronization [20], [21].

The first field was topology awareness. One of the important aspects were to support the automatic inclusion of default spares, which can be later used either for redundancy or for extensions. Other properties were the automatic inclusion of redundant links to reach a specific level of redundancy in a spanning tree structure.

A. Topology generation

The size of the network has a negative impact on the achievable QoS. The engineering tool could, within defined limits, aim for reducing the network's critical parameters and provide an updated approximation of QoS parameters. In topology engineering, the primary goal with regard to delay and reconfiguration time is to reduce the longest critical path.

First the critical path can be identified using Critical Path Method (CPM) and then equalized with a tree-equalization algorithm. The equalization can be supported by the configuration tool with allowing the exchange of network infrastructure with low effort (e.g., a larger port count switch instead of a smaller one).

When the topology is finalized, protocols running on the network might be optimized further, e.g., by manual assignment of the RSTP root bridge, which has an optimal place in the *middle* of the network: the point most centrally located with regard to network paths.

If the QoS requirements cannot be fulfilled with the actual design (e.g., redundancy offered by RSTP), the engineer can be informed and the network topology can be transformed in order to meet the requirements. This can, e.g., result in changing a ring network into a redundant star (shorter paths with the expense of higher cabling cost) or adding a secondary network (if bumpless redundancy is required).

In case the QoS requirements of the critical path cannot be fulfilled with topology manipulation, a technology with intrinsic QoS can be recommended. The proof-of-concept although supports configuration of several devices, the connection between them is implicit and the tool has no information about the planned topology.

B. Traffic prioritization

Traffic prioritization in Ethernet is offering a feature which can be easily configured and achieves a level of DiffServ-like operation with relative-priority traffic classes. Network devices support a number of priority queues and important traffic is preempting less important frames. Depending on the prioritization scheme, a probabilistic value for network delay and loss can be given for the specific traffic classes. These classes can be shared between several different traffic sources, which might result in internal queueing. The correct selection of the traffic to priority mapping is important for the desired operation. Strict priorities might lead to excessive delays on low priority traffic if the higher priority traffic is utilizing most of the available bandwidth. To avoid exhaustion, the loose policy is supporting not only priority and First In First Out (FIFO) scheduling of the priority queues but also ageing between the queues.

In an engineering tool, the priority-traffic mappings could be done automatically in addition to the selection of scheduling policy.

C. Traffic optimization

Multicast and broadcast is often used in automation protocols. Aggregation of traffic on LANs is less important in a non-industrial environment, primarily because of the less strict QoS requirements and the flatter architecture. In the industry-typical ring topologies, where traffic is aggregated between a high number of nodes, it can be beneficial to use traffic aggregation to avoid queueing. During engineering, multicast grouping protocols like Internet Group Management Protocol (IGMP) can be used.

D. Time synchronization

Time synchronization is a critical feature on industrial networks and some aspects have to be supported in the engineering phase. The selection of the synchronization protocol used poses different requirements towards the infrastructure elements. SNTP is generally supported in all network equipment, and since it is software only, it can be also deployed in nodes which does not support it by default. PTP on the other hand requires hardware support for the preferred precision and thus limits the possible range of network equipment used.

IX. Engineering support

There is a considerable potential to cut costs in network engineering if appropriate tools are available. Although network management software are available and widely used in office environments, their resource need and cost render them unrealistic for industrial deployment.

The proof of concept implementation of a configuration tool, which can partially automate the setup of Ethernet switches aims to reduce the engineering complexity and to support QoS aware planning and deployment of networks. The main difference compared to proprietary solutions is, that this tool supports multiple vendors and with a vendor independent representation of configuration data, also allows future extensions.

Testing of the tool revealed several issues associated with device configuration, especially related to problems caused by the topology and the complexity of generating identical configurations for switches from different vendors.

X. Conclusion

QoS is an important property of a communication network, independently whether it is used in an industrial or another environment. The issues associated with providing specific service levels on an inherently non-deterministic packet switched network are the same, although the importance of the metrics differ.

The uncertainty related to the probabilistic transfer time bounds provided by Ethernet initially cause scepticism towards the extended use of the technology. Most of these negative opinions have roots in the past and refer to problems which are mostly non-existent on current, typically 1G, full-duplex, switched networks. To ensure, that Ethernet can successfully overtake as primary communication technology on all levels of industrial networks, a set of QoS metrics need to be defined with appropriate weights to allow calculation of expected network performance.

Current metrics and weights are focused on different applications, mostly AV, whereas industrial uses require a different weight composition. The paper has pointed out several of these metrics, e.g., redundancy, time synchronization, prioritization, packet loss and delay which are more important in the industrial field than in AV in contrast to, e.g., bandwidth, which in the majority of cases is not a primary concern in industrial environments.

Industrial topologies are also introducing problems which were considered as non-existent in the office domain because of different network structures. Rings and deep trees are possibly avoided in other networks but are preferred in the industry sector. The depth of an industrial network can be approximated with, e.g., $(O)(\log_6 n)$ versus the office $(O)(\log_{16} n)$ where 6 and 16 is the branching factor, *n* is the number of nodes. This results in a weaker operation of several protocols (like RSTP) and result in a worse QoS.

A proof-of-concept implementation of a bulk configuration tool is shown, which can serve as a basis for a more complex network engineering and support system. Bulk configuration of devices is the first step towards using already existing QoS functions in industrial applications without requiring expert knowledge during planning and commissioning.

The possible extension of the tool with topology manipulation will enhance the QoS of the system by transformations using well-known algorithms and open for selecting critical areas, where the required parameters can only be reached by using intrinsic QoS technologies.

REFERENCES

[1] Gy. Kálmán, Mass Configuration of Network Devices in Industrial Environments, in Proceedings of International Conference on Networks (ICN) 2013, pp. 107-111

[2] Kleineberg et.al., Automatic device configuration for Ethernet ring redundancy protocols, Emerging Technology and Factory Automation (ETFA) 2009.

[3] Industrial Ethernet: A Control Engineer's Guide, Cisco White Paper, 2010.

[4] C. Rojas, P. Morell, Guidelines for Industrial Ethernet infrastructure implementation: A control engineer's guide, IEEE IAS/PCA 2010.

[5] G. Adelson-Velskii, E. M. Landis, An algorithm for the organization of information, Proceedings of the USSR Academy of Sciences 146, pp. 263-266. (Russian) English translation by Myron J. Ricci in Soviet Math. Doklady, 3:1259-1263, 1962.

[6] H. Kirrmann, Highly Available Automation Networks, Standard Redundancy Methods, Rationales behind the IEC 62439 standard suite, ABB, 2012.

[7] Communication Networks and Systems in Substations - Part 5 Communication Requirements for Functions and Device Models, IEC 61850-5, 2003.

[8] EtherCAT Technology Brochure, EtherCAT Technology Group, November, 2012.

[9] D.L. Mills, A Brief History of NTP Time: Confessions of an Internet Timekeeper, ACM SIGCOMM, Computer Communication Review, vol. 33, no. 2, pp. 9-22, April 2003.

[10] M. Ussoli, G. Prytz, SNTP Time Synchronization Accuracy Measurements, Emerging Technology and Factory Automation (ETFA) 2013.

[11] P. Ferrari, A. Flammini, S. Rinaldi, A. Bondavalli, F. Brancati, Experimental Characterization of Uncertainty Sources in a Software-only Synchronization System, IEEE Transactions on Instrumentation and Measurement, vol. 61, no 5, pp. 1512-1521, May 2012.

[12] T. Neagoe, V. Cristea, L. Banica, NTP Versus PTP in Computer Networks Time Synchronization, in Proceedings of IEEE International Symposium on Industrial Electronics, 2006, vol. 1, pp. 317-362.

[13] IEEE Standard for a Precision Clock Synchronization Protocol of Networked Measurement and Control Systems, IEEE Std 1588-2008, 2008.

[14] Media Redundancy Concepts, High Availability in Industrial Ethernet, Hirschmann White Paper, 2011.

[15] Imtiaz et.al., A novel method for auto configuration of Realtime Ethernet Networks, Emerging Technology and Factory Automation (ETFA) 2008.

[16] Reinhart et.al., Automatic Configuration (Plug & Produce) of Industrial Ethernet Networks, INDUSCON 2010.

[17] Rugged Operating System v3.10 User Guide, Ruggedcom, January 19th, 2012.

[18] Reference Manual, Command Line Interface Industrial Ethernet Gigabit Switch Release 7.0, Hirschmann, 2011.

[19] Datasheet, EDS-508, Moxa, 2010. May 5th

[20] P. Ferrari, A. Flammini, S. Rinaldi, E. Sisinni, On the Seamless Interconnection of IEEE 1588-based Devices Using a PROFINET IO Infrastructure, IEEE Transactions on Industrial Informatics, vol. 6, no. 3, pp. 381-392, August 2010.

[21] G. Gaderer, P. Loschmidt, T. Sauter, Quality Monitoring in Clock Synchronized Distributed Systems, in Proceedings of IEEE International Workshop on Factory Communication Systems, pp. 13-21.