# Dependability and Security Aspects of Network-Centric Control

Björn Leander*†, Bjarne Johansson*†, Tomas Lindström*
Olof Holmgren*, Thomas Nolte†, Alessandro V. Papadopoulos†
* ABB Process Automation, Process Control Platform, Västerås, Sweden, {tomas.lindstrom, olof.holmgren}@se.abb.com
† Mälardalen University, Västerås, Sweden, {bjorn.leander, bjarne.johansson, thomas.nolte,alesandro.papadopoulos}@mdu.se

***Abstract*—Industrial automation and control systems are responsible for running our most important infrastructures, providing electricity and clean water, producing medicine and food, along with many other services and products we take for granted. The safe and secure operation of these systems is therefore of great importance.**

**One of the emerging trends in industrial automation systems is the transition from static hierarchical controller-centric systems to flexible network-centric systems. This transition has a great impact on the characteristics of industrial automation systems. In this article we describe the network-centric design strategy for industrial automation systems and describe the impact on dependability and security aspects that this strategy brings, looking at both challenges and possibilities.**

## I. Introduction

The safe and secure operation of industrial automation systems is of great importance, from an economic and societal perspective. Therefore, understanding the dependability and security impact on emerging technical design strategies is paramount.

Traditional manufacturing systems are optimized for high-volume production of identical products, resulting in complex and specialized systems, which are costly and difficult to retrofit to adapting changing production demands, new innovations, and customized products. Evolving technologies within the Industry 4.0 paradigm aims toward design strategies for cost-efficient production environments that allow fast adaptations to fluctuating demands, innovations, and customized products. These evolving system design strategies, such as Modular Automation [1], have a fundamental impact on the technical characteristics of the system.

From a control systems perspective, one of the major enabling technical trends for Industry 4.0 is the transition towards a service-oriented approach throughout the system. Different services will need access to different signals, and even process control is seen as a service among many others. This approach leads to a design strategy that we call Network-Centric Control (NCC) [2], as compared to Controller-Centric Control (CCC) which is the current norm in control systems architectures.

**Problem statement.** The transition from CCC to NCC has a huge impact on the dependability aspects of an industrial control system. With NCC the Operational Technology (OT) is definitely parting with hard-wired point-to-point connections between a controller and its sensors and actuators, instead using ubiquitous networking techniques for these interactions. Even though the trend toward NCC has been going on for many years, there is a lack of a stringent description of exactly what it is, and how it compares to previous design strategies, with regard to security and dependability aspects. The background on this problem and previous related works are further described in Section II.

**Research objective.** With this paper, we aim to describe the network-centric architecture for industrial control systems and to systematically describe its challenges and solutions related to dependability and security attributes. Dependability is co-dependent on security [3], and therefore dependability attributes are complemented with security attributes derived from the IEC 62443 standard which is one of the most used cybersecurity standards for industrial automation and control systems.

**Contributions.** The main contributions are:

- A description of the design strategy for NCC. (Section III)
- Correlation of classical dependability attributes with foundational security requirements as defined in the IEC 62443 standard. (Section IV)
- A description of technical concerns related to NCC on security and dependability attributes. (Section V)
- Challenges and opportunities related to NCC implementations. (Section VI)

Also in Section VI, the results are summarized and possible future directions of work are outlined.

## II. Background and Related Work

In 2009, Thyrbom et al. mentioned an emerging trend toward NCC in Distributed Control Systems (DCSs) [2] and in 2014 Van Lier [4] identified NCC as an enabling concept for Industry 4.0 from a systems perspective. Moreover, in the Open Process Automation Standard (O-PAS) Part 1 by the Open Group[1], a technical architecture concept is described, which is closely related to the NCC architecture in that it describes communication between different distributed control nodes using a unified connectivity framework. However, none of the above clearly defines the NCC architecture for distributed control, and such a definition is, to the best of the authors' knowledge, non-existing.

We will consider NCC architectures utilizing Switched Ethernet, with available dependability properties for Time

[1] www.opengroup.org

Sensitive Network (TSN) amendments and Open Process Communication Unified Architecture (OPC UA), utilizing the publish-subscribe pattern for cyclic process data exchange and client-server for configuration and high-level control.

Among previous works, Alvarez *et al.* [5] provides an overview of fault-tolerant Ethernet and Zanasi *et al.* [6], and Tange *et al.* [7], which provide a survey of IIoT security requirements.

As security and dependability are interdependent [3], we discuss aspects of both and their interplay and effects on NCC. We aim to make a holistic overview of NCC and its impact on dependability and security attributes of an industrial control system.

## III. Architectures

### A. Controller-centric architecture

Hierarchical, controller-centric architectures have traditionally dominated DCS design. CCC means that a controller manages a set of Input/Output (I/O) signals connected through a fieldbus protocol [8], see Fig. 1a. It provides low latency and hard real-time guarantees but has limitations regarding flexibility, bandwidth, and interoperability [9]. The controller pair that form the controller redundancy in the controller-centric paradigm are often physically near and connect with a dedicated link for redundancy-related communication[2].

### B. Network-centric architecture

Following an NCC architecture, all entities in the control system are expected to be physically or logically connected to the same network. To allow for high flexibility, access to resources on this network is following a service-oriented approach. In practice, this means that, e.g., a controller can access any I/O, regardless of where the signal is physically connected.

Communication between entities in the system must follow a standardized protocol, with OPC UA being one of the currently most widely accepted alternatives, prescribed by the O-PAS Standard. The usage of a widely adapted interoperable standard allows for a control system owner to mix devices from different vendors as is best suited for its needs. O-PAS connectivity framework is the O-PAS terminology for the logic network shown in Fig. 1b.

An NCC architecture with hardware-agnostic redundancy allows a flexible redundancy. For example, combining orchestrator-based failure recovery with the controller redundancy or utilizing computational power in the device-cloud continuum as a backup [10].

### C. Trust-models

Traditionally, security in CCC is focused on network segmentation with strong perimeter protection and security zoning. Within the zones, the interaction between entities is in general permitted. This security model is based on *implicit trust*, in that an entity is trusted based on its logical or physical address. The controllers in CCC are usually *dual homed*, with the north side connected to a system network and the south side connected to I/O and field equipment. The controllers do not route traffic directly from one side to the other. This means that the controllers act as gateways between the north zone and the south zone, which aligns well with the implicit trust model. CCC can be seen as the implementation of the segmentation between level 0 and level 1 in the Purdue [11] model for the security zoning of industrial control systems.

Zero-trust is used to describe a cybersecurity paradigm that moves from static network-based perimeter protection with implicit trust within a network, toward explicit per-use authentication and authorization [12]. Zero-trust is originally a response to the Bring Your Own Device (BYOD) trend in enterprise networks, embodied by the widespread use of, e.g., personal cell-phones, tablets, and smartwatches at work, connected to office networks.

In NCC there is an increasing volume of interconnections between entities in the system, including edge and cloud-connected services, based on service-oriented architectures and digital entities with more autonomous behavior. The use of wireless devices such as cell-phones and tablets is also becoming more common within industrial networks[3]. These technological advances and evolving characteristics of Industrial Automation and Control Systems (IACS) related to NCC, as well as the increasingly hostile environment with regards to cyber-threats [13], implies the need of redefining the trust models used for industrial networks, with zero-trust as a viable model also for these systems [6].

## IV. Correlating security requirements and dependability attributes

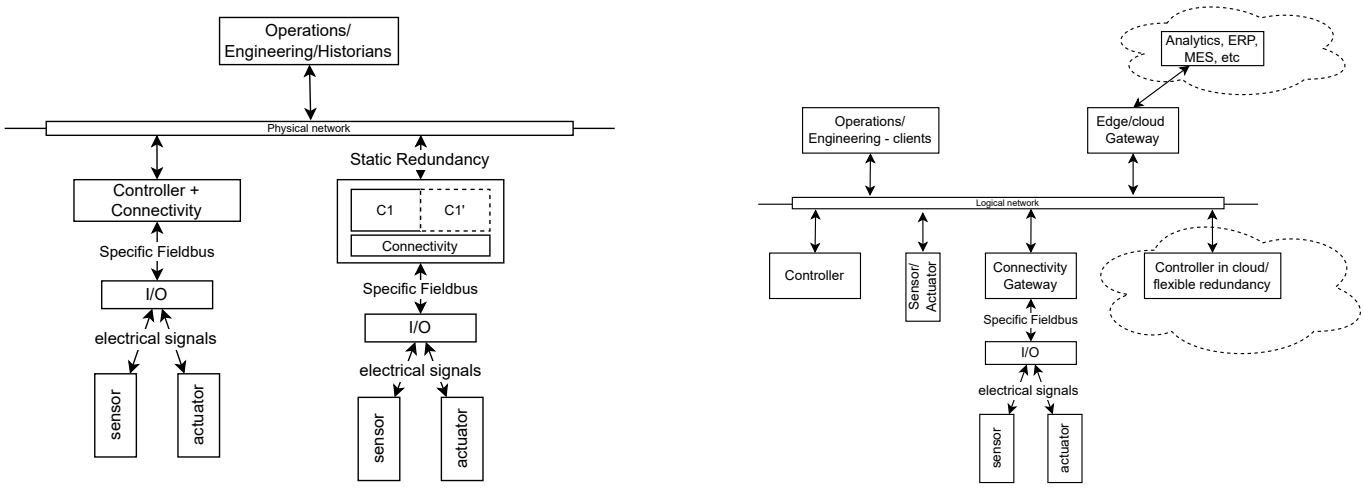
Dependability is a broad term consisting of several attributes [14]: availability, reliability, maintainability, integrity, and safety. As dependability is closely related to cybersecurity [3], exploring different aspects of security for industrial control systems, and how those aspects relate to dependability is important. A major source for guidance and certifications for cybersecurity used within IACS is the IEC 62443 standard series. Parts 4-2 and 3-3 of the standard contain requirements and guidance related to system and component design, based on seven foundational requirements:

1) Identification and Authentication Control (IAC)
2) Use Control (UC)
3) System Integrity (SI)
4) Data Confidentiality (DC)
5) Restricted Data Flow (RDF)
6) Timely Response to Events (TRE)
7) Resource Availability (RA)

Some of these foundational requirements correlate with dependability aspects. Others are either part of a non-covered aspect or are a mitigating measure against a fault category. In Fig. 2 the relationship between dependability aspects and foundational requirements is illustrated.

[2]https://search.abb.com/library/Download.aspx?DocumentID=3BSE038018-600

[3]See, e.g., new.abb.com/industrial-software/connected-workforce




(a) A controller-centric architecture.

(b) A network-centric architecture.

Fig. 1: Example architectures for network- and controller-centric design models respectively.

Foundational requirements on IAC and UC are basically related to the need of having access control in the system, meaning that entities must be identifiable, that the authenticity of the entities can be securely verified, and that there are rules and rules-enforcement for how entities are allowed to interact. The principle of least privilege [15] is one of the guiding principles for use control. IAC and UC are enabling dependability attributes on integrity and availability since they can help avoid malicious as well as non-malicious faults from occurring in the system. Furthermore, basic access control is a prerequisite for the confidentiality attribute. Use Control includes requirements on contents and protection of audit logs, related to Timely Response to Events below.

System Integrity (SI) is directly related to the integrity aspect of dependability with the additional attributes of, e.g., communication integrity, software, information integrity, etc. These attributes are meant to counter intentional as well as accidental integrity faults, thus helping with fault prevention as well as fault removal.

Data Confidentiality (DC) has no direct relation to dependability aspects but is a separate security-related aspect [14].

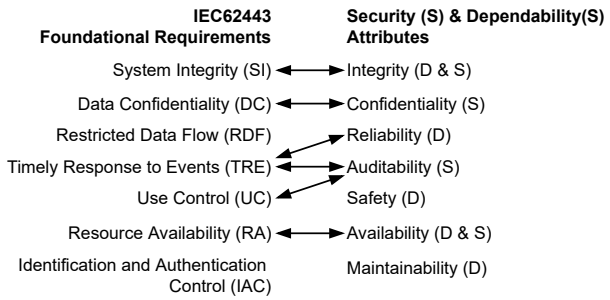



Fig. 2: Correlation of IEC 62443 foundational requirements and defined Security & Dependability attributes.

The requirement on Restricted Data Flows (RDF) concerns network segmentation into zones of different criticality, and strong zone boundary protection. RDF counter some classes of intentional malicious faults during system execution, and are therefore related to protecting integrity, safety, and reliability of the system, i.e., being a fault preventive measure. The NCC design strategy may seem to indicate RDF being less useful, but it still plays an important role in providing basic protection, against, e.g., DoS attacks, lateral network movement, etc.

Timely Response to Events is concerning collection and response to security-related events. The rationale of the requirement is to be able to detect malicious behavior to react promptly, and to be able to establish chains of events when doing a forensic analysis of security incidents. Prompt reaction to security-related events is partly correlated with Reliability. The requirement on collecting and preserving logs of security events does however not directly correlate either to a dependability aspect or as a fault-preventive mechanism. Therefore we will suggest using *Auditability* as a separate security aspect in the following analysis. We define auditability as the ability of a system to establish the sequence of events leading to a specific state. Proper Identification and Authentication control is a prerequisite of auditability.

The Resource Availability requirement is closely related to the traditional availability aspect of dependability, with additional attention to abnormal situations or malicious threat actions not putting the system in a faulty or undefined state, e.g., using a well-defined degraded mode for DoS scenarios, implementing backup routines so that the control system can be restored if necessary, etc.

## V. Dependability and Security Aspects on NCC

Using the attributes of dependability and security as defined in Section IV, the network-centric architecture is further discussed in this section, along with related technologies and concerns.

TABLE I: Ethernet frame failure rate.

| Mbps | FLPH (single NW) | FLPH (red. NW) | FLPY (red. NW) |
|---|---|---|---|
| 1 | 0.35 | $4*10^{-7}$ | 0.004 |
| 50 | 17.9 | $2*10^{-5}$ | 0.19 |
| 500 | 179.9 | $2*10^{-4}$ | 1.9 |

### A. Reliability

Uninterrupted control is the core feature of a control system, and reliability is the likelihood of continuous interrupted service in a bounded time interval. The threats to reliability are faults, errors, and failures, and they vary with the life cycle [14], [16]. We look at reliability in an NCC system in the use phase from the angle of the fault mitigation provided by different technologies that lay the ground for NCC, starting from the lower layer, with switched Ethernet networks and the TSN amendments followed by OPC UA PubSub. We use the four fault mitigation means presented by Al-Kuwaiti et al. [16], which are (i) fault avoidance, (ii) fault tolerance, (iii) fault detection, and (iv) fault restoration.

*1) Ethernet:* The discussion in this section assumes Gigabit Ethernet on twisted-pair copper wire, IEEE 802.3ab networked with IEEE 802.1Q without TSN amendments.

**Ethernet - fault avoidance.** Gigabit Ethernet IEEE 802.3ab specifies a Bit Error Rate (BER) smaller than $10^{-10}$. Table I shows the expected Frame Loss Per Hour (FLPH) and Frame Loss Per Year (FLPY) at different bandwidth utilization.

Single Event Upset (SEU) probability increases as circuits become smaller [17]. Hence, SEU fault avoidance in network equipment is increasingly important since SEU can corrupt frames stored in queues or, worse, affect the configuration. An SEU corrupted configuration can impact the whole network.

IEEE 802.1Q prioritizes traffic using the three-bit Priority Code Point (PCP) but does not guarantee end-to-end communication time. Switches supporting PCP have eight queues per port, equal to the number of PCP priority levels. PCP can help prevent temporal faults by assigning high-priority PCP values to time-critical traffic. However, PCP may not always be sufficient for meeting deadlines due to network load, jitter, and latency requirements. End-systems must also prioritize the network traffic processing to avoid priority inversion or latency when connected to a converged network [18], [19].

**Ethernet - fault tolerance.** The wide-spread use of Ethernet in IT and OT has rendered many fault-tolerance and resilience solutions [20], further discussed below.

Ring protocols prevent networking loops in ring topologies with port blocking which ensure only one path between network nodes, as loops in Ethernet networks can cause network storms and congestion. The protocol monitors the network and unblocks blocked ports to open redundant paths if necessary due to a failure.

Two well know ring protocols are the Spanning Tree Protocol (STP), specified in IEEE 802.1D, and the Rapid Spanning Tree Protocol (RSTP) IEEE 802.1w. Both originate from IT and have recovery times in the seconds range [20]. The Media Redundancy Protocol (MRP) is an OT ring protocol from Hirschmann/Belden, standardized in IEC 62439-2, with recovery times as fast as ten ms [21]. In addition, companies have proprietary ring protocols, such as Westermo‘s FRNT and Moxa‘s Turbo ring, with similar recovery times as MRP [22].

Ring protocol loses frames during recovery; a parallel redundancy does not. Parallel Redundancy Protocol (PRP) IEC 62439-3 Clause 4 duplicates frames on two separate networks. High-availability Seamless Redundancy (HSR) IEC 62439-3 Clause 5 connects the end-systems in a ring. HSR does not require infrastructure duplication and can be a cost-effective but limited alternative to PRP [23].

Table I shows the FLPH and FLPY for a redundant network with frames replicated over disjoint paths, such as PRP, compared to a single path solution or ring redundancy. A ring redundancy protocol does not replicate frames; hence it does not improve transient loss.

Link aggregation is an IT network technology for fault tolerance (and performance) that resembles PRP; one or more physical interfaces form a Link Aggregation Group (LAG). The Link Aggregation Control Protocol (LACP), IEEE 802.1AX, manages the LAG and provides failure recovery in seconds.

Software-Defined Networking (SDN) is a technology for separating the control and data plane. SDN can provide failure tolerance to OT networks [24] by utilizing a backup link when the primary fails.

**Ethernet - fault detection.** The Ethernet Frame Check Sequence (FCS) has a Hamming distance of four and a Mean Time To False Packet Acceptance (MTTFPA) of 60 billion years [25].

IEEE 802.3 dictates Ethernet devices use Link Integrity Test (LIT) pulses to detect link failures. A link is down if a receiver doesn’t receive data or LIT within 50 - 150 ms.

Connectivity Fault Management (CFM) for Ethernet was standardized with IEEE 802.1ag in 2007 and incorporated into IEEE 802.1Q-2011. However, CFM support in industrial switches is close to nonexistent.

Link Layer Discovery Protocol (LLDP) allows adjacent devices to detect each other and exchange information and can be used to detect configuration mistakes [26]. LLDP is utilized by industrial protocols, like PROFINET, to monitor the devices connected.

Ring protocols like MRP are only as efficient as their fault detection. Parallel redundancy solutions, like PRP, do not require fault detection per se due to preventive frame duplication. However, unrepaired faults lead to network redundancy attrition and increased failure risk. Therefore, PRP supervises links with periodic messages and makes the information available [27].

**Ethernet - fault restoration.** Fault information needs to come to the attention of system management personnel. DCSs like 800xA provide plugins for monitoring network equipment[4]. Network management tools are monitoring capable, and the landscape is vast [28]. Moreover, companies

[4]https://new.abb.com/control-systems/system-800xa/cyber-security/pc-network-and-software-monitoring

such as Westermo and Hirschmann/Belden promote their network management tools, WeConfig[5] and HiVision[6].

Redfish is an open standard and specification developed by the Desktop Management Task Force (DMTF) as an attempt to address the plentitude of management protocols required to maintain the data center infrastructure [28]. In data centers, twice as many errors result from human mistakes than hardware failures [29].

With a more capable network infrastructure comes an increasing need for infrastructure life cycle management. For example, a replacement switch must have the correct software version and configuration.

*2) TSN:* TSN consists of several amendments to IEEE 802.1, resulting from the TSN task group work, and is recognized as the future of industrial automation communication [8].

**TSN - fault avoidance.** TSN addresses latency fault avoidance in end-to-end communication. The Audio Video Bridging (AVB) IEEE 802.1Qav provides bandwidth reservation and traffic shaping [30]. IEEE 802.1Qbv provides time-triggered, scheduled traffic [31], allowing low latency communication.

TSN amendment IEEE 802.1Qcc describes network configuration with stream reservation. The network infrastructure and end-points confirm bandwidth requests, providing early detection of network overutilization.

**TSN - fault tolerance.** The TSN Frame Replication and Elimination for Reliability (FRER), IEEE 802.1CB replicates frames over disjoint paths. TSN amendment IEEE 802.1Qci protects against babbling idiots, e.g., a node that, due to an error, transmits much more than it should, and the data is most likely nonsense.

**TSN - fault detection.** FRER discards duplicated frames replicated over a disjoint path when the path joins again, and FRER keeps track of the discarded frames. If the discarded frames are below a threshold, the links lose more frames than intended, indicated in FRER status. However, the realization has limitations that can cause frame loss below a threshold to go undetected [32].

IEEE 802.1Qci provides diagnostics related to the babbling idiot protection.

**TSN - fault restoration.** A replacement switch must have or retrieve the correct configuration. This need is not specific to TSN, but the configuration complexity increases with TSN amendments such as IEEE 802.1Qbv. The IEEE 802.1Qcc amendment supports a fully distributed mode, as well as a centralized mode, for configuration. Lo Bello *et al.* [33] argue that the centralized mode suits industrial automation better. In addition, there are attempts to reduce the need for vendor-specific management tools [34].

*3) OPC UA PubPub:* OPC UA PubSub standard describes four different transport protocols (i) UDP, (ii) Ethernet, (iii) Advanced Message Queuing Protocol (AMQP), and (iv) Message Queue Telemetry (MQTT). We focus on the UDP realization since it does not require a broker and is likely to show better real-time properties than the broker-based alternatives.

**OPC UA PubSub - fault avoidance.** The secure profile excluded, see Section V-D, OPC UA PubSub Unified Architecture Datagram Protocol (UADP) does not specify corrupt message fault avoidance; it relies on mechanisms in the underlying layers, i.e., UDP checksum and FCS. The UADP maximum size is 65535 bytes and fragments into 44 standard 1500 bytes Ethernet frames. More frames increase error probability since a one-bit error in any of the 44 frames invalidates the whole message. A full-size UADP packet sent twice a second has a yearly message loss of 3332.3, while a UADP message that fits into one 1500 Ethernet frame sent 88 times a second has a yearly loss of 3332.4. Both variants require the same bandwidth, and the expected message loss difference per year is 0.1. Hence, reducing the size of the UADP payload has a minor fault avoidance impact compared to frame duplication over redundant networks, see Table I.

OPC UA PubSub prevents aged data faults through the use of a publishing interval and keep-alive time mechanism by publishers, and a timeout by subscribers. The UADP message includes a sequence number to detect and discard old messages.

Brokerless UDP-based OPC UA PubSub utilizes multicast and Internet Group Management Protocol (IGMP) for broker functionality. IGMP snooping optimizes layer two by forwarding multicast messages to specific ports based on IGMP knowledge, reducing broadcast traffic and avoiding multicast flooding faults. The OPC UA PubSub standard recommends using switches with IGMP support, and OPC UA applications shall use IGMP, i.e., joining the group where the values of interest are published. However, the standard does not specify how to divide multicast groups. Hence, the more coarse-grained division, the more network traffic.

**OPC UA PubSub - fault tolerance.** Automatic Repeat Request (ARQ) [35] techniques are unsuitable in publisher-subscriber context, but having a publishing interval $N$ times shorter than the message receives timeout can allow for a temporal redundancy to guard against transient faults. Besides that, OPC UA PubSub over UDP has to rely on the underlying network fault tolerance.

**OPC UA PubSub - fault detection.** The standard outlines configurable diagnostic levels and statistics counters for failed transmissions and subscribed data timeouts. Combined with Ethernet and TSN diagnostics, these diagnostics can help identify issues.

**OPC UA PubSub - fault restoration.** Restorable faults on OPC UA PubSub level concern configuration mismatches. The diagnostic counters described under fault detection can aid in detecting such an error and thereby ease the restoration.

### *B. Availability*

Availability is the system's uptime expressed as a ratio of its Mean Time to Failure (MTTF) to the sum of MTTF and Mean Time to Repair (MTTR). For example, a level two network using the Westermo RedFox-7528, a 12-port

[5]https://www.westermo.se/solutions/weconfig

[6]https://hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/network-management-software/index.phtml

gigabit switch with an MTTF of 763,000 hours and a repair time of two hours, would have an availability of 99.9997%, resulting in an average downtime of 1.4 minutes per year for a single switch network. However, a network with 100 switches would have an average failure time of two hours and 17 minutes, resulting in an availability of 99.97%. Thus, larger networks are more likely to experience failures and require maintenance to ensure availability.

NCC enables cloud and virtualization technology for control systems' fault tolerance and resource management [36], [37]. O-PAS describes an on-premises local cloud (ACP) to host virtual controllers. Kubernetes, a container management system, offers failure recovery functionality that reduces repair time and improves availability [10].

**Perimeter protected networks, restricted data flows** In traditional controller-centric systems, the main protective mechanism is by separating the system into different security zones and conduits, as described e.g., in the IEC 62443 standard series. Communication between zones are protected by firewalls and similar mechanisms, communication within zones are in many cases unchecked. The way for an attacker to gain access to resources to a system constructed using this strategy is by what is called *lateral movement* between zones. When access is gained for a zone, the attacker can in theory gain access to all the resources within that zone.

The network-centric design strategy implies a greater level of connectivity between devices, and a more difficult situation in defining strict zones, especially for scenarios with flexible redundancy schemes, etc. However, NCC gives the possibility of implementation and configuration of interoperable security solutions between service endpoints. If e.g., using OPC UA for communication, there are standardized methods for securing data in transit, client authentication, authorization, audit logging etc.

In the Zero-Trust architecture defined by NIST [12], an *implicit trust zone* is used for devices on the south side of a policy enforcement point. For NCC, we argue that each *Resource Server* must be seen as a separate implicit trust zone, since the resource server is the service end-point for accessing a resource. The resource server must therefore at least contain a policy enforcement point, but may actually not contain a policy decision point, if using policy delegation mechanisms, e.g., as described in [38].

### C. Maintainability

The fault restoration points in the reliability section cover the network aspects of maintainability. On top of that comes life cycle management of the switches and other network infrastructure concerning software maintenance. With more intelligence and network infrastructure capabilities comes an increased need to keep the equipment up to date to reduce the probability of failure due to known, corrected errors. A lesson learned by Google that led to a frequent update policy [39]. A policy introduced even though maintenance, especially manual maintenance, can be error prone [29], [39].

Zero-trust requires that the security posture is continuously re-evaluated, that the identity and integrity of devices, services, users, resources are always checked before use, and that permissions are intelligently described, checked and enforced for all resource requests. In a large and complex system, there is a risk of a great effort being needed to maintain and monitor this. As much as possible of these mechanisms must be automated to be manageable.

One aspect of a Zero-Trust architecture is to separate the data plane from the configuration plane [12], so that the configuration of devices is communicated using a separate physical or logical network. In this way, Zero-Trust puts requirements on the maintainability attributes of network and device configurations.

### D. Integrity and safety

Integrity addresses unintended application states and goes hand in hand with security and safety. There is no OPC UA profile for safety based on OPC UA PubSub. The OPC UA Safety profile[7] builds on OPC UA Client Server, and it describes a Safety Communication Layer (SCL). A safety profile building on OPC UA PubSub with PROFIsafe as the SCL is in the making. At the time of writing this, a joint working group has been formed between the OPC Foundation[8] and the PI organization[9].

**Integrity of information and data** Typical approaches for protecting data from faults are to add different types of checksums, Cyclic Redundancy Checks (CRC) or hash functions, such as, e.g., the IPv4 header checksum[10] or, for integrity protection, the Secure Hash Algorithm (SHA)[11]. Different mechanisms have different properties, where CRCs and simple checksums can prevent unintentional faults, the cryptographic hash algorithms protect from tampering. Some methods can provide authenticity protection, i.e., the true sender of the data can be proved, e.g., in the case of key-Hashed Message Authentication Code (HMAC)[12]. In the OPC UA profile for secure communication, different levels of integrity protection can be added, including message authentication. This however does apply only to OPC UA client/server communication, other solutions for integrity and authenticity protection of data sent using the PubSub pattern may be needed. Secure PubSub[13] provides a shared-key solution which provide confidentiality and integrity, but not authenticity.

**Access control** is a security mechanism directly affecting the integrity and safe operation of an industrial control system. One important principle in control system design is the singularity in the relationship between controller and output-signal, only one controller should be able to set a signal value controlling an actuator. The system would behave in an unpredictable way if several entities could set the same output signal.

[7] https://reference.opcfoundation.org/Safety/docs/
[8] https://opcfoundation.org/
[9] https://www.profibus.com/pi-organization/
[10] RFC 1071, www.rfc-editor.org/info/rfc1071
[11] nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf
[12] https://www.rfc-editor.org/info/rfc2104
[13] OPC UA 10000-14, chap. 5.3.5 Message Security

One of the major differences between CCC and NCC is that of ownership of I/O, and how access to I/O is controlled. In CCC, the I/O is physically connected to the controller, and can only be accessed through the controller which manages and external access to the I/O. Controller configuration is typically surrounded with rigorous access control, and only possible to perform when the system is in specific states. Therefore, the I/O is somehow isolated on the south side of the controller, thus residing in a separate network zone.

In NCC the I/O and controllers are independently deployed on the same network, and in principle anyone on the network could read and write I/O signal values. This is one of the major advantages with the NCC approach, as it allows for a flexible deployment of controllers, without the need of being physically connected to the I/O. However, the principle of one output-signal $\Leftrightarrow$ one controller still has to be enforced. This means that, in order to protect output-signals, a rather fine-grained access control for the relationship between I/O and controller has to be defined, configured, and enforced.

Access control for I/O may also include input channels if there is a need for preventing unauthorized reading of measurement values. The needed granularity will depend on the granularity of the information classification.

Furthermore, the increased connectivity that allows other entities, e.g., operator HMIs or data historians, the possibility to access the I/O directly, without going through a controller, implies that access control for direct connection to I/O must be extended to also include the authentication and authorization of human entities, something traditionally handled by the controller, or even by the upper level operations and supervision systems.

Using a zero-trust approach implies that no one is implicitly trusted. Therefore, the identity and authenticity of devices, services and users must always be checked, each connection and resource request must be intelligently authorized, and relevant events must be audit logged and monitored in order to detect potential anomalous usage. Furthermore, the security posture of the system shall be continuously reevaluated.

### *E. Confidentiality*

Confidentiality is an aspect which has so far been rarely applied in industrial automation and control systems. If adopting the zero-trust approach for network-centric control systems, there are good reasons for considering measures of preserving confidentiality of data at rest as well as data in transit, as data flows can be eavesdropped, and potentially sensitive information therefore leaked to an unintended party.

Usage of different methods of cryptography is the typical way of providing confidentiality of data, however, such mechanisms always carry a cost in computational load as well as message sizes, meaning careful assessment of sensitivity-level of data in the system should be done before deciding on what and how to encrypt. Especially asymmetric cryptography, used, e.g., in session establishment, is costly [40].

**Data in transit:** Confidentiality protection of data in transit is typically done by using layer 3 or layer 6/7 protocol encryption. Most traditional control network protocols do not directly support confidentiality, and some of them cannot be adapted to secure communication, but the IP-based protocols, such as Modbus TCP, PROFINET, etc, could be transported over IPSec. IEC 62351 describes security adaptations for several industrial communication protocols. OPC UA supports secure data transport on the application layer (layer 7)[14], and can also use Transport Layer Security (TLS).

**Data at rest:** protecting data at rest can be done at several levels, using disk encryption, strict and fine-grained access control on file storage, methods and processes for correctly decommission devices with potential sensitive data in storage, etc. Protection is also required for sensitive files that are to be exported out from the system, such as access logs, which will require a file encryption scheme.

### *F. Auditability*

One important cybersecurity-aspect is the ability to audit security relevant events, so that a post-incident forensic analysis can be done, to ensure repudiation, and to use as an early indication on suspicious events in the system, e.g., reporting to a Security Information and Event Management (SIEM)-system [41]. This is not a novel aspect of DCSs, but NCC adds in complexity and scale. The OPC UA specification describes the creation of audit events which, if enabled, supports this aspect, though the handling of the events are up to the system owner[15].

The practice of audit logging security relevant events puts additional requirements on protecting the integrity, availability and confidentiality. The data contains potentially sensitive information which should not be leaked, and must be kept tamper-proof to hinder a threat actors from hiding their traces. Therefore, the measures discussed for integrity and confidentiality above applies to log data.

## VI. Conclusions

Adopting a network-centric control design strategy profoundly impacts the technical characteristics of industrial control systems. In this article we have described network-centric control, iterated enabling technologies and discussed challenges and solutions in relation to dependability and security, which are key attributes for the continuous operation of an industrial control system.

NCC introduces novel technologies and concerns into industrial automation and DCSs, while also enabling several desirable characteristics. Among the main challenges, aspects of adopting a zero-trust security approach are among the most important. Defining and upholding fine-grained access control rules and continuously assessing authenticity, state and privileges of devices, services and users for all interactions is a far leap from the current state of practice.

We have added confidentiality and auditability as fundamental attributes related to network-centric control, based on industrial requirements derived from the IEC 62443 standard.

[14]OPC 10000-6, chap. 6, Message Security Protocols.

[15]OPC 10000-2, chap. 6.11 Audit Event Management.

However, one aspect not covered is privacy. Privacy is not traditionally seen as an important attribute of an industrial system, but will be of growing importance considering, e.g., collaborative manufacturing systems which enables several different entities performing production on the same site.

The network-centric architecture requires high network reliability and network-redundancy solutions, with PRP being particularly attractive due to its proactive frame replication. Proactive frame replication over disjoint paths gives zero recovery time and significantly reduces transient frame loss probability.

A proper configuration is necessary to manage latency for time-sensitive traffic, highlighting the importance of network infrastructure management. Management includes different aspects such as spare handling, configuration handling, and network software life-cycle handling. Network-centric control emphasizes requirements on spare handling when replacement network equipment needs the correct software version and configuration. Furthermore, the more capabilities network equipment provides, the likelier the need for software updates, emphasizing the need for a life-cycle management plan that includes network infrastructure software. In addition, effective diagnostics are needed to monitor the network and prevent network attrition.

## ACKNOWLEDGEMENTS

This work is supported by ABB AB; the industrial postgraduate school Automation Region Research Academy (ARRAY), funded by The Swedish Knowledge Foundation (KKS); by The Swedish Foundation for Strategic Research (SSF), project FuturAS, and the European Union's Horizon 2020 ECSEL JU project InSecTT under grant agreement No 876038[16].

## REFERENCES

[1] ZVEI—German Electrical and Electronic Manufacturers' Association, "Process INDUSTRIE 4.0: the age of modular production," Frankfurt, White Paper, 2019.

[2] L. Thrybom *et al.*, "QoS in switched Industrial Ethernet," in *IEEE Conf. on Emerging Technologies and Factory Automation*, 2009.

[3] D. Serpanos, "There is no safety without security and dependability," *Computer*, vol. 52, no. 6, pp. 78–81, 2019.

[4] B. Van Lier, "Developing the industrial Internet of Things with a network centric approach: A holistic scientific perspective on smart industries," in *Int. Conf. System Theory, Control and Comp. (ICSTCC)*, 2014.

[5] I. Álvarez *et al.*, "Fault tolerance in highly reliable ethernet-based industrial systems," *Proc. IEEE*, vol. 107, no. 6, pp. 977–1010, 2019.

[6] C. Zanasi *et al.*, "A Zero Trust approach for the cybersecurity of Industrial Control Systems," in *IEEE Int. Symp. on Network Computing and Applications (NCA)*, 2022.

[7] K. Tange *et al.*, "A systematic survey of industrial internet of things security: Requirements and fog computing opportunities," *IEEE Comm. Surveys & Tutorials*, 2020.

[8] D. Bruckner *et al.*, "An Introduction to OPC UA TSN for Industrial Communication Systems," *Proc. IEEE*, 2019.

[9] M. Wollschlaeger *et al.*, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE Ind. El. Mag.*, vol. 11, no. 1, pp. 17–27, 2017.

[10] B. Johansson *et al.*, "Kubernetes orchestration of high availability distributed control systems," in *ICIT*, 2022.

[11] T. J. Williams, "The purdue enterprise reference architecture," *Computers in Industry*, vol. 24, no. 2, pp. 141–158, 1994.

[16]The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.

[12] S. Rose *et al.*, "Zero Trust Architecture," NIST, Gaithersburg, MD, Tech. Rep., 2020.

[13] T. Miller *et al.*, "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," *Int. J. Crit. Infr. Prot.*, 2021.

[14] A. Avizienis *et al.*, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dep. and Sec. Comp.*, 2004.

[15] J. Saltzer *et al.*, "The Protection of Information in Computer Systems," in *Proc. IEEE*, vol. 63, no. 9, 1975.

[16] M. Al-Kuwaiti *et al.*, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *IEEE Comm. Surveys & Tutorials*, vol. 11, no. 2, 2009.

[17] F. Wang *et al.*, "Single event upset: An embedded tutorial," in *Int. Conf. VLSI Design (VLSID)*, 2008, pp. 429–434.

[18] M. Lee *et al.*, "Priority-based network interrupt scheduling for predictable real-time support," *J. Comp. Science & Eng.*, 2015.

[19] I. Behnke *et al.*, "Interrupting real-time IoT tasks: How bad can it be to connect your critical embedded system to the internet?" in *Int. Performance Computing and Comm. Conference*, 2020.

[20] M. Huynh *et al.*, "Resilience technologies in ethernet," *Computer Networks*, vol. 54, no. 1, pp. 57–78, 2010.

[21] A. Giorgetti *et al.*, "Performance analysis of media redundancy protocol (mrp)," *IEEE Trans. Industrial Informatics*, vol. 9, no. 1, 2012.

[22] L. Wisniewski, "Communication reliability," in *New methods to engineer and seamlessly reconfigure time triggered Ethernet based systems during runtime based on the PROFINET IRT example*, 2017.

[23] R. Hunt *et al.*, "Comparison of prp and hsr networks for protection and control applications," in *Western Protective Relay Conference*, 2015.

[24] D. Dolezilek *et al.*, "Fast fault detection, isolation, and recovery in ethernet networks for teleprotection and high-speed automation applications," in *CIGRE Mexico Int. Colloquium, Mexico City*, 2016.

[25] R. Walker *et al.*, "64b/66b coding update," *Presentation at IEEE*, 2000.

[26] O. Kleineberg *et al.*, "Network diagnostics for industrial ethernet," in *IEEE Int. Conf. Emerging Technologies and Factory Automation*, 2008.

[27] H. Weibel, "Tutorial on parallel redundancy protocol (PRP)," *Zurich University of Applied Sciences*, 2011.

[28] G. Gonçalves *et al.*, "A standard to rule them all: Redfish," *IEEE Comm. Standards Magazine*, vol. 3, no. 2, pp. 36–43, 2019.

[29] J. Meza *et al.*, "A large scale study of data center network reliability," in *Internet Measurement Conference 2018*, 2018, pp. 393–407.

[30] A. Gogolev *et al.*, "Tsn traffic shaping for opc ua field devices," in *IEEE Int. Conf. Industrial Informatics (INDIN)*, vol. 1, 2019, pp. 951–956.

[31] S. S. Craciunas *et al.*, "Scheduling real-time communication in ieee 802.1 qbv time sensitive networks," in *Int. Conf. Real-Time Networks and Systems*, 2016, pp. 183–192.

[32] R. Hofmann *et al.*, "Challenges and limitations of ieee 802.1 cb-2017," *IEEE Embedded Systems Letters*, vol. 12, no. 4, pp. 105–108, 2019.

[33] L. Lo Bello *et al.*, "A perspective on IEEE time-sensitive networking for industrial communication and automation systems," *Proc. IEEE*, 2019.

[34] M. Gutiérrez *et al.*, "Self-configuration of IEEE 802.1 TSN networks," in *IEEE Int. Conf. Em. Tech. and Factory Autom. (ETFA)*, 2017.

[35] S. Lin *et al.*, "Automatic-repeat-request error-control schemes," *IEEE Comm. Magazine*, vol. 22, no. 12, 1984.

[36] T. Goldschmidt *et al.*, "Software containers for industrial control," in *Euromicro Conf. Soft. Eng. and Adv. Appl. (SEAA)*, 2016, pp. 258–265.

[37] T. Goldschmidt *et al.*, "Container-based architecture for flexible industrial control applications," *J. Syst. Arch.*, vol. 84, 2018.

[38] B. Leander *et al.*, "Access control enforcement architectures for dynamic manufacturing systems," in *2023 IEEE 20th International Conference on Software Architecture (ICSA)*, 2023, pp. 82–92.

[39] R. Govindan *et al.*, "Evolve or die: High-availability design principles drawn from googles network infrastructure," in *ACM SIGCOMM*, 2016.

[40] F. Kohnhäuser *et al.*, "On the Feasibility and Performance of Secure OPC UA Communication with IIoT Devices," in *Lecture Notes in Computer Science*, 2022, pp. 189–203.

[41] S. Bhatt *et al.*, "The Operational Role of Security Information and Event Management Systems," *IEEE Security & Privacy*, no. October, 2014.