A Survey of Security Frameworks Suitable for Distributed Control Systems

Elena Lisova*, Elisabeth Uhlemann*, Wilfried Steiner‡, Johan Åkerberg*, Mats Björkman*
*Mälardalen University, Västerås, Sweden
‡ TTTech Computertecnik AG, Vienna, Austria
{elena.lisova, elisabeth.uhlemann, johan.akerberg, mats.bjorkman}@mdh.se, wilfried.steiner@tttech.com

***Abstract* — Nowadays distributed control systems have become more and more common and important in everyday life. However, as many distributed control systems become mobile, wireless, autonomous, ubiquitous and connected, the need for secure communication is imminent. In particular, the need for a general security framework with sufficiently flexible structure, and applicable for various use cases, emerges. Especially this applies to control system based on heterogeneous networks consisting of a wired and a wireless parts. Wired networks are nowadays often connected to Internet and thereby more exposed to potential attackers, and wireless networks are, by nature, more vulnerable to eavesdropping, jamming and hijacking. In this paper we define a scope of use cases based on distributed control, together with requirements for evaluating existing security solutions and frameworks. In addition, several frameworks, mainly from the area of industrial automation, are surveyed and evaluated based on the identified use cases and security requirements.**

Keywords — heterogeneous networks; security framework; threat modelling.

I. INTRODUCTION

Applications using distributed control are becoming more and more frequent. Examples can be found in areas as diverse as aerospace, automotive, automated factories, chemical processes, civil infrastructure, energy, healthcare, robotic networks, manufacturing, transportation, entertainment, and consumer appliances. The most common form is a set of embedded systems, communicating through some type of network. Rather than having a centrally located device controlling all the embedded subsystems that are part of the control system, each embedded subsystem controls its own operation in a distributed fashion. Nowadays, the possibility to merge several different heterogeneous subsystems into one distributed control system (DCS) is an important requirement [1]. Heterogeneity implies coexistence of many different types of nodes, traffic classes and/or communication links. Networks dealing with different types of nodes and traffic classes can support applications with different criticality levels and be more flexible and efficient. To meet current market demands, more and more technologies are also targeting a wireless or mixed wired and wireless solution [2]. Wireless networks have some evident advantages for DCSs, such as mobility and simplicity for the industrial automation area, and weight and size for the automotive area. Wireless solutions can potentially widen and enhance the application areas [3], but come at a price as wireless channels easier can be influenced and affected by malicious intruders.

As security risks are becoming a showstopper for deployment of DCSs, it is considered as an increasingly important requirement [4]. Security risks exist if there is a vulnerability and a threat. A vulnerability is simply the opportunity to cause damage, and it can be due to a design flaw, an implementation flaw or some weaknesses in terms of oversimplified passwords or keys [5]. A threat exists if there is some value in breaking the system. The term "security" covers a wide range of provided services, so-called security objectives, ranging from a parity code to detect compromised data, via encryption to compromised node detection. A security objective describes what type of threat the system needs to be secured against. Different DCSs have different security objectives. In some networks, data is not confidential and all that is needed is data origin checking, whereas in other networks it is crucially important to keep data confidential, due to e.g., the need to protect product recipes, and in this case encryption is needed. However, since all DCSs are time-critical, they all imply some kind of scheduling [6], and thus it is possible to cause system disruption within a DCS by targeting the clock synchronization functionality. There are many ways of influencing the synchronization, but one of the most difficult to detect and counteract is the delaying attack, as the adversary does not need to alter any data, but only to delay a few synchronization messages to put a node into unsynchronized mode [7].

The main contribution of this paper is a detailed investigation of existing security solutions and frameworks to determine their applicability to heterogeneous DCS. Such an investigation simplifies the choice of technology already at the design stage of new DCS and allows identifying security gaps in existing solutions. To this end, we also propose an approach for comparing and evaluating the suitability of existing security frameworks for the specific security requirements derived from DCSs. This allows a well-founded comparison.

The possible range of use cases for DCS is extremely wide, and they all have different application areas, purposes and ways of realization. However, we target a general profile of use cases based on DCS with similar core characteristics specifically related to distributed control, namely systems requiring high reliability, timeliness and availability, and where something can be controlled from a distance if security

is breached. The general profile therefore includes heterogeneous networks employed in different environments, having different topologies and including links of different qualities. Also it covers various types of use cases, e.g., factories and plants with limited physical access possibilities for intruders or private cars with unpredictable human behavior. However, we target security use cases and requirements suitable for generic DCS, where the main characteristics are real-time constraints, reliability, availability, heterogeneity and ability to support different traffic classes. By security framework we consider a proposal in which several different security objectives are achieved. As security is a multifarious term, there cannot be one single separate solution covering all emerging DCS demands. Therefore, an aggregation of several solutions should be considered to achieve a framework with appropriate quality of security system performance.

The remainder of the paper is organized as follows. Section II describes important terminology for communication security, whereas Section III presents the scope of use cases within distributed control. In Section IV, the system model is described and in Section V requirements for the considered frameworks are investigated. Sections VI and VII present our evaluation of existing security solutions and frameworks respectively, and, finally, Section VIII concludes the paper.

II. Components of Communication Security

To evaluate different security frameworks, we need to define the main terminology. In particular, we consider the following components, organized as proposed in Fig. 1. *System assets* are the features that we want to protect in the system. They are the main assets of the use case, as they affect its workflow most and have the highest value. For example, in a system with sensitive data, the data confidentiality is an asset. *Adversary goals* represent the possible targets of a potential malicious intruder. If we consider intrusion detection systems in plants, a possible adversary goal is system hijacking. An *adversary model* represents a set of possible adversary features, such as geographic location, time and budget. The adversary model is extremely important for correct risk estimation and appropriate security design.

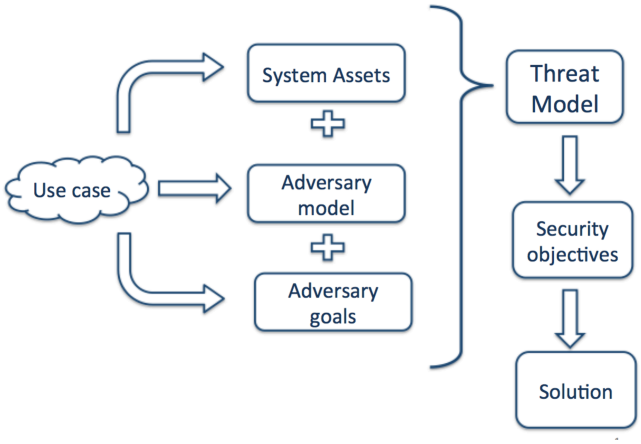

Fig. 1. An approach for security framework derivation.

The system assets, the adversary model and goals can all be derived from the considered *use case*, as shown in Fig. 1, since they reflect specific properties of the use case. Together, these three features form a *threat model*. The threat model is an aggregation of security aspects to address in the system. The threat model is needed to formulate a set of *security objectives*, describing the security features and services we need to have in the *solution*.

III. Distributed Control Systems

A DCS refers to a control system, in which the controller elements are not central in location, but distributed throughout the system, and each sub-system is controlled by one or more collaborating control units. The entire system of subsystems and controllers is connected by a network for communication and monitoring. DCS is a very broad term used in a variety of areas, to monitor and control distributed equipment. However, for any application based on DCS to be fully functional, information must be interchanged in a timely and reliable manner among the controllers, actuators and sensors in the communication network. Thus, DCS has stringent requirements on both reliability, availability and timeliness, the latter in terms of real-time deadlines. If the deadline is missed, the packet is considered useless, similarly to a lost or erroneous packet in a non-real-time system. The effect of packet scheduling attacks on shipboard networked control systems was evaluated in [8] and clearly shows that such attacks can be easily mounted to both wired and wireless communication channels leading to time varying delays packet scheduling anomalies.

Traditionally, most DCSs are based on wired networks, e.g. fieldbus systems [9] such as the CAN bus, HART, FlexRay or PROFIBUS. However, employing wireless communications offers significant advantages to DCSs, as they become mobile, autonomous and connected [3, 10, 11]. Wireless channels are, by nature, more exposed to noise and interference than their wired counterparts. Consequently, it implies a considerable challenge to fulfill the real-time requirements with sufficient reliability for proper functionality of applications based on DCSs [3, 11]. In particular since for wireless DCS, not only system reliability needs to be considered, but also individual link reliabilities.

Since the use of wireless communications in DCS becomes more and more common and since it is difficult to solve all application requirements with only one communication standard [2, 12], heterogeneous networks are introduced. By heterogeneity is meant that the networks consist of different types of nodes and different communication links. Most emerging DCS also needs to support several types of data traffic classes with different levels of criticality. This is termed a converged network, typically supporting three different traffic classes: Time-Triggered (TT), Even-Driven (ED), and Best-Effort (BE) traffic. These three traffic classes have different applicability, scheduling requirements and temporal characteristics.

It is rarely possible to add a security framework to an existing system without considerable changes [12]. For example, time-triggered systems, frequently encountered in DCSs, im-

ply the need for scheduling. Scheduling is an essential part of the correctness of the system. Security implementations on top of such a system can affect the scheduling, impose delays and increase the frame length [13], and, therefore, security objectives should be considered in the scheduler as well. Obviously, if the security constraints are taken into account already at the system design stage, it has several advantages.

IV. System Model

Note that we do not target a specific use case, but a wide range of use cases based on DCS. In order to specify and characterize them, their common aspects related to distributed control are considered. Hence, the use case is systems requiring high reliability, timeliness and availability and where something can be controlled or interfered with from a distance if security is breached. We target heterogeneous networks consisting of different types of nodes and communication links with support for three different data traffic classes TT, ED and BE. Also, to be able to consider time-critical applications, security support for applications with real-time constraints needs to be added as a requirement, as security solutions always affect the delay and time properties of the system. Hence, synchronization is an important asset.

A. Security objectives and Threats

To characterize the required security profile for DCSs, we need to derive the adversary goals, the system assets and the adversary model [14] for it as it proposed in Fig. 1 . This will allow us to build a threat model for the profile. Based on the threat model we can derive the profile security objectives. The security objectives specify what types of threats the system is to be secured against.

For the use case communications in a DCS to be feasible, it must be safe for humans and the environment, provide timely and reliable data delivery and be available to perform the task at hand. As we consider applications with real-time requirements, one of the main system assets is clock synchronization and thus many attacks target clock synchronization [15]. For some DCSs carrying sensitive information, data confidentiality can be considered an asset. In this case a potential adversary can exploit eavesdropping to achieve his goal. However, for many DCS, it does not matter if data can be eavesdropped as long as it cannot be compromised or altered. A particular feature of DCS in this respect is that in order to compromise the data, it is enough to delay it, since in a real-time system it is not only the data itself that is of importance, but also when in time it is presented. As TT traffic requires a low jitter, it is enough for an intruder to cause a random delay of TT packets affecting the periodicity, to compromise the functionality. For ED traffic, a temporal delay of an alarm or a warning, will cause system malfunction. A delay therefore also affects the reliability and availability of the system. For safety-critical systems, availability is one of the main assets, as system shutdown has an extremely high cost. A Denial of Service (DoS) attack can then threaten to decrease the availability of the system. Certain safety features often implemented in DCSs for increased data reliability, like robustness and fault tolerance mechanisms, can directly contribute also to achieving specific security goals, such as excluding the possibility of DoS attacks.

There are many possible goals for an adversary targeting DCSs, but according to [16] the following three can be considered as general adversary goals: system disruption, eavesdropping and system hijacking. All three are possible within the considered profile and will lead to that the adversary can control or interfere with something from a distance if security is breached. If we consider a power plant generating electric power to a city, the adversary can try to disrupt the system. For factories producing products according to secret recipes, like Coca-Cola, the adversary is likely to target system eavesdropping. Even machines that operate in a closed system without contact to the outside world can be eavesdropped upon via monitoring electro-magnetic transmissions generated by the hardware. In a sensor network checking paper humidity during production, an adversary can target system hijacking, so that he can replace the sent data during its transmission. In this case, an incorrect function of the paper machine can be hidden from the control center for a long time, causing tremendous money loss for the factory. One important topic in the near future is hijacking, since communication links, not properly protected, are appealing for an adversary. This is especially important for DCS, as an adversary can e.g., target automated factory hijacking or vehicle control hijacking which can lead to significant damages or even loss of human lives.

The adversary model strongly depends on the specific use case, but we can still list several generally applicable suggestions about the adversary. We assume that he is capable of intercepting any transmitted message and he is also able to alter and retransmit it. In addition he can create his own messages and perform data processing using publicly available system credentials. Besides these abilities, the adversary can also be characterized by the following criteria: whether he is adaptive or static, his computational power (typically proportional to the targeted systems assets and values), whether he is mobile, etc.

V. Evaluation Methodology

In this paper, we consider a security framework to be a set of interconnected solutions that satisfy the system requirements on security by providing all necessary security services required within the network. To investigate existing security solutions and frameworks, we need to have a tool to evaluate them. The set of security objectives derived from our targeted use case can be such a tool, as we can compare solutions through the subsets of security objectives they are able to cover.

A. Security Concepts

An attack is an intentional attempt to break a security objective made by an adversary. There are innumerable types of attacks for all kinds of applications, and the amount grows every day. Nevertheless, it is possible to provide a general classification of possible attacks types relevant to most types of DCS. According to [5], attacks can be grouped into the

following categories: DoS, eavesdropping, man-in-the-middle (when an attacker pretends to be a legitimate partner in the middle of the communication process) and intrusions (breaking into a system using a virus, a Trojan, or a worm, i.e. a malicious code that targets to exploit system vulnerabilities). All attacks target to violate the security objectives of the system. The classical triad of security objectives is Confidentiality, Integrity and Availability (CIA). Considering the DCS scope it can be completed with authentication, authorization, non-repudiation, and third party protection [17]. For each use, case it is possible to form a list of objectives that are specific for that particular application.

B. Security for wired and wireless networks

Traditionally, security has not been considered from the very beginning in wired networks for DCSs, as they conventionally are both static and closed. Mobility is seldom required, so the network configuration is usually static. In wired networks it is more difficult to join the network illegally, compared to a wireless one, and, therefore, many wired networks are regarded as closed. Moreover, some wired networks are considered to be secure due to their location, especially in environments, which are difficult to reach, e.g. the embedded systems in cars. Therefore, the probability to breach the system in such networks is considered low, but, of course, everything depends on the gain and the system values. However, with growing levels of automation in diverse application areas, security concerns in wired industrial networks are rising as well.

In contrast, security, especially in terms of encryption, is basically always considered for wireless networks. The security approaches for wireless networks reflect specific features such as easy access to the communication links, vulnerability due to the propagation characteristics of wireless signals etc. Different approaches imply different tradeoffs between security services and network performance [18].

C. Security solutions on different layers

Security solutions can be implemented on different layers of the OSI model. Usually, the application, network and link layers are considered as main candidates for introducing security features. In this subsection, all three options are investigated and compared from the specific point of view of developing a flexible security framework for heterogeneous networks.

Security features implemented on the application layer can allow end-to-end checking of the system assets and also provides a high security level due to targeting a specific use case. For security on the lower layers in the communication stack, a more general approach needs to be adopted, whereas application layer security solutions are a good choice when the application can be well specified. One example of such a solution is presented in [19], where the author proposes a security solution targeting initial trust establishment for industrial heterogeneous networks. On the other hand, security solutions on the application layer can lead to lack of flexibility and also a factor, which needs to be considered, is that the user interacts directly with the security solution and thus the security performance can depend on the individual user's skill.

The network layer is widely studied for applying security solutions. A logical conclusion from some of these studies was the development of IPSec [20]. The main advantage of this approach is that security solutions implemented here will be hidden from the user. Moreover, it is suitable for heterogeneous networks without any precise connection to the specific use case being necessary nor exact knowledge about the underlying links.

Security solutions can also be implemented on the link layer. One example of an architectural framework for security on the link layer was presented in [21]. The authors propose a security solution over Ethernet, providing such services as key management and countermeasures to DoS attacks. Generally, the link layer is a convenient place for data management security solutions, dealing with bootstrapping, access control etc. The main disadvantage is dependency on system configuration, and knowledge about whether it is a wireless or wired network, as these have different mechanisms for channel access (MAC sub-layer) and services provision (LLC sub-layer).

A security framework implementation can also be done as a separate additional layer, it can be merged with an existing layer or it can be split between layers, so that different layers have different security functionalities. The latter is often more efficient, as it allows combining the advantages of security implementations on several different layers.

D. Security Framework for DCSs

The security framework should be designed considering the exact set of security objectives derived from the use case. Such an approach allows efficient and adequate protection of the system assets. Also, the suitability of security framework depends on the specific system structure. For heterogeneous DCSs, it should include solutions to achieve an appropriate level of safety in the wireless part of the system and a corresponding level of security in the wired part of the system [17].

The security framework can be implemented on different layers in the OSI model, as each layer has its own advantages and disadvantages. Therefore, the most promising solution seems to be a cross-layer architecture. For example, the core solution can be implemented in one layer, and completed by a set of optional extensions operating on others layers.

VI. EVALUATION OF EXISTING SECURITY SOLUTIONS

In this section we investigate existing security solutions specific for either wired or wireless networks. The majority of the existing solutions evaluated in this paper comes from the area of industrial control. The reason for this is that this is the most mature application area exploiting DCS and thus all protocols and security solutions are already in commercial use since several years. However, most of them do not support emerging applications based on DCS, becoming mobile, autonomous and connected.

Different solutions are available for wired and wireless systems, and solutions can also vary depending on where in

the OSI model they are applied and what type of traffic policy is used in the network.

While adversaries constantly come up with new types of attacks, system developers continue to design new countermeasures. Countermeasures as well as security solutions can specifically target wired or wireless networks, and they can be applied on different levels in the OSI stacks resulting in different properties. On the physical layer, a possible countermeasure to channel jamming is frequency hopping. On the application layer, a possible countermeasure to eavesdropping is encryption.

A. Solutions for Wired Sensor Networks

DCS are traditionally based on wired networks. Most of these have weak support for security that demonstrates the need for a flexible security framework, able to meet the requirements of merging application areas with high demand on reliability, timeliness and availability.

HART (Highway Addressable Remote Transducer) is an industrial automation protocol, which is widely used in factory automation as a reliable and long-term solution for plant operators. However, considering security aspects it only has single parity checking [22]. Single parity check codes, originally intended to detect communication errors caused by the channel, can also be used as an indication that part of the message was intentionally changed. Hence, in this sense it is a security solution, albeit not a strong one, as it cannot help when a malicious node changes the message and re-calculates the checksum. HART is thus an example of a network that traditionally has been considered closed and thereby better protected.

TTEthernet (Time-Triggered Ethernet) [23] is a platform that extends classical Ethernet so that it becomes possible to use for safety-critical application with real-time requirements. This protocol can be used for systems that have several levels of time and safety requirements due to its support for several different traffic classes. However, like HART, TTEthernet does not provide any specific security service [24] .

CAN (Controller Area Network) is one of the most broadly used technologies for in-vehicle communication. Regarding security properties, CAN supports data transfer security, i.e. it can detect an error and signal about it. Its main security weaknesses were investigated in [25], and they include initial broadcast nature of all packets, extreme vulnerability to DoS attacks, lack of authentication fields, and week access control. All these weaknesses originate from the initial assumption that networks using the CAN protocol are closed for intruders, but it is not always a case. Especially, when a wireless gateway is introduced.

Evaluation. Neither CAN nor TTEthernet support heterogeneous networks and neither CAN nor HART can provide real-time support for three different types of data traffics. It is also noticeable that the set of security objectives for each solution depends on the concrete application area.

B. Solutions for Wireless Sensor Networks

There are several technologies and standards that are intended for wireless sensor networks and many researches target their future exploration, comparison and development. IEEE 802.11 (WiFi), IEEE 802.15.1 (Bluetooth) and IEEE 802,15.4 (Zigbee, WirelessHART) are compared and investigated in [26] as possible solutions for sensor networks in industrial applications. WirelessHART is mentioned there, as one of the most robust protocols with high quality real-time performance technology, but having poor link throughput and network scalability.

Also, there are some existing researches evaluating security aspects in wireless sensor networks. IEEE 802.15.1, IEEE 802.11 and IEEE 802.16 (WiMAX) are compared in [27] from the security point of view for the use case of wireless sensor networks. The author considered such security techniques as authentication, key-distribution and cryptographic concept, their specific features and flaws. In all these standards and technologies, different security approaches and techniques are used. Some examples are considered in more detail below.

An analysis of the security support within the 802.15.4 standard was made in [28]. A link layer security protocol provides the following services: secure access control, message integrity, message confidentiality and replay protection. Also there are eight different security suits that imply various combinations of security services and three supporting keying models. The authors outline such protocol weaknesses as lack of group keying, easy to break integrity protection etc.

Evaluation. The technologies mentioned above do provide security services, but suffer from the lack of safety. Therefore, to be able to cover heterogeneous networks they need to be complemented with suitable safety extensions. Lack of reliability leads to straitened TT data traffic support and reduced availability. Safety and security protocols are similar, as they are designed to limit the probability of malfunction or misuse. The main difference is that in order to reduce the risk of non-authorized access or similar, security protocols use cryptography, instead of relying on CRCs only, as most safety protocols do. A combination of these methodologies, limits the probability of successful attacks further, as safety protocols will detect deviations in timing or in configuration data immediately, which is yet another barrier for an intruder to bypass in order to get unauthorized access. If the safety protocol detects runtime deviations, the system will go to a safe state mode and can only be put into operation again by manual and a physical reset of the safety system. In addition, the safety system will alert the staff by high priority alarms when a deviation is detected for sake of limiting harm to people, property or environment.

VII. EVALUATION OF EXISTING SECURITY FRAMEWORKS

We consider here several examples of security frameworks representing different approaches of development; a framework for mixed wired and wireless networks and frameworks applying security on the application and IP layers respectively.

A. Security framework for heterogeneious networks

In [17] the author presents a framework for mixed wired and wireless industrial sensor networks using HART and WirelessHART for communication in process automation. It

can be concluded that there is usually a lack of security in wired networks and a lack of safety in wireless networks, as traditionally most systems have only one of them [29]. The author targets bringing both security and safety together for heterogeneous networks. The solutions are retrofitted on an existing architecture, to enable integration of wireless communications into existing wired networks. The idea is based on introducing a security module that provides end-to-end security and maintains authentication, integrity and confidentiality. This module is an additional security layer used on top of PROFINET IO [30]. PROFINET IO deals with peripheral devices and controls data-exchange. The framework treats safety and security in the same way and hides the differences. It is based on the idea of the black channel with which each level in the network provides services for both safety and security without relying on other layers. The black channel principle is based on that the safety layer has to implement measures to all possible error cases, and not rely on existing measures in other layers, in order to avoid a safety case for all intermediate layers, components and nodes. Thus, this introduces redundancy since most of the error cases are handled in parallel by other layers as well, but with varying residual risk of detecting each error case. The security and safety layers are thus separated and can be deployed independently. Such an approach can be considered as an example of the "defense-in-depth" method.

Evaluation. The framework supports mixed wired and wireless networks and its wireless part covers such security objectives as authentication, integrity and confidentiality, which is a benefit. However, the framework does not support ED or BE traffic classes. This solution is used in industry for many applications, but its applicability for highly critical use cases still needs further evaluation.

B. Security framework on the application layer

One example of a security framework working on the application layer is presented in [19]. The framework includes iterations with users in the loop, and solutions embedded into devices, hidden from the users are mostly discussed. The author proposes an approach for initial trust bootstrapping and life cycle managing. The application area is industrial networks and the solution is valid for heterogeneous networks. The security objectives considered are availability, device authentication, confidentiality, and system resilience. The proposed framework is based on the workflow that regulates the communication between the users of the network and the network itself. The framework consists of three main phases: initial trust establishment, device verification, and key generation. The approach was proved by implementation. The workflow protocol supports predefined configuration of the involved parameters (an approach which is common for wired networks), as well as adaptable configuration, when a device can join the network after successful authorization (an approach common in wireless networks). Also the framework supports the possibility to enter configuration data manually in new devices. Finally, it is able to support symmetric and asymmetric key distribution and does not require using shared predefined secret parameters. Another advantage of the solution is that the framework is flexible considering dynamic roles of employees.

Evaluation. This is a high-level framework. Therefore, it is suitable for heterogeneous networks and for different traffic-classes as there are no dependencies with lower layers. This independence is one of the main advantages. However, this also leads to a more limited set of possible security objectives. The framework targets authorized network access, but neglects such objectives as availability and reliability. This solution can be a part of a many-layers framework for DCS. It can be combined with low-level solutions that would protect, e.g., clock synchronization.

C. Security framework on the network layer

IPSec (Internet Protocol Security) [31] operates on the network layer and supports such security services as message integrity authentication, data encryption by different encryption algorithms, and message replay attack protection. There are two feasible ways of its realization, either in the End-Host or in the Router. Also, there are three possible architectures: integrated, BITS (bump in the stack) and BITW (bump in the wire). The first one implements IPSec directly into the IP layer itself. This way looks very natural, but since only IPv6 was designed to support IPSec, IPv4 still have to use BITS. BITS implies that IPSec becomes a separate layer between the network (IP) and the data link (network interface) layers, which will introduce some overhead in the stack. Finally, BITW assumes that hardware devices that can provide IPSec services can be added, which may or may not be possible. Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols are two principal parts of IPSec. AH supports message integrity, data authentication and replay attack protection services, whereas ESP supports encryption of whole datagrams. IPSec deals with keys through the Internet Key Exchange (IKE) protocol.

Evaluation. The framework is suitable for heterogeneous networks and can potentially support different data traffic classes. However, it lacks real-time support, but this could potentially be achieved by using an extension targeting enhancement of real-time properties, e.g., as in [14]. The framework also covers such basic security objectives as data integrity, confidentiality, and authentication. However, the ability to provide objectives such as reliability and availability will depend on the concrete implementation as well as the application requirements.

D. Frameworks comparison

The three considered frameworks are examples of solutions deployed on different layers and targeting different security objectives. Nevertheless, they can still be compared based on suitability for DCS. In Tab. 1 columns A, B, and C stand for the corresponding frameworks from subsections A, B and C respectively. CIA in the table stands for confidentiality, integrity and authentication. The evaluation shows that if we target several security objectives in one system, none of the frameworks fulfill all requirements. This means that existing

frameworks must be enhanced and combined in order to achieve the desired security level in networks for DCSs.

TABLE I. IDENTIFIER DECLARATION

Feature	A	B	C
Mixed network support	✓	✓	✓
Different traffic classes support	✗	✓	✗
Real-time support	✓	✓	✗
Covered security objectives	CIA for wireless part	Authorized network access	CIA

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we have investigated existing security solutions and frameworks suitable for a distributed control systems profile. We also specified the security requirements for the considered application domain and investigated the basic component of threat modeling. We considered three main types of classification of security frameworks; depending on if wired or wireless communication links are included, if support for different data traffic classes is provided and, finally, the layer in which the security framework is implemented on. We also investigated several existing security solutions and frameworks for wired and wireless industrial sensor networks and found that although they all have different benefits and drawbacks, and no existing solution or framework has all the required properties. We can also conclude that if security can be added already at the design stage, much is gained.

IX. ACKNOWLEDGMENTS

The research leading to these results has received funding from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme FP7/2007-2013/ under REA grant agreement n°607727. E. Uhlemann is partly funded by the Knowledge Foundation through the WIRE project. E. Uhlemann, J. Åkerberg and M. Björkman are partly funded by the Knowledge Foundation through the READY project.

REFERENCES

[1] P. Gaj, J. Jasperneite, and M. Felser, "Computer Communication Within Industrial Distributed Environment—a Survey," *IEEE TII,* vol. 9, no. 1, pp. 182-189, Jul 2012.

[2] J. Åkerberg, M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," *in Proc. INDIN*, Portugal, July, 2011, pp. 410-415.

[3] V.C. Gundor and G.P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches," *IEEE TIE,* vol. 56, no. 10, pp. 4258-4265, 2009.

[4] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE TII,* vol. 9, no. 1, pp. 277-293, Feb 2013.

[5] D. Dzung, M. Naedele, T. P.Von Hoff, and M. Crevatin, "Security for Industrial Communication Systems," *Proc. IEEE,* vol. 93, no. 6, pp. 1152-1177, 2005.

[6] H. Kopetz and W. Ochsenreiter, "Clock Synchronization in Distributed Real-Time Systems," *IEEE Transactions on Computers,* vol. C-36, no. 8, pp. 933-940, 1987.

[7] M. Ullmann and M. Vögeler, "Delay attacks - implication on NTP and PTP time synchronization," *in Proc. International Symposium on Clock Synchronization for Measurenment, Control and Communication (ISPCS)*, Brescia, Italy, Oct., 2009.

[8] E. Penera and D. Chasaki, "Packet scheduling attacks on shipboard networked control systems," *in Proc. Resilienca Week (RWS)*, Philadelphia, PA, 18-20 Aug., 2015, pp. 1-6.

[9] J.-D. Decotignie, "Ethernet-Based Real-Time and Industrial Communications," *Proc. IEEE,* vol. 93, no. 6, pp. 1102-1117, Jun 2005.

[10] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proc. IEEE,* vol. 93, no. 6, pp. 1130-1151, 2005.

[11] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection," *IEEE TII,* vol. 4, no. 2, May 2008.

[12] J. Åkerberg, M. Gidlund, T. Lennvall, J. Neander, and M. Bjorkman, "Efficient Integration of Secure and Safety Critical Industrial Wireless Sensor Networks," *EURASIP J. on Wireless Commun. and Netw.,* vol. 2011, no. 1, November 2011.

[13] T. Xie and X. Qin, "Scheduling security-critical real-time applications on clusters," *IEEE Transactions on Computers,* vol. 55, no. 7, pp. 864-879, Jul 2006.

[14] E. Lisova, E. Uhlemann, J. Åkerberg, and M. Björkman, "Towards secure wireless TTEthernet for industrial process automation applications," *in Proc. Emerging Technologies and Factory Automation (ETFA)*, Barcelona, Spain, Sep., 2014.

[15] T. Mizrahi, "Time Synchronization Security using IPsec and MACsec," *in Proc. IEEE ISPCS*, Munich, Germany, Sep, 2011, pp. 38-43.

[16] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Sensor network security: more interesting than you think," *in Proc. USENIX HotSec*, San Jose, CA, Jul, 2006, pp. 5-5.

[17] J. Åkerberg, *On Safe and Secure Sommunication in Process Automation*, Doctoral thesis, Mälardalen University, 2011.

[18] R. A Gupta, A. K. Agarwal, M.-Y. Chow, and W. Wang, "Performance Assessment of Data and Time-Sensitive Wireless Distributed Networked-Control-Systems in Presence of Information Security," *in Proc. MILCOM*, Orlando, FL, Oct, 2007, pp. 1-7.

[19] A. Ray, *Initial Trust Establishment For Heterogeneous Industrial Communication Networks*, Licentiate thesis, Mälardalen University, 2014.

[20] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 24011998.

[21] H. Altunbasak and H. Owen, "An arhitectural framework for data link layer security with security interlayering," *in Proc. SoutheastCon*, Richmond, VA2007, pp. 607-614.

[22] S. Raza, A. Slabbert, T. Voigt, and K. Landernas, "Security considerations for the WirelessHart protocol," *in Proc. ETFA*, Mallorca, Spain, Sep, 2009, pp. 1-8.

[23] W. Steiner, G. Bauer, B. Hall, and M. Paulitsch, "*TTEthernet: Time-Triggered Ethernet*," in *Time-Triggered Communication*, R. Obermaisser, Ed., ed CRC Press, IDate, 2011.

[24] W. Steiner, "Candidate security solutions for TTEtnernet," *in Proc. DASC*, East Syracuse, NY, Oct, 2013, pp. 1-10.

[25] K. Koscher, A. Czeskis, F. Roener, and S. Patel, "Experimental Security Analysis of a Modern Automobile," *in Proc. IEEE Sym. SP*, Oakland, CA, May, 2010, pp. 447 - 462.

[26] S. Giannouslis, C. Koulamas, C. Emmanouilidis, P. Pistofidis, and D. Karampatzakis, "*Wireless Sensor Network Technologies for Condition Monitoring of Industrial Assets*," in *Advances in Production Management Systems. Competitive Manufacturing for Innovative Products and Services*, ed: Springer Berlin Heidelberg, IDate, 2011, pp. 33-40.

[27] G. Lackner, "A Comparison of Security in Wireless Network Standards with a Focus on Bluetooth, WiFi and WiMAX," *Int. J. Netw. S.,* vol. 15, no. 6, pp. 420-436, 2013.

[28] N. Sastry and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks," *in Proc. ACM WiSe*, Philadelphia, Pennsylvania, Oct, 2004, pp. 32-42.

[29] C. W. Axelrod, "Applying Lessons from Safety-Critical Systems to Security-Critical Software," *in Proc. IEEE LISAT*, Farmingdale, NY, May, 2011, pp. 1-6.

[30] A. Poschmann and P. Neumann, "Architecture and Model of Profinet IO," *in Proc. AFRICON*, Sep, 2004, pp. 1213-1218.

[31] S. Kent and S. Seo, Security Architecture for IP IETF RFC 4301, Dec 2005, http://www.rfc-editor.org/rfc/pdfrfc/rfc4301.txt.pdf