Attitudes and perceptions of IoT security in critical societal services

Mikael Asplund, *Member, IEEE,* Simin Nadjm-Tehrani, *Member, IEEE,*

***Abstract*—A quiet revolution that impacts several sectors, ranging over transport, home automation, energy, industrial control, and health services is undergoing with addition of new networked devices leading to enhanced services. In this paper we aim to identify information security requirements that are common over several (vertical) sectors, and in particular, ones that impact critical societal services, namely the energy, water, and health management systems. We present the results of an interview-based study where actors in these sectors were asked about their perceptions and attitudes on the security of Internet of Things (IoT). We set these perceptions and attitudes in context through a literature review of IoT security, and relate to current challenges in this area. The study demonstrates that despite an overall optimistic view on IoT in critical societal services, there is a lack of consensus on risks related to IoT security.**

***Index Terms*—Internet of Things, Security, Risk, Critical infrastructure, Health**

I. Introduction

The modern society depends on critical infrastructures and the services they provide, here referred to as critical societal services (CSS). They provide us with electricity, water, heat, and ways to travel, communicate, and trade. Traditionally, these vital systems have been kept isolated to avoid security threats and performance disturbances. However, a silent revolution is underway as more and more of them are becoming part of the Internet of Things (IoT), e.g., through smart grids, intelligent transportation systems, body sensor networks and intelligent habitats. There is a strong rationale for this transformation. For example, Internet-connected embedded systems can be upgraded and adapted to changing needs on demand, useful information can be immediately collected from remote geographic areas, and fault diagnosis and system restarts can be made more efficient and cost-effective by not having to send out technicians to remote places.

While several sectors, e.g. smart metering infrastructures and car-to-car communication are moving forward driven by markets and technological advances, some sectors are more hesitant to make new investments within CSS. These are being held back by the fact that Internet-connected systems are also more vulnerable to security threats. Key actors in these industries are aware of the potential benefits of IoT-technologies but are not willing to risk their core assets to be compromised as demonstrated in the case of the Stuxnet attack where Iranian SCADA systems believed to be protected from Internet access were infected with malicious code.

Department of Computer and Information Science, Linköping University, Sweden e-mail: (mikael.asplund@liu.se, simin.nadjm-tehrani@liu.se)

Thus, eagerness for reaping benefits from the technology go in parallel with consciousness about its pitfalls. For example, while there is a clear drive for utilising the potential of IoT in the so called smart grids, e.g. in the national action plan for Sweden 2015-2030, the working group notes the necessity of security awareness (recommendation 4.2.4) and customer privacy (recommendation 4.3.2) among a long list of recommendations regarding political, marketing, societal and individual user perspectives [1].

In another major field of IoT applications, the smart home, including wearables and fitness enhancing applications recent documents entirely devoted to the security requirements are being discussed (with a release of draft 2 of the online trust alliance in October 2015[1]). Clearly, IoT will infiltrate everyday life in many shapes and forms, and the research community needs to prepare for a security-conscious development of these technologies for the society to embrace the front edge of innovation.

The purpose of this document is to highlight the risks and attitudes to risks of IoT in some of the core services of society, electricity, water, and healthcare. These sectors, while in many respects very disparate, each with its own community, regulatory bodies and set of technologies, are also in many respects similar. They are all critical, and cannot be allowed to fail, at least not for any extended period of time. As these sectors inevitably move to adopt IoT solutions, they also open up for new cyberattacks that were previously not possible. While recent surveys have made a clear case for the security challenges in IoT within industrial contexts, our work confirms the points made by performing interviews in three hitherto not elaborated application areas. Sadeghi et al. [22] have a focus on IoT in industrial production systems, and Granjal et al. [7] review the communication protocol aspects with a focus on physical and MAC layer protocols, equally applicable in any area adopting those protocols. Jing et al. [11] analyse security issues on three layers: perception, transportation and application layers. They cover issues in transportation and smart building applications. In our case, the focus is on risk assessment as perceived by actors in critical societal services (energy, water and health monitoring).

In order to facilitate the uptake of IoT solutions in these critical sectors, one has to address the security concerns that otherwise hamper the development of better, more efficient and potentially safer systems. Our contribution to this process is to:

[1] https://otalliance.org/initiatives/internet-things

- Provide a literature review of security research related to IoT in these domains.
- Investigate the attitudes and perceptions among industry actors on opportunities and risks associated with IoT in their sectors.

The results in the paper builds on workshops and interviews where input from 18 participants within these sectors was gathered, as well as a literature review. The workshops were organised to gather key experts and stakeholders from the three targeted sectors. These workshops served both as a means to identify known core issues related to IoT in the respective areas, and also to try to find commonalities and differences between sectors to see what, if any, these sectors can learn from each other on IoT security.

The interviews were conducted with representatives from these industries and were based on questions that were produced as outcomes from the pre-interview workshops. The interviews provided a means to reach out to a larger group of stakeholders without requiring an unreasonable amount of time from their part.

The rest of this paper is organised as follows. Section II provides an overview on the literature related to IoT security in a number of society-critical vertical sectors. We then proceed to present the interview study we performed with actors in three of these sectors, first describing the methodology in Section III, the results in Section IV and our attempt at synthesis of these results in Section V. Section VI concludes the paper.

II. Emerging Threats

When moving from the enterprise networks to networks built from a mix of end devices (handheld devices, embedded devices, isolated sensors) together with operation centre computers we are faced with two security issues: a) new attack surfaces appearing, and b) the old defence strategies no longer being valid.

A. New attack surfaces

In the past two years news are flooded with items where the main message appears to be the emerging threat of massive IT breaches. In January 2014, Proofpoint a leading security-as-a-service provider reported a (claimed) first uncovering of massive IoT originated attacks[2]. In a two week period where massively distributed malicious mail was profiled, over 25% of the volume was generated by things that were not laptops or computers. So what does this entail for future deployments of IoT i critical societal services?

The health sector may be viewed from two perspectives. Compared to other sectors, it is both more conscious of attacks and vulnerabilities [9], [17], and less willing to incorporate security. The latter is due to the fact that the sector sees the potential of IT solutions against the background of increasing costs for health services – only in Sweden the IT costs in the health sector (Landstinget) were 8.56 billion SEK in 2013 (this against the total public healthcare costs that in total amounted to 238 billion SEK in 2012). Hence, from the second perspective, there are numerous potentials for deploying new technology to improve current services (e.g. Najera et al. [18], Amendola et al. [2]). Lake et al. [13], from Cisco systems, clarify a provider perspective, and emphasises the necessity of understanding the device data life cycles when considering the architectural security implications.

From the first perspective, a representative example is in the diabetes area (artificial pancreas experiments). A review of 33 studies has shown that consideration of the wireless security dimension was absent, and the review provides a good starting point for future systematic studies [20]. Kumar and Lee [12] cover a wide range of misuse leading to data integrity and privacy issues when sensors are used in the medical applications.

Somewhat paradoxically, the sector is extremely aware of the trade-off between patient safety and access barriers for the sake of security. Wilkowska and Ziefle [25] provide a user perspective and study security and privacy requirements using an empirical approach based on focus groups. They found that females and healthy adults insist on highest levels of security standards, compared to males and ailing elderly subjects.

The big picture with respect to incorporation of IT in health services, is thus very complicated. New dimensions are being added to the classic threat picture as a result of incorporation of digital patient records[3], and one could argue that not all of the new elements added to the threat landscape are related to deployment of IoT.

In what follows we give a selection of potential IoT-specific attacks disclosed in the scientific literature or news media. In July 2015 the US Federal Drugs Administration (FDA) stopped an infusion pump due to a security breach[4]. The reason mentioned was that the the computerized pumps could be accessed remotely through a hospital's network, but it doesn't know of any cases where that has happened. Earlier the same year the FDA and the Homeland Security Department's Industrial Control Systems-Cyber Emergency Response Team issued warnings about potential vulnerabilities of Hospira's LifeCare PCA 3 and PCA5 pumps. According to the supplying company a newer version of the product (Plum 360), does not have the same vulnerability.

Moving to other domains, the automotive sector has had a visible position in the news streams. The well-known FIAT-Chrysler hack[5], resulted in 1.4 million recalls in May 2014. Following reports that cybersecurity researchers had managed to turn off the engine of a Jeep Cherokee while driving, exploiting a wireless network interface. Later in February 2015 reports showed how BMW cars were found to use insufficient security when adopting DES encryption for their Connected-

[2]Multiple attacks originating from IoT: http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

[3]Electronic records hack: https://securityledger.com/2015/07/doctors-still-in-the-dark-after-electronics-records-hack-exposes-data-on-4-million

[4]Infusion pump stopped by FDA: http://www.stltoday.com/business/local/citing-hacking-risk-fda-says-hospira-pump-shouldn-t-be/article_ff050ace-44fc-5c31-8419-0359fc7a46f8.html

[5]FIAT-Chrysler hack: http://www.reuters.com/article/2015/07/31/us-fiat-chrysler-hacking-regulator-idUSKCN0Q525U20150731

Drive capability[6]. Attacks through a CAN network of a car is being taken seriously as a safety hazard, and lawsuits in this context are mounting up[7]. In a more recent account, also using wireless connection, a car anti-theft capability was disabled [24].

Within the home automation sector, we have seen attack vectors towards several household items, including a fridge[8], and a smart TV [19]. While these threats individually may not be considered serious from a societal security perspective, the large scale exploitation scenario mentioned by Proofpoint above, makes all such seemingly low level vulnerabilities important.

Moving on to the energy distribution sector, several recent papers show that opening up the SCADA networks to external devices enables adversaries to perform attacks on the networks (that obviously relate to critical services). Among the protocols that appear in the context of SCADA networks we find Modbus, DNP3, and IEC-60870-5-104. Several recent works address attacks and countermeasures for networks operating these protocols.

To mention a few, a man-in-the middle attack on the IEC-60870-5-104 protocol was described by Maynard et al. [16]. Further work by Yang et al. [26] lists eight known attacks on the IEC-60870-5-104 communication and builds a signature-based defence approach on these. Other work describes attack step sequences that include crafting legitimate but malicious DNP3 packets so that 4 circuit breakers can be opened simultaneously in a 30 bus network [14]. Hoyos et al. [10] describe a message authentication attack on a network operating with the IEC-61850 standard and running the GOOSE protocol. Several examples of attacks feasible on Programmable Logic Controllers (PLCs) that run a Modbus protocol are described in the literature [8]. Caselli et al. [3] describe how message sequences can be abstracted to obtain a discrete time Markov chain model for three different protocols in the SCADA contexts. This may pave the way for SCADA-specific intrusion detection approaches. Moving on to smart grid infrastructures we see descriptions of potential attacks on smart grids and how the dynamics of such networks differ in terms of timing characteristics compared to traditional ones [23].

Altogether, these analyses indicate that a serious look at risks is needed before an unprotected device is embedded in potentially sensitive contexts. However, the residual risks may not be easy to mitigate as we indicate below.

B. Old strategies no longer useful

A basic problem that has to be resolved with respect to securing IoT applications is the question of resource efficiency for security building blocks.

Although studying the cost of hardware designs for security is subject to meticulous studies (see e.g. Good and Benaissa [6]), the resource costs of adding security implemented in software is much less studied. A relatively early study of the resource costs was in the context of adding security mechanisms to tactical networks [15]. Lake et al. [13] state that the "the biggest challenge from the device side is that a lot of M2M/IoT devices do not have enough capability to do the encryption on the device."

One of the most well-known and well-used intrusion detection mechanisms is Snort with rules dynamically updated to recognise tens of thousands of adverse conditions. Chang et al. [4] compare the RAM usage benchmarking of Snort, which at peak rate shows a 1.2 GB memory usage, with the 512MB of RAM in a Raspberry Pi computer. They then describe the steps taken to enable lightweight intrusion detection by implementing memory-efficient representations of Snort rules and CPU-efficient algorithms to work in real-time in tactical devices. Any new mechanism that addresses adding new devices to a network needs to enhance the arsenal of defence mechanisms that work in the resource-constrained settings.

A timing attack on the IEC-61850-8-1 authentication mechanism [10] shows that since the computation capacity of embedded processors for running an authentication algorithm currently exceeds the needed 4ms response time, a successful attack would be able to create an automation breakdown, including damaging circuit breakers and power transformers.

A recent survey of IoT technologies [5] includes some exposure to how IoT technologies (device management, wireless connectivity, protocols) address security issues. In general, no IoT-specific security mechanisms with well-understood resource footprints are currently available.

III. Interview study

In this section we describe the interview method and provide an overview of the type of questions we asked, the selection of respondents and the rationale for making these choices.

A. Questions

The questions that were asked in the interviews were designed in a set of workshops with participants from Linköping University, security consultancy company Sectra, and two utility companies from central/south Sweden (Tekniska Verken and Mälarenergi). Fig 1 presents an overview of the methodology for the study. The principles guiding the questionnaire design were:

- The questions should be answerable by persons with varying technical background and expertise, as well as from different sectors.
- The questions should be open enough to catch trends, ideas and phenomena that we did not foresee from the start.
- The questions should be specific enough to provide insights into the state of IoT security.
- The length of the interviews should not exceed one hour.

The full set of questions is available in the Appendix. In summary, the questions are divided in three sections (1) general background to get basic data about the organisation and persons being interviewed, (2) questions on the respondents perceptions about enablers, drivers and obstacles of IoT in

[6]BMW ConnectedDrive: http://m.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html

[7]Lawsuits against car manufacturers: http://www.computerworld.com/article/2895057/telematics/lawsuit-seeks-damages-against-automakers-and-their-hackable-cars.html

[8]Fridge revealing password: http://summa.talentum.se/article/dt/senaste/kyl-delar-ut-gmail-losen/207838

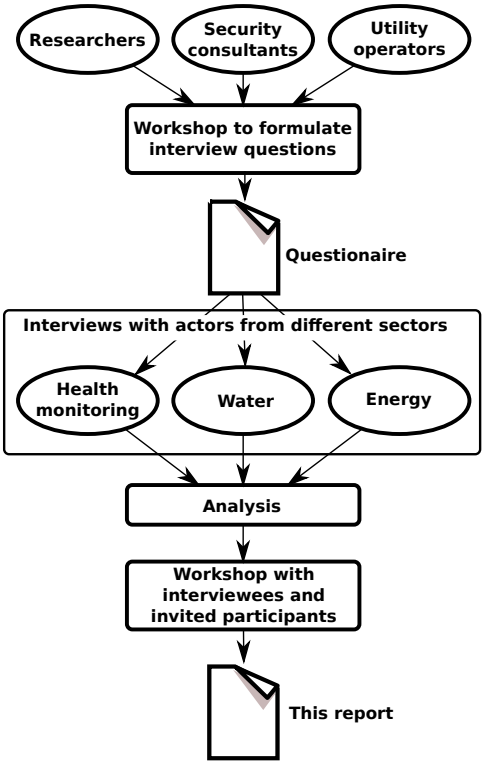

Fig. 1. Methodology overview

their sector at large and (3) questions regarding risks, threats and critical infrastructure in relation to IoT.

B. Actors

As one of the ambitions in this study is to find common security challenges and solutions for IoT in critical services, we have made an effort to include representatives from different sectors in the study. We have chosen to focus on both on the traditional critical infrastructure sectors water and electricity as well as the health sector where a new form of critical infrastructure is emerging in the form of home care and telemedicine.

We conducted interviews and workshops with representatives from the following organisations:

- Tekniska Verken, Swedish utility provider
- Xylem, International water technology provider
- Mälarenergi, Swedish utility provider
- Vattenfall, International electric utility provider
- Svenska Kraftnät, Swedish National Grid, main transmission system operator
- Linköping university, Dept. of Medical Technology, academic institution
- Region Östergötland, Regional public health care
- STRI, consultancy in the electricity sector
- Nielsen Innovation, consultancy in the health sector
- Tritech, embedded systems supplier and consultant
- Respiheart, small startup in the health sector

Table I shows the distribution of participants according to sector and type of role that the participants had in the organisation. In cases where multiple cells would be applicable, we have chosen the one with the best match.

TABLE I
PARTICIPANTS IN THE STUDY CATEGORISED BY SECTOR AND TYPE OF PROFESSIONAL ROLE

	Electricity	Health	Water	Total
Strategy	3	1	1	5
Development	5	2	1	8
Operation	2	1	2	5
Total	10	4	4	18

IV. Results of interviews

We now proceed to summarise the responses given in the interviews and workshops on the role of IoT in the respective sectors, and the associated risks and infrastructure dependencies that surround it. Due to the complexity of the subject and the variation in professions the result of the interviews is presented primarily in the form of summaries and quotes. To protect the individuals and companies that kindly agreed to participate in the study we do not provide the exact source for each quote (they are intended to illustrate a point rather than to be propagated as being the official opinion of a given organisation).

A. General perceptions on IoT

Before diving into questions on IoT adoption and security, we asked the respondents what they associated with the concept Internet of Things. Apart from a couple of people that had not previously heard the term, most associated it with consumer products such as home automation and connected vehicles. Some brought up connection with their own field and the increase of connectivity and intelligent control that is happening in society today. We also adopt this latter definition of IoT that includes all kinds of connected devices whether they be consumer products, medical equipment or industrial control systems.

B. IoT drivers, enablers and obstacles

a) Drivers: With a common understanding of the definition of Internet of Things that includes the transformation of existing and often isolated control and monitoring systems to networked systems, we asked the respondents about what they see as the main benefit of IoT in their specific field in the coming 5-10 years.

As expected, the responses focus on improving existing services. In many cases the ability to monitor equipment from a distance is seen as the main advantage, since this saves time and money compared to personnel physically travelling to the site. This also affects the equipment suppliers that can perform maintenance and install software updates automatically. Moreover, the information gathered is often perceived to be of better quality (more data and more frequently) than before. In the water sector, there is significant environmental regulation that must be followed, something which is facilitated with IoT technology. In healthcare, the time of the doctor can be used

more efficiently than having to take samples and having to wait for results if the information is already available at the first meeting with the patient.

"The patient can do more already before they arrive at the hospital"

Many of the cost savings associated with IoT seem to be indirect in the sense that this technology allows increased services to be provided without increasing the staff. In some cases the costs are actually increasing (e.g., additional investments in equipment).

"We can push the net a little closer to its limit"

In addition to improving existing services, IoT is often hailed as a technology that can revolutionise industries by providing completely new business models. Instead of a supplier just providing a product, IoT allows the product to be made into a service where the consumers pay for what they use. However, it seems as if critical infrastructure such as water and electricity cannot be that easily fit into this business model. In the health sector there is clearly a trend where healthcare and fitness applications converge, for example in the form of heart rate monitors, something which can also can work as a driving factor.

b) Enablers: We asked the respondents what they believed to be the enabling factors for IoT in their sector. The question was initially phrased as an open question, but the respondents were also given alternatives to complement their immediate reaction.

Improved technical solutions is perceived as the primary factor, with some respondents explicitly mentioning the common IP standard as a key factor. Moreover, the lower cost of equipment are considered by some as important. Several of the respondents emphasized an aspect that we had not foreseen, which is that young people, both customers and employees expect systems to be connected and available.

"It is a generational difference"

Finally, factors such as legislation, standards, and reference projects were mentioned but only by two people.

c) Obstacles: The opinions regarding obstacles to IoT in the respective sectors of the respondents were more diverging. In contrast to the enabling factor of young people expecting a certain technological level of system, there seems also to exist a deep scepticism to adding new unproven technologies to critical systems. In particular the utility companies described their sectors as conservative, and also lacking in IT competence.

"There is a lack of IT maturity"

"All new technologies have childhood drawbacks"

Raising the above point confirms the healthy skepticism towards adding new IoT technologies in the utility sector. This was strengthened by another comment

"All protection mechanisms come with a threat to availability"

The respondents lift the importance of including aspects such as IT security to engineering education in general, since future engineers will encounter these issues to an increasing extent. Moreover, one must also recognise that while IT is rapidly becoming an integral part of most critical infrastructures, there are also elements that are essentially the same now as 20 years ago. Investments made in electrical distribution systems can have an economic life of 40 years or more.

"Retrofit is expensive"

Adding IoT solutions to legacy systems is much more expensive than including them in the development of new products. Therefore, the transition to "connectivity anywhere" for critical infrastructure is likely to go on for many more years.

IT security is brought up by several respondents as an obstacle for IoT deployment. In the medical sector for example, all equipment must be tested and certified by appropriate authorities before allowed in medical use. The regulations surrounding these products is of course an obstacle for rapid deployment of IoT, but probably something we should be grateful for.

Finally, the lack of standards and interoperability is brought up as obstacles. In particular for next generation consumer product development where wireless connectivity is an important feature, there is great uncertainty how the market will evolve in the coming years.

C. Risk perceptions

In the interviews we asked the respondents a number of questions specifically intended to find out their attitudes in relation to risks and threats associated with IoT in their respective sectors. We first asked this as an open question where they answered spontaneously, and then followed up with a number of specific threats and asked them to rank the risk (which we explained as being the combination of probability and likelihood) as low, medium or high.

In response to the first open question, we got a wide range of answers with no clear common theme. Several alluded to the fact that we are building systems where the risks and threats will be seen only at a much later stage.

"We create an infrastructure on which we then start to depend"

"It is easy to connect things together, but much harder to decide what should be allowed to steer what"

Several mentioned cyberattacks as a threat, with some varying ideas on their potential motive, including youngsters doing it for fun, terrorism, and financial gain. In the health sector for example, medical data could be considered valuable for insurance companies.

"There is a market for this type of information"

Finally, several of the respondents were of the opinion that there are no significant risks associated with IoT, since all risk factors are already accounted for in the normal design of systems.

Going into details of specific threats, this "low risk" perception was the dominating one. Table II details the answers to

TABLE II
RISK PERCEPTIONS FOR SPECIFIC THREATS AGAINST IOT IN CRITICAL SERVICES

Threat	Low	Medium	High	Unsure	Total
Communication failure	9	3	2	0	14
Power failure	8	3	1	2	14
Failing equipment	6	3	2	3	14
Data loss	7	4	1	2	14
Confidentiality loss	8	2	1	3	14
Integrity loss	7	3	0	4	14
Deliberate hacking	4	5	1	4	14
Malicious code	4	4	2	4	14
Total	53	27	10	22	112

this question (only by those participating in the interviews not in workshops). However, in almost all cases there were those who labelled the same threat as a high risk. The difference in responses does not follow any particular pattern with regards to sector or professional role. Rather, it seems like the attitudes with regards to IoT risks are based on individual experiences and perception of what might come in the future.

D. Infrastructure dependencies

Finally, introducing IoT in previously isolated. stand-alone systems creates new infrastructure dependencies since both electricity and communication is required for IoT solutions to function. Therefore, we queried the respondents on their current requirements with regards to these two infrastructure services as well as what they believed the requirements would look like in 10 years time (year 2025).

The result is clear. Provision of electricity is predictable, available (more than 99.99% at the distribution level), and is surrounded with regulation, processes and a culture of rigorous testing before new deployments. In the cases where even higher service availability is required (e.g., some medical services) there are battery solutions as well as emergency power production systems.

Communication infrastructure on the other hand seems to be much more of a patchwork. Organisations that require a very high degree of availability and reliability for their communication systems create their own network (as in the case with Svenska Kraftnät), whereas other organisations struggle with sometimes failing network links. Several of the respondents mention that their respective organisation is in the process of creating redundancy solutions to reduce the consequences of a failing network link. Note that this difference cannot be seen in Table II (rows 1 and 2), thus underlining that there is a large degree of uncertainty on how large these risks actually are. If the risk of communication failure is low, why then invest in more redundancy?

There was a wide consensus that the requirements on reliability and availability of communication infrastructure will be increasing in the coming years. Both in terms of regulatory requirements (e.g., the recent prescripts by Swedish Post and Telecom Authority on dependability of communication networks[21]), as well as requirements based on operational needs.

V. SYNTHESIS

We now try to make a synthesis out of the workshop and interview material and provide our own reflections on the similarities, differences, and the main take-aways from this study.

A. Similarities and differences between verticals

One of the hypotheses that motivated the cross-sectorial nature of this study was that IoT security poses similar challenges in otherwise very disparate businesses. The result of the interviews partly supports this hypothesis. Some commonalities that appears across sectors include:

- IoT is mainly seen as a way to improve existing services and reducing costs.
- Legacy systems and high criticality of services sometimes restrict or slow down adoption of IoT solutions.
- System availability is more important than confidentiality of data.
- There is a large degree of uncertainty and lack of consensus regarding threat assessment and potential risks related to IoT.

There are also some differences in attitudes and rate of change in these sectors. The electricity sector sticks out since the respondents themselves describe it as “conservative” and reluctant to change. This is clearly related to the culture of maintaining safety, and availability, thus requiring a technology to be mature and well-tested before being introduced in these systems. Standardisation work plays an important role in the development of new technologies, since operability is of key importance.

The health sector on the other hand, appears to be more dynamic, with a multitude of ongoing IoT-related projects and initiatives. Since the patient safety is always put in the first room, the consequences of failure of most IoT-related equipment are well-considered. First, the failure of medical equipment seldom affects more than one patient, second, all medical treatment has a human in the loop that can react to anomalies in the data, and finally, an incorrect or missing action can often be corrected before it results in negative consequences (i.e., there are fewer cases where correct decisions must be taken within milliseconds). This allows a larger degree of versatility in prototypes and potential IoT-related products.

The water sector shares some of the characteristics with the electricity sector, but is again associated with a longer time scale. Moreover, the respondents in our interviews described the water sector as being “behind” the electricity sector on issues related to ICT, in particular with regards to dependability and security.

B. Who cares for IoT security?

An important and unforeseen aspect that came up in the interviews with people from different roles in the organisations, was the risk of cybersecurity for SCADA systems ending up without a clear organisational match. Most larger organisations have established roles, policies and processes for IT security of their enterprise systems. Typically there is an IT-department

that is responsible for procurement and maintenance of IT equipment. However, SCADA systems are considered the responsibility of the developers and technicians that operate them. In at least one of the organisations we were in touch with on this issue clearly stated that the person responsible for information security did not want to take responsibility for security of the SCADA systems.

This means that the persons that develop and operate the SCADA equipment need to have skills and competence in cybersecurity. Moreover, security is not just about doing it right the first time when creating a system (i.e., ensuring that communication protocols offer the appropriate level of protection and having sufficient authentication mechanisms). At a minimum it also requires continuous software updates, policies for key and password management and renewal, staff training and mechanisms for monitoring system integrity.

C. How to make threat assessments

Given the large variety in risk perceptions related to IoT security in our study, it is relevant to ask why this is so, and what needs to be done to dispel the shrouds of uncertainty that seem to surround this question. As we stated in Section IV-C, we could not see any particular pattern among the respondents that could explain the variation, and we hypothesise that it is up to individual assessment of how cyberthreats will develop in the coming years.

Underestimating the risks of cyberattacks can lead to serious damages if they do occur and overestimating them will probably result in unnecessary investments in security products, personnel costs, and consultancy services. Moreover, if one is focusing on the wrong type of threats one might even end up with both of these negative effects. Therefore, it is of utter importance for actors that provide critical services to society to correctly asses what the major risks are and how to tackle them.

To summarise the insights from the three subsections, there are more commonalities than differences to these seemingly different sectors. In all the sectors there was a diversion of opinions in terms of risk perception, which may result in scenarios with security being retrofitted. Future investments in protection mechanisms should be grounded in a clear awareness of risks. Adding competence to organisations is an enabler of increased awareness.

VI. Conclusions

The interviews confirmed many beliefs we had at the start of the study such as how availability rather than data confidentiality is prioritised in critical domains and that the rate of adoption of IoT is slower in these sectors partly due to concerns around security. There were also some surprises, like the large variations in risk perceptions associated with cyberthreats against IoT systems, the lack of ownership of IT security for embedded devices, and the overall assertion that despite whatever risks there might be, the advantages of IoT outweigh the drawbacks. The number of interviews performed is, however, not large enough to mandate a general classification of security risks in the given areas.

The studied literature in this study leaves no doubt that security ought to be an important part of future deployment of IoT in critical services. If the existing threats are not taken seriously, and the countermeasures against them are not created in a well-thought and holistic fashion, we will end up in a patchwork of multiple technologies with too many holes to be able to economically address them in future scenarios. Of course, there is a growing amount of security competence in the IoT developer community. Leveraging this competence is dependent on the investor perspective. If the awareness of risks and the need for a given protection level is not present, then no one will place an order for it. Hence, our study has focused on the purchaser perspective as opposed to the provider perspective.

While our review of recent research indicates that the new threat landscape and the criticality of application of IoT mandates a focus on new technical research in the energy sector, the e-health provides a richer set of problems. Several aspects of e-health are intertwined with the home-care and the smart home arena. Here, the usability aspects are already challenging and a major focus of research. Adding security will accentuate that challenge and needs to be in concert with it.

Finally, the incorporation of IoT can itself be part of the solution and not only part of the problem. There are indications that the whole landscape of threats and countermeasures is undergoing a new transformation, where the same technology, e.g. viral spreading of code to harm, may have a benefit as a countermeasure if used in the right way in the IoT context.

Acknowledgement

The authors would like to thank all the people that kindly agreed to participate in interviews and workshops. The work was initiated in a project supported by Vinnova, Formas and the Swedish Energy Agency under the IoT strategy program and completed within RICS: the research centre on Resilient Information and Control Systems (www.rics.se) financed by Swedish Civil Contingencies Agency (MSB). The first author was also supported by CENIIT project 14.04.

References

[1] Planera för effekt! Final report from the Coordination Council for Smart Grids (in Swedish), Swedish Government Official Reports (SOU 2014:84). ISBN:978-91-38-24204-9.

[2] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco. Rfid technology for iot-based personal healthcare in smart spaces. *Internet of Things Journal, IEEE*, 1(2), 2014. doi: 10.1109/JIOT.2014.2313981.

[3] M. Caselli, E. Zambon, J. Petit, and F. Kargl. *Critical Infrastructure Protection IX: 9th IFIP 11.10 International Conference, ICCIP 2015, Arlington, VA, USA, March 16-18, 2015, Revised Selected Papers*, chapter Modeling Message Sequences for Intrusion Detection in Industrial Control Systems, pages 49–71. Springer International Publishing, Cham, 2015. doi: 10.1007/978-3-319-26567-4˙4.

[4] R. J. Chang, R. E. Harang, and G. S. Payer. Extremely lightweight intrusion detection (elide). Technical report, Adelphi, Army Research Laboratory, 2013.

[5] V. Gazis, M. Gortz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger, and E. Vasilomanolakis. A survey of technologies for the internet of things. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*, 2015. doi: 10.1109/IWCMC.2015.7289234.

[6] T. Good and M. Benaissa. Asic hardware performance. In M. Robshaw and O. Billet, editors, *New Stream Cipher Designs*, volume 4986 of *Lecture Notes in Computer Science*, pages 267–293. Springer Berlin Heidelberg, 2008. doi: 10.1007/978-3-540-68351-3˙19.

[7] J. Granjal, E. Monteiro, and J. S. Silva. Security for the internet of things: A survey of existing protocols and open research issues. *IEEE Communications Surveys Tutorials*, 17(3), 2015. doi: 10.1109/COMST.2015.2388550.

[8] D. Hadžiosmanović, R. Sommer, E. Zambon, and P. H. Hartel. Through the eye of the plc: Semantic security monitoring for industrial processes. In *Proceedings of the 30th Annual Computer Security Applications Conference*, ACSAC. ACM, 2014. doi: 10.1145/2664243.2664277.

[9] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy (SP)*, 2008. doi: 10.1109/SP.2008.31.

[10] J. Hoyos, M. Dehus, and T. Brown. Exploiting the goose protocol: A practical attack on cyber-infrastructure. In *Globecom Workshops (GC Wkshps), 2012 IEEE*, 2012. doi: 10.1109/GLOCOMW.2012.6477809.

[11] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu. Security of the internet of things: perspectives and challenges. *Wireless Networks*, 20(8), 2014. doi: 10.1007/s11276-014-0761-7.

[12] P. Kumar and H.-J. Lee. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1), 2012. doi: 10.3390/s120100055.

[13] D. Lake, R. Milito, M. Morrow, and R. Vargheese. Internet of things: Architectural framework for ehealth security. *Journal of ICT Standardization, River Publishing*, 1, 2014. doi: 10.13052/jicts2245-800X.133.

[14] H. Lin, A. Slagell, Z. Kalbarczyk, and R. K. Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids (poster). In *Proceedings of the 7th International Conference on Security of Information and Networks*, SIN. ACM, 2014. doi: 10.1145/2659651.2659746.

[15] B. Matt. The cost of protection measures in tactical networks. In *Proceeding of Army Science conference*. McAfee Research, 2005.

[16] P. Maynard, K. McLaughlin, and B. Haberler. Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks. In *Proceedings of the 2Nd International Symposium on ICS & SCADA Cyber Security Research 2014*, ICS-CSR 2014. BCS, 2014. doi: 10.14236/ewic/ics-csr2014.5.

[17] K. Mowery, E. Wustrow, T. Wypych, C. Singleton, C. Comfort, E. Rescorla, J. A. Halderman, H. Shacham, and S. Checkoway. Security analysis of a full-body scanner. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 369–384. USENIX Association, 2014.

[18] P. Najera, J. Lopez, and R. Roman. Real-time location and inpatient care systems based on passive {RFID}. *Journal of Network and Computer Applications*, 34(3), 2011. doi: 10.1016/j.jnca.2010.04.011, {RFID} Technology, Systems, and Applications.

[19] M. Niemietz, J. Somorovsky, C. Mainka, and J. Schwenk. Not so smart: On smart tv apps. In *Proceedings of the International Workshop on Secure Internet of Things (SIoT)*, 2015.

[20] D. T. O'Keeffe, S. Maraka, A. Basu, P. Keith-Hynes, and Y. C. Kudva. Cybersecurity in artificial pancreas experiments. *Diabetes technology & therapeutics*, 17(9), 2015. doi: 10.1089/dia.2014.0328.

[21] PTSFS. Post- och telestyrelsens freskrifter om krav p driftskerhet (PTSFS 2015:2).

[22] A.-R. Sadeghi, C. Wachsmann, and M. Waidner. Security and privacy challenges in industrial internet of things. In *Proceedings of the 52nd Annual Design Automation Conference*, DAC. ACM, 2015. doi: 10.1145/2744769.2747942.

[23] T. Shawly, J. Liu, N. Burow, S. Bagchi, R. Berthier, and R. Bobba. A risk assessment tool for advanced metering infrastructures. In *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*, 2014. doi: 10.1109/SmartGridComm.2014.7007777.

[24] R. Verdult, F. D. Garcia, and B. Ege. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. In *Supplement to the 22nd USENIX Security Symposium (USENIX Security 13)*, pages 703–718. USENIX Association, 2015.

[25] W. Wilkowska and M. Ziefle. Privacy and data security in e-health: Requirements from the users perspective. *Health Informatics Journal*, 18(3), 2012. doi: 10.1177/1460458212442933.

[26] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. Wang. Intrusion detection system for iec 60870-5-104 based scada networks. In *Power and Energy Society General Meeting (PES), 2013 IEEE*, 2013. doi: 10.1109/PESMG.2013.6672100.

Mikael Asplund Mikael Asplund is a Senior Lecturer at the Real-time Systems Group in Linköping University, Sweden. From 20112012 he worked one year as a Research Fellow in Trinity College, Dublin. He received his M.Sc. degree in Computer Science and Engineering in 2005 and his Ph.D. in Computer Science in 2011 both from Linköping University. His Ph.D. thesis focused on design and analysis of partition-tolerant distributed systems, including development of middleware services for maintaining consistency and information dissemination algorithms for disaster area networks. His current research interests include dependable distributed systems, mobile and vehicular computing and real-time systems.

Simin Nadjm-Tehrani received her B.Sc. degree from Manchester University, UK, and did her post-graduate studies leading to a Ph.D. in Computer Science at Linköping University, Sweden, in 1994. During 2006-2008 she was a full professor at University of Luxembourg, and is currently a Professor in Dependable Distributed Systems at Department of Computer and Information Science, Linköping University, where she has led the Real-time Systems Laboratory since 2000. Her research interests relate to networks and systems with dependability requirements and resource constraints. During 2015-2020 she leads the national research centre on Resilient Information and Control Systems (RICS) financed by Swedish Civil Contingencies agency.

Appendix: Questionaire used in interviews

General background questions

1. What is your formal role in the organisation?
2. What types of customers/clients does the organisation have?
3. Approximately how many customers/clients do you have?

Questions on IoT

4. What do you associate with the term ”Internet of Things”?
5. Is IoT relevant in your field on a 5-10 year horizon?
    a) Followup question if no: Do you not consider X to be part of IoT?
6. Can you see IoT contributing value to your sector (within 5-10 years)?
    a) New services
    b) Better services
    c) Reduced costs
    d) PR and marketing
    e) Other
7. What factors do you believe will enable faster integration of IoT in your field?
    a) Improved technical solutions
    b) Knowledge of customers and operators
    c) Guidelines for deployment of IoT
    d) Regulation
    e) Lower costs
    f) Other
8. What are the obstacles to introduction of IoT in your sector?
    a) Lack of security / reliability
    b) Costs
    c) Maintenance
    d) Unproven technology
    e) Lack of usability
    f) Lack of know-how
    g) Regulation
    h) Other

Risks, threats and critical infrastructure

9. What risks or threats to you associate with IoT in your sector?
10. How severe do you rank the risk (low, medium, high) of:
    a) Communication failure
    b) Power failure
    c) Failing equipment
    d) Data loss
    e) Confidentiality loss
    f) Integrity loss
    g) Deliberate hacking
    h) Malicious code
11. What is the reliability/availability of power and communication to your critical operations today?
    a) How well are your communication requirements met by your current Internet connection?
12. What do you think the requirements on power and communication will be in 2025?
13. What kind of measures/actions are needed to deal with the potential obstacles/risks that you have identified and thereby enable a faster adoption of IoT?
14. Do you have any final comments?