university of groningen / faculty of economicsand business / operations

Societal Impact of Wireless Revolution in the Netherlands and Possible Measures

Authors (RuG): Prof.dr.ir. J.C. Wortmann, Drs. J.B. van Meurs, Dr. Ir. F.B.E. van.Blommestein, Prof. dr. G.B. Huitema

With support of TNO: Dr. Ir. M. Djurica, Ir R. Hensbroek, Ir E.F. Matthijssen

Groningen, 10 March 2014.

Contents

Management Summary

This report assesses the consequences of the wireless revolution in the society in The Netherlands. The report is written in response to a request by Agentschap Telecom (AT). In line with the request, the report focuses on two sectors, viz. Healthcare and Industry.

The report shows that there are substantial differences between Industry and Healthcare with respect to the use of wireless applications. In Industry there is still a considerable reluctance to use wireless communication in production processes, especially in the high-end of technology as in process industry. Much in contrast, in Healthcare a rapid growth of wireless applications is expected in the care-related processes, not only in the high-end of technology as in hospitals but also in the low end of technology as in home care. Because of these differences, this study employs different research methodologies for both sectors. The Healthcare sector is mainly approached by case studies via interviews; the industry sector is mainly approached via a questionnaire. However, the results are consistent and provide interesting insights.

The report concludes the following:

A key distinction should be made between situations where professional risk management is in place and situations where this risk management is lacking. In hospitals and in larger industrial sites under responsibility of a single owner, risk managers are aware of potential risk of interference. Moreover, these risks can be mitigated or controlled because the hospital or site can be physically controlled by responsible managers. Therefore, both in hospitals and in larger industrial sites, there is relatively little reason to be concerned about the consequences of the wireless revolution. In the case of hospitals, managers choose to adopt wireless technologies, but to take measures to cope with interference, such as redundant communication channels. In the case of larger industry, managers choose to refrain from wireless technologies for critical process control operations, at least until now. In both cases, however, explicit spectrum management could contribute to more sophisticated risk management.

The situation where professional and mature risk management is lacking gives rise to more concerns. This case may occur e.g. in smaller industries with less advanced manufacturing technology or in home care service delivery. In such cases, there is no risk management in place and/or there is no authority to mitigate or control risks. None of the stakeholders feels the urgency to act before problems become manifest. The report concludes that serious concerns have to be raised about the awareness amongst users and providers, because they rely on services which may fail or degrade. The report highlights several scenarios which may lead to such failures.

As a final note on the distinction between licensed and license exempt frequencies, the report highlights that the field overall is not aware of this this distinction.

The recommendations following from this rapport can be summarized as follows:

Advice to government and regulator:

1. The government should raise awareness of risks involved in the use of wireless technologies. The general public and many small businesses are not aware of these risks and expect the same performance as in case of wired communications. This holds in particular for mission-critical communication. The risks are not only the inherent risks of using a wireless technology, but also the risks of failure in the whole service provisioning chain. In particular the distinction between licensed and license exempt frequency ranges and the related risks of congestion due to interference should be widely communicated. The regulator could stimulate education and training for risk managers with spectrum risk mitigation duties.
2. Evidently government should continue to play its role in the setting of regulations and standards with respect to wireless communication particularly on the point of mission critical applications and consistency between standards. The government should maintain the option for parties concerned to use the licensed and/or exclusive frequency range for mission-critical applications. The increase of license exempt ranges

should therefore be treated prudently. European regulations should cover some serious interferences issues in hospitals, see Appendix C for a complete list.

Advice to professional organization using wireless communication:

3. For mission critical applications as in Healthcare there is a need for reliable and resilient systems that in case of failure will cause no harm, or at least a minimum of harm[1]. This may especially be the case in environments where there is no authority controlling the physical environment. This may lead to regulation in parts of the spectrum reserved for such applications. The same may apply to industrial sites without central authority, anticipating future preference for wireless applications in Industry.
4. Organizations where professional risk management is in place, should be advised to implement spectrum management as an additional field.

For Healthcare with respect to the high care environment (hospitals) the following specific recommendations are made:

- Accommodate wireless networks further in integral risks management of the hospital among others by implementing spectrum management within hospital perimeter and specifying wireless services clearly via service level agreements to manage the expectations.
- Implement knowledge transfer from experts to the field and create awareness about the risks of wireless technology to support massive deployment.

With respect to low care (care homes and home care) advises should be different as no integral risk management is in place:

- Learn from experiences and practical solutions implemented in the high care environment especially when patients have an increased vulnerability
- Wireless networks will enable the low care environment to reduce on personnel. Have procedures in place for massive failures. Guarantee that alarms are signaled and make sure that the call center can operate without disturbance.

As the variations between industries are larger than in Healthcare it is not possible to be as specific as in Healthcare, however for industry in general these recommendations can be emphasized:

- Recommendation to industry to implement professional risk management and include in the risk assessment the possible failure of wireless devices due to congestion or interference.
- Introduction of additional, licensed and/or exclusive frequency ranges for critical wireless applications should be considered.
- Recommendation to industry to use application specific or exclusive frequency ranges for mission critical applications, and not the non specific frequency ranges that are for example used for WiFi.
- Recommendation to industry to use standard protocols for industrial applications rather than ad-hoc protocols that are specific to the devices used.
- Recommendations to back-up critical applications with wired solutions. As long as congestion is not monitored or controlled, industry should be aware that wireless connections may fail.
- Recommendation to industry to monitor the availability and capacity of bands in industrial areas.

—

[1] In certain sectors the term fail-safe is used.

1. Introduction

Need for mobile ICT services
Wireless services and applications are part of the modern society. Obviously, there is an increasing need for mobile ICT services (voice and data) in various sectors of society. Wireless systems offer several practical advantages such as location flexibility, speed of deployment and reduced construction costs for cabling. The technological developments in areas such as miniaturization, computing power, the IP protocol and wireless technology (modulation, coding, antennas), enable the industry to develop and provide a variety of useful and attractive (networked) applications at reasonable prices.

Increase of demand for bandwidth
In the past decade, the demand for bandwidth for mobile communication and the popularity of the license-free frequency bands have greatly increased. Examples include the rapid increase of the use of WiFi (wireless internet) but also to the growing number of practical applications based on short range wireless technology in unlicensed bands. Spectrum is now regarded as a key driver of economic growth and there is a public interest to utilize this natural and scarce resource. One of the consequences of this development is an ever greater need for spectrum (the ether), which increases the likelihood of coexistence problems between systems and networks. At the beginning of the twentieth century, when the possibilities of radio communications became apparent, it was realized that there were international and national rules needed for proper use of the available frequencies. Bands were reserved for radio, television, wireless telephony, etcetera. As a consequence the main part of the spectrum was brought under government regulations, and was made subject of a system of permits that would provide to the permit-holders a degree of protection against interference by other “trespassing” users. Moreover, regulation was used to create clarity to the market about major technical requirements. International harmonization of frequency bands was and still is important to facilitate international standardization of system specifications. However in the past decade it was understood that flexibility in spectrum assignments and license exempt use of spectrum is also of great social importance. Many new applications of wireless communication only will thrive, when the availability of a (harmonized) spectrum is no obstacle.

Risks of wireless technology
As the dependency upon wireless systems and networks has grown immensely over the years, the risks of failures and related problems have increased, partly due to the inherent nature of wireless transmission but probably to a larger extent due to interference issues caused by intensive spectrum use. We have in The Netherlands a modern and reasonably flexible regime, but one could state that the issue of failures and risks has made its come-back. In 2011 Agentschap Telecom (Agency Telecom) went public with the message "Gestoord van storingen" (Source: AT digital newsletter June 2011) where the agency expressed its concern about the increase of complaints about interference related to the use of license-free wireless systems. The question is whether we are in all respects well prepared. Do we understand the consequences in every way and in all different aspects? Can we absorb this wireless (r)evolution without having to deal with higher probabilities of disruptions and subsequent system failures? Agentschap Telecom in this context used the term *tele-vulnerability*. The remedies, like better education of the user, tighter regulation, greater tolerance for wireless transmission failures in system and network designs have not yet crystallized. This issue will not only be limited to the license exempt bands but will probably also extend to bands in which sharing among users will be strongly promoted in order to reduce spectrum scarcity. The current policy initiatives by the European Commission point in that direction.

The risks related to wireless communication can be classified into:

1. Risk of malicious action, leading to violation of privacy and/or (again) interruptions of availability communication services
2. Risk of EMI and/or risk of failure of technical components, leading to interruptions of available communication services

3. Risk of congestion or interference, leading to increased latency or (again) interruptions of available communication services

This report concentrates on the second and third categories, because the first category is not affected by the licensing regime. Interference (in-band and out-of-band) does not necessarily imply a risk for (wireless) systems, because well designed systems should have a certain resilience. However if the nature or intensity of the interference exceeds the tolerances, the whole system is at risk of failure and/or unexpected behavior can occur .

Risk management

Depending on the actual application to which the wireless system belongs, a possible risk arises, namely a (temporary) dysfunction because a data connection falters or fails. At this higher level the effect of an electromagnetic interference can be perceived by the user. Depending on the context and purpose of the application it may have an impact on the value to the user(s) that is realized with the application. It may be of vital importance, such as in the case of medical equipment, but more often there is a definite economic damage or just discomfort. Faults can thus introduce certain risks. Such risks could lead to a crisis in which there is disruption of an organization or ecosystem.

Whether and how such a particular risk is assessed depends on the normative framework that one uses. Some examples:

- If users are not accustomed to slow or intermittent internet connections, the use of WiFi may bring unexpected risks. This is the case when expectations of users are not consistent with reality
- However, if users are accustomed to slow or intermittent internet connections, then the risk of congestion in WiFi is easily accepted.
- The assessment of the risk may be very different when at home viewers notice hitches in the digital television broadcast of a popular football match,
- ....or when failure of the connection occurs while mobile banking.
- .....Or when someone accidentally opens a door for thieves with a remote control

Up to now regulation has been focused on avoiding risks. Nowadays , the availability of risk management is more a guiding paradigm. In business, risk management is an integral part of management.

Need for analysis of societal impact

The Ministry of Economic Affairs (EZ Min) , responsible for radio spectrum policy in the Netherlands focusses on deepening and exchange of knowledge of issues related to the radio frequency spectrum and its usage . Special interest has possible adverse effects in society of the use of wireless technology in particular license exempt applications and unwanted / unintended effects on equipment (in hospitals , or production environments).

Given the developments described above regarding wireless usage and the intention of government to have a stronger focus on risk management, Agentschap Telecom (AT) has contracted RUG to perform, with the help of TNO, a multidisciplinary analysis focusing on the social implications of the risks of the uptake of (license exempt[2]) wireless usage. It is requested to focus this study on the domains of Industry and Healthcare (especially hospitals). These domains are chosen as it is assumed that in these the societal impact of failures of wireless networks will be significant (sometimes even life-threatening), or at least that in these domains one will have the best experience how to handle the risk of such failures. AT also asks for advice on possible enforceable measures of technical , managerial or preventive nature against these adverse effects .

—

[2] License exempt refers as well to the specific parts like DECT as to the non-specific like the ISM band that provides for WiFi.

Setup of the study

Basis of the study has been a multidisciplinary approach based on the abstract concept of risk management in relation to the practical use of wireless applications. The objective of the study is to identify possible threats , risks and adverse effects (social impacts) of using license exempt wireless applications in critical environments. On this basis, recommendations are made to counter or deal with these adverse effects . These recommended measures may differ in nature for different stakeholders , and can range from legal nature (e.g. legislation) , managerial nature (e.g. the steps in a procurement process) , technical nature (e.g. use of security protocols) or social nature (e.g. the establishment of courses).

In Chapter 2 forecasts are made based on international academic and professional publications, and a wider view is provided on the use of the wireless technology especially in the license exempt areas, and particularly from the perspective of risks . In the Chapters 3 and 4 respectively, the specific domains of Healthcare and industry will be investigated in more detail. In these domains integral risk management should also include the risk of the use of wireless networks. In chapter 5 the findings of chapter 3 and 4 are generalized and a generic analysis of the ecosystem is made with reference to the relevant types of stakeholders, their interests and relationships for a better understanding of risks and responsibilities . Finally, in chapter 6, the findings and conclusions will be summarized together with a set of recommendations.

2. Developments in wireless communications

In this chapter we will explore some relevant developments in the domain of wireless communications.

2.1 Wireless Connectivity

Over the past decades wireless communication has changed our daily life significantly. People are getting more and more used to the ubiquitous access to a large variety of communication services and applications even to such an extent that they depend heavily on the availability of such services. Currently broadband wireless connectivity enables a large variety of services such as internet access, audio applications (access to internet radio or online music archives), video and multimedia (mobile broadcast, video-on-demand, interactive TV), social networking/media and cloud applications. The introduction of smartphones and tablets has boosted innovation in wireless services and applications even further which leads to a further increase in the demand for wireless broadband connectivity.

The increase in demand for wireless connectivity is not only occurring in the consumer sector but also in the professional services, processes and applications. Besides for professional communications and ICT applications in office environments wireless transmission is getting also more and more used for industrial purposes. Wireless systems are finding their way in industrial environments where they can provide enhanced efficiency of processes. This is often for monitoring, telemetry or wireless control functionality. In Fig 2.1. below this is indicated as the second wave of wireless device development.

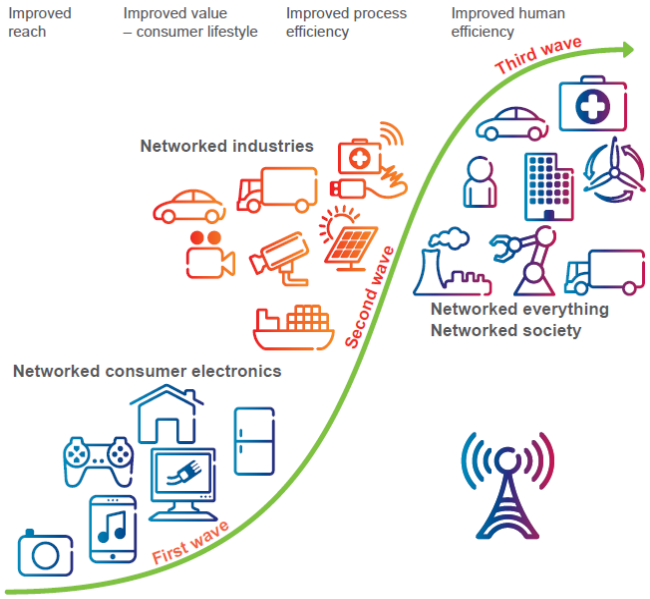

Figure 2. 1 Three waves of wireless device development (Ericsson [1]).

In the third wave, wireless devices evolve further and become part of many systems and processes. This includes vital services such as the energy grid, intelligent transport systems, medical care, road safety systems and process industry. In this stage wireless devices become a crucial element for a well-functioning society and it gets of crucial importance that the radio communication is not disturbed. This third wave of wireless development is also known under the term 'Internet of Things' since not only people communicate with one another, but to an ever further extent machines mutually exchange information both wired as well as wireless.

Modern Machine-to-Machine (M2M) communications, where devices and systems exchange data autonomously, has expanded beyond a one-to-one connection (of for instance sensors) and changed into a system of networks that transmits data between all kinds of appliances. M2M

will allow a wide variety of innovative applications and new business opportunities. Examples of current application domains are personal navigation systems, smart energy measurement, control systems and intelligent transport systems or the water management in a polder as wired communications becomes too expensive to maintain . For M2M applications in a large variety of domains a significant demand for wireless communication, and thus spectrum resources, is expected.

2.2 Expected growth in wireless applications

Market research performed by various organizations shows a significant growth in connected devices expected over the coming years. The GSMA[3] expects a total number of 24 Billion wireless connected devices by 2020 (cited from [2], p.20). What can be seen from their forecast a major increase is predicted in the number of M2M devices. These will mostly be wireless connections partly via communications based on mobile network infrastructures but more importantly using devices capable of local communications.

According to the observations of the GSMA Europe is expected to represent a quarter of the total number of wireless connected devices thus a number of 6 Billion. A rough estimation to the situation in the Netherlands can be made based on the number of inhabitants, which would result in an expected number of 140 Million connected devices by 2020.

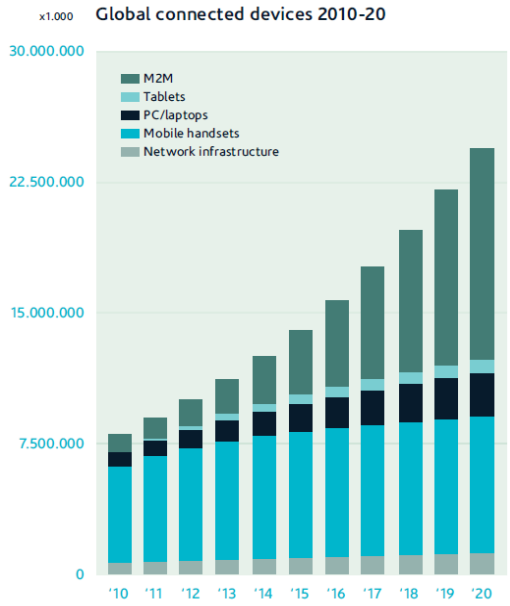

Figure 2.2. Global number of connected devices for the period of 2010-2020 ([2], p.20).

The large growth in the number of connected devices that is expected for the coming years consist for the major part of wireless systems. Globally a growth in terminals for mobile communication is expected, but even more significantly is the increase in the number of short range wireless devices. According to the GSMA market expectations the number of short range devices, which is currently about 25% of the number of mobile/smart phones, will be nearly equal to the number of mobile/smart phones by 2020.

—

[3] GSMA (Groupe Speciale Mobile Association), an interest group for mobile communications

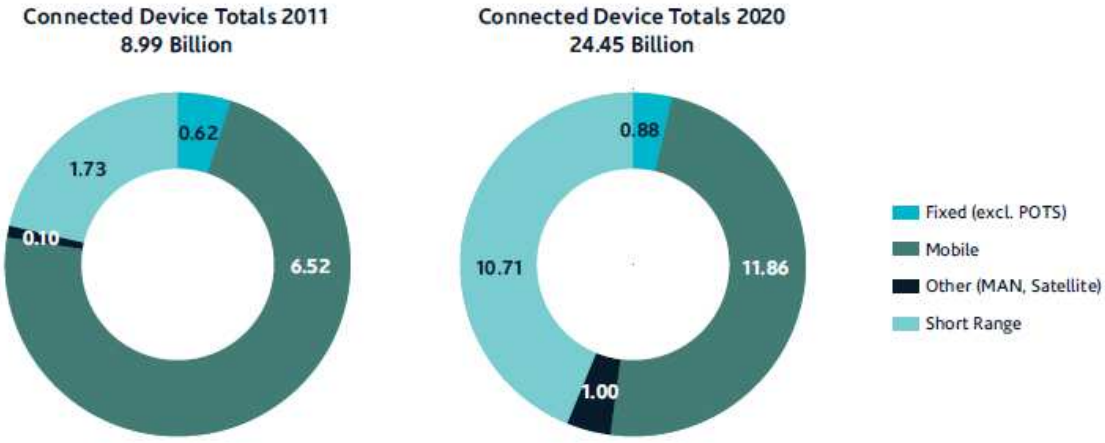

Figure 2.3 Global number of connected devices 2011 (estimation) and 2020 (forecast), from [23], p.19, based on market research from GSMA.

2.3 Classes of wireless communication systems

Wireless communication systems can in general be divided into classes depending on their range of operation: personal/body, local, wide area. This is depicted in Figure 2.4. Typically PAN en LAN types of systems are low power and therefore have a limited range and for this reason are also indicated as Short Range Devices (SRD).

Figure 2.4.a. PAN/BAN, LAN and WLAN

	Personal Area Networks (PAN). Including: Body Area Networks (BAN) Sensor Networks	**Wireless Local Area Networks (WLAN)**	**Wide Area Networks (WAN)**
Existing technology/standards	Media transfer: • Bluetooth • WirelessUSB • Ultra Wide Band Sensor & control: • IEEE802.15 • Zigbee • Z-wave • One-Net • Sub-1GHz SRD • Wireless HART • ISA 100.11a • 6LoWPAN • KNX-RF • EnOcean • Proprietary solutions • …. Identification • RFID • NFC Medical systems: • Wireless Medical Telemetry Service (WMTS)	Data/Internet connectivity: • WiFi (IEEE802.11,b,g,a) Voice, data: • Digital Enhanced Cordless Telephony Car-to-Car & Car-to-Roadside comms • IEEE802.11p	Mobile network infrastructure: • GSM: Global System for Mobile communication • UMTS: Universal Mobile Telecommunication System • LTE: Long Term Evolution Private mobile network infrastructure: • TETRA (Terrestrial)
Emerging	• White Space Devices (WSD); E.g.Weightless	White Space Devices (WSD)	• LTE-advanced
Typical spectrum access	License exempt	License exempt	Licensed
Typical Range	< 10 m	<200 m	<10 km

Figure 2.4b Wireless applications in Personal, Local and Wide Area Networks; PAN, WAN and WLAN [TNO based on inventory of various sources]

When considering these categories of wireless communication systems the following characterization can be made:

Wireless Wide Area Networks (WAN)
These are typically cellular networks for mobile communications either for commercial wireless communication services or private networks for closed user groups as is the case for the public safety sector. WANs usually work in licensed spectrum that is assigned to an operator on basis of exclusive use by that operator, and is well regulated and 'controlled'. Having available sufficient spectrum resources enables operators to provide voice, data and multimedia services with a national coverage, high availability and quality of service.

The enormous growth in demand for these kinds of wireless communications has resulted in a corresponding increase in the requirement for radio spectrum. The total amount of spectrum currently available for terrestrial mobile broadband services is 990 MHz, all allocated below 3 GHz which is considered most valuable for wide area mobile network deployments. The growth in mobile data traffic has led to the urgent objective to make at least 1200 MHz of spectrum available for terrestrial mobile broadband services (within the range 400 MHz to 6 GHz) by 2015. On the longer term, toward 2020, the spectrum demand is expected to increase even further.

Wireless Local Area Networks (WLAN)
Wireless Local Area Network (WLAN) systems were developed for internet connectivity in private networks for application in office and home environments. For this reason WLAN devices were developed in a frequency band (2400 – 2483 MHz) which can be used under a license exempt regime. In order to enhance coexistence between multiple wireless local area networks and with other application in the band, the devices have low transmit powers and apply 'politeness' rules with respect to spectrum access.

The past decades have shown the enormous success of the license exempt bands by the large variety of innovative systems and applications developed for these parts of the spectrum. For instance the 2.4 GHz band is, besides WiFi, used by systems as Bluetooth, Zigbee, wireless telephones, wireless camera systems, baby monitoring systems, systems for wireless video transfer, magnetrons, and so on. As mentioned earlier also the number of devices in the license exempt bands is increasing rapidly.

A recent study by WIK and Aegis [4], funded by the European Commission, highlights the importance of WiFi for connecting EU citizens to the Internet. In 2012 71% of all wireless data traffic that was delivered to smart phones and tablets in the EU was delivered via WiFi. It is estimated that this figure will grow to 78% by 2016. Mobile data traffic is estimated to grow at 66% annually for the period 2012-2017, but at the same time almost 80% of all traffic to mobile devices is predicted to come over WiFi. The reason for this is that most smart phone use occurs at home or in the office. Eventually this has resulted in a situation that the 2,4 GHz band congested as was reported by Agentschap Telecom and the University of Twente [5,6].

To relief the congestion in the 2.4 GHz band and support the expected growth in WiFi systems, besides the spectrum already available in the 5 GHz band (5150 – 5350 MHz and 5470 – 5725 MHz) the European Commission has taken the initiative to make available more spectrum in this band. The target is to make about 800 MHz of spectrum in the 5 – 6 GHz band available for WiFi services.

Personal Area networks (PAN)
The class of Personal Networks is not addressed in this report as there are still many technical developments and usage is mainly in the informal area. Consequently its societal impact is difficult to assess. Examples of use are watches that can communicate with the smart phone of the owner or Bluetooth connections in house with speakers. In Healthcare short range wireless networks would ease patient care in the emergency room or the intensive care. However this is not yet implemented on a wide scale apart from supervision of the heart function of cardiac patients in the hospital ward.

Application domains
With respect to the domain we can identify the following important wireless applications (as been mentioned before, this report will focus on Health(care) and Industry):

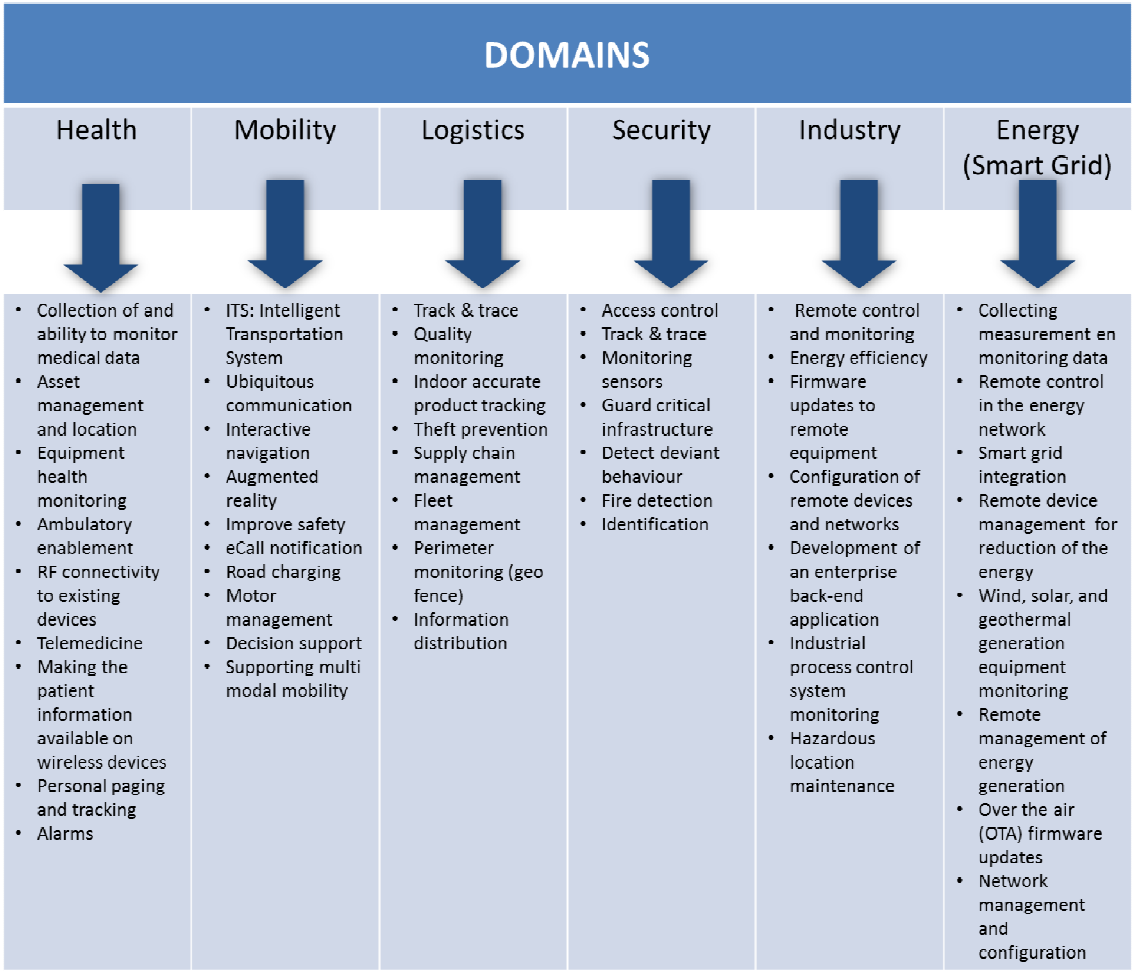

Figure 2.5 Wireless applications in the different domains. [TNO based on various sources]

2.4 Spectrum allocation and assignment

Optimizing use
The total mobile broadband traffic demand is predicted to increase by a factor thousand by the year 2020 [7]. To meet this immense growth in the demand for wireless transmission capacity the industry is constantly challenged to introduce new technologies and concepts to optimize the use of the radio spectrum. Important measures to cope with this challenge are innovations in transmission technology, achieving the transmission of higher data rates within the same amount of spectrum and increase the level to which spectrum is shared between various services, systems and users. The enhancement of spectrum sharing can be realized by optimizing regulations and procedures but also by introducing more dynamic forms of frequency sharing, enabled through cognitive (smart) radio technologies.

In the spectrum from 400 MHz to 6 GHz allocations for a large variety of services are contained. For several of these services there are also requirements for enhanced communication possibilities and wireless services requiring broader bandwidths. Examples are aeronautical communication, public protection and disaster relief, intelligent transport systems, automation and security applications. Thus the increased need for spectrum not only applies for the commercial broadband wireless communication networks, but also for other domains. This increases the pressure on the spectrum even further.

It is essential to use the spectrum as efficiently as possible. Underutilization of frequency bands can hardly be justified in the current situation of scarcity. In contrast to what used to be the case it is becoming less obvious to gain exclusive rights for the use of a frequency bands. Users will be more and more obliged to share spectrum. Shared spectrum access is considered as an essential contribution to meet the demand for spectrum for wireless broadband services. This means that additional to the sharing arrangements that are already in practice for several frequency bands, new opportunities for shared spectrum access have to be explored. Systems supporting Dynamic Spectrum Access (DSA), i.e. Cognitive Radio, are considered enabling technologies for enhanced shared spectrum access.

Allocations
At global level, within International Telecommunication Union (ITU) [http://www.itu.int/itu-r] decisions are made on making allocations for radio services in particular frequency bands.
At Regional level (European: EC) and National level frequency bands are assigned to applications, users or systems. The frequency allocations and assignments for the Netherlands are recorded in the 'National Frequentie Plan' (NFP) [8].
It can be seen that in almost all bands allocations exist for multiple radio services. Also in the bands where license exempt use is present, there is in many cases also use of other (licensed) applications. Some examples:

- 2400 – 2483 MHz --- Amateur Satellite (Licensed), Electronic News Gathering/Outside Broadcasting (ENG/OB) (licensed), Short Range Devices (License exempt)
- 5250 - 5925 MHz --- Earth Exploration Satellite Service (EESS), Short Range Devices (SRD) (license exempt), Radar (licensed), Fixed Satellite (Licensed)

License exempt use
In various frequency bands license exempt use is permitted under specified conditions. Different applications each have a specific band in which license exempt use is possible.
The brochure 'Vergunningsvrije radiotoepassingen' [9] of Agentschap Telecom provides the exact overview of applications, frequency bands and conditions for license exempt use of spectrum.

Licensing regimes & stimulation of spectrum sharing
In order to enhance the efficient use of radio frequency resources, different spectrum sharing arrangements are currently in place. An overview of the spectrum sharing mechanisms is very well formulated in a document of DigitalEurope [10]in which a literal transcription is given below:

Un-coordinated secondary usage (UWB, overlay-underlay, etc.): Primary user has no knowledge of Secondary user(s). However, Primary user is guaranteed to use the spectrum. The Secondary user(s) can only use the channel if it is not in use by the Primary. Mechanisms have been proposed to detect unused spectrum which involve sensing and information gathering. While these mechanisms have spurred the largest amounts of interesting research, harmful interference has been the biggest concern.

Semi-coordinated secondary use (Database Access, Cognitive Pilot Channel): Primary user is aware of Secondary users' existence. A database contains spectrum that can be shared. The Secondary user queries the database, as in the case of TV White Spaces (TVWS), or obtains information about available channels from a cognitive pilot channel. The Primary user is not aware of how many Secondary users exist in a given location, however, they have the guarantee that none exist where the Primary is using the spectrum.

Fully coordinated hierarchical use (Licensed Shared Access (LSA) also called Authorised Shared Access(ASA)): These are evolving schemes where the incumbent and the new users (LSA licensees) fully coordinate on the use of a given spectrum. The LSA licensee obtains rights and guarantees to the incumbent user's spectrum rights. This means that when the incumbent makes available the spectrum to the LSA licensee for a given period of time, depending on the license agreement, the incumbent cannot interfere with the LSA licensee for that duration (unlike the two sharing mechanisms above). In addition, unlike the previous two schemes, the incumbent user is likely to be financially compensated for sharing their spectrum.

2.5 Conclusions

Obviously, there is an enormous growth in the demand for wireless communications. This growth occurs in various domains, applications and scales (PAN, LAN, WAN). Consequently there is a comparable large requirement for spectrum.
Therefore, there is an urging need to increase the sharing of spectrum, and the exclusive use of spectrum is becoming less general. For sharing various regimes exist or are emerging. However, it is essential that the rules or etiquette are obeyed. Current practice shows interference incidents already occurring. Accordingly, the use of wireless technology in critical environments deserves additional attention to minimize risks.

3. Risks of Wireless Communications in Healthcare

3.1 Wireless in Healthcare

Wireless technology is used already extensively in Healthcare. Up till now, wireless technologies are applied as they are being used elsewhere in society (WiFi, Phones, and several access systems with RFID-pass and other communications). The only critical medical application is cardiac telemetry: Patients can move freely in the cardiac department during their treatment while the medical staff monitors the functioning of their heart (moving around belongs to therapy). The other well-known use of wireless technology are the pagers that are still used to inform the doctor when (s)he is needed for consultation or an urgent medical intervention. Also cordless phones based on DECT technology are widely used. At the early stages of the introduction of wireless technology in the hospital there was concern about the interference between wireless devices and medical equipment. For this reason normal mobile phones were not allowed in the hospital.

Currently most of the hospitals are introducing new wireless technologies carefully. Particularly WiFi networks are deployed for the medical staff but in many cases also as a service to the patients. Policies towards the use of mobile phones are more relaxed. Many members of the medical staff use their smartphone in the hospital for their medical duties. The main reason that patients and visitors are still not allowed to use mobile phone is to provide a quiet environment to enable the medical staff to do their work. The use of RFID is emerging, however still on a lower scale present than WiFi and mobile networks.

RIVM has asked with their report “Risks related to the use of eHealth technologies”[18] for special attention to prevent or minimize risk for the patient. According to this report, wireless provisions in Healthcare should be considered as part of the eHealth technologies. We will return to the RIVM report in our recommendations, which could be considered among others as a further implementation of the RIVM recommendations. Other documents that have been the basis of this study are [19] describing use of wireless in hospitals in the US and [20] the report about the state of wireless use in The Netherlands.

Apart from the experience of the authors in the field of Healthcare communication technology and knowledge of the literature, the information in this chapter is based on three case studies, viz, a university hospital, a regional hospital and a mental care hospital. The latter two of these hospital organizations were also responsible for care homes and home care (here referred to as low care in contrast to high care in hospitals). Below in Section 3.2 a classification of wireless technology usage is presented, which emerged from the research work. Thereafter in Section 3.3 we provide the results of the case studies.

These results are based on twelve interviews. The interviewees are ranging from medical specialists in intensive and emergency care to managers responsible for ICT and technical infrastructure .

3.2 Usage of wireless technologies in Healthcare

Based on our interviews the usage of wireless technologies in the Healthcare domain can be classified into three groups:

1. To monitor the patient. Vital parameters of many patients need to be monitored e.g. oxygen saturation and hart functions. In an emergency room or an intensive care unit about ten wires are connected on average to the patient. This is a hindrance for the patient and certainly also hinders the treatment and the medical examination.
2. To have access to medical data. The medical staff prefers to have a comprehensive status of the patient at the bedside. What are the latest results from the laboratory and pictures from radiology? They like to consult on site the medical literature and to prescribe the proper medication based on the latest patient data.

3. To optimize the processes in the hospital also wireless technologies are used. Particularly to locate medical staff and equipment. An example is tracing beds and patients via RFID. RFID is also applied in the sterilization process of medical equipment. By doing so response time can be reduced and efficiency can be improved.

In all three areas a substantial growth in usage is expected in numbers and in applications. In the area of patient monitoring the most technical innovations are anticipated.

3.3 Wireless technologies in high care

Our research has been especially focused on the use of wireless technologies in the high care as in hospitals. Although all hospitals interviewed were considering further deployment of wireless technology, there still are considerable differences. The actual names are not shown because the specific examples should be considered as prototypic for the field.

3.3.1 Academic hospital

Results of the interviews

The wireless networks in this academic hospital are perceived as part of the total ICT environment. No proper wireless network will operate without a reliable fixed network. Availability is of key importance. An uninterruptable electricity supply is essential to guarantee this high availability. Wireless is considered as a major trend in the ICT network facilities.

Usage of wireless technology in the academic hospital

Wireless communication supports the medical processes already for a long time. At first pagers were introduced to alarm the doctors. In cardiology ambulant patients are already for many years monitored via wireless communication.

Many doctors have smartphones and laptops connected to the mobile network and the local WiFi network. More and more doctors use their smartphone to access state of the art medical references and to determine tailored medication for their patient based on pharmaceutical databases. The security level is sufficiently high that they also can access the medical status of their patient. All doctors with operational responsibility have also a pager. In the vast majority of the cases when immediate contact with a doctor is required the pager is used.

The WiFi network in the hospital is separated in three logical networks for patients, for students and for the medical staff with each different security levels. The WiFi network for the medical staff is still in a pilot phase, but is already in use. No serious problems with this network have been encountered.

It is expected that the usage of wireless communication will grow the near future considerable in all areas.

High availability, risk assessment in academic hospital

To achieve high availability an integral approach is required based on careful assessment of risks. Several provisions are made to mitigate these risks:

- Parts of the ICT facilities are in two external computers centers where the computers are each other's backup;
- The hospital has its own generator to guarantee high electricity availability and has several connections to the public high voltage electricity grid. This is also true for the computer centers;
- Communication among the medical staff has several backup scenarios. When immediate contact with a doctor is required the pager is used. Doctors with operational duties have mobile phones that make them also available outside the hospital. But there are also fixed telephone lines in each rooms and there is even a "red telephone" provision for large calamities.
- A multi-vendor policy reduces the dependencies of a single telecommunication provider. The provider for the mobile network is different from the provider of the fixed network together with the Wi-Fi network.

- Sufficient capacity of the wireless networks also is part of the availability considerations. The WiFi network can even cope with numbers of students leaving a large lecture room

The highest risks for a successful deployment of the wireless network are considered as:

- Decreased protection against cybercrime. The hospital faces on a daily basis attacks via the Internet
- An negative attitude and adverse reactions in the general public with respect to EM-radiation

ICT department in academic hospital

The hospital ICT department plays a pivotal role in the operation and maintenance of the ICT facilities, residing both at the hospital premises and in large computer centers in the region. ICT expertise is available in the own department and expert knowledge is hired via consultancy companies. New ICT systems are developed together with the respective medical departments. The main ICT outsourcing contracts are maintained by the ICT department.

3.3.2 Regional hospital

Results of the interviews

This regional hospital is of a normal size and is ranked high on different comparison lists of care quality. It relies for its top referent care on other hospitals in a distance of 40 km. The hospital is the dominant hospital of a group of Healthcare centers and care homes for which they provide the infrastructural facilities.

Use of wireless technology in the regional hospital

Currently the hospital is actively deploying their internal WiFi network to support several care functions among others telephone and bedside facilities for the medical staff (computer on wheels). This implementation of the WiFi network that started 2009 is considered as the first step in the deployment of other functions based on network technology. As an example by means of this WiFi network employees can be located within the perimeters of the hospital.

The use of RFID is considered to trace medical equipment as beds and oxygen bottles and also to assure that babies are not to be removed without permission from the maternity unit. The mobile phone is used for the communication with the medical staff when outside the hospital for instance to activate the stand-by chirurgical team during night watch in the emergency room. The traditional pagers are still in use as it is required by the fire brigade, however costs are considered high with little added value.

WiFi for the care homes of the group is not yet considered as those provisions are perceived as too costly at current price levels.

Integral risk management in the regional hospital

The WiFi network is actively monitored and interference has been detected from outside parties that apparently did not comply with the rules for limited energy levels.

The hospital is also implementing a quality program based on key performance indicators. The quality of the WiFi network is not part of this program, as it is for instance considered of lower importance than the cleanliness of the medical facilities.

However when the quality program is operational and the WiFi becomes an essential part of the medical process, the quality of the wireless network could be surveyed as part of this existing quality program.

3.3.3 Mental care hospital

Results of the interviews

This large mental Healthcare organization provides a variety of services ranging from ambulant services, intramural services, service for the elderly with mental problems and forensic care

Where possible the mental hospital tries to implement a comprehensive ICT vision as a result of their corporate strategy. As an example, the hospital wants to position their facilities such that these provide openness for the visitors and safety for the patients, their relatives and the

general public. Consequently there are specific strict ICT rules for privacy and security with respect to for instance the data of the patients.

Usage of wireless technology in mental hospital

Currently the mental hospital uses systems based on DECT technology for their intramural facilities, however they are in a migration phase towards in house GSM. Especially for the lower care facilities they are implementing domotics technologies to ease nursing. To avoid wandering and consequently avoiding risk of falling the mental hospital is implementing special camera systems that detect when patients leave their bed during the night. The business case is justified by the fact that this will reduce night staff.

The dominant health insurance company requires that over time 20% of care for elderly will be provided via eHealth solutions. This is a difficult task to implement. This goal will be achieved mainly by using video communication. For this purpose a WiFi-network is installed when the patient is at home. A Living Lab environment is established to investigate the possibilities or shortcoming of new technologies especially for the elderly care.

Integral risk management in mental hospital

Risk management is part of the corporate policy. When needed the ICT facilities have a no-break electricity supply.

When domotics is introduced in the lower care facilities and consequently the number of onsite staff can be reduced, the need for additional staff will increase in case the facility has to be evacuated. Mental patients in case of emergency show sometimes behavior deviant from the healthy public. They do not participate actively in the evacuation, but hide themselves in the building. Currently the use of volunteers living in the vicinity is considered to curb these risks.

For elderly at home the ICT facilities and particularly the WiFi network are considered under the responsibility of the house- owner and the internet provider. There are not yet special requirements for such services with respect to availability.

The organization is too early in the deployment of WiFi facilities to report operational disturbances caused by the wireless network.

3.3.4 Additional requirements on availability

From our interviews it became apparent that the availability of a WiFi network is to a great extend determined by the quality of the electricity supply and the wired network. In general the WiFi network is used to obtain access to the local IT services and to the internet. Consequently these aspects are additional requirements for the quality of the wireless network. In the next few years wireless will be fully deployed and has become an essential part of Healthcare. Than requirements for electricity supply, wired network and wireless network should be well aligned and part of the later mentioned integral risk management of the hospital.

3.4 Risk Management in high care

Risk management is an essential part of Healthcare and should be understood in wider perspective than the use of wireless as such.

3.4.1 Integral risk management in high care

In all examples based on the interviews the risk of the use of wireless technologies is mitigated by the fact that an integral risk management is in place. The medical staff and the board with its supporting departments (especially the department responsible for the medical facilities) is trained to deal with risks and makes every day risk assessment. The inherent nature of a hospital is to be prepared to respond swiftly to the entrance of a seriously ill patient and assess the risks concerned.

During their study medical doctors are educated and trained how to act during accidents, how to set priorities, how to make optimal use of the available facilities and how to assess risks. While monitoring patients via wireless or wired connections doctors and nurses are used to failure of these connections. Medical equipment for instance gives an alarm when the hart monitoring signal disappears.

Discussions with the medical staff about the use of wireless technology every time focused at the advantages it provides for the patient and how to deal with the failure of the wireless connection. The doctors had a clear view how to resolve the consequences of such failures.

3.4.2 Risk Management in hospitals

The Dutch law "Kwaliteitswet Zorginstellingen **1996**" requires hospitals to deliver "responsible care". Hospitals presently are required by the Health Inspectorate ("IGZ") to do prospective risk analysis on the care processes and to operate a medical care incident reporting systems ("vms" = Veiligheids Management System). The Inspectorate has criticized hospitals for not installing adequate vms-systems. The inspectorate is expected to publish its recent investigation on incident reporting in all hospitals shortly. No hospital can ignore the results of this investigation.

In this context it should be mentioned that for Medical Equipment a "Convenant safe application" has been agreed recently. For ICT systems such agreements are coming up internationally, but not yet common in The Netherlands. We expect quick adoption of these agreements, however. Accordingly, we conclude that there is substantial attention for risk management in hospitals in The Netherlands, and that professional risk management is becoming the norm. Nevertheless, there is room for improvement, for example some hospitals do not test their electrical emergency system; in that case it is not known if the ICT systems survive electrical outages. (A sound evaluation of real outages that occurred generally is not available). Recently a hospital discovered that the cooling of the server room was not on the emergency electrical system by mistake [21].

3.4.3 Risk Management for medical equipment

Risk Management was introduced for medical electrical equipment in 1966 already (standard IEC 60513). This standard explicitly states the facts why Risk Management in Healthcare differs from other areas like "Household" or "Industry". These facts are also relevant for I(C)T systems in hospitals as well. The facts are:

- Patients can be more sensitive or vulnerable than healthy people (due to physical weakness),
- Patients can be passive or dependent on medical equipment (due to treatment),
- Patients can have restricted capability to observe their surroundings (due to anesthetics or medicines),
- Patients can be mechanically restricted (due to fixations),
- Their (skin) barriers can be impaired (due to surgery, wounds, drains).

These facts are consequently brought into the Risk Management for every type of medical equipment (IEC 60601-series). This results in worldwide agreement on the safety of medical equipment and systems. The most important (stringent) safety aspects of medical equipment are: fire safety, electrical safety, continuity of use and no hindrance of alarms.

3.4.4 Risk Management for ICT in hospitals

I(C)T systems being part of medical equipment or systems have to fulfil the medical equipment requirements as well. Medical equipment manufacturers cover these requirements when they implement IT systems in their medical systems.

IT systems on their own are generally not considered to be "medical equipment". Therefore they do not (need to) fulfil the medical equipment requirements. However, because these IT systems are applied in direct vicinity of patients, they are a risk. Risk management standards for medical IT networks are in preparation [3]. The future formal status of these standards is yet unknown.

Hospitals will certainly be advised by the IGZ. For the time being the information systems in hospitals are covered by national standards on security and privacy (NEN 7510 in the Netherlands).

3.4.5 Risk Management for wireless systems

Although medical staff is highly experienced and motivated to safeguard patients from failures in technology, this will be impossible if failures occur unnoticed or at many places at the same time in a department with many patients. Therefore even failures that seem harmless can be dangerous, if there are many of them. Two aspects might fall in this category:

- Interference (EMI) on medical equipment by wireless systems,
- Continuity of service, “uptime” and reliability

Immunity to interference is a design parameter for medical equipment. The immunity requirements are raised permanently through the years because the threats from wireless technology augment: more wireless systems are brought into the hospital with stronger transmitting power levels / field strength. In Appendix C of this report more details can be found.

3.5 Selection of specific technologies (licensed vs license exempt)

Part of our investigation was concerned with the criteria used in selection of specific technologies. When discussing wireless technologies, the interviewees were hardly aware of the difference between licensed and license exempt bands. Accordingly, the specific focus on license exempt wireless technology as requested by the principal of this research was not well understood by the interviewees. Rather, other criteria were mentioned e.g. the inherent risks of the specific technology; how responsibilities were allocated; which technologies were available in the market and at what price; what were the additional functionalities that the technology provided, like the ease of remote management. Last but not least, available knowledge and expertise was a consideration in selecting technologies. Particularly private experience with WiFi and 3G/4G technology is a convincing argument. In several cases for smartphones a "bring our own device” policy augmented with additional security procedures for the access to the hospital network was implemented. Consequently the focus was on the dominant players and technologies in the market, not at all at the licensed or license exempt nature of the frequencies used.

3.6 Specific (legal) responsibilities in Healthcare

In Healthcare there are additional legal responsibilities for the medical staff apart from the normal legal professional responsibilities. Before applying medical tools the medical staff should verify that these tools work appropriately and adequate. It is the responsibility of the Healthcare organization that the medical staff can perform such an assessment without delay. Therefore, the medical staff must be able to rely on the information provided by the Healthcare organization. This leads to requirements of high infrastructure availability and data integrity.

3.7 Wireless technologies in low care

With respect to the use wireless technology in low care like care homes and home care, the regular technologies are used as is common in private homes or offices. Currently homecare organizations are installing video communications[22] to reduce the need for home visits and sensors to detect falls especially during the night. In many cases WiFi is installed as this is cost efficient and preferred by the patient.

In most cases the responsibilities for the functioning of the wireless network is delegated towards home owner or lender as it also done with the telephone services.

Existing technology sets expectation for future technologies that are sometimes too difficult to match. In the past, for example, the alarm system relied on the very reliable fixed line plain old telephone system. As this system also provided 48 V, the availability of the alarm was determined by the very high availability of the telephone especially because functioning of the home equipment was monitored via the same telephone line. This is no longer possible as the telephone system will not provide 48 V anymore. These old alarm systems have set very high standards and expectations for future systems. Currently separate ad hoc alarms systems are developed and deployed that avoid the use of this abandoned telephone technology.

Certainly there is no integrated risk management in place and consequently responsibilities are not well allocated nor is there a clear understanding what level of availability is required and guaranteed.

3.8 Risks of serious incidents with major social impact

There have been problems with the use of wireless technologies in hospitals. Two areas should be highlighted:

1. Especially in the clinical neurophysiology department where small electric signals from the neurological system are measured it is quite likely that some of the operational disturbances were caused by interference. However no reports were found.
2. Problems have been reported of interference between mobile phones and medical equipment. However no serious accidents were found caused by interference by wireless technologies.

The foremost reason why risks of serious incidents caused by wireless technology in hospitals should be considered as rather low is the fact that an integral risk management is in place. If this risk management is not sufficiently in place other risks like the risk of a microbiologic contamination (MRSA infection) or failure of the electricity supply are much higher to cause serious incidents.

Risks in low care are much more difficult to assess because there is still very little large scale experience. However, as integrated risk management is much more difficult to implement in low care, it is likely that risks cannot easily be identified and remedied.

Two of the more likely scenarios that could cause a serious accident with a major social impact are outlined below, in the following presumed context.

Presumed Context:

The next few years common WiFi technology is successfully implemented on a large scale. Patients and the nursing staff are pleased with the functionality. Patients can stay longer at home. Most patients and their families prefer home stay compared with admission into a care home. Nursing staff is also pleased as they can visit their patients only when real help is needed. Due to the increased need for home care and to continuous pressure on costs the nursing staff will be reduced in numbers compared to number of patients.

Two types of incidents are likely:

> Scenario 1. Due to the overloading of the wireless network in the municipal environment the quality of the network deteriorates. Consequently initial quality of the telecare services degrades which could give additional stress to the patient and reduce quality of the Healthcare services. Questions will be asked, e.g.: Who advised and selected this unreliable technology? Who should cover the cost of this failure?
>
> Scenario 2. A more serious accident is failure of the WiFi networks in a large area of the country for instance caused by a poor software update by the internet provider or a disturbance in the network control center. This would deprive thousands of patients of their telecare facilities. This will also occur when there is a large electricity outage. Likely there will be no sufficient numbers of nursing staff to visit all patients at home. Especially the more vulnerable and frail patients will be at risk.

The risk is even higher because nursing staff is less trained to deal with serious accidents and current procedures for serious accidents are not adequate. Normally serious accidents like a major fire or an aircraft crash are localized. Procedures are based on this locality assumption. Emergency vehicles with their personnel from a large area are directed to the accident. On a national level a coordination center is established that among others asks which hospitals have spare capacity. Failure of the WiFi network in a large area cannot be accommodated by such locality based procedures.

3.9 Specific issues with wireless in Healthcare (standards and regulations)

Hospitals have already an integral risk management approach as described above. For integral risk management attention is required for details in every aspect. Standards and regulations with respect to wireless communication in a Healthcare environment are far from consistent and complete. Now the usage of wireless communication increases it is also important to improve the quality of these standards and regulations. This is not only important from a risk management perspective, but also from the perspective of costs, as these inconsistencies cause also additional costs.

Particularly from the perspective of standards and regulations the following topics should be addressed:

- Disturbance of medical equipment. In several parts of the medical environment equipment is used that is susceptible to EM-radiation for instance in Neurology. However also some very mundane interference problems have been reported for instance causing disruption of the airflow in the operating theatre.
- Interference between wireless networks.
- Inconsistency between standards and lack of standards have been reported. This is a hindrance for proper implementation of these standards and consequently causes risks.
- Use in hospital environments (e.g. 3G/4G usage) is not in accordance with standards and internal risk procedures. Such a situation obviously causes risks

For more in-depth information is referred to appendix C in this report.

3.10 Specific recommendation with respect wireless in Healthcare

The RIVM report “Risks related to the use of eHealth technologies” comes to the following recommendations to prevent or minimize risk for patient safety:

1 Keep the Healthcare community alerted with regard to the risk issue;
2 Carry out follow-up research on the risks of ICT in Healthcare that focuses on establishing the magnitude and nature of such risks;
3 Establish a system to reliably report and document identified incidents consistent with existing systems;
4 Call for the application of existing norms and risk management tools in all phases of the life cycle as per NEN-EN-ISO 14971

We support the recommendations of RIVM, however eHealth has a much wider scope than wireless consequently we can be more precise and particularly with respect to point 4 we are more specific to standards and regulations for wireless (see Appendix C)

3.10.1 High care

With respect to the high care environment our advises are :

- Stimulate the maintenance and extensions of the standards and procedures with respect to use of wireless technology in Healthcare
- Accommodate wireless networks further in integral risks management of the hospital among others by implementing the next more detailed advises:
  - Implement spectrum management within hospital perimeter (especially for guidance to external contractors) but also to identify areas in the hospital with increased risks.
  - Specify wireless services clearly within the hospital even if this service is provided by an internal department. It is likely the wireless technology will be successfully deployed and the expectations will be high. Service level agreements are a proper vehicle for such specifications to manage the expectation and have clear understanding for what purpose with what quality these services are provided for instance outside the normal working hours.
- Implement knowledge transfer from experts to the field and create awareness about the risks of wireless technology to support massive deployment.

3.10.2 Low care

With respect to low care (care homes and home care) advises should be different as no integral risk management is in place:

- Learn from experiences in high care environment especially when patients have an increased vulnerability
  - Implement router with battery back-up or other facilities to guarantee uninterruptable power supply
  - Monitor interferences, especially gradual degradations (due to increased density of routers)
  - Have additional communication channels for alarms in case of failures of the wireless network
- Wireless networks will enable the low care environment to reduce on personnel
  - Have procedures in place for massive failures of wireless networks (e.g. incorrect software update, failure public network control center)
  - Implement additional data connections with call center of home care organization, to guarantee that alarms are signaled and make sure that the call center can operate without disturbance.

4. Risks of Wireless Communications in Industry

4.1 Introduction

In this chapter an assessment is made of the use of license free wireless frequency bands in the industry. A distinction is made between the (large scale) process industry and (small and medium sized) general industry.

For the assessment in the large scale process industry, the state of the art of application of wireless technologies was mainly drawn from literature and from the wide experience the researchers have in this field. The situation in smaller scale general production was assessed by means of a survey. The great number and wide variability of production sites, ranging from primitive manual operations of a few workers to highly automated sites with a few thousand employees, makes the method of interviewing of several key experts less suitable.

There is an essential and inherent difference between Healthcare and Industry in their use of wireless technology as in Healthcare:

- General public comes inside Healthcare premises
- Healthcare is also provided outside Healthcare premises
- Healthcare professionals use of common-off-the-shelf technology for job (smartphones, tablets)
- In Healthcare there is larger similarity between organizations than in Industry

Consequently recommendations will differ.

4.2 Process Industry

The authors of this report have a rich experience in establishing process control applications in the process industry. Most of the findings stated below were drawn from that experience. Additionally, an interview was held with an engineer with 26 years of experience in designing (mainly) petrochemical process plants (for Shell, GDF Suez, Total, BP, ABB , etc.). The interview confirmed these findings.

The process industry (e.g. chemical, petrochemical, pharmaceutical, food, metal production industry) typically occupies large, well-controlled production sites. Safety management, with environmental control, has the highest priority of production management. Monitoring of the process is essential.

Within a large scale production process, not all data is equal. Some data is useful to the efficiency of the process, while other data can be critical regarding the safety of the process. The prime focus of production management is on decreasing the risk that processes will become uncontrolled. The basic term describing how critical data is for particular process is called SIL (Safety Integrity Levels) which establish the probability of an acceptable failure in the system. This must be taken into account when designing the system. A more detailed description of SIL and what it means for design of the system is covered by IEC61508, see[11] and a book on design of SCADA (control and acquisition systems) in [12] and [13].

The process is controlled by several control loops. In the first loop process safety is controlled. Technology used for this loop is proven and thoroughly tested. Usually this loop is double or triple equipped, without a single point of failure (this is in relation to SIL levels, and overall design of SCADA systems for plants. For the transfer of measured (observed) values for monitoring elements (pressure sensors, temperature sensors, …) and also for the transfer of controlling signals back to actuating elements (motors, valves, switches, …) protocols such as Fieldbus, Profibus and HART are used. Introducing redundancy in communication lines for the most critical elements of the monitoring and control system is the method to decrease the

probability of failure. Another method is using geographical separation of the communication paths, and also for location of the controlling elements.

On a physical level, these protocols are always wired. They are not very flexible, as the wiring dictates the topology of the network. But, they are proven technology and have been used for years in the process industry, and that makes them extra attractive. Main challenge with the use of wireless communication for transfer of measured values from sensors and sending back of the controlling signals back to actuators is the potential risk of losing data. So that probability can be taken into account when designing the SCADA for a particular plant. Still, with no long track record (time-wise), wireless communication is still seen as a high risk, which suppresses the main advantages of fast and cheap installation.

4.2.1 Quick overview of SCADA and its workings

A typical process control system architecture is shown in the figure 4.1. In the upper row we see a number of controlling units, which are calculating the currently observed state of the system which is based on inputs coming from the elements in the field. Based on those observed measurements, and preferred state of the system, a number of control signals is calculated and fed back to actuating elements in the field.

As mentioned, currently, in (petro)chemical process plants, all of the communication links are wired, and links for data which is considered to be critical for safety of the process (also people, environment) are double or sometimes triple implemented.

A number of standardization bodies have developed standards for describing, quantifying and proposing methods to decrease risks of dangerous situations happening. One such example we find in the International Electro technical Commission's (IEC) standard IEC 61508 ([14]). This standard defines risk in terms of SIL (Safety Integrity Level) which is an exercise in risk analysis where the risk is associated with a specific hazards. In the process industry SIL is widely used.

4.2.2 Wireless communication in monitoring systems

Depending on the communication protocol used, the interruption of the communication line might result in loss of data or in the retransmission of packets, where it would result in increased latency of data arriving. Interruption of data arrival, resulting in losses or increased latency, may have significant impact on the control of the production process. Both loss of information or increased latency can result in instability in the control systems, and therefore are not acceptable, as lack of control can lead to potentially disastrous situations where safety is compromised. In large scale process industries, wireless communication is therefore normally not used for critical applications or safety control (the first control loop).

The second control loop is used for additional data collection. Data collected is used for off line process analysis and simulations. Process engineers determine by analysis the optimal settings of the parameters in the first loop. Data collection, data processing and the use of IT for process analysis are cornerstones of modern production processes. Networks may be composed of many different types of sensors such as seismic, thermal, visual, acoustic, radar, magnetic, infrared, and many others which are able to monitor a wide variety of ambient conditions such as: environmental and weather conditions, pressure, temperature, gas, fire, sound, humidity, vibration, electrical characteristics, mechanical stress, soil makeup, object movement, presence or absence of objects, speed, direction, and size of an object, location etc. What process properties need to be monitored is usually a result of previous analysis.

Wireless monitoring systems add flexibility in positioning and location of monitoring nodes and add flexibility in communication to and from monitoring nodes towards process analysis systems. Wireless technology is beneficial in many regards. Eliminating the need for cables can contribute to reduced installation and operating costs, it enables installations in remote areas, and it allows for cost efficient, temporary and mobile systems. The use of wireless systems in the second control loop is therefore increasing.

In order to increase the reliability of wireless communication, a number of protocols and other standards have been developed. One example is IEC 62591-1 (Wireless HART), see [15], [16] and [17]. The HART application layer has been in existence since the late 1980s. In its initial release,

the HART Field Communications Protocol was superimposed on a 4-20mA signal (its physical layer) providing two-way communications with field instruments without compromising the integrity of the analogue output. Clear advantage was that any broken wire could be easily and quickly discovered. This was not possible any more with the move towards wireless communication. For wireless communication a set of diagnostic tools was needed to discover link interruptions.

Also, since wireless links depend on a number of factors that can degrade the connection, it was necessary to lower the risk of bad links by designing the network layer as a fully meshed network, where data has multiple (possible) paths to get from one point (device) to another point (device), thus increasing the probability that data will come through, even if one on the links has failed. . So, a meshed network with its multiple paths for data, and fast re-routing protocols is a direct answer to the required SIL and to the probability of data loss on wireless links, see Figure 3.1.

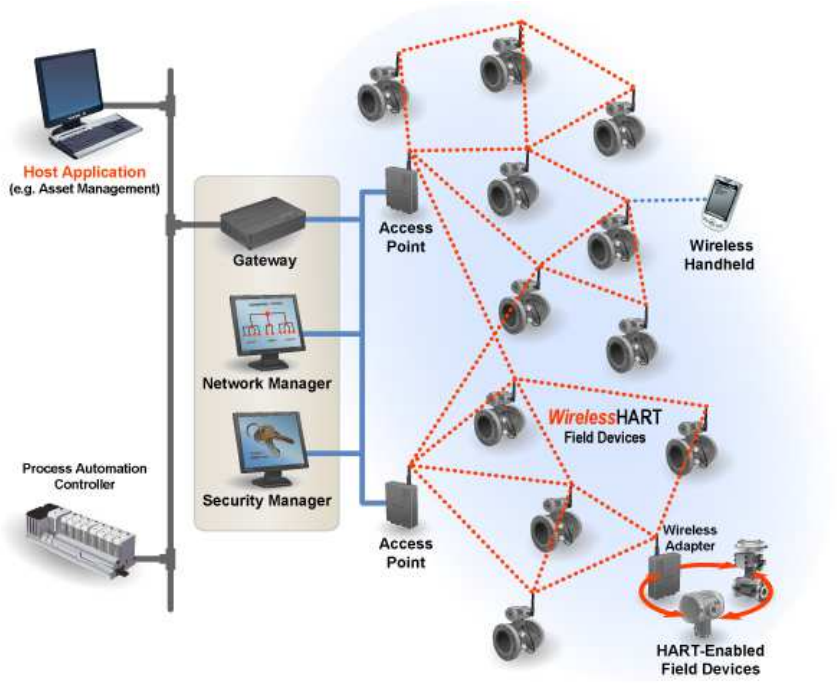

Figure 4.1. Wireless HART

Another consortium providing wireless monitoring solutions for process industry is ISA100. It also has, like WirelessHART, its background in wired monitoring solutions. Proposed solution is similar to WirelessHART, with meshed connections between devices.

Note that both WirelessHART and ISA100[4] are basing their solutions in the 2.4GHz ISM band (well known for WiFi), which is worldwide and license exempt. Worldwide availability is an important element for deployment by multinationals, who prefer to run the same (or similar) equipment in their plants.

Large scale production sites in the (chemical and metal processing) process industry are strictly controlled. Only devices are allowed access to the site that do not interfere with process control. Because of the mere size of the sites, little interference exists with the wireless facilities of neighboring sites. Due to the range limitations which apply to systems in the ISM band due to transmit power limitations, the process industry effectively controls its own ether.

—

[4] Both WirelessHART and ISA100 solutions don't comply with the legal conditions for unlicensed use of the 2.4 GHz ISM band in the EU. Therefore it is not allowed to use these systems in this frequency band in the EU.

NB: It is important to note that since currently offered wireless monitoring systems use the ISM band at 2,4GHz, which is also used by other devices (smartphones, laptops, multimedia players) plant operators MUST take additional steps to ban additional equipment which might use same band, and enforce policies. This is a critical but necessary step in order to maintain integrity of monitoring and control systems that use wireless communication in this band.

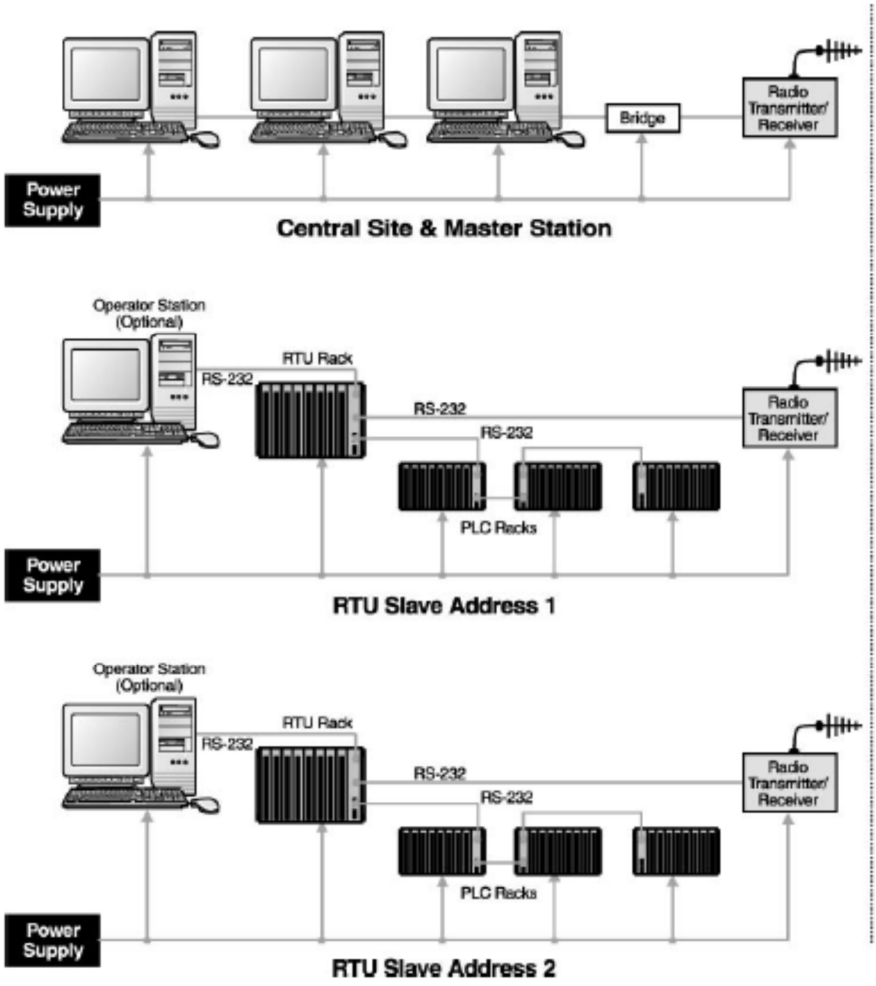

Figure 4.2 : Example architecture of an industrial control system

It can be concluded that currently the wireless technologies are only used in the (large scale) process industry for collecting data to improve or fine-tune the process. Wireless technologies are at this moment not used for process-critical applications and certainly not when safety is at stake. When wireless technologies are used, their performance is monitored and controlled. If wireless technologies could be sufficiently reliable, they could be of great value because of flexibility. As described in this chapter, protocols and methods are being developed and standardized to improve reliability. Large scale production facilities are able to control their spectrum. A knowledge infrastructure exists for the professionals in this area to apply the state of the art of standards and technology.

4.3 General industry

General industry (e.g. metal and wood processing, machinery) is different from process industry in that the variability is much greater, both in the size of sites, the level of automation, the knowledge and the controllability. Not much is known about the state of the art and its application. Interviews as a research method seemed because of the variability not as a suitable

first approach to be a suitable instrument. Therefore a survey was held among these companies in the Netherlands accompanied with additional interviews

A questionnaire was sent to 1600 mail addresses of metal and wood processing and machine building companies. The addresses were drawn from the Yellow Pages. A response was received from 68 companies. For this type of surveys such a low response is not uncommon. The questionnaire has been attached to this report. In addition five interviews were held among specialists of wireless industrial applications and people responsible for such applications. The findings in the survey were confirmed by the views of the experts and the additional interviews.

4.3.1 Survey

The survey revealed the following:

76% of the companies use WiFi, but only 29% of the companies use WiFi or other wireless technologies in their production process. This latter percentage varies somewhat with the size of the company.

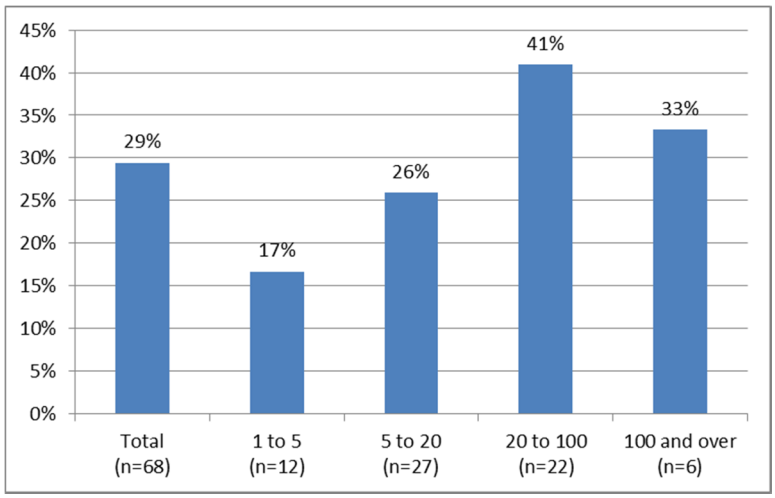

Figure 4.3. Use of wireless technologies in production by number of employees

Wireless technologies that are used include WiFi connections between production machines and application servers, DECT telephones and wireless barcode readers (presumably also using WiFi). One company reported the use of non-WiFi wireless protocols between production machines and computer equipment.

The importance of wireless technologies to the company processes vary. On the question whether WiFi or other wireless technologies are important for their business, almost half of the companies responded that such technologies are hardly important. Only 19% responded that wireless technologies are essential.

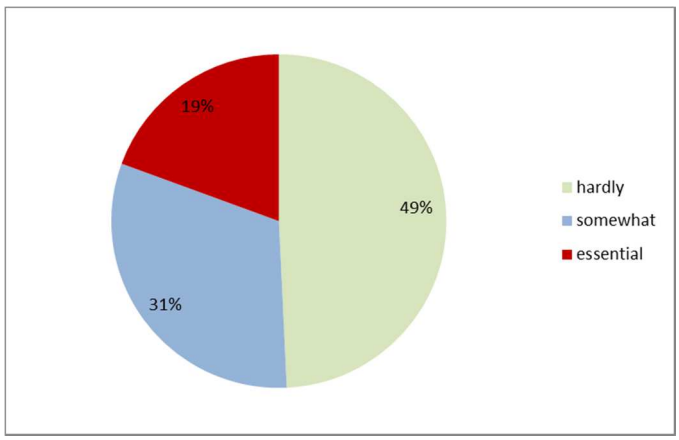

Figure 4.4. Importance of wireless applications

Among the companies that use wireless technologies in their production environment, 45% respond that these technologies are essential and only 15% that they are hardly important.

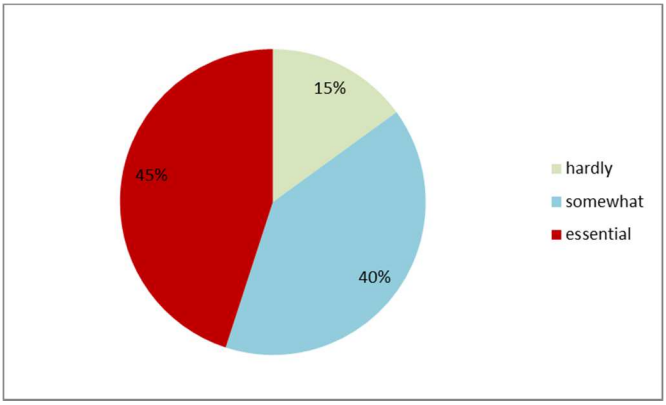

Figure 4.5 Importance of wireless applications for companies that use wireless technologies in production

Companies that use wireless technologies in production, also report that outage of wireless services for a longer period of time would cause them damage.

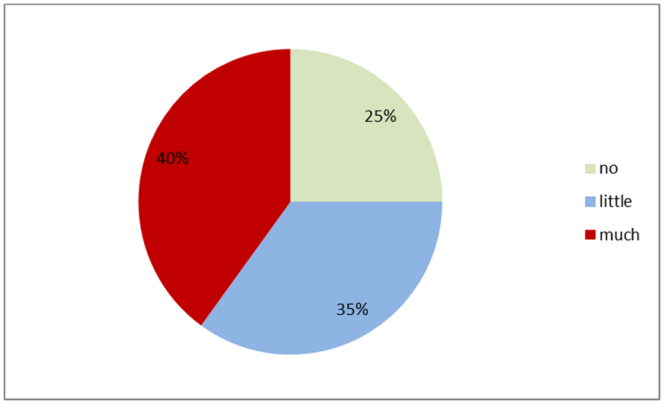

Figure 4.6. Expected damage as a result of long lasting outage for companies that use wireless technologies in production

The type of damage that is caused when the wireless infrastructure fails seems however not very severe. No company reports safety risks. Most problems that may arise have to do with having to install cables and suffering some production loss. Many companies report they already installed cable back up.

4.3.2 Interviews

The interviews confirmed the survey findings, although big differences exist between companies. Some large companies have installed professional risk management with regard to wireless applications, although the risk assessments often do not mainly apply to the use of spectrum or protocol. They focus on the reliability of the entire application that includes mobile equipment and central processing. In other companies, no risk assessment is applied, but the policy is restricted to reaction to outages and performance decrease.

Awareness with regard to potential congestion and interference issues is generally low. Wireless applications are assessed in isolation, not in combination with each other. In larger plants (interviews were held with representatives of sites with a surface of several acres) all use of

license exempt frequencies can be controlled by the company itself. Smaller companies, especially those with locations that are crowded with other companies, have much less control over the available bandwidth. In general all respondents have confidence in regulation and public management of frequencies. Most are not aware of the difference between regulated and license exempt bands. One respondent has the policy not to use the 2.4GHz band for production related application, but to use the 5GHz band for those purposes.

Typically, industrial companies are very reluctant to use wireless technology for critical production processes. In some cases however, such technologies are applied, e.g. for communication with PLCs and bar code scanners, without wired back up. Different from large scale process industry, smaller scale companies cannot control the use of frequencies at their site, the neighbors are too close, especially at industrial areas. They cannot control the risk of congestion. For some companies, the failure of wireless connections may cause severe damage.

The capacity of applicable license exempt bands may be increased by allowing specific protocols per band. Protocols can be (and are) made more "intelligent" with regard to bandwidth efficiency. Multiple protocols may cause unpredictable interference. In industrial areas the level of congestion may be monitored. Companies using wireless technologies should be more aware of the risks.

Based on the interviews a number of typical cases were developed. These cases are the following:

4.3.2.1 Electrical appliances

Company A each year produces 10 million pieces of electric consumer appliances. They have installed two WiFi networks: one closed network for internal use and one open network for guests. The internal network is used by laptops and phones of employees and by bar code scanners for production monitoring. The 600 manufacturing machines only use wired connections for monitoring and control.

There has been some interference between production equipment and the bar code readers. This has been solved by different positioning of antennas.

If the bar code equipment fails, production does not halt. Monitoring transactions can be fed to the production system using keyboards, although this would be cumbersome. No procedure is yet in place for such manual back up.

The production site is large enough not to have neighbors interfering with the system or consuming bandwidth. The open WiFi system has a potential risk that strangers consume bandwidth by parking close to the company gate. This phenomenon has not yet caused problems.

4.3.2.2 Rolling stock maintenance

Company B maintains rolling stock at several (remote) locations with some 1400 employees. All employees are equipped with tablet computers. The tablets are used as the interface with the ERP system and as a device for communication of detailed work instructions, including technical drawings, photos and videos. The tablets use WiFi, but can switch to 3G GSM for back up. In the past the employees had access to fixed workstations, but these are now removed.

The performance of the system is permanently monitored. The monitoring however applies to the total functioning of the system, especially the responsiveness of the ERP system, not specifically to the wireless communication link. As the production sites are remote, no interference with WiFi systems of neighboring companies exist.

4.3.2.3 Electrical equipment

Company C produces large scale, high voltage electrical equipment. Wireless communication is used for operating overhead cranes, factory doors and warehouse trucks. Most wireless communication uses equipment-specific protocols. WiFi is only used in the warehouse.

When installing the equipment, no risk analysis has taken place. Equipment failure sometimes occurs, but seldom in relation to interference or bandwidth congestion. Cranes and doors are inspected regularly. Bad connections are repaired by different positioning of antennas, etc. Doors can be operated manually if needed.

The size of the building prevents neighbors to interfere with the wireless systems.

4.4 Conclusion

In large scale process industries, wireless technologies are only used for (additional) data collection in order to improve and fine-tune the process. Yet, reliable wireless technology might considerably improve process and business efficiency. Dedicated protocols per frequency band, tailored for process-critical applications and with built-in reliability, could be a solution.

In small and medium size general industrial enterprises, an increasing use is made of general purpose technologies, such as WiFi. In most cases, wireless technologies for mission critical operations are backed up by wired solutions, but not always. Small enterprises cannot control the saturation of the frequency bands they are using and they can hardly measure congestion. They may suffer production loss or other damage when their wireless communication systems fail.

Awareness of the risk of the use of license exempt frequency bands is low. In larger companies risk management with regard to mission critical applications is in place (in most smaller companies it is not), but risk assessment is not focused on the wireless connections. Instead, the application in its totality is assessed. Cross-application risks, such as congestion of frequency bands, are not assessed.

4.5 Specific recommendation with respect wireless in Industry

- Recommendation to industry to implement professional risk management and include in the risk assessment the possible failure of wireless devices due to congestion or interference.
- Introduction of additional, licensed and/or exclusive frequency ranges for critical wireless applications should be considered. WiFi and other wireless techniques may be very advantageous to industry for reasons described above. As congestion risks in license exempt bands are uncontrollable, use of these techniques is presently too risky. Additionally licensed and / or exclusive frequency ranges can increase capacity and controllability. Industry should be recommended to use distinct frequency ranges for distinct protocols and applications.
- Recommendation to industry to use specific or exclusive frequency ranges for mission critical applications, and not the frequency bands that are used for WiFi. One of the interviewed companies mentioned that their policy is to use the 5GHz band for these purposes, instead of the 2.4GHz band.
- Recommendation to industry to use standard protocols for industrial applications rather than ad-hoc protocols that are specific to the devices used. Standard protocols have better capabilities for reliability, performance and congestion management and may use the available bandwidth more efficiently.
- Recommendations to back-up critical applications with wired solutions. As long as congestion is not monitored or controlled, industry should be aware that wireless connections may fail.
- Recommendation to industry to monitor the availability and capacity of bands in industrial areas. For bands, dedicated to a protocol, the protocol can be made more intelligent, increasing the capacity and catering for graceful degradation.

Recommendations towards government and regulator are the same as the general recommendations

5. Stakeholder analysis for use of wireless technology

5.1 Introduction

The main conclusion in Chapters 3 and 4 shows a remarkable similarity between the two sectors of investigation, viz. Industry and Healthcare. In both sectors, the risks of wireless technologies was found not so much in the high-end of the sector (hospitals and large industries), but more in the low-end where local Healthcare centers can be encountered in shopping centers or where small industries can be found in business parks.
Below in Section 5.2 we will provide an analysis of the behavior of stakeholders in the "low-end" situation, based on the attributes of the stakeholders involved. In Section 5.3, we will pay attention to the legal situation of complex services offered using wireless technology.

5.2 Stakeholder behavior

For a deeper analysis of this situation in terms of stakeholders and their actions, we use the seminal work of Mitchell et al. [23]. These authors provide three attributes of stakeholders for analyzing stakeholder action, viz,

- Power, defined as a relationship between stakeholders where one stakeholder A can get another stakeholder B to do something that B would not have done otherwise
- Legitimacy, defined as a generalized perception that actions by a stakeholder are appropriate within a system of norms
- Urgency, the degree to which stakeholder claims call for immediate attention.

These attributes are placed in a Venn-diagram by Mitchell et al, see figure 5.1 below. Their claim is that pressures from stakeholders are more successful if these stakeholders accumulate the attributes. Stakeholders with all three attributes are called *definite* stakeholders, and are presumably most effective in getting their priorities accepted.

When looking at wireless networks one can identify the following groups of stakeholders:

- The ***users of the wireless network***. Examples in Healthcare are forensic patients that are monitored not to enter specific areas, or elderly users of public transport based on location services. Examples in Industry are employees of small firms in industry parks using WiFi to check and control the status of machinery. Often, WiFi in public space is also used by unintended users.
- The ***customers of the wireless network***. These are the parties who pay the bill for service providers and operators. Often, these customers are local societies of entrepreneurs (e.g. in shopping malls).
- The ***owner*** of the premises concerned**.** The owner (landlord) may or may not act as customer.
- The ***operators of these wireless networks*** and ***providers of services*** based on the wireless networks. Examples are a wireless network in a shopping mall or services during a music festival.
- The ***suppliers, providing the equipment and the (wired)networks*** that provide the basis of the wireless network. Examples are the telecom operators and technology companies providing wireless routers via internet sales channels. Also consultancy firms that provided advice and assess the quality of the networks be included.
- ***Government, standardization- and regulating bodies*** that set the rules to which wireless networks should comply and that monitor and safeguard that providers comply with these rules.
- ***Governmental bodies responsible for public space,*** governing admission for activities and physical assets from many points of view of varying from cultural heritage, and biodiversity, to competition and public health.
- Also the ***general public*** and organizations representing the general public like consumer organizations.

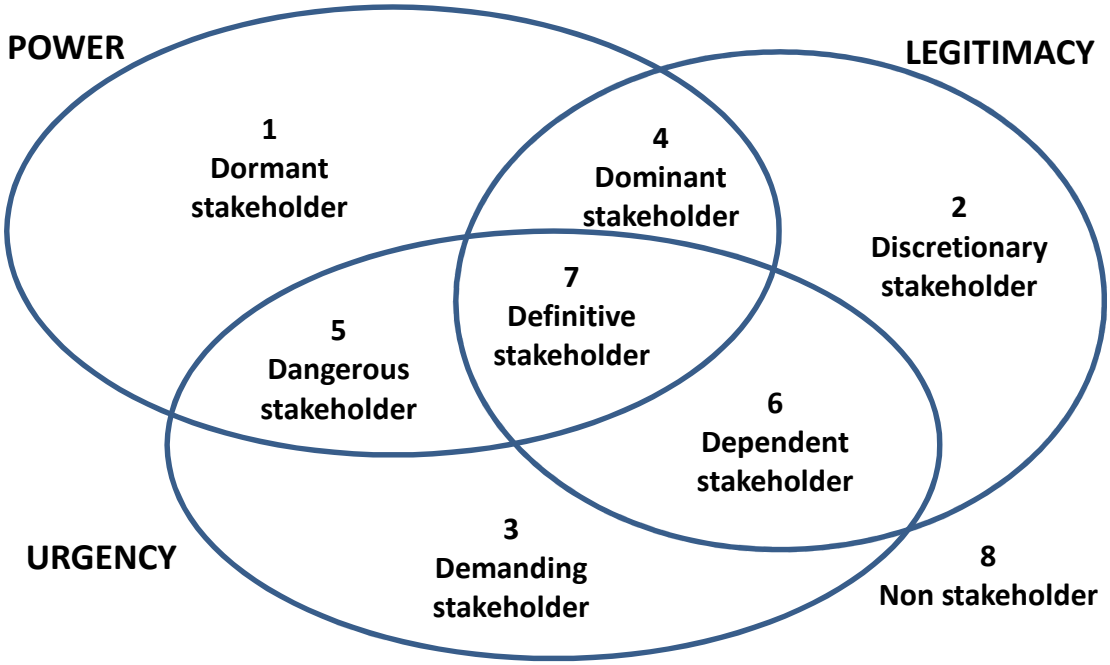

Figure 5.1. Stakeholder typology (from [23], p. 874)

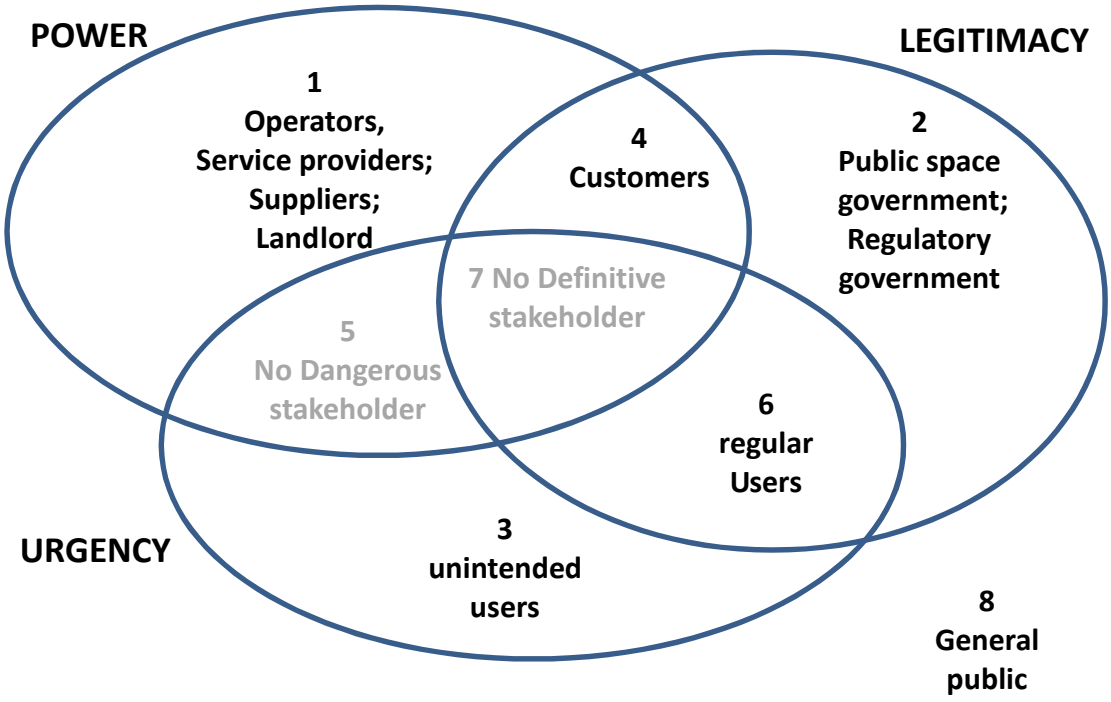

Figure 5.2. Stakeholders in the case of wireless technology, where there is not a single party responsible for risk management of the premises

These stakeholders are positioned in figure 5.2, following the typology of figure 5.1. With respect to the risk of wireless technologies, we have positioned the operators (service providers), the suppliers and the landlord in the position of dormant stakeholder, because they have the power to take risk mitigating measures, but they do not have a sense of urgency to act, nor are they generally perceived as the legitimate party to mitigate such risks. Such legitimation resides with

customers and governments, but these parties lack urgency. Regular users, finally, have legitimacy, but no power. Only in case of degrading performance, they get urgency.
As shown in figure 5.2, there are no definite stakeholders in this "low-end" situation in Healthcare and Industry. This is in sharp contrast to a situation within a hospital or inside larger industry, where risk managers have the power, the legitimacy and the urgency to take risk mitigating measures.

l

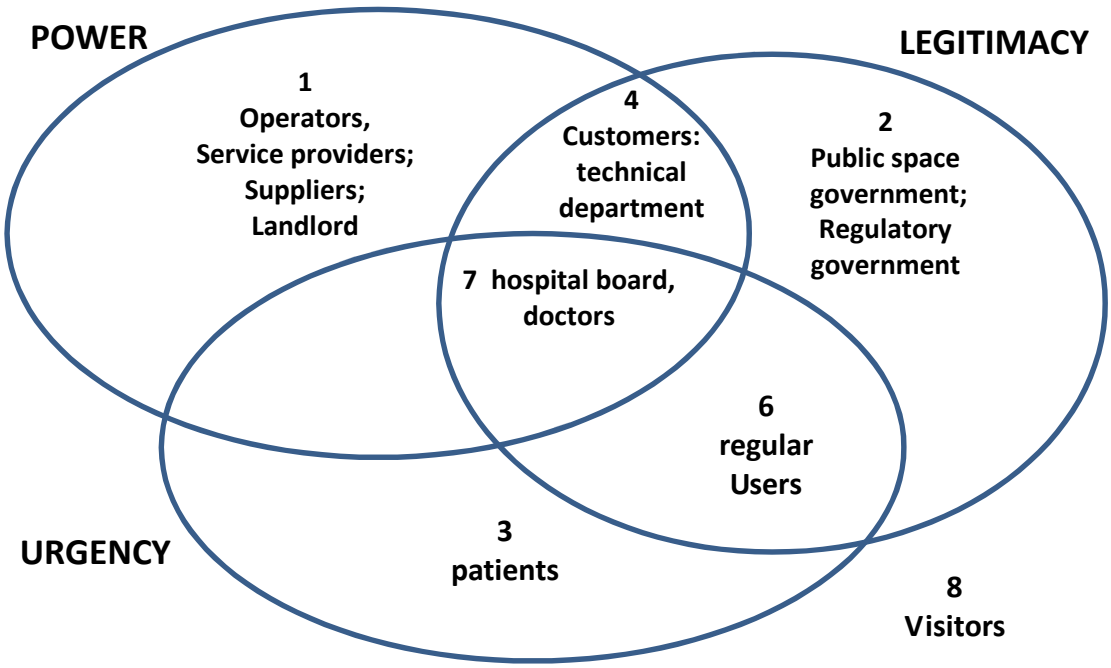

Figure 5.3. Stakeholders in the case of wireless technology usage in a hospital, where there is a single party responsible for risk management of the premise

Although in general a stakeholder analysis should be made for a specific occasion, the similarity between hospitals is very large and consequently a generic stakeholder analysis is possible here. Evidently the hospital board has the power, the legitimacy and the urgency to play their role with respect to the hospital wireless network. The technical department has the power and the legitimacy. They have the contract with the operator and they have the task to maintain the network. Patients definitely feel the urgency when the network is not working properly. The doctors will also feel the urgency of a proper working network, however due to their formal legal position (see 3.8) they have the legitimacy and probably also the power for instance via IGZ (Inspectie voor de Gezondheidszorg) to resolve issues with respect to the quality of the wireless network.

In low care many of the responsibilities of keeping the wireless network are delegated to the patient and its informal care environment. Wireless network facilities vary from home to home and contract structure is not well documented. The responsibilities of a home care organization are much more limited. The over-all power to resolve issues is much lower not only because the ability to execute of the average patient is rather low. The Mitchell diagram is consequently much more difficult to draw as it will vary from case to case.

Also in Industry responsibilities of the different stakeholders vary, but as remarked before in the large industrial chemical plants the physical boundaries of the plant are well marked and there is little chance of outside interference. Also within the plant safety procedures are an essential part of the operation and aligned with risk management.

Hypothetical case in industrial park
An industrial park locates several SMEs. Two firms A and B have adjacent facilities already operational for more than five years and over time the relation between the two firms has deteriorated due to a commercial dispute.

Firm A has improved recently their production line with an industrial robot that by its nature needs to move freely. The robot is controlled via WiFi and latency is important to guarantee proper functioning.

Firm B has several service engineers in the field. At their home base they back up their portable service computers and install new manuals via the WiFi system of Firm B.

Occasionally firm A has production problems resulting in quality issues in delivered products. Firm A addresses the supplier of the industrial robot, but this supplier cannot find to cause of the problem. Test sequences don't show any malfunctioning. After several months it appears that the cause of the problem is in the WiFi network, due to interference of the WiFi signals of both firms.

What can firm A do to resolve to problem and is there a possibility to recover the costs of production loss and claims of his customers?

The supplier of the robot feels the urgency but lacks the power or the legitimacy to resolve the problem.

The landlord of the industrial plant has only limited power and legitimacy to force firm B to change his WiFi usage. From a regulator perspective there is no reason to intervene. The landlord feels also little urgency to resolve the problem.

Firm A consequently has the urgency to resolve the problem. However he cannot force firm B based on his contract with the landlord, so he has limited power and no legitimacy.

One can conclude that none of the stakeholders have the urgency, power and legitimacy to resolve this problem.

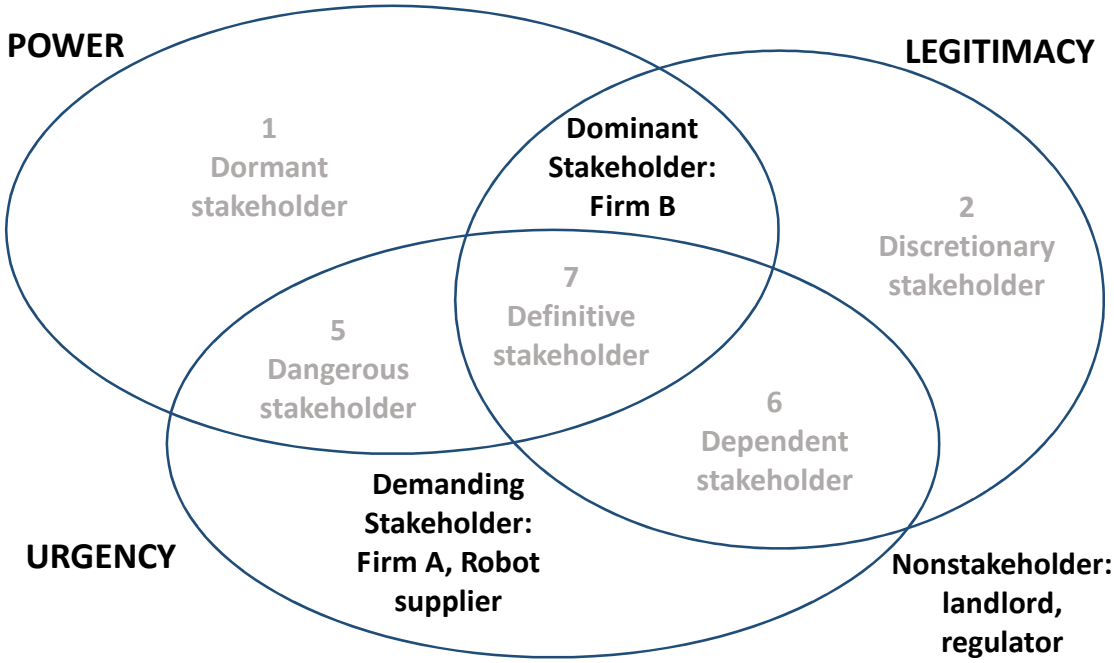

Figure 5.4 Stakeholders in the case of wireless technology, for a hypothetical case in industrial park

A Mitchel type analysis should be part of the total risk management procedures for a specific case, and should be used particularly to assess if responsibities for risk management are properly allocated in the organization and if the linkage with the board is properly established.

Concluding this analysis, it is clear that the attributes power, legitimacy and urgency should be combined to gain effective action. When there is no central authority in a premise taking responsibility for risk management, the urgency is lacking until the problems become manifest Once problems are manifest, there is no authority who has sufficient power to act and safeguard mission critical applications.

5.3 Legal aspects of stakeholders and their roles

A wireless network is the result of human acting. One or more organizations provide such a network with the assumption that intended users with appropriate devices can use this specific network. In some cases there is a contract between the provider of the network and the user, as it is with mobile telephone networks. In many cases there is no contract with the users, but only with customers , who provide services to users, whether employees or other human end users.

In many cases one can identify stacks or chains of services. For example, consider the following use case scenario: *in a city center there exists a WiFi network provided by the local shops. A group of volunteers provide historical data about the city center in the form of digital services. These digital services are based on the* WiFi *network combined with location services. A hotel in the city advises its customers to make historic city tours. A tour operator offers city trips with historic focus including a stay in this hotel.* May a customer of this tour operator reasonably assume that he can enjoy this city trip?

We know wireless networks can fail. However to what extend can users rely of services based on a wireless network? How should users assess and curb the risks caused by the usage of the wireless network? For industry and Healthcare these issues were elaborated in the previous chapters.

When analyzing such scenarios from a legal perspective, the first question which emerges refers to the contracts which are in place. If there are contracts in place between parties involved, then these contracts provide a legal basis for action by parties who consider other parties to breach their obligations. There is no reason to call for new legislation in this particular case. When there is no contract between parties, there may nevertheless be expectations raised by parties. These are governed by existing legal practice, just as in any other case where expectations are raised which are not met. Here too, the existing legislation seems adequate.

As a consequence, the management of risk is not so much a legal problem but more an awareness problem, In The Netherlands, there is a legal framework available covering services in general, which is also applicable in this area, However the general public is not sufficiently aware of inherent risks in wireless technology, such as outages for a longer period or in a larger area (see Section 3.10).

Certainly there is difference in the role of stakeholders when licensed or license exempt technology is used. In the case of licensed networks the position of telecom provider is better defined. However for successful risk management it is more important if the is a stakeholder that combines urgency, power and legitimacy. The differences between licensed and license exempt manifest particularly in an individual case when the actual service level agreements are considered.

5.4 Conclusion

The above stakeholder analysis supports the earlier conclusion that risk management by a central authority in a premise is essential to mitigate the risks of wireless technologies (EMI, malicious action, congestion and interference). Moreover, the legal analysis shows that the problem is not so much a problem of legislation and legal framework but more a problem of awareness.

6. Conclusions and Recommendations

Agentschap Telecom asked on behalf of the ministry of Economic Affairs to perform a multidisciplinary study on the societal implications of the risks of the uptake of (license exempt) wireless usage. The study had to focus on the Industry and Healthcare domain
From the perspective of society it is likely that the large success of wireless technology (and in particular WiFi) will contribute to its risk of failure. Expectation and adoption are very high. However the general public is not sufficiently aware of the inherent limitations of wireless technology, especially in license exempt bands (and notably applicable to WiFi.)
In The Netherlands, where population density and usage of internet are high, the limitations will manifest themselves rather early. This may cause disappointments about the technology.

Our conclusions are the following:

- The field is not aware of the distinction between licensed and license exempt frequency ranges in wireless communication.
- The risks of wireless communication can be classified into:
    1. Risk of malicious action, leading to violation of privacy and/or (again) interruptions of availability communication services
    2. Risk of EMI causing failure of technical components, leading to interruptions of availability communication services
    3. Risk of congestion and interference, leading to increased latency or (again) interruptions of availability communication services
- These risks apply in principle for all wireless communication, regardless whether or not the frequency range is licensed. The second risk, EMI is not always due to telecommunication devices, but can also be caused by other electro-mechanical devices used in Industry or Healthcare
- There are technical and contractual measures by which users of services can mitigate the above risks. However, in a specific area these risks, can ultimately only be mitigated by parties who exercise control over that area.
- Therefore, the risks of cannot be controlled in areas where no controlling party is present, such as in shopping malls or industrial parks.
- Accordingly, mission-critical applications are at risk when they rely on wireless technology. Licensed and/or exclusive frequency ranges for such applications may contribute to mitigating these risks.
- However, regulation of frequency ranges does not by itself control the risks in such mission critical applications. These risks have to be mitigated by other accompanying measures by authorized parties. Standardization and the involved interaction between the regulator and industry also plays a role in lowering the risk associated with a particular application.

We recommend that

1. The government should raise awareness of risks involved in the use of wireless technologies. The general public and many small businesses are not aware of these risks and expect the same performance as in case of wired communications. This holds in particular for mission-critical communication. The risks are not only the inherent risks of using a wireless technology, but also the risks of failure in the whole service provisioning chain (e.g. failure in the operator control center). In particular the distinction between licensed and license exempt frequency ranges and the related risks of congestion due to interference should be widely communicated. The regulator could stimulate education and training for risk managers with spectrum risk mitigation duties.
2. Evidently government should continue to play its role in the setting of regulations and standards with respect to wireless communication particularly on the point of mission critical applications and consistency between standards. The government should maintain the option for parties concerned to use the licensed and/or exclusive frequency range for mission-critical applications. The increase of license exempt ranges

should therefore be treated prudently. European regulations should cover some serious interferences issues in hospitals, see Appendix C for a complete list.

3. For mission critical applications as in Healthcare there is a need for reliable and resilient systems that in case of failure will cause no harm, or at least a minimum of harm[5]. This may especially be the case in environments where there is no authority controlling the physical environment. This may lead to regulation in parts of the spectrum reserved for such applications. The same may apply to industrial sites without central authority, anticipating future preference for wireless applications in Industry.
4. Organizations should take into account the risks of wireless failures by reconsidering their risk mitigation measures. As wireless technologies will be used more and more for the business critical systems, services or processes, it becomes essential to take into account the involved risks of outages of these technologies during the design process. This requires thinking in advance about the countermeasures that are required to implement backup scenarios or to enable temporary degraded performance operation. Furthermore, companies have to increase awareness by training of their employees and staff. A guideline can be the Risk Management Standard.

For Healthcare with respect to the high care environment (hospitals) the following specific recommendations are made:

- Accommodate wireless networks further in integral risks management of the hospital among others by implementing spectrum management within hospital perimeter and specifying wireless services clearly via service level agreements to manage the expectations.
- Implement knowledge transfer from experts to the field and create awareness about the risks of wireless technology to support massive deployment.

With respect to low care (care homes and home care) advises should be different as no integral risk management is in place:

- Learn from experiences and practical solutions implemented in the high care environment especially when patients have an increased vulnerability
- Wireless networks will enable the low care environment to reduce on personnel. Have procedures in place for massive failures. Guarantee that alarms are signaled and make sure that the call center can operate without disturbance.

As the variations between industries are larger than in healthcare it is not possible to be as specific as in healthcare, however for industry in general these recommendations can be emphasized:

- Recommendation to industry to implement professional risk management and include in the risk assessment the possible failure of wireless devices due to congestion or interference.
- Introduction of additional, licensed and/or exclusive frequency ranges for critical wireless applications should be considered.
- Recommendation to industry to use application specific or exclusive frequency ranges for mission critical applications, and not the non specific frequency ranges that are for example used for WiFi.
- Recommendation to industry to use standard protocols for industrial applications rather than ad-hoc protocols that are specific to the devices used.
- Recommendations to back-up critical applications with wired solutions. As long as congestion is not monitored or controlled, industry should be aware that wireless connections may fail.
- Recommendation to industry to monitor the availability and capacity of bands in industrial areas.

For healthcare and industry the more detailed recommendations can be found in the specific chapters. One of the differences between in healthcare and industry recommendation are on the advice to introduce additional exclusive bands. In healthcare there is a stronger motivation to use common of the shelf technology than in industry. In healthcare for doctors and nurses a

—

[5] In certain sectors the term fail-safe is used.

“bring your own device” policy is currently adopted with additional security provisions. This is certainly the case in low care. In industry the common standard is to use special professional equipment for process control. Consequently it is more obvious to introduce special bands for this purpose. In healthcare this is also true in the area of patient monitoring especially in the high care environment. For healthcare also detailed recommendation with respect to standards can be found in appendix C.

References

[1] Ericsson white paper, *More than50 billion connected devices*, February 2011, http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf

[2] Berenschot (met medewerking van o.a. TNO), *Roadmap Short-range wireless communications*, in opdracht van Innovatie Zuid, door Mei 2012, p.20 http://www.bom.nl/include/OI/Short_Range_Wireless_Communications-_Roadmap

[3] **IEC 80001-series:**

- **IEC 80001-1:2010** Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities
- **IEC/TR 80001-2-1:2012**, (...) Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples
- **IEC/TR 80001-2-2: 2012**, (...) Part 2-2: Guidance for the communication of medical device security needs, risks and controls
- **IEC/TR 80001-2-3: 2012**, (...) Part 2-3: Guidance for wireless networks [This part of IEC 80001 supports the HDO in the RISK MANAGEMENT of MEDICAL IT-NETWORKS that incorporate one or more wireless links. The report provides technical background concerning wireless technology and examples of HAZARDS to be considered when wireless technology is used in MEDICAL IT-NETWORKS and suggests RISK CONTROL measures to reduce the probability of UNINTENDED CONSEQUENCES.]
- **IEC/TR 80001-2-4: 2012**, (...) Part 2-4: General implementation guidance for Healthcare Delivery Organizations
- **IEC/DTR 80001-2-5**, draft (...) Part 2-5: Guidance on distributed alarm systems ["Alarms presented on e.g. smartophones, tablets, etc. – WiFi, GSM, etc.]
- **IEC/DTR 80001-2-6**, draft (...) Part 2-6: Application guidance -- Guidance for responsibility agreements
- **IEC/NP 80001-2-7**, draft (...) Part 2-7: Application guidance -- Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1

[4] WIK and Aegis, *Study on Impact of traffic off-loading and related technological trends on the demand for wireless broadband spectrum*, A study prepared for the European Commission DG Communications Networks, Content & Technology, 2013

[5] Agentschap Telecom, 2012*, Agentschap Telecom waarschuwt voor verstopping WiFi-verkeer*, www.agentschaptelecom.nl/actueel/digitale-nieuwsbrief/ontwikkelingen-de-markt-juni-2012/agentschap-telecom-waarschuwt-voor+verstopping+WIFI-verkeer

[6] Universiteit Twente, *WiFi loopt binnenkort tegen grens aan*, June 2012, http://www.utwente.nl/archief/2012/06/ut_onderzoek_wi_fi_loopt_binnenkort_tegen_grens_aan.doc/

[7] European Commission, Information, Society and Media Directorate-General, Electronic Communications Policy *Perspectives on the value of shared spectrum access,* 2012

[8] Agentschap Telecom, *Nationaal frequentieplan 2005* (geconsolideerd 30 november 2012), , 2012

[9] Agentschap Telecom *Brochure vergunningvrije radiotoepassingen*, 2012

[10] DIGITALEUROPE *Position on Licensed Shared Access (LSA),* 2013

[11] EXIDA, *IEC 61508 Overview Report*, 2006. (via TUEindhoven site http://www.win.tue.nl/~mvdbrand/courses/sse/1213/iec61508_overview.pdf)

[12] Clarke, G., Reynders, D. and Wright E., *Modern SCADA Protocols*, Elsevier publishers, 2004.

[13] Stoufer, K., Falco, J., Kent, K., *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, NIST, 2006., (http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf)

[14] Calcagnini, G. O. a.o.: *Electromagnetic compatibility of wlan adapters with life-supporting medical devices*. Health Physics, Volume 100, Issue 5, May 2011, pp 497-
[15] Petersen, S. and Carlsen, S., *WirelessHART vs. ISA100.11a: The Format War Hits the Factory Floor*, IEEE Industrial Electronics Magazine, Vol. 5, No. 4, Dec. 2011, pp. 23-34. (http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6102417&tag=1)
[16] Nixon, M., *A Comparison of WirelessHART™ and ISA100.11a*, Whitepaper, Emerson Process Management, 2012, (http://www.controlglobal.com/assets/12WPpdf/120904-emerson-wirelesshart-isa.pdf) 501.["Interference may occur if WLAN antennas are used at very close distance (<10cm) to the medical device".]
[17] Emerson Engineering Guide, *IEC 62591 WirelessHART® System Engineering Guide*, 2012. (http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/EMR_WirelessHART_SysEngGuide.pdf)
[18] RIVM, *Risks related to the use of eHealth technologies, An exploratory study*, Report 360127001/2012
[19] Judgment Call, *health devices* october 2012, 314-329, www.ecri.org
[20] Agentschap Telecom, *Staat van de Ether 2012*, juni 2013
[21] Hensbroek, R. *TNO-rapport* 2012 R10683 dd. oktober 2012, See: http://resolver.tudelft.nl/uuid:23c42c28-4993-4b15-8e23-bb2d84a0b766
[22] Vitavalley – Actiz, *Vitaal thuis*, 2013.
[23] Mitchell, R. K. , Agle, B. R. , and Wood, D. J. (1997) "Toward a theory of stakeholder identification and salience : Defining the principle of who and what really counts" Academy of management review, pp. 853-886.

Other literature used

[24] Verkenning 2010 Van gezond naar beter, 2010, RIVM, Bilthoven
[25] High Tech Systemen: Short-range Wireless Communications, Innovatie Zuid, Mei 2012
[26] Vergunningsvrije Radiotoepassingen, Agentschap Telecom, Februari 2012
[27] lmproving Home Healthcsre through the Use of Simple' lnteroperable' Wireless Connectivity Solutions, Adams, MSEE, Member IEEE, HIMSS, ATA Freescale Semiconductor, Tijdschrift van het NERG deel 77-nr 2-2012
[28] A framework for performance and data quality assessment of Radio Frequency Identification (RFID) systems in Healthcare settings, Remko van der Togt, Piet. J.M. Bakker, Monique W.M. Jaspers, Journal of Biomedical Informatics, 2011
[29] Altijd en overal online, want zonder wifi geen leven, NRC 22 aug 2013.
[30] Report on the second joint cross border R&TTE Market Surveillance campaign carried out in 2005/06 by European Market Surveillance Authorities, ADCO 25(07)02 final, 2007
[31] Perspectives on the value of shared spectrum access, Simon Forge, Robert Horvitz and Colin Blackman, 2012
[32] Estimating the Utilisation of Key Licence-Exempt Spectrum Bands, MASS, 2009
[33] Report on ASA concept, CEPT WG FM52, FM52(12)INFO4, 2012.
[34] GSMA Policy Position on Licensed Shared Access (LSA) and Authorized Shared Access (ASA), GSM-A, 2013
[35] WGFM QUESTIONNAIRE ON THE CURRENT STATUS OF DFS (DYNAMIC FREQUENCY SELECTION) IN THE 5 GHZ FREQUENCY RANGE, CEPT Working Group FM22, FM22(12)Info04rev1, 2012
[36] Spectrum policy, Analysis of technology trends, future needs and demand for spectrum in line with Art.9 of the RSPP, Analysis Mason, A study prepared for the European Commission DG Communications Networks, Content & Technology, 2012
[37] RAND Europe (Rand Corporatiopn): See: http://www.rand.org/pubs/technical_reports/TR608.html ["Interference remains the single biggest obstacle to RFID roll-out in Healthcare, as there is a direct risk to patien safety". See page xxi of the report],
[38] EMT expert rapport. See: http://medischetechnologie.fhi.nl/images/stories/pdf/vws026-1[1]_3[1].pdf ["Interferentie wordt ca. 20x genoemd als mogelijk risico"]
[39] ECRI Institute: "Getting the message – Results of our survey on Cell phone/Smartphone policies. In magazine: Health Devices April 2013, pp.126-132. [In this publication 1m separation distance is advised + policies on departments where critical equipment and patients are present. Note that US mobile phones transmit at lower power levels than European phones 0,6 W versus 2W)!]
[40] Hensbroek, R. "96 medical apparatuses tested for interference by WLAN/WiFi signals" TNO Report KvLP&Z 2007.117; 17 September 2007; Available on www.tno.nlwww.tno.nl
[41] Togt, R. van der, Bakker, P.J.M. a.o. *A framework for performance and data quality assessment of Radio Frequency Identification (RFID) systems in Healthcare settings*, Journal of Biomedical Informatics, 2011 ["The correct way to implement wireless systems (RFID)"]
[42] Kapa, S. a.o.: Electromagnetic interference of magnetic field based auto identification technologies in Healthcare settings, International Journal of Medical Informatics 80 (4), 2011, pp. 239-250. ["Low frequency, magnetic field based autoidentification technology induced distance dependent EMI in Healthcare settings (…). (…) requires rigorous in vivo testing to ensure the antenna is located a safe distance away"].

[43] Censi, Federica a.o. RFID in Healthcare Environment: Electromagnetic Compatibility - Regulatory Issues, 32nd Annual International Conference of the IEEE EMBS, Buenos Aires, Argentina, August 31 - September 4, 2010.
["The analysis of the regulatory issues (…)is essential to evaluate the possible risks to electromagnetic interference on medical devices."]
[44] Yue Ying, Dirk Fischer, Uvo Hölscher: Electromagnetic Interference with RFID Readers in Hospitals WC 2009, IFMBE Proceedings 25/VII, 2009 pp. 872–875.
["The electromagnetic field generated by the RFID readers may interfere with medicval devices"]
[45] MASS Consultants report for OfCom, " Estimating the Utilisation of Key Licence-Exempt Spectrum Bands", 2009.,
(http://stakeholders.ofcom.org.uk/binaries/research/technology-research/wfiutilisation.pdf)
[46] Golmie, N. and Mouveaux, F., " Interference in the 2.4 GHz ISM Band: Impact on the Bluetooth Access Control Performance|", NIST, International Conference on Communications, 2001.,
(http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=936608&tag=1)
[47] NAMUR report NE133, " Wireless Sensor Networks: Requirements for the Convergence of existing Standards", 2012., (www.namur.de)

-

Appendix A. Questionnaire to Industry.

Geachte heer/mevrouw,

Het Agentschap Telecom is onderdeel van het Ministerie van Economische Zaken en bewaakt de toekenning en het gebruik van etherfrequenties voor, onder andere, computertoepassingen zoals WiFi. De faculteit Economie en Bedrijfskunde van de Rijksuniversiteit Groningen doet samen met TNO in opdracht van het Agentschap onderzoek naar de effecten van verstoringen van die toepassingen als gevolg van congestie (overbelasting) en interferentie (storing).

Belangrijk: dit bericht is bestemd voor iemand in uw bedrijf die inzicht heeft in het gebruik van ICT en communicatie. Wilt u dit bericht aan diegene doorsturen?

In het kader van dat onderzoek vragen wij u vriendelijk onderstaande vragen te beantwoorden en die antwoorden in deze email te retourneren. Invullen kost enkele minuten.

De antwoorden worden geheel anoniem verwerkt. Uw email adres wordt niet aan het antwoord gekoppeld.

De vragen:

1. Is uw bedrijf een industriële onderneming? (ja/nee)

2. Hoeveel personen werken op uw bedrijfsvestiging?

3. Gebruikt u draadloos internet (WiFi) binnen uw bedrijf? (ja/nee)

4. Gebruikt u WiFi of andere draadloze toepassingen in uw productieinstallatie? (ja/nee)

5. Zijn WiFi of andere draadloze toepassingen belangrijk voor de bedrijfsvoering? (essentieel - enigszins - nauwelijks)

6. Als de draadloze verbindingen voor langere tijd uitvallen, zou uw bedrijf dan schade oplopen? (veel - weinig - geen)

7. Welke problemen voorziet u als de draadloze verbindingen uitvallen?

Alvast hartelijk dank! Als u belangstelling hebt kennis te nemen van de resultaten van het onderzoek, kunt u dat hieronder aangeven.

Ik heb wel/geen belangstelling voor de resultaten van het onderzoek.

Prof. dr. ir. Hans Wortmann
Rijksuniversiteit Groningen
Faculteit Economie en Bedrijfskunde
Vakgroep Operations

Appendix B. Interference by Wireless Systems

B1. WiFi Interference

WiFi is originally developed for use in the license-free ISM (Industrial, Scientific and Medical) band at 2.4 GHz, but later also added other frequencies were added (5 GHz, 60 GHz, 5.9 GHz) . Impact on WiFi by other devices operating in the 2.4GHz band can be seen in the rise of the noise. For successful reception of data, receiving device needs to get (from its antenna and later input pre-processing stage) signal which will also contain certain amount of noise. If the Signal-to-Noise Ratio (SNR) comes below a certain threshold, the receiving device is not able to decide a signal, and packet or bits of data are lost. Errors in reception can be handled by error coding or by retransmissions of whole or portions of data. When other (non-802.11) devices are transmitting in the same frequency band, their contribution is seen as the rise in the noise floor, thus decreasing the SNR that is achievable on a particular 802.11 link, resulting in lower data rate. Another problem regarding WiFi is that originally IEEE has defined 11 channels in the ISM band, but only three of them are non-overlapping. In practice, only channels 1,6 and 11 are non-overlapping. Overlap between two channels results in increase of the noise floor in both of them resulting in lowering of the data capacity. Other devices operating in the 2.4GHz band, like wireless point-to-point links for transferring tv signal in home, Bluetooth communication, or 802.15.4 (LR-WPAN) based devices, they all contribute to the rising of the noise floor, which will impact available data rate.

B2. Immunity to proximity fields from 4G/LTE communications equipment

At the moment next to 3G and WiFi equipment 4G products and networks will be commercially available and hence deployed. In a recent report on the EMC standard the following details on test details for a safe use of 4G/LTE equipment is presented, see table below (reduced from Table 9 of IEC 60601-1-2: Medical electrical equipment – Part 1-2: General requirements for basic safety and essential performance – Collateral standard: Electromagnetic disturbances – Requirements and tests).

Note that these are test figures. A guess is that the interference distance for LTE will vary between 0 – 1,5 m (rough calculation). For a sound advice on the performance and risks of 4G/LTE equipment measurements should be done in the real field.

Test frequency (MHz)	Band (MHz)	Service	Modulation	Maximum Power (W)	Distance (m)	IMMUNITY TEST LEVEL (V/m)
710	704 – 787	LTE Band 13, 17	Pulse modulation [b)] 217 Hz	0,2	0,3	9
745						
780						
810	800 – 960	GSM 800/900, TETRA 800, iDEN 820, CDMA 850, LTE Band 5	Pulse modulation [b)] 18 Hz	2	0,3	28
870						
930						
1 720	1 700 – 1 990	GSM 1800; CDMA 1900; GSM 1900; DECT; LTE Band 1, 3, 4, 25; UMTS	Pulse modulation [b)] 217 Hz	2	0,3	28

Appendix C. Suggestions on regulations for wireless technology in hospitals

The suggestions below relate to interference ("EMI") by mobile transmitters (in licensed and license exempt frequency bands) on medical electronic equipment in hospitals. Equipment outside hospitals is not covered by the text below. Since 2011 at RFID and WiFi frequency bands allows more transmitting power than medical equipment can survive. In these bands the so-called license-free application. This implies that up-till these maximum powers these wireless systems are allowed to be sold installed and used without special permits. Details can be found in the brochure "Vergunningsvrije toepassing feb 2012" [7] which summarizes national and European regulatory documents.
Mobile transmitters in hospitals in licensed bands are GSM, UMTS, C-2000 and very soon LTE/4G. The fixed base stations in these systems operate in licensed bands (the handsets are not). Because these systems can cause EMI in medical electronic equipment, especially the new LTE system – the following suggestions are formulated. The Dutch / European regulations with the allowed field strengths in the specified frequency bands can be found in the brochure "Vergunningsvrije toepassing feb 2012" [7].

C1. RFID 125 kHz interferes with medical equipment

- In the Jama publication based on a report by TNO and quoted below EMI was reported by 125 kHz RFID signals of magnetic field strength 95 dBμA/m at 1m.
- Europe allows at 125 kHz up to 126 dBμA/m at 1 m distance. This is 31 dB = Factor 35 X stronger than the interference level published in the Jama at which EMI in medical equipment occurs.
- In the (newest draft of) the EMC standard **[ ]** for EMC of medical equipment no susceptibility requirement is set at 125 kHz. Magnetic fields at this frequency are "under consideration" for many years already.
- ADVICE: Reduce the allowed magnetic field strength in hospitals at 125 kHz and test medical equipment with this field.

Jama / TNO-report:
125 kHz: At the maximum antenna transmission level that could be set (95 dBμA/m at 1m) about 20 per cent of the tested medical apparatuses (8 out of 41) showed interference at 5cm or greater distances. Distances where interference occurred varied from 5cm up 2m.
Jama: http://jama.jamanetwork.com/article.aspx?articleid=182113

C2. RFID 868 MHz interferes with medical equipment

- Published in Jama: Interference by 868 MHz at transmitted power of 0,5W.
- Europe allows for RFID 868 MHz up to 0,5W.
- Europe allows for RFID 867 MHz up to 2 W with certificate.
- Europe plans to allow for 4 W RFID at 915 – 921 MHz.
- These are field strength that can interfere with medical electronic equipment.
- ADVICE: Reduce the levels that are allowed in hospitals and have medical equipment tested with these fields

TNO report:
868MHz: At the lowest power that could be set (0,5 W) about 40 percent of the tested medical apparatuses (15 out of 36) apparatuses tested showed interference at distances of 0cm up to 4m.
At the highest fixed antenna transmission level that could be set (2,4W) more than half of the tested medical apparatuses (26 out of 41) showed interference at 0cm or greater distances. Distances where interference occurred varied from 0cm up 6m.
See Jama: http://jama.jamanetwork.com/article.aspx?articleid=182113

C3. WLAN/WiFi 2,4 GHz interferes with medical electronic equipment; RFID 4 W will interfere as well!

- TNO reports (MKB, AMC, OLVG) prove that interference is acceptable by 2,4 GHz with radiated power of 100 mW at distances 0 – 50 cm from the equipment ,

- Europe allows for RFID 2,4 GHz up to 4 W (and 1 W at 5,6 GHz; some sources mention 2 W at 5,6 GHz?),
- This is 4 / 0,1 = Factor 40 X stronger power (about 6 X bigger amplitude). Medical equipment can be interfered at 0 – 3 m (rough calculation),
- ADVICE 1: Reduce the levels that are allowed in hospitals and have medical equipment tested with these fields
- ADVICE 2: Do not allow battery chargers for e.g. Smartphones with WiFi directly **on** medical electronic equipment (unless proven)

TNO reports (MKB, AMC, and OLVG):
WiFi 2,4GHz (IEEE 802.11 b and g): When continuously transmitting (long packages of information) at 100mW about 10% of the tested medical apparatuses (10 in 96) were disturbed. Distances varied from 0cm to 50cm.
At 5GHz (a: 200mW): comparable results (too little tests).
Report:
www.tno.nl/downloads/TNOKvL_RapportVeiligheidDraadlozeNetwerkeninZiekenhuizen.pdf

C4. Unavoidable interference by GSM900 and GSM1800 and by (new) LTE
GSM900 and GSM1800 can interfere with medical electronic equipment. Also data transmission (GPRS) can interfere. LTE can be expected to interfere as well

- Europe defines LTE800 MHz up to max. transmitted power of 200 mW.
- The interference distance for LTE will vary between 0 – 1,5 m (rough calculation).
- This distance is a risk because LTE is expected to be transmitting permanently (which is not the case with 2G or 3G). Therefore LTE is expected to be a "permanently switched-on source of interference" carried around by their users all around the hospital.
- ADVICE 1: Have interference tests performed to have evidence on the interference distance of LTE to medical electronic equipment. Surprisingly enough nobody published any results.
- ADVICE 2: Do **not withdraw the present restrictions** where mobile phones are forbidden in hospitals because it will be very difficult to re-introduce such restrictions if they might appear to be needed next year.
- ADVICE 3: Have p-GSM tested for interference in medical equipment. Based on the low transmitted power in active time slots (10 mW) it can be expected that little interference will occur (no publications yet).

TNO reports and publications:
- Published in *Critical Care* 2007: A GPRS signal (GSM900: 2W) induced interference in 25 of 61 tested medical apparatuses at distances of 0 – 5m,
- In TNO-rapport: GSM 900 2W induced interference in 101 of 205 tested medical apparatuses at distances 0 – 5m; 3% of the apparatuses tested were interfered at 1,5 m distance.

C5. Unavoidable interference by C2000/TETRA
The C2000 system includes ambulance services as users. The ambulance personnel are not always able to switch off their TETRA portophones when entering the hospital. The portophones interfere with medical equipment (See TNO report). A code of practice has been settled and published. In the news it was announced that hospitals should improve the in-house coverage. This obligation appears not to exist because the C2000 signal strength (reception) is not good in any (relatively big) building.

- ADVICE: Transfer the code of practice for ambulance personnel about using C2000 portophones to police and fire brigade organizations. These two organizations may act or have exercises in hospitals and need to be aware of the medical equipment interference issue as well.

TNO report:
- In TNO-report: TETRA 1W (400MHz) induced interference in 49 of 90 tested medical apparatuses at distances 0 – 8m,
- This distance is a risk, but the effect is known to the ambulance personnel.

New risk when using mobile ICT equipment (Source: EWCRI Institute):

- Medical equipment appears to be unplugged from the electric power supply in favor of electric chargers for mobile devices.
  ADVICE: Place a warning in the instructions for use of the mobile devices.
  Explanation: The instructions for use contain a warning message for interference on medical equipment as well.

C6. Test method Medical Equipment with mobile transmitters
Medical industry formed a consortium within IEC to define a test method to determine the interference probability by mobile transmitters including RFID on medical equipment.
ADVICE: Include ICT industry formally in this initiative.
Explanation: The working group issued a complete proposal but the worldwide medical industry (members of the working group) voted against it. At present for certain mobile transmitters no tests are prescribed and for some others no adequate tests. The 4th edition (draft) of the standard IEC 60601-1-2 now takes the stance that mobile transmitters (handsets) will be used very close to medical equipment. However in the 3rd edition which is actually applicable still the position is that for every type of wireless technology another separation distance can be prescribed to the user. This is impractical for understandable reasons.

C7. Radiation methods
All test standards radiate towards (medical and non-medical) equipment from 4, 5 or 6 directions during immunity testing. TNO from 1985 on has radiated from all directions with as many polarizations as possible. Therefore TNO always found more susceptibility! Several scientific publications reporting that "no interference was found" can be disqualified because of the incomplete way of testing (in the vision of TNO). Another disqualifier is that no or little information is transmitted during interference testing. In some communication systems - for example WiFi – the transmitted power is low – only beacons are transmitted instead of information. TNO always radiates a worse case signal – e.g. with a permanent stream of information - if applicable. ADVICE: Standardize internationally these test methods: Radiating fully around and with 100% of time filled up with information.

C8. The Radio & Telecommunication Terminal Equipment Directive (R&TTE) and the Medical Devices Directive (MDD) refer to each other but the belonging standards are developed in quite isolation.
The well-known role of the R&TTE is the co-existence of telecommunication systems. The role of the MDD to have safe medical equipment and medical devices in general on the market. The EMC standard IEC 60601-1-2 for medical equipment permanently lags the allowed transmitting levels (field strength or power) for wireless systems. The 4th edition (draft 2013) of this standard raises the test levels (most wireless systems ca. 30 V/m; WLAN: ca. 10 V/m), while at the same time Europe plans to allow RFID at 4W (or even 10W?). See [ETSI TR 102 649-2 V1.3.1 (2012-08)]. ADVICE: Submerge standardization groups in cooperation; exchange of information is not enough.

Summary
ADVICE: ETSI standards allow at present and/or in future for such high transmission levels (field strength or power) that certain wireless systems can electromagnetically interfere (EMI) with medical electronic equipment. Have coordination between levels allowed in hospitals with manufacturers of medical equipment.
Explanation: The situation differs per wireless system. ETSI standards were prepared with the main goal to have no interference between different transmitting systems (including classical broadcasting). Possible electromagnetic interference (EMI) on non-communication equipment is not the main issue (this could be called out-band interference or also "EMC").It is supposed generally that the EMC directive will safeguard (via its belonging standards) that non-communication equipment will be enough immune against this EMI. Or that the MDD will guarantee this. It is not always realized that the EMC Directive is overruled by the MDD as far as medical equipment is concerned and that the MDD has not all arrangements in place still.
Note: At the same time it is still debatable how close to medical equipment the transmitters (phones/ ICT/ RFID) need to be operated. Generally the EMI occurs at close distances from the medical equipment. Another fact is that medical technology standards generally develop slower

than telecom standards. The reason is that telecom systems would not operate unless a standard is agreed. Transmitter and receiver would otherwise interfere with other systems or not connect at their frequencies at all. Therefore telecom standards are developed before a telecom system is brought in operation. This is certainly not the case with medical technology systems.