Wireless location tracking
in Industry 4.0

Opportunities

In 2017 Lectra launched several “Industry 4.0” services to their customers, allowing them to react to increasingly quicker requests of new designs[01] or highly customized gear like athletic footwear. The Industry 4.0 (I4.0) term was coined in the recent years (see NFC Tag lower right for details), forecasting a more connected, flexible and transparent production of goods and services using information technology (IT). In I4.0 there are the following opportunities for tracking: First, the resource itself for a production process, allowing middleware to allocate the workpiece, enabling the business to move a workpiece through the manufacturing with individualized work orders, while doing stock-keeping and probably showing the customer where his product is. Secondly, as part of Augmented Reality, which will require accurate tracking of the personal using it, to overlay the reality with enriched content based on the organisations databases[18]. Finally, people working in I4.0 may require location tracking, due to the requested of more flexible working times and changing places[02]. Location tracking of people could be associated with business work flows, allowing the IT systems to track that and for how long a work piece is worked on. In hazardous or risky environments like mines, tracking can avoid accidents[03].

Sensors & Waves

With sensors, there is the measurand (*what*) and the transductor (*how*) allowing data processing[04]. Here, the ultimate measurand is the location of a tracked item, the intermitted measurand in tracking with wireless devices is mostly based on signal strength or an identification number. Base of these technologies is the approach in IT to replace wires[05] and allow wireless data transmissions. Signal distance are bound to the frequency and their typical blockage. Figure F.2a.2 shows the wavelength spectrum and highlights the radio waves. Waves with a higher frequency have a very short-wave length, usually blocked quicker than low frequency and long-wave length[06]. Organisation need to carefully when choosing a technology for location tracking, considering the surrounding factors like building materials or room dimensions.

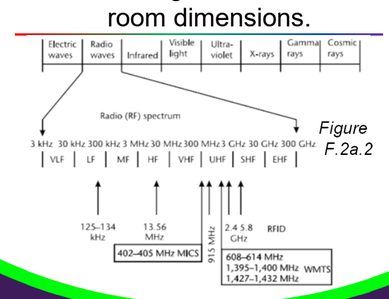

Figure F.2a.2

Wireless technologies

Wireless data transmission techniques allow, to some extent, to be used for location tracking. GPS tracking is not suitable for indoor tracking, given that the client must have a clear line of sight to satellites.

WLAN 802.11

The wireless network that an organisation has put in place for data communication, can be used for location tracking. Memory producer Hynix did so in 2005[08], with the real-time location systems (RTLS), using the 802.11 wireless network for tracking of material and staff. Figure F.2bI.1 shows that RTLS uses the measured distances (di1, di2, di3) to the transmitter, by means like signal strength, to triangulate the location of the target relatively to the three transmitters. RTLS was prepared with the location data of all the transmitters, and the combine outcome is the location of the target. 802.11 operates at 2,4 or 5GHZ, providing ranges of up to 70 meters and 1,3GBit/s.

The **ZigBee** Protocol operates on 2.4 GHz and 868 MHz (Europe) the latter provides good penetration through walls and alike, has lower power consumption and hardware cost is low[05]. Two changes to 802.11: There must be a main transmitter with a connection to a middleware software, called Coordinator. Secondly, other transmitters (called routers) can natively relay data packages, called *peer-to-peer*, they do not need a wired connection, see figure F.2bII.1. These networks are called Wireless Sensor Networks (WSN)[09]. Again, Signal Strength and RTLS is used for location tracking. Another method is *fingerprinting*, which can also be used in 802.11 WLAN[10]. During an offline phase, see figure F.2bII.2, a target-simulator scans and walks through the area of interest and maps reference locations on a grid. On each location, the specific signal strength will be and stored as a *fingerprint* in a large database. In the online phase, targets submit their signal strength and the central system looks the closest value up in its database, and assign it the pre-defined location for this *fingerprint*. Maximal speed is 250kbit/s at an indoor range of 20m.

Near-field communication (NFC) clients are referred to as tags which are very cheap and can store data. The transmitter needs to supply power to the passive tag to exchange information. This data is passed to a middleware, deciding on the next step of the business process. For location tracking, the middleware will have a location per transmitter and know where the item is, based on the received data the middleware can then decide and initiate the next step. NFC is usually on frequency (13,56MHZ), has a low price, no power consumption, and very low distance (10 cm) and billions of tags are applied each year[15].

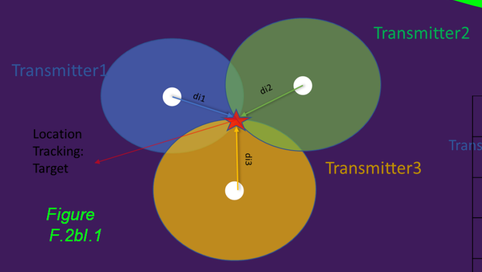

Figure F.2bI.1

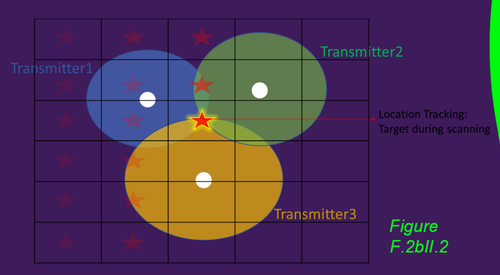

Figure F.2bII.2

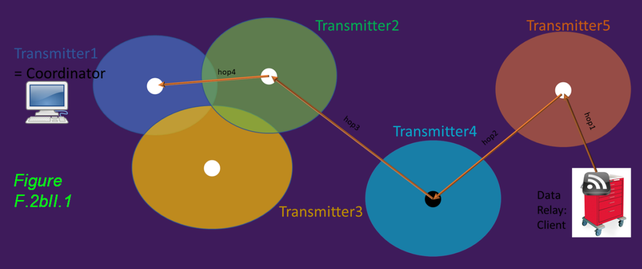

Figure F.2bII.1

Challenges

Main **technical challenges** are interference and obstacles causing radio waves not to be read correctly by the transmitter, induce variances in the signal and calculated location. Good planning of the area that will be used for wireless, for example via a building information model (BIM) can reduce such impairments[11].

Business case and value chain modification: Often organisation’s premises have no full coverage of any wireless network due to costs calculations. Established businesses may not have found the need of using any wireless tracking technology, seeing no reason why to invest[12]. When the business has decided to setup wireless tracking for a process in the value chain, planning (like BIM) will be important, to estimate the transmitter density and the resulting accuracy required for the use case. It could be found that the project would be excessively expensive with no return of invest.

Security: For NFC tags, their serial number is their MAC address, which can only be written with factory equipment, setting a high hurdle for scammers[06]. Wireless communication can be impacted by intentional denial-of-service (DoS) attacks like jamming, undeliberate misuse or overloading by use of others stopping communication. Where an organisation is relying on wireless location tracking, safety measures like physical shielding and contingency plans for a downtime should be put in place and tested regularly[13]. Security of any data must be guaranteed during the three states: while in transit and when stored in the middleware, with access only to authorized personal [06].

Privacy & Law: Loss of trust in data security, like the current Facebook debate[14], is building up resistance to adapt new technology like NFC[15]. Building trust is one of the key points when working with customers, but also with staff. Key words for ethical standards are honesty, predictability, fairness and openness[16]. So when people are tracked, they should be informed about it and allowed to “opt-out” of such tracking to establish a sustainability relationship with either high workforce moral or satisfied customers. As technology has no moral, organisations need to ensure the encoded processes are reflecting the ethical standards of the society the technology will be used in[06]. Organisations must be abided the applicable law: EU does dictate General Data Protection Regulation (GDPR) with a Privacy by Design and Privacy by Default clause, allowing anonymous use of any service, but with the large amount of data that can be tracked back to one person by using a IOT or mobile devices, it is mandatory to rethink how to programme [17].

Conclusion

Existing wireless **data network** covering the organisation’s premises, allow for quick enablement of location tracking. **ZigBee** hardware cost is low[05] if there is no existing network and only low data bandwidth is required. Only routers require power, only coordinators middleware connections, costs for network cable, installation, network hardware can be saved, this allows the network to be installed or moved quickly and with low effort.

Loyalty cards can move their tracking to **NFC**, allowing for further big data processes like data mining as well as saving money on the plastic card, when using the banks NFC chip[15].

Any organisation should consider building **big data use cases**, but needs to ensure **data security and privacy** to maintain trust of customers and staff.

References

01. HARARI, D. (2018). Lectra: Trending in Industry 4.0 with SaaS. New Delhi: Stitch World / Apparel. 02. Hecklau, Galeitzke, Flachs, & Kohl. (2016). Holistic Approach for Human Resource Management in Industry 4.0. 6th CIRP Conference on Learning Factories (pp. 1-6). Berlin: Procedia CIRP. 03. Hedley, M., & Gipps, I. (2013). Accurate wireless tracking for underground mining. IEEE International Conference on Communications 2013: IEEE ICC'13 - Workshop on Advances in Network Localization and, (pp. 42-46). 04. Kalantar-zadeh, K. (2013). Sensors - An Introductory Course. New York: Springer Science+Business Media. 05. Yang, S.-H. (2014). Wireless Sensor Networks, Signals and Communication Technology. London: Springer-Verlag. 06. Lehpamer, H. (2012). RFID Design Principles (second ed.). Norwood: Artech House. 08. PR NEWSWIRE EUROPE. (2005, December 02). Ekahau wireless location tracking improves the semiconductor production process for Hynix. 09. De Sales Bezerra, T. A., De Sousa, J. A., Da Silva Eleuterio, S. S., & Rocha, J. (2015). Accuracy of propagation models to power prediction in WSN ZigBee applied in outdoor environment. 6th Argentine Conference on Embedded Systems (pp. 19-24). CASE. 10. Swangmuang, N., & Krishnamurthy, P. (2008, December). An effective location fingerprint model for wireless indoor localization. Pervasive and Mobile Computing, 4(6), p. 836-850. 11. Park a, J., Chen b, J., & Cho, Y. K. (2017). Self-corrective knowledge-based hybrid tracking system using BIM and. ScienceDirect, Advanced Engineering Informatics 32, 126–138. 12. Lee, J., Bagheri, B., & Jin, C. (2016). Introduction to cyber manufacturing. ScienceDirect, 11-15. 13. Larsen, E., Haubitz, C., Wernz, C., & Ratwani, R. (2016). Improving Electronic Health Record Downtime Contingency Plans with Discrete-Event Simulation. Hawaii International Conference on System Sciences, 49, 3179-3188. 14. Yadav, S. (2018). Facebook data breach: Digital experts analyse the after-effects. Adgully 15. Voges, D. (2017). NFC – Great Innovation Is On The Rise, But The Market Remains Very Fragmented - The Diffusion Of Innovation Using The Example Of Near Field Communication (NFC) Multiapplication Platform. Sweden: Kth Royal Institute Of Technology - School Of Industrial Engineering And Management. 16. Ebert, T. (2009). Trust as the Key to Loyalty in Business-to-Consumer Exchanges: Trust Building Measures in the Banking Industry. Wiesbaden: Gabler. 17. Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer. 18. Pierdicca, R., Frontoni, E., Pollini, R., Trani, M., & Verdini, L. (2017). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 4th International Conference, AVR (pp. 389-401). Ugento: Springer.

Figure F.2a.2 Source: Adapted from Lehpamer, H., RFID design principles (Second ed.), Norwood: Artech House, 2012, figure 2.2, p. 7 ; Figure F.2bI.1, F.2bII.1, *F.*2bII.2 Source: Author (Frederik Unser)