Internet of Things in Surface Mount Technology Electronics Assembly

ANDREAS SYLVAN
English title

Internet of Things in Surface Mount Technology Electronics Assembly

Swedish title

Sakernas Internet inom Ytmontering av Elektronik

Author

Andreas Sylvan, sylvan@kth.se

Submitted for the completion of the KTH program;
Media Technology, Master of Science in Computer Science and Engineering.

Supervisors: Rebekah Cupitt, KTH, School of Computer Science and Communications, Department of Media Technology and Interaction Design.
Tord Karlin, Mycronic AB.

Examiner: Henrik Artman, KTH, School of Computer Science and Communications, Department of Media Technology and Interaction Design.

Date of submission: 2017-06-20
ABSTRACT

Currently manufacturers in the European Surface Mount Technology (SMT) industry see production changeover, machine downtime and process optimization as their biggest challenges. They also see a need for collecting data and sharing information between machines, people and systems involved in the manufacturing process. Internet of Things (IoT) technology provides an opportunity to make this happen. This research project gives answers to the question of what the potentials and challenges of IoT implementation are in European SMT manufacturing. First, key IoT concepts are introduced. Then, through interviews with experts working in SMT manufacturing, the current standpoint of the SMT industry is defined. The study pinpoints obstacles in SMT IoT implementation and proposes a solution. Firstly, local data collection and sharing needs to be achieved through the use of standardized IoT protocols and APIs. Secondly, because SMT manufacturers do not trust that sensitive data will remain secure in the Cloud, a separation of proprietary data and statistical data is needed in order take a step further and collect Big Data in a Cloud service. This will allow for new services to be offered by equipment manufacturers.

SAMMANFATTNING

I dagens ärende upplever tillverkare inom den europeiska ytonteringsindustrin för elektronik produktionsomställningar, nedtid för maskiner och processoptimering som sina största utmaningar. De ser även ett behov av att samla data och dela information mellan maskiner, människor och system som är delaktiga i tillverkningsprocessen.


Studien belyser de hinder som ligger i vägen för implementation och föreslår en lösning. Detta innebär först och främst att datainsamling och delning av data måste uppnås genom användning av standardiserade protokoll för sakernas internet och applikationsprogrammeringsgränsnitt (APIer). På grund av att elektroniktillverkare inte litar på att känslig data förblir säker i molnet måste proprietär data separeras från statistisk data. Detta för att möjliggöra nästa steg som är insamling av så kallad Big Data i en molntjänst. Detta möjliggör i sin tur för tillverkaren av produktionsmaskiner att erbjuda nya tjänster.
**Internet of Things in Surface Mount Technology**  
**Electronics Assembly**

**Andreas Sylvan**  
Royal Institute of Technology  
114 28 Stockholm, Sweden  
sylvan@kth.se  
+46 73 441 73 04

**ABSTRACT**
Currently manufacturers in the European Surface Mount Technology (SMT) industry see production changeover, machine downtime and process optimization as their biggest challenges. They also see a need for collecting data and sharing information between machines, people and systems involved in the manufacturing process. Internet of Things (IoT) technology provides an opportunity to make this happen. This research project gives answers to the question of what the potentials and challenges of IoT implementation are in European SMT manufacturing. First, key IoT concepts are introduced. Then, through interviews with experts working in SMT manufacturing, the current standpoint of the SMT industry is defined. The study pinpoints obstacles in SMT IoT implementation and proposes a solution. Firstly, local data collection and sharing needs to be achieved through the use of standardized IoT protocols and APIs. Secondly, because SMT manufacturers do not trust that sensitive data will remain secure in the Cloud, a separation of proprietary data and statistical data is needed in order take a step further and collect Big Data in a Cloud service. This will allow for new services to be offered by equipment manufacturers.

**Keywords**  
Internet of Things; Cyber Physical Systems; Smart Factory; Operational Technology; Surface Mount Technology.

**1. INTRODUCTION**
IoT technology is used today in home automation, where smart lightbulbs, robot vacuum cleaners and lawnmowers, burglar alarms and power sockets are wirelessly connected to gateways and hubs, for either local control and scheduling or connections to Cloud services. [25, 24, 49, 51]. Application Programming Interfaces (API) allow integration of systems from various vendors in one central automation platform, which can be controlled by an app, a web interface, smart remotes or be voice commanded using smart speakers [4, 24, 41].

IoT is increasingly being implemented for telemetry, remote control and feedback loops, for example by retrofitting environmental sensors in office buildings to control ventilation, heat and light in the commercial sector. [75]. IoT has made it possible for companies to offer their products as-a-service rather than just selling a device. [14, 27]

IoT is not only limited to the private consumer or business markets but is also being discussed in the manufacturing industry. While there are many potential benefits, the industry’s requirements on reliability, safety and security may prove to be major challenges in implementing Industrial IoT.

**2. BACKGROUND**
The German strategic initiative Industrie 4.0, the North American Industrial Internet Consortium (IIC) and the Chinese Internet+ all see a potential in IoT as one factor that can potentially contribute to increased efficiency in industrial manufacturing. [20, 23, 32, 34, 71, 72]. Industrie 4.0 aims at reindustrializing Europe and describes how people, machines, equipment, logistics systems and products communicate and cooperate in a Smart Factory [23, 55]. This is realized by horizontal integration of information flows through IT systems within the supply chain and vertical integration with networked manufacturing systems. [12] This integration is also often referred to as Information Technology (IT) and Operational Technology (OT) convergence. [23, 20]

**2.1 Electronics production**
The focus of this study is on IoT in European Surface Mount Technology (SMT) electronics production. The process of electronics manufacturing involves attaching electronic components such as Integrated Circuits in various package shapes on a bare substrate called Printed Circuit Board (PCB). There are two major methods of assembling electronics. Through-hole technology is a way of mounting components in holes on the PCB. The other method is SMT. SMT is the most suitable method of the two for high speed automated assembly, which today is a prerequisite for profitability in manufacturing. Sometimes a mix of the two technologies has to be used. The populated and finished electronic product is called a Printed Circuit Board Assembly (PCBA). An example of a mixed technology PCBA is the popular Raspberry Pi 3 single-board computer seen in Figure 1, which uses both surface mounted components, commonly referred to as Surface Mount Devices (SMD) and hole mounted connectors. [57]

![Figure 1. The Raspberry Pi 3 single-board computer is one example of a PCBA made in SMT factories.](image-url)

Switching the product being produced in a production line to another often takes a lot of time since it involves material preparation and machine configuration. Machine downtime lowers throughput and decreases efficiency. Process efficiency is
dependent on operator knowledge. For issues like these, the Smart Factory could potentially deliver the following solutions:

- Minimal production changeover time and increased flexibility
- Predictive maintenance and automatic fault detection
- Machine and process optimization
- New business models
- Feedback for development of the next generation production equipment [34, 31]

To succeed in turning the automated SMT factory into a ‘Smart SMT Factory’, adoption of standardised data communication, data collection and IoT technology is needed. With the introduction of IoT and related technology such as Cloud services comes a new demand to develop strategies for IT risk assessments and focus on enforcing IT security. A good start in implementing IoT in SMT is to find and tailor a contextually suitable and secure IoT architecture. [3] These concepts will be described in the next chapter.

3. KEY CONCEPTS

Since the current state of IoT is a multitude of abbreviations and catch-phrases which in many cases are overlapping concepts, these will first be defined with a SMT manufacturing context in mind. Then the IoT technology used to build a Smart Factory will be explained and exemplified for SMT.

3.1 Internet of Things

Ever since Kevin Ashton used the term Internet of Things as the title for a presentation about the usage of Radio Frequency IDentification technology in supply chain management back in 1999, the meaning has evolved. [5] Today, there are many interpretations and descriptions of IoT. [68] Du and Chao describe IoT as a combination of information sensing devices and the Internet, forming a network facilitating identification, management and providing services to people everywhere. They also state that "The most important part in the network of things is the interconnection and interoperability between the machines, which is often called M2M [Machine-to-Machine].” [19]

The International Organization for Standardization (ISO) defines IoT as “An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.” [29] This definition by ISO will be the guiding definition for this work, but a few more example definitions will be described for reference. Cisco uses the term Internet of Everything, claiming that IoT is a networked connection of physical things and that IoT adds people, data and process on top of that. [16, 44] However the ISO and Cisco terms can be said to describe the same thing. The Industrial Internet Consortium uses the term Industrial IoT (IIoT) to define "systems that connects and integrates industrial control systems with enterprise systems, business processes, and analytics.” [40]

IIoT is a contextual definition of IoT used in the industrial realm and it resembles the definition of Industrie 4.0. [31] In this paper the term IoT will be used, since the industrial context has already been established.

In an attempt to demystify IoT, Voas works with the presumption that “it’s fundamentally about communication, computation, sensing, and actuation”. He also states that “things do not need to be connected directly to the public Internet, but they must be connectable via a network”, and proposes the term Network of Things (NoT), in order to distinguish between things only connected in a Local Area Network (LAN), and IoT’s “things” which normally are tethered to the Internet. [68] While the introduction of yet another IoT related term was meant to clarify, it may add to the confusion. An alternative is to simply accept that IoT, despite having Internet in its name, does not have to involve an Internet connection, which fits with the definition from ISO as well. IoT things could be both very simple or complex objects. These are described in the next section.

3.1.1 Things and SMT Operational Technology

According to the Institute of Electrical and Electronics Engineers (IEEE), a thing in IoT denotes the same concept as a physical entity. [26] Alternative terms used are device, node or terminal. In the context of SMT electronics assembly, a thing can be a barcode reader in the production line, an eLabel or much more complex production systems and machines, generally referred to as Operational Technology (OT). Such OT may be a SMT Pick and Place (PnP) robot or a solder paste Jet Printer (JP) as shown in Figure 2. These mechatronic systems are in themselves NoT, containing many embedded systems such as sensor and motor controllers communicating over for example a Controller Area Network (CAN) data bus. With that said, a SMT IoT thing may be a complete machine.

![Figure 2. SMT production line with JP, PnP and SMD component storage. Courtesy of Mycronic AB](image-url)

3.1.2 Cloud and Edge computing

A key technology of IoT today is Cloud Computing. It eradicates the hassle of operating server hardware in a private physical data center while providing auto scaling of virtual servers and convenient services on top of a virtual infrastructure. [10] In IoT, the Cloud acts as a hub between geographically connected things and can provide asset management, scalable data storage, analytics, rule engines and other computational resources.

In IoT applications which require low latency, produce large amounts of data or contain sensitive information, sending data to the Cloud may not be a viable option. In those cases, Edge Computing at the edge of the LAN can provide local or near-local data processing, caching, device management, information protection and reduction of traffic to the Cloud. [10, 64] The terms Fog and Edge are often used interchangeably. Dastjerdi and Buyya describe how Fog computing seamlessly integrates Edge devices and Cloud resources, providing Cloud-like services at the network’s edge. [17]

3.1.3 Protocols and standardization

Meddeb has made a survey of standardization activities which shows that several organizations including ISO and IEEE are actively working on IoT definitions, architectures, and security aspects. [45] During design, the technology used in each layer in the communication stack will depend on the specific IoT
application domain and thing types. [18, 21, 56]. By, using a reference models like the IoT Architecture Reference Model (IoT-ARM) which defines a specific set of technologies to use, a general consensus may be achieved where several standards can coexist. [21]. As an example, the IoT-ARM communication stack suggest a number of suitable protocols for wireless IoT. (see Figure 5).

Figure 5. IoT-ARM Communication Stack [21]

Among the IoT standards available, there are a couple in the Application layer (see Figure 5) which are widely used in IoT and may be of interest for a SMT IoT solution. [35] The lightweight publish/subscribe Message Queuing Telemetry Transport (MQTT) protocol is ISO certified and commonly used for IoT telemetry [52]. MQTT is mediated through a broker, so there is no direct connection between the things publishing or subscribing to messages. MQTT in itself is not encrypted but can be using Transport Layer Security (TLS). [1] Encryption is important in order to avoid security issues such as eavesdropping.

Another widely used application layer protocol for constrained IoT devices is the Constrained Application Protocol (CoAP). CoAP is a client-server REpresentational State Transfer (REST) protocol. It has the same request/response verbs as the Hypertext Transfer Protocol (HTTP) for fetching, creating, updating and deleting resources. In the transport layer CoAP uses User Datagram Protocol (UDP), which is optimized for streaming data and Datagram TLS (DTLS) to make it secure. [1, 65] The data payload is typically sent as JavaScript Object Notation (JSON), which has supplanted eXtensible Markup Language (XML) as the data format of choice for the web. One reason JSON is favoured in IoT communication is its small size when serialized, which reduces power consumption. [42] However, some argue that JSON should be replaced with even more lightweight binary formats. [13]

3.1.4 Architectures

Due to the tremendous number of different communications standards available for IoT, ISO sees the need for a generic reference architecture to use when implementing IoT. [29] However, a single IoT reference architecture suitable for every application is not achievable due to domain specific requirements. There are several reference architectures available. Two of them are the Internet of Things - Architecture (IOT-A) and the Industrial Internet of Things Reference Architecture (IIRA). [20, 73] In 2012 the European IOT-A introduced references for building compliant IoT-architectures. It focuses on high level views and perspectives that are of interest of IoT stakeholders, for example compliance with standards and best practices, however it does not provide any concrete reference implementations. [9] The IIC presents an IIRA reference implementation which may be suitable for connecting stationary SMT machines (Figure 3).

Figure 3. Gateway-Mediated Edge Connectivity and Management Pattern [40]

It uses an Edge gateway to mediate communication between the factory LAN with the outside world Wide Area Network (WAN). This allows for protocol bridging and local data processing such as aggregation and analytics, without compromising sensitive data by sending it outside the LAN. The Edge gateway acts as the single point of entry so the nodes are not directly accessible from the WAN. [10, 20, 40]

IoT applications are essentially about data being collected, transported, stored, processed and made available. [18] For a complete IoT application stack from thing to Cloud, Ara et al. present what they call a novel secure service provisioning framework. [3] It is similar to the four-layer architectures presented by Rad et al. and Dorsemained et al. [18, 59] These architectures specify how data is collected in a perceptual layer, which is where things and sensors reside. Then how data is transported over the network layer, typically the Internet, and collected in the platform layer. The platform layer is typically a Cloud platform or backend, providing publish/subscribe messaging, database storage, computation and security and policy management. The fourth and final layer is the application layer. An example application is a graphical user interface which presents data from the platform layer to the users, who may be production managers or OT service engineers. Figure 4 shows the layers of the 4-layer architecture.

Figure 4. 4-layer architecture
3.2 Cyber Physical System (CPS)

“Cyber physical system” is a term coined by Dr. Helen Gill. [31] In previous research IoT and CPS is sometimes used interchangeably. [26] But Lee defines CPS as “integrations of computation and physical processes” with feedback loops between physical and computational processes. [38] So CPS can rather be considered to be an entity enabled by IoT, connecting things and services, thus gaining its computational “intelligence”. [26, 31] In addition to the physical thing level, the CPS entity incorporates a “cyber level” which holds a “cyber twin”. This cyber twin is a representation of each thing or CPS generated by collected machine data. [39] This fusion of the physical and the virtual world through CPS is a key concept in the Smart Factory. [34] In practical applications today, the cyber level typically resides in a Cloud or Fog computing platform. On the cyber level the cyber twin can be stored, compared or otherwise processed and combined with other information. Figure 6 illustrates a connected SMT assembly line which forms a CPS.

In the large commercial IoT Cloud platforms today, the current state of the cyber twin for a connected thing goes under various names such as “thing shadow”, “device state” and “device twin”. These documents are normally stored in JSON format. [6, 22, 48].

![CPS Diagram]

Figure 6. Physical SMT OT assets in an assembly line, their cyber-twins and computational services forming CPS

3.3 The Smart SMT Factory

In SMT production today, OT is most commonly placed in-line with high assembly throughput. Miniaturization of electronics has led to an increasing need of closed loop feedback between solder paste application equipment such as screen printers, jet printers or dispensers, and solder paste inspection machines to make sure that accuracy of the solder paste print on top of the landing pads of the PCB is maintained. If the data from each machine involved in the manufacturing process could be collected and tracked, it would be possible to investigate fault development over the whole process chain. Evaluating this data could lead to a predictive manufacturing process. [33] Once CPS has been implemented, the machines will be able to share data in the platform layer. [39]

3.3.1 Big Data and data analytics

Large volumes of relevant data are commonly referred to as Big data. It is defined by being of high volume, high-velocity and can be of any data type such as text, audio or video. [60] Wang et al. writes: "For big data to come true, [the] Smart Factory should be constructed in a data centric way". They argue that in order for different information systems to operate on the same data object sets, a unified data model including vocabulary, syntax and semantics needs to be defined. [70] At the moment, the challenge for the realization of the Smart SMT Factory lies in the standardised and secure retrieval and storage of the Big Data from OT on the shop floor into either local or Cloud databases. [34, 60] But once that can be solved, the collected and analyzed data can pave the way for several new benefits.

3.3.2 Potential SMT use cases

An obvious example usage of the collected data is to evaluate and improve new generations of SMT equipment. [67] Today it is common to perform maintenance on SMT OT at constant intervals. This maintenance occasionally includes age-based part replacement, so called preventive maintenance. This reduces the risk of unplanned failure of the OT, but may not be carried out at the optimal service interval. [36] According to Gilchrist, predictive maintenance is commonly the first IoT opportunity industrial companies see because it gives the quickest results and return on investment. [20] By constantly monitoring the health of machines and aggregating and combining Big Data from several systems of the same type, the resulting CPS can by itself determine if it is in need of service. This can be signalled to the operator with instructions on how to perform the maintenance, or be offered by the OEM as a remote monitoring service. [60]

Jeschke et al. point out how important the aggregation and evaluation of Big Data is for self-diagnosis and self-optimization in CPS. Relying on human expertise alone will not suffice. [31] One example of optimization enabled by IoT comes from the avionics industry. Peter Chapman at Rolls-Royce, the aircraft engine manufacturer, said in an interview 2016 that they have a heritage of predictive maintenance. Now they want to use the public Cloud to aggregate data from different sources in order to provide new services to their customers such as fuel efficiency and aircraft availability. [14] An additional maintenance aid for CPS is Augmented Reality (AR) which can be used to project metrics and instructions on top of real-world objects. [60]

Today, PCBs are often uniquely identified using barcode labels which are read with OT vision system cameras. An alternative, but more expensive, way of tracking products is to use RFID chips mounted on the PCB [43] or possibly even ink-jet printing passive chipless RFID tags. [63, 31] The possibility of tracking each individual PCB along the assembly line is crucial for this concept of smart products. Smart products have unique IDs, can be located at all times and know their current and target process states. The smart product will allow for individualized production steps. [23, 34]

3.4 IT Security

Safety and security are both equally important in smart manufacturing systems. The production facilities or products should not a pose danger to people or the environment. The data in in both facilities and products have to be protected against unauthorized access. [34] Ara et al. identified a number of potential threats to each layer of CPS Cloud Computing Systems. [3] A sample of their findings is presented in Table 1. These threats need to be considered when designing an IoT architecture.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application / Frontend</td>
<td>DDoS, injection, session hijacking</td>
</tr>
<tr>
<td>Cloud / Backend</td>
<td>Data breach or loss, account hijacking, service abuse</td>
</tr>
<tr>
<td>Network / Internet</td>
<td>Eavesdropping, data modification, identity spoofing</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Thing / IoT Gateway</td>
<td>Physical device destruction, manipulation or malfunction</td>
</tr>
</tbody>
</table>

3.5 Related work
In a recent study made by MPI for Rockwell Automation, 350 U.S. industrial manufacturers were asked about their readiness for IoT in their processes and products. The report showed that only 12% had a strategy for IoT, and similarly, only 12% of the OT was capable of M2M. The study also revealed that the manufacturers don’t know what they should be doing to implement IoT and that there is a lack of example implementations. [11]

Tang et al. gives an example implementation of CPS using the term Cloud Robotics. [66] They describe a system architecture where robots of various models and makes are connected to a common Cloud infrastructure. By aggregating information from robots in the Cloud database, the robots can cooperate and share information. CPU intensive data processing can also be performed in the cloud to offload each robot, which may be limited in computing power. Tang et al. also point out that data formats greatly differ between vendors. In order for the interaction between the robots and the Cloud platform to work, the data format needs to be converted into a unified format which can be handled and stored in the Cloud service. [66]

3.6 Research question
Given the key concepts for IoT and the theoretical use cases in SMT leads to the question: What are the potentials and challenges of IoT implementation in European SMT manufacturing?

4. METHOD
To understand the European SMT industry's perception of the concepts presented in the studied literature, eight semi-structured on-site interviews were carried out. [8] The interviewees professions ranged from CEOs and production managers to engineers. All had good knowledge of their PCBA process and OT. As a base for the interview guide, published white papers, corporate reports and research articles were used to formulate a comprehensive list of potentials and challenges of IoT. The open-ended questions were predefined in the interview guide, which was tested and refined twice before the interviews were conducted. The interviews were divided over Germany, The Netherlands and Sweden. In three cases, the interview was also followed by a tour of the shop-floor and in depth presentation of the SMT process. Practically all of the participating companies were contract manufacturers dealing with confidential production data, making products for aerospace, space, automotive, medical and military customers.

4.1 Method criticism
Possible drawbacks of semi-structured interviews include the risk of asking leading questions and the risk of improper construing. Face to face interviews on site allowed for exploration around the predefined questions, a good contact with the person and the possibility for guided tours of the shop floors. But the interviews were carried out mostly at factories who used SMT PnP and JP machines from the same vendor. The interviewees who had OT equipment from other vendors were interviewed at an exhibition, thusly, their production process could not be studied in the same detail as with the other interviewees. There were indications from some of those interviews that other OT vendors indeed offered OT which both can communicate with each other and to remote web-based services. A greater number of interviews would have increased the statistical significance of the results. Further, It was not possible to achieve a gender equal interview base. In fact, all of the interviewees were male.

4.2 Network diagrams
This usage of pictures in interviews is called photo elicitation. [62] In this study, two diagrams (Figures 6 and 7) were used during the interviews to stimulate the interviewee to collaborate, describe their current situation and share thoughts around the scenarios being presented. [37] The first one of a isolated PCBA production network was created based on information from informal interviews and SMT equipment manuals (see Figure 7). The interviewees were encouraged to participate and sketch on the diagram, an example is seen in Figure 9.

![Figure 7. Isolated PCBA production network](image)

The diagram in Figure 8 was made to visualize a suggested gateway mediated IoT-network. Using this, topics on IoT, Cloud and data sharing were illustrated and discussed.

![Figure 8. Cloud Connected Smart Factory](image)

4.3 Analysis
The qualitative data has been analysed using thematic analysis using notes and transcripts to understand how people who are running SMT production perceive topics relevant to IoT in their environment. Themes were discovered by arranging and grouping answers into tables, including comments which were not direct answers to the questions in the interview template. [50] Small amounts of quantitative data was obtained from the qualitative data by keyword frequency counting and presented in bar graphs. [74, 47] This quantitative data is by no means of any statistical significance, due to the small sample size, but it offers some guidance for the discussion.

4.4 Ethics
Each interviewee was promised that they and their company would be kept anonymous in the report. Thus, each interview is referenced to as I1-I8.
5. RESULTS

The following themes derived from the interviews are presented: IT and IoT implementations; Networked communication; Data and SMT process.

5.1 IT and IoT implementations

The interviews were initiated with questions about what IoT was, and the following answer summed it up pretty well:

*Ask ten people and get ten different answers.* (I2)

Indeed, none of the answers were exactly the same. I5 defined IoT as:

> IoT devices and apps send information over the Internet. (I5)

I8 thought of IoT as:

> Different connected devices which are easy to hack. (I8)

The definitions may differ, but most seemed to agree that it had something to do with the exchange of information. But a majority of the interviewed people said their companies had not implemented any IoT or Industrie 4.0 recommendations. When asked why, I4, which represented a small company doing short PCBA batches for medical, industrial, space, avionics and defence customers, commented that they didn’t have enough resources to implement it. There was however an interest in making use of data from the OT, for example I3 described how there was lots of data to be collected and evaluated. He expressed that while they really wanted to get hold of the data, it was not without effort:

> We must get all this data. There is a problem with old machines. Must get time to summarize this data, but it is important. (I3)

5.1.1 IT systems

The companies of all interviewees except for I8 had internal IT departments and five out of eight said that their IT and OT people work close together. I6 and I7 were very familiar with the concepts and ideas of Industrie 4.0. Their focus was on their own in-house developed IT systems, for instance I6 had developed their own backend for aggregating data from Manufacturing Execution Systems (MES), Operational Technology (OT) and Enterprise Resource Planning Systems (ERP). This backend was also pushing data one way to a web frontend (see Figure 9).

![Figure 9. Sketch made by interviewee](image)

I7’s company had developed their own local dashboard which combined information from several OT systems. One feature was that the operators had to state reasons of stoppages and slow performance in this interface. I2 said that they had implemented connected machines, M2M, MES and customer driven traceability, but the discussion did not go into further detail. I7 said they were dependent on machine vendors who were not interested in making communication between different brands work:

> If machines are not talking to each other, there will never be a complete line. The system should tell the operator what to do. [The] complete line should be like one machine.” (I7)

5.2 Networked communication

A majority, 6 out of 8, of the interviewee’s companies had their OT connected in local factory Ethernet (IEEE 802.3) networks but most of them had restricted or no Internet access (see Figure 10). I2’s company had a unique network setup compared to the other interviewed companies, it was not separated from the office network and it was interconnected through encrypted Virtual Private Network-tunnels to several other factory networks across continents to synchronize databases and for collaborative work.

![Figure 10. Factory network configurations](image)

5.2.1 IT Security and Cloud

Interestingly enough, as we see in Figure 10, six out of eight said that they could open the firewall to temporarily allow remote access to computers in their factory LAN. This was mostly used in troubleshooting by service engineers. The connection was generally made with a third party software like Teamviewer, with one exception in I2 whose supplier of OT had their own online service for this. On the topic of IT security issues, I1, I3, I4 and I8 were all concerned about industrial espionage and sabotage. I3 said:

> Someone could get our proprietary data, [Bill of material] BOM files contain part prices. It is bad if competitors get this. We could lose our customers. (I3)

I2 and I6 were worried about technical issues with networking and IT while I3 mentioned power cuts. I5 said that a virus could shut down production. He also mentioned that people could pose risks too and gave examples of how the Stuxnet worm was deployed in an isolated network in Iran by people using thumb drives. [61] I8 was also of the opinion that employees could do harm to the business by disclosing sensitive information, for example by taking photos with their smartphones, or causing problems through human error.

On the topic of IT security concerns and Cloud, I1 though that Cloud was too fragile and he had heard of many attacks. According to I5, It’s a security question. One can’t guarantee that there is no breach. Besides, the Cloud demands internet access. And what about backup, how fast can it be up
again if it fails. I2 was also unsure if it was secure. I7 was concerned with being dependent on vendors:

> If everything is connected to [the] outside, we become dependent on the [machine] vendor. (I7)

While another was suspicious and wanted to wait and see, but also gave a hint on how to nicely package the service:

> I want to hear from enough people that Cloud services are stable. Authorities will want to have keys and backdoors to Cloud services. Your cloud service is in a place we can not control. ... Maybe if [the OT vendor] brings me the hardware with a red little ribbon... (I8)

I3 agreed with the rest of the interviewees:

> Too early for us, thinking of our IT security. (I3)

Although I7 though nothing is safe, perhaps sending certain data to Cloud could be possible:

> Nothing is safe. But if only PnP data, why not. Not customer PCB data. (I7)

Another great insight was that if data is centralized, it would provide a tempting opportunity for hackers:

> Allowing access outside world equals risk of hacking. ... If [the OT manufacturer’s] Cloud is hacked, it is more important than each customer, since it would be a collection of data from all customers. (I6)

It is clear from all answers that the concept of Cloud, or any type of Internet connectivity, is associated with risks and not particularly with benefits.

### 5.2.2 Protocols and APIs

Protocols and APIs were not specifically predefined as questions in the interview guide but rather emerged from some discussions. I6 wanted to “log all errors with IoT” and addressed the need for a standardised protocol, mentioning the Open Manufacturing Language (OML) and how OT suppliers focus on enabling communication only between their own products. He also pointed out the need for APIs from the machine vendors. I7 said it was a big issue with protocol standardization and that customers want it, but machine vendors do not. I7 and also mentioned that all machine vendors make their own protocols and that there is a need for APIs. I8 agreed to this in saying:

> Standard protocols sound like a prerequisite. (I8)

### 5.3 Data

The interviewees were asked about willingness to share certain types of data from the OT with the OT manufacturer (see Figure 11).

![Figure 11. Which type of data would you share?](image)

I3 gave a clear picture of their view on OT data. His company wanted to store data locally, but they were also willing to share data with the OT manufacturer. He pointed out that it depends on IT and perhaps also on customer specific data, and referred to Non-disclosure agreements (NDA) they had with their customers. I6 also said they could not share data due to NDAs but that they were collecting data locally. I3 saw a use for the data:

> We need data from the factory to optimize. (I3)

I4 also indicated that it was depending on customer data:

> Yes, we would like to, but customers would say no. (I4)

#### 5.3.1 Data types

The five data types in Figure 11, were analysed to see how likely it was that they would be shared, also referred to as shareability. Based on this the data types were further sorted into the following three categories.

##### 5.3.1.1 Statistical data

The answers indicate that statistics and errors from OT sub-systems are most likely shareable:

> It would make sense to give this feedback to the manufacturer. (I2)

Like I2, almost all people interviewed were ready to share this with the supplier, something they actually already did by manually sending log files to the supplier for troubleshooting when needed. I3 had a comment on that:

> but [The OT manufacturer] service can’t really look at the problem in real time." (I3)

This was also considered to be data that could help the supplier develop a better system and help its customers with better support as I8 pointed out:

> Yes, we like [the OT manufacturer], it could lead to product development. (I8)

Even I1, who at first answered that they were not willing to share any data, said that statistical data was the most feasible type of data to share. This was remarkable because this answer was given in the context of sending data to a Cloud service operated by the supplier.

##### 5.3.1.2 General production data

Template and utilization data is potentially shareable in some cases. It describes the shapes of the parts, tools and movement speeds used in the product and statistics about utilization and idle time for each machine. Four out of eight interviewees said they would share template data with the supplier. An important note here is that certain machines like PnP machines come with a default package database which is then over time altered by each user in order to optimize the machine performance. I3 said:

> It would be helpful to share package data. A database for tested and approved packages. (I3)

A further note is that I6 and I7 said that they were actually sharing this type of data with each other already.

##### 5.3.1.3 Sensitive production data

Certain types of data may be very sensitive and needs to be protected. Such data is the production data which originates from original Computer Aided Design drawings of the electronics, and has been converted with a Computer Aided Manufacturing software to suit the format of each machine type. Production data contains product and part names and coordinates. The data usually comes from the SMT manufacturers customer and is sometimes referred to as customer data. None of the interviewees would share this type of data, due to the previously mentioned NDAs with their customers and the concerns described in the next section.
5.4 Expert views on the SMT process

Key issues in SMT production could be sorted into three major issue topics: downtime, optimization and changeover. Figure 12 visualizes in how many interviews each topic was brought up.

![Mentioned SMT process issues](image)

**Figure 12. Mentions of important SMT process issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime</td>
<td>This means unplanned OT downtime, and not getting service on time. This was the most mentioned issue.</td>
</tr>
<tr>
<td>Changeover</td>
<td>This includes lead time from customer order to finished product, planning, data conversion, the time it takes to move component parts from storage to the production line and the complete process of preparing the SMT OT in the line for producing a product batch.</td>
</tr>
<tr>
<td>Optimization</td>
<td>This can mean Overall Equipment Efficiency, Machine speed/performance and overall line speed. Process -knowledge and -transfer.</td>
</tr>
</tbody>
</table>

5.4.1 Downtime

I2 mentioned that they use Total Productive Maintenance (TPM) from the Lean Production concept. TPM strives for no equipment breakdowns, no stops, slowdowns or defects. [69] I5 indicated that downtime was sometimes an issue:

*The biggest issue is to get service on time when something breaks* (I5)

I7 had a similar though and elaborated:

*A maintenance engineer is usually expensive and he's probably not available, so how do I set our internal production engineers, solving ... problems of a machine?* (I7)

He also pointed out that there are already an equipment manufacturer who provide Augmented Reality service solutions for the purpose of aiding in troubleshooting OT. [54]

5.4.2 Changeover

I4 stated that unplanned jobs from customers and short lead times were their key issues. I3 went into detail on how changeovers were their foremost key issue. They had one week to manufacture and produce a batch of PCBAs and at the same time having 4-5 changeovers per day, per machine:

*Time to get components from the stock to the machines takes too long.* (I3)

I6 said that the changeover time, which currently was about one hour, could be 15 minutes. Here it is important to understand that he preparation of a PnP machine is particularly time consuming. It includes loading several different types of component reels in magazines and trays, loading production data, testing and trimming the machine. This normally needs to be done every time a new product is being produced. I7 said that pre-production time is too long and brought up how we before the industrial revolution always had a batch size of one, since everything was hand made:

*Batch size one, every item is unique, every item is customized.* (I7)

The story was that craftsmen would produce one product at a time on demand. But with the industrial revolution and mass production, the option of customization became limited, and he illustrated this by quoting Henry Ford, "Choose any color so long as it is black."

I7 went on to describe:

*But now you see the tendency to get back to batch size one again. Everyone wants to be unique* (I7)

And the term “automated craftsmanship” emerged from the discussion. The bottom line here was that their customers now demanded very small batch sizes but still wanted to pay the same as for large batch sizes:

*We've got customers who want only one board, but he wants the price for a hundred* (I7).

I7 saw the changeover time as an unwanted cost and asked:

*How do I get the changeover as short as possible, instead of hours, how do I get it in minutes?* (I7)

I7 then emphasised that changeover time must go towards zero.

I8 simply pointed out flexibility as their biggest issue, since they had a large amount of different jobs to run running on four lines.

5.4.3 Optimization

I2 said they were implementing Overall Equipment Effectiveness (OEE). The OEE metric is a measurement of the truly productive time of planned production. [69] I6 expressed how they want to record what operators are doing, because they all have their own shapes for components. He wanted to know why the operators adjust the data. He also said that:

*Engineering needs to know which component packages speed up mounting* (I6)

I6 meant that it would be nice if the OT supplier had access to every customer's production database in order to give advice on improvements, and that they wanted to work more predictively, that all decisions in the line should be digitized and that big data collection was important. Further, they wanted to know why parts of the process go right or wrong sometimes and be able to spread that knowledge among the operators. I7 explained that:

*Now there is one operator per machine in the factory. In Industrie 4.0, operators go around loading several machines.* (I7)

meaning that the efficiency of operators could be substantially increased leading to fewer operators per production line. On production planning optimization, I7 brought up a use case for CPS in a visualized virtual factory:

*How do I make a virtual twin of my factory? ... How do I get a completely digitalized factory that I can play forward for instance? I want to make sure that a product is producible, I can physically do it in the virtual factory to show what the production bottlenecks are, show what the problems are going to be, does it fit?*. (I7)

All of these perspectives on the three SMT process issues are important in order to understand how IoT can be introduced as a solution.
6. DISCUSSION
We are seeing how IoT is already being actively implemented in consumer and commercial applications. At the same time, Industrial IoT in European SMT manufacturing is still mostly in the concept stage. As stated, this study has explored previous work to see the industrial implementation potentials of IoT, and interviews were conducted to investigate the electronics industry’s view upon the suggested implementations. SMT manufacturers have three major concerns in their production process: machine downtime; job changeover time and machine and process optimization. These can all be seen as opportunities for implementing IoT. Further, IoT is a prerequisite for creating CPS which are in turn the building blocks of the Smart Factory. [38, 31, 26, 34]

6.1 Communication standards
Currently, the lack of standards for communication between machines of different brands acts as a blocker for IoT. The interview results made it clear that the SMT manufacturers wish for standardised M2M and IoT communication and APIs for easy integration with MES and other IT systems. This section is a discussion on how IoT standards can apply to SMT OT.

Wireless technologies are commonly seen as enablers of IoT. [68, 1, 15, 26] IoT things in commercial and consumer applications often are small, battery powered and in many cases mobile. Also, many IoT gateways are connected over telecom networks where data rates may be expensive. Such conditions demand the use of wireless technology while sending data with sparse intervals to both save battery and money. The prerequisites for IoT in a SMT factory are different from most consumer and commercial applications. The SMT machines are stationary and have a steady supply of power. As we saw from the interview results, wired 802.3 Ethernet is already an established standard in SMT factories, so it would make sense to use this in the physical and data link layers for SMT IoT implementations. 802.11 wireless LAN or 802.15.4 Low-Rate Wireless Personal Area Network could of course be used in an SMT IoT architecture, however this would be a potential security risk since anyone with access to the signal can attempt to capture and compromise data. [2] While Ethernet is available on most SMT assembly machines, this is normally not used for M2M. One reason is that despite the fact that Ethernet is widely available In SMT manufacturing, there is currently a lack of M2M communication protocol standards. This results in machines of different make not being able to communicate with each other. One exception is the widely implemented Institute of Printed Circuits Surface Mount Equipment Manufacturers Association (IPC SMEMA) standard. [28] It has been in effect for over 20 years and provides a minimalistic electrical interface with one single purpose; to communicate if a machine is ready to send or receive a PCB along the production line.

In 2017, a new open SMT M2M protocol called Hermes was revealed, backed up by several manufacturers of SMT equipment. [15] It is TCP/IP and XML based and aims to replace the very limited IPC SMEMA. The idea is to let all machines, regardless of make, communicate more detailed information about each PCB being transported along the line to keep track of each individual product. The Hermes standard has a potential of realizing parts of the smart product concept where a PCB only needs to be located once in the production line. [23, 34] Hermes is however not designed to be a complete IoT protocol and only communicates between adjacent machines in the line.

In another attempt to standardise the SMT PCB assembly process, OML has been proposed. [46, 53] OML is meant to solve the practical realization challenges of the Industry 4.0 and the Smart Factory, as well as enable automated collection of traceability data. It defines sending JSON messages over TCP. The OML design suggests adapter components called OML Producers which will connect to OT on the factory shop floor such as PhP, JP, inspection equipment and reflow ovens and translate their respective protocol into OML. OML Consumers such as user interface applications will then use the standardised data format. While OML looks like it has been designed with IoT in mind. For instance, IoT data payload is commonly in JSON format, just like in OML. This makes OML a candidate messaging language to achieve a standardised SMT IoT solution. However, so far there is an absence of concrete implementation examples and a lack of interest from OT manufacturers. At the same time as the SMT industry is busy inventing its own domain specific standards, IoT standardization is moving forward. [56, 45] In the application layer, there are a few major application protocols which would be suitable for SMT IoT such as MQTT and CoAP. These should be considered and evaluated to ensure future compatibility between things.

6.2 SMT IoT potentials
An emerging pattern in consumer IoT and home automation is that even though every vendor has their own wireless technology and gateway, the gateway often provides an API which enables integration of several brands in one home automation platform. This pattern would be applicable to SMT IoT as well while waiting for the final universal standard which may never come anyway. For example, a local Edge server for OT brand can be responsible for collecting, storing and processing data from all machines of the same brand and provide this data to other systems in the factory LAN through a HTTP REST API, CoAP or MQTT broker.

6.2.1 IT and OT convergence
Local data sharing is demanded by many SMT manufacturers and is the first step which needs to be taken on the path to Smart Factories. It enables cooperation between OT, IT production systems and people involved in the production process. Earlier we saw how the convergence between IT and OT is critical in the realization of the Smart Factory of Industry 4.0. The IoT enabled CPS integrated in manufacturing operations enables the context-aware Smart Factory which can assist people and machines in the production process. [23] Therefore it was positive to learn that seven out of eight interviewee’s companies had internal IT departments and that five out of eight said that their IT and OT people work close together. It is clear from the result that SMT manufacturers want to make use of all data possible from their machines to improve the production process, make predictions and trace errors. The sketch in Figure 9 shows how one of these SMT manufacturers, despite the lack of easy to use APIs, already have begun aggregating data from their OT using an in-house designed backend which aggregates data from databases of each production system and presents some of this data in a web-service available to their customers. This is however a rare case where the company has had enough IT competence to be able to design and implement such a solution.

The issue with changeover is mostly caused by the time it takes for human operators to prepare and load the machines in
the production line, and there is a heavy focus today to solve this issue. There are for instance already several IT systems developed by OT manufacturers in place which aim to guide and assist the operators to perform this procedure in a more efficient manner. And while it is mostly a matter of operator training and more efficient and automated storage solutions, better communication between machines and humans on the shop floor can aid in this process as well. For instance, if there is an issue in any machine along the production line, the responsible operator should be able to see this immediately wherever he or she stands. The system should also give clear instructions on how to solve the issue, or in best case solve it automatically by itself. From the interviews we got examples of how virtual twins of CPS could be used to simulate the production ahead in order to plan the next job. While there already exists production software which simulates assembly time for the next job to run based on models of the machines, it is not based on data from the whole production line. A CPS simulation system would also benefit from IoT related technologies such as machine learning.

6.2 Cloud and Big Data
The next step in creating a complete Smart Factory is to collect and aggregate Big Data from several SMT production facilities in an IoT Cloud platform. This has potential of enabling great benefits for both OT users and manufacturers. From previous work we saw some example industrial usages of IoT, such as predictive maintenance and optimization. [20, 60, 31, 14] Cloud connected SMT machines will allow the OT manufacturer to monitor machine performance and health, combine Big Data from several machines, and analyze this data to predict failure and suggest optimized settings.

The issues of machine downtime and optimization have a good potential of being addressed with this kind of Cloud IoT solution. When the OT manufacturer’s service, test and R&D departments can be in constant contact with the machines they have produced and installed on customer sites, the whole game is changed. Engineers will be able to compare the state of sub-systems from several machines running production in the field and be able to find weaknesses in system design and to provide corrective action at an early stage. It will enable new services like predictive maintenance, secure automatic updates and remote monitoring, allowing for less unplanned downtime, quicker solutions to technical issues, and less travel for service engineers, which in turn may reduce carbon dioxide emission. [36, 60, 20]

But the Cloud will also enable new business models such as Machine-as-a-Service (MaaS). [27, 14] Further, it can open up for system software features management, or Software as a Service, with easy purchase, evaluation or rental of software-features in the OT.

6.3 SMT IoT challenges
A prerequisite for the Cloud connected Smart SMT Factory is of course an Internet connection. And while most SMT factories have internal networks and can temporarily open firewalls for external access through the Internet, the default mode is an isolated production network. The outcome of the study indicates that the European SMT industry is not preparing for the connected Smart Factory, similarly to what Rockwell and MPI saw in their survey in the US. [11] SMT manufacturers are not only unwilling to connect their manufacturing networks to the Internet, they are also sceptical about Cloud storage. The main reason to that is that they see more risks with it than benefits.

6.3.1 Mistrust in Cloud security
We can see from the interviews that industrial espionage is of great concern for the SMT industry. If competitors get hold of sensitive information many things would be on stake for the SMT manufacturer. It could mean loss of profit due to competitors offering lower prices on the same product and losing customers and damaged reputation due to violation of NDAs.

The current method of protection against threats such as industrial espionage and sabotage is the isolated production, protecting it from hacking attempts. But as a couple of the interviewees pointed out, threats can still find their way into an isolated network as people working in the factory could always pose a potential risk in several ways. The most common risk perhaps being to err and cause data loss and production stoppages, or in worse cases even to steal proprietary data or sabotage the production. But an even greater mistrust was found in using a Cloud service for storing and processing sensitive information and a sense of losing control. Many were for instance sure that government agencies would be interested in getting hold of their sensitive information and demand backdoors to the Cloud service for this purpose. Others pointed out how collecting data from several production sites in one central place would make it ideal for hacker attacks. This scepticism is somewhat justified by reports of recent cyber attacks such as Cloud Hopper against managed service providers. [58] The report shows that industrial espionage, where sensitive data from sectors including industrial manufacturing is the target, is a real and ongoing challenge.

Taking a look at Table 2, we can see that data breach or loss are possible security threats in the Cloud layer. Any system which is somehow accessible from the Internet always faces these potential risks. However, Cloud services normally utilize encryption and authentication with TLS for both data transfer and resource management. This is considered to be very secure. Wang et al. points out: “We cannot place too much emphasis on security aspects. Without security, we dare not bring our smart factories into service. … Encryption and authorization are generally used in cyber security domain, which will be still useful in smart factory or Industrie 4.0 applications; but these mechanisms are not enough.” [71] Even though data is securely transferred, a human error could for instance cause a serious data leak or security breach. Therefore proper training, routine and best practice for developers and operations personnel is key to a secure IoT Cloud solution.

The whole concept of IoT has also gotten a bit of a bad reputation from several IoT related security incidents. This was reflected in one answer which stated that IoT is: Different connected devices which are easy to hack. (I8) Chris Jaikaran, Analyst in Cybersecurity wrote an article on the Mirai botnet. The Mirai malware targets very poorly secured IoT things such as routers and cameras, infect them with itself and use them to launch Distributed Denial of Service Attacks. One example was the DDoS against security journalist Brian Krebs's blog. [30] While it is difficult to prevent a DDoS attack against a front end in the application layer, it can be handled. And a well designed IoT architecture which does not directly make things reachable from the Internet will not allow hackers to take over machinery or get hold of sensitive information in the factory LAN.

6.4 Potential SMT IoT solution
The study found that SMT manufacturers are very willing to share data with the OT manufacturer in order to get something back and
to help improve the equipment design. The unwillingness to allow the data to be sent over the Internet can at first be seen a major blocker. But instead, it may be a sound starting point for a secure Cloud connected SMT IoT architecture. As we could see from the results, data can be divided into categories. With this categorization in mind, it is possible to separate sensitive business information from very useful but rather harmless statistical data from OT. This is a step towards a secure SMT IoT solution. Sensitive production data today already resides in a dedicated database server located in the production network, whereas statistical data is normally logged in each machine.

As the collection of SMT OT statistics is a base in the formation of SMT CPS, the previously discussed Edge server providing an API for collected statistical data will be a key node in a SMT IoT architecture. As a second step towards the connected Smart SMT Factory, the Edge server API can interface an IoT gateway, combing the data separating Edge server with the gateway mediated Edge [61] pattern. The gateway will enable IoT telemetry and CPS asset management in an IoT Cloud platform, and is the only contact point towards the Cloud. Depending on chosen protocol, the gateway may also have to act as a protocol gateway, translating messages between the thing layer and the Cloud layer. [1] The gateway synchronizes the thing states with a cloud IoT platform. It also handles the certificates provisioned from the IoT cloud platform used for data encryption and authentication of things [7]. Streaming telemetry from the SMT network to the IoT cloud will be most common but communication can occur bi-directional. Here it is important to restrict what types of commands can be sent from the cloud to the SMT network. For instance it should be possible to notify the production network of available software updates and request file uploads of log files to secure and verified locations in the IoT cloud service. It will not be possible to control OT or retrieve production data. The collected statistical data will be rather harmless in the worst case of a security breach in the IoT Cloud service and the OT manufacturer will have no access to their customers networks where the sensitive production data is stored. The initiative for SMT IoT needs to come from the OT manufacturers, since only they can provide additional OT software features such as IoT protocols, and the fact that not every SMT manufacturer has the resources to develop their own software.

6.5 Future work

A SMT IoT architecture needs to be practically developed and evaluated. Further investigation and determination of the most suitable communications protocol should be carried out. The idea of data separation can be evaluated in a similar study. This will involve prototyping and testing of local data collection and sharing between OT and Edge server, IoT gateway and Cloud service. Data security and integrity of the SMT IoT architecture also has to be evaluated and penetration tested. Figure 14 illustrates a possible SMT IoT architectural pattern which can be used as a starting point in the evaluation. The SMT IoT architectural pattern introduces some new hardware in the form of the Edge server and IoT gateway, but also requires new software features to be developed for the existing OT systems.

7. CONCLUSION

IoT is about collecting and sharing information between machines, systems and people. CPS are entities formed using IoT and constitute important building blocks of the Smart Factory concept. IoT implementation in SMT manufacturing is possible but needs to happen in stages, beginning with local data collection and sharing. This is because SMT manufacturers see more risks than benefits of connecting their equipment over the Internet to the Cloud. At the same time, they want to collect and process data from their OT, and share data locally to aid in solving their process issues. This can be achieved by collecting statistical data from the OT in an Edge server which provides access to the same data through an API, allowing for better collaboration between machines, people and IT-services in the SMT production process. Further, this work shows that by separating sensitive proprietary data, which is kept safe in the isolated production network, from useful statistical data which can be streamed to the Cloud, a gateway-mediated Cloud connected SMT IoT architecture becomes possible. The Cloud and Big Data opens up for new services in SMT manufacturing such as predictive maintenance, machine and process optimization and MaaS. But using a Cloud service also adds new IT challenges such as the need for new developer skill sets and an addition of security threats which the SMT industry may not be willing or ready to tackle.

8. REFERENCES


Brecher, C. 2012. Integrative Production Technology for High-Wage Countries. SpringerLink. 1,33-34.


Jianqiu, Z. and Mengke, Y. Internet Plus and Networks Convergence. 42,48.


9. APPENDIX

Appendix 1 - Interview guide questions

1. What do you know about Industrie 4.0 and Industrial Internet of Things?
   a. Have you implemented any such thing?
      i. Why/why not?

2. Sketch 1 Are your production machines connected to a network?
   a. Does the factory network have internet access?
      i. Does any equipment communicate with an external service?
      ii. Can service engineers access your machines remotely?
         1. How? Good?
         2. Would you like them to?
      iii. Why/not?

3. What are your key issues in the SMT manufacturing process?

4. Sketch 2 If there was a cloud service which would help you reduce downtime and optimize your machines and fix other key issues as well, Would you be willing to send/share data to the machine manufacturer to get these benefits?
   a. Examples:
      i. Statistics from sub systems, such as motor frictions, current consumption and sensor values?
      ii. Error statistics, such as pick-, vision- and mount/dispense errors?
      iii. Template data, such as package data, fiducial and other geometrical data
      iv. Idle/utilization data
      v. Layout data, anonymous

5. Would you be willing to anonymously share some data with the machine manufacturer and perhaps competitors if they too shared similar data?
   a. Examples:
      i. Package data
      ii. Shape data
      iii. Utilization/optimization statistics so you can compare with each other

6. Your view on storage of your data in a cloud service?

7. Your greatest concerns regarding IT-security in your production environment?
   a. Consequences?
   b. Could you grade it, Severity (1-4), probability (1-4)

8. Does your IT work close with your SMT production?
   a. Do you have a method of risk assessment for your IT and software in production? (FMEA, ITIL)
   b. In house IT or external?

9. General thoughts and comments