

# Security in Precision Agriculture

*Vulnerabilities and risks of agricultural systems*

Marc Window

**Information Security, master's level (120 credits)**  
**2019**

Luleå University of Technology  
Department of Computer Science, Electrical and Space Engineering

## Table of Contents

Acknowledgements .....	3
Introduction .....	4
Motivation .....	4
Research field .....	5
Related work.....	6
Research gap.....	7
Research questions .....	7
Limitations.....	7
Literature Review .....	9
Overview of topic and objectives of the literary review .....	9
Adoption of Precision Architecture.....	10
Cybersecurity related risks in Precision Agriculture.....	11
Data Privacy .....	13
Aerial Drones.....	15
Tractors.....	16
Wireless Sensors.....	17
Literature Review Conclusion.....	18
Research approach.....	19
Background and outline.....	19
Research approach - overview.....	20
Discarded research approaches.....	22
The research process in more detail .....	23
Data Collection methods .....	23
Interviews – Semi-structured interviews .....	23
Survey.....	24
Data Analysis methods .....	25
Validity, reliability and generalisability .....	26
Empirical data collection and analysis .....	28
Results and Analysis .....	38
Discussion and Conclusions.....	40
Appendix A .....	46
Interview Guide .....	46
Appendix B .....	48

Survey questions.....	48
<b>Format 1</b> .....	49
<b>Format 2</b> .....	52
Appendix C .....	54
Initial research plan .....	54
Bibliography .....	55

## Acknowledgements

I would just like to extend my thanks to all participants in this research for allowing me to take up their time and ask sometimes seemingly pointless questions, and especially Professor John Lindström for guiding my thesis

Furthermore I would also like to thank all my fellow students (especially those in our Facebook messenger group) who may or may not have made it to the end of this course but have been invaluable in offering their support throughout it; and also all of the teaching staff at LTU for their patience with us as we tried to learn. The tutors were always happy to reply with patience and sound information to queries at any time, and for this I am extremely grateful.

# Introduction

## Motivation

The motivation for this research comes from the desire to determine if the area of PA (part of National Critical infrastructure) is protected in the same way that other industrial Critical Infrastructure components are. This information is also of relevance to all of the participatory agents in the field, they need to be aware that there is a potential risk to their products or usage, their data and finances.

The research aims to make clear if the area of agricultural use of IoT, industrial sensors and adapted technologies mean that agriculture is vulnerable to risks not normally associated with the use of this technology, or are the risks very similar to those of industry in general. Much research has been done into industrial risk, and also into the use of this technology in agriculture but there is limited specific agricultural risk research. As this is an evolving area of technology, many of its implementations use equipment adapted from other fields of technology, this introduces risks from many different sources. There has been some research on the topic of cyber-attacks in agriculture, but this has looked at the problem purely from a conventional attack perspective and diagnosed via network traffic. It has ignored other vulnerabilities which may not always be detected in this way, such as occurred with the Stuxnet attacks where the attack vector was via a non-industrial access agent (Nourian and Madnick, 2018).

Furthermore PA can generate large volumes of data. Who would own the valuable data obtained from the crop mapping, or nutrient usage or crop yields? Would the large volumes of data be viewed as personal data and so subject to GDPR, or other regulations (Kritikos, 2017) and vulnerabilities (Chi et al., 2017)? As mentioned earlier many of the risks from data confidentiality, also apply to the ownership and usage of this data. These are all areas of risk which have not yet been investigated fully but on which this research hopes to throw a spotlight.

There is a lot of new work appearing on this subject all the time as it is a new field, during the course of the research some new papers and discussions have been published As more research is done on PA and more areas are impacted by it, so the scope of the vulnerabilities and risks associated with it also grow. The potential for exploitation is high as this appears to be an area in which security is not a major factor in development, except in certain areas. The areas of tractor connectivity have some degree of security due to the implementation of ISOBUS; this is an ISO protocol developed from the SAE J1939 protocol – this was a standard for vehicle communication and as such had already been exposed to security breaches (Burakova et al., 2016; Murvay and Groza, 2018).

Many of the risks associated with PA come about because it is such a broad area of industry. It uses many of the technologies of other industries but potentially without adequate cybersecurity measures being taken to secure these technologies and the associated IOT connections. Farming as an industry is changing so radically, as it moves from labour intensive non-technical to low labour, technologically skilled workforces. Furthermore the introduction of technology means that previously unavailable information, facilities and resources can now be utilized. This brings many new areas of risk and vulnerability which

will need to be researched to find their weaknesses and methods of protecting them. The danger is that the discovery of these may often occur after they have been exploited, but that is common to all protection.

Areas that previously would have had no impact on agriculture are now major elements, for example Heating, Ventilation and Air Conditioning (HVAC) were not part of agriculture previously; but now livestock and plants are raised in controlled environments where such systems are critical; grain is also stored in silos in which temperature is monitored and ventilation applied but which is monitored and can be over-ridden from Internet controls. Also technological knowledge is becoming as important as mechanical knowledge for participants in agriculture, the danger being that the limited knowledge of many subjects may mean that participants do not have the detailed knowledge to see risks.

The purpose of this thesis is to increase the awareness and spectrum of this problem. The concept of PA is more than just GPS monitoring on a tractor, or sensors detecting temperature in a greenhouse. It covers arable farming, livestock farming, fruit and vegetable production and even fish production. Such a broad range of environments would create a problem for just one item of technology to be specialised to work in all environments; however this is the introduction of new technologies from existing industries, as well as the creation of specialisms which previously did not exist. Such a large field cannot be comprehensively covered in this proposal, but areas of interest and concern can be demonstrated so that further more specialised research may be done in the areas of concern.

The importance of disruption to PA could potentially be as severe, if not worse, than disruption of other parts of the Critical Infrastructure of a nation in ways not previously considered (Niglia, 2016). In the event of warfare the disruption of PA could have the same potential damage as ancient warfare methods of “Slash and Burn”, leaving a populace unable to feed itself and its economy in disarray.

The objective of this thesis is to highlight the vulnerabilities and risks which can occur from the use of technologies from other areas of industry in PA, and the associated risks accruing from them.

### Research field

Some areas where PA can be vulnerable or at risk, as it becomes increasingly connected to the Internet and other devices, are:

1. Data confidentiality – health (animal and plant), yield figures, or cost of production are examples where security of the data is critical (in all areas of transmission, processing, storage and when required secure deletion). Another area is access to drone mapping, which could give a foreign power important agri-data on the state of food production, or locations of critical infrastructure. The sale of data to competitors would also have a grave effect on the agricultural economy. Data confidentiality is required in all of these cases and is dependent on security being implemented in all aspects (software, hardware, data collection, communication, systems access); the ramifications of loss of data confidentiality could lead to financial, physical or criminal losses.
2. Integrity – introducing rogue data or falsifying data in systems to cause damage such as withholding feed or water to livestock, or over applying fertilisers is an area of

risk. Another associated problem is inadequate AI systems with poor reliability or failsafes implemented, these can lead to reduced or stopped production, or even harvest failure in the extreme. The integrity of the devices employed is also critical as overseas suppliers may incorporate backdoors for foreign agent to access the equipment being utilised.

3. Availability – John Deere refusing access to their code is one example. Deliberate sabotage of a critical system to prevent its use at a critical time (e.g. disabling a combine harvester at harvest time) is another potential area of vulnerability and risk. Critical feed-in systems are also vulnerable such as GPS, fuel supply, comms network access, data storage, blocking physical storage (disabling electronic doors etc.). Badly integrated comms systems (GPS, WEP, 4G, 5G, Bluetooth, proprietary and WiFi) / software introduce risk that there will be incompatibilities and poor or no communication between devices and systems. The corruption of autonomous vehicles is a development from the denial of use of a machine, this can be done via a number of systems leading to it either performing incorrectly or not at all.
4. Other risks can be seen as the use of mobile phones in underdeveloped countries to buy and sell goods direct to market. These are very dependent on a reliable communication network, if this is removed then the economy could collapse in these regions.

Many projects press ahead with the increased use of technology, but omit to include security in their models. A research paper on strawberry production talks about the use of sensors and Farm as a Service (FaaS), AI usage and the IoT, but does not include any reference to the security of the system or the potential threats and risks (Kim et al., 2018). Even articles that include risks frequently see these as accidental, and not as potential attack surfaces for deliberate disruption (Walter et al., 2017).

All of these risks are in addition to the standard IT risks from vectors such as Spearfishing, corrupted USB drives, user error, malware (e.g. Viruses, Trojans, Worms, or Spyware) and social engineering.

### Related work

There has been only a limited amount of work dealing specifically with security in PA, this is beginning to change as more people become aware of the cybersecurity risks presented in PA (Chi et al., 2017; Federal Bureau of Investigation, Cyber Division, 2016; Sweeney et al., 2016). The USA has begun to realise the potential to exploit PA in various ways, this may be as a nation state attacking, or as organised crime disabling devices and extorting money to enable them, large companies controlling the working of the products they produce (Deere and Company, 2015). Capgemini Consulting in the Netherlands (Capgemini Consulting and Wageninngen UR, 2016) have published a document outlining some of the dangers of unsecured data in agriculture. They mention that data exchange is increasing due to technology, traceability, sustainability information requirements, furthermore they state that farmer's data may be the next revenue source alongside agricultural production. An article by West (West, 2018) looks at the vulnerability to cyberattacks of PA technologies using IoT sensors in Australia, but the principles are applicable globally. The EU has not made so prominent a factor, cybersecurity in PA, but in a paper on Bio and Agroterrorism (Mårtensson et al., 2013) the potential danger was acknowledged (though Bio terrorism was the main focus). The dangers of ignoring potential cybersecurity risks in agriculture were highlighted also in the International Food and Business Review (Geil et al., 2018) where the

problems of a lack of responsiveness to questions on security based questioning was also noted. Their research was primarily focused on the PC based use of technology and AV protection however.

There has also been some recognition of the dangers of reusing existing technologies and some research has been done into securing sensors further by employing additional layers of security (Chae and Cho, 2018). However this is hampered, as stated in this research by Dr. Alan Millard of Plymouth University, by the abilities, performance and requirements of the sensors. It may not be possible to add extra security except at the design stage.

### Research gap

The research gap in cybersecurity in PA is quite large, there appears to be little consideration given to the dangers which can be encountered by the extensive use of technology. The IoT sensors employed, the wireless communications, the data exchanges, the data security and usage, the UAVs, the self-steering vehicles, GPS and RTK are all items which have been subject to investigation and research in isolation or in other industries. However in PA the meeting of these technologies and the further problems created by the slow, sporadic or non-existent communication in additional areas can potentially increase the risks. These may be further increased by the isolated working conditions of many agricultural practices, a lack of interaction and idea exchanges may potentially lead to even greater risk in PA.

The existing research on the technologies has been mainly in the areas of IoT sensors for temperature and humidity, but there needs to be a focus on other areas as well such as the control of implements and devices attached to tractors, UAVs used in remote regions and their security (physical and logical), the use of the collected data as a method to influence and control markets, the awareness and education of participants in PA of the cybersecurity risks which these technological advances bring with them. Education of users is a large area to be addressed, as is the education of manufacturers and developers of the need to consider cybersecurity at a very early stage. This should be at a level greater than purely meeting current legal requirements.

### Research questions

The primary research questions that the research addresses are:

- 1) Does the re-use of technology from other industries create additional security risks in Precision Agriculture?
- 2) As agriculture moves from a labour intensive, low technology industry to a highly technological and complex industry, what new risks are evolving?
- 3) Is the drive for greater use of technology putting agriculture at greater risk than before?

### Limitations

The limitation on the research in this paper have come from both within and external to the research. The time constraints on the research, as well as the timing have meant that it has been difficult to find and read relevant documents, prepare research questions, gain sufficient interviews and information, analyse and collate the results and then draw a conclusion.

Access to research documents has also been a problem, the ongoing dispute with Elsevier has made it difficult to access a number of current papers that would have been potentially beneficial. This has been compounded by my inability to access a number of books that I



wished to use. This has been due to my location outside of Sweden, which has meant I cannot access e-books through the library nor can I borrow physical copies as I am outside of the Swedish national borders.

Other factors external to the project have also limited its effectiveness. These have been in getting responses, finding companies, and the nature of the research. As with any research which involves contact with multiple entities, there has been a limited response; this may be due to the work schedules of the companies involved, their lack of desire to aid in the projects research aims, lack of understanding of the requested data or simply that the research does not touch on areas in which they are involved. It has also been time consuming going through lists of agricultural companies and developers trying to ascertain their involvement in PA and their application to it. Many prospective companies were not actively using PA technology, or were only at a theoretical stage of development; whilst other potential contacts had not got any application of technology in their business.

The other major limiting factor in obtaining responses was the subject matter of the research. Many companies did not wish to respond about the security they employed, their attitude to security and how they envisaged the future of PA cybersecurity. This may have been for a number of reasons such as:

- 1) The researcher was unverified and therefore was a potential security risk in themselves (revealing data could have been revealing it to a hacker, competitor, criminal or other malicious agent)
- 2) It may have revealed potential weaknesses in the product and thus allowed a competitive advantage to a competitor.
- 3) The companies did not want to reveal their attitude to security (none, lax, moderate or strict) and their implementation of it.
- 4) They had not considered cybersecurity in their products, and did not want this known.
- 5) Their products could not support any level of cybersecurity additional to that provided by the products they utilised in its development.

Other limitations may have occurred in the methods of primary data collection as the optimal methods may not have been employed due to inexperience in these practices. This would be addressed in any further research conducted in the light of the current research methods employed. The limited sample size has also been a limiting factor in obtaining strongly representative data, as has the paucity of available literature on the specific subject of cybersecurity in PA; however the common responses across the research suggest that the conclusions are correct.

## Literature Review

### Overview of topic and objectives of the literary review

The current developments in agriculture are to a large extent driven by technology from the Internet Of Things and Cloud computing, these demonstrate themselves to the farmer as Precision Agriculture and Smart Farming. There is a degree of dispute as to the meanings of them, generally they are accepted as being:

Precision farming: “*Precision agriculture (PA) or precision farming, is a modern farming management concept using digital techniques to monitor and optimise agricultural production processes.*” (Publications Office of the European Union, 2018a). Precision farming uses data about a specific location and crop collected by sensors on machinery and the farm. These, combined with controlled application methods, are utilised so as to optimise the production processes (drilling, weeding, fertilising, irrigating and harvesting) and the crop’s growth conditions. This will then reduce costs, soil and environmental damage and improve resource utilisation.

Smart farming: “*Smart farming (also known as Farming 4.0 and digital farming) is the application of information and data technologies for optimising complex farming systems.*”(Giesler, 2019). The mix of digital agricultural sensor and control technologies blended with current data technology, allows agricultural practices to be refined to individual fields and even specific plants or animals. This use of intelligent networks and data management tools to create decision making, is based upon the data collected and implemented in PA.

As technology has encroached onto farms, so differing equipment formats has been used. The European Agricultural Machinery Association (CEMA) goes into detail explaining the lack of standardisation and the need for connectivity of objects, as well as the need for data volumes to be manageable. All of this is stressed to aid the farmer in maintaining control of his data and machinery, for maximum resource and cost benefit (CEMA - European Agricultural Machinery, 2017). What is not mentioned is the need to secure all of these connections and data from being intercepted and corrupted or reused for illegal purposes, even the 2018 EU paper “*Precision Agriculture and the future of farming in Europe*”(Publications Office of the European Union, 2018a) does not mention the need for security although it suggests promoting PA.

The aim of this review is to look at the current state of PA and some of the associated publications, and from this to draw a view on how well, if at all, cybersecurity is implemented.

### Adoption of Precision Architecture

Studies have shown that the adoption of PA is influenced by the size of the farm, financial resources and availability of equipment. Education and awareness are also major factors in the adoption of PA, as is the need for PA to make an activity cheaper and more efficient. (Pierpaoli et al., 2013). This however is often not a good match for security, unless the users of the technology have the need for security explained and the measures needed to implement it, then it will not be implemented.

In a presentation in 2012, Robert Mueller famously said:

*” I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”* (Mueller, 2012)

This very succinctly sums up the situation facing companies involved in PA., that they must take cybersecurity and related risks seriously. It affects the mechanical and digital aspects of PA equally, security breaches can occur in any area that an agent feels that they can exploit. Some of these vulnerabilities are similar to those found in industrial applications of technology (use of data security, drones, sensors and controls), but others are more specialised such as autonomous vehicles and RFID tags involved in agricultural procedures. Agricultural businesses are vulnerable to the usual cyberattacks of malware, spearfishing, technology corruption, data breaches for economic manipulation or theft of intellectual property, as well as being a potential focus of activist groups (animal rights, anti-GMO), and state actors wishing to cause serious economic or political disruption. They must take measures to reduce their vulnerabilities and attack surfaces, and protect against financial and legal penalties incurred as a result of these attacks (Sweeney et al., 2016). However many of these businesses do not see their use of technology as being a danger to their businesses, they are focussed on the potential benefits.

The problem of farmers and those in the industry having formal training and an inclination to learn new skills is a large hurdle to overcome. In the UK, only 27% of farmers have received formal training in agriculture and 59% of farmers are over 55 years old. This makes the likelihood of formal training in PA and its risks is unlikely to succeed, a better method would be to utilise existing farming networks and groups to inform them of new developments and approaches (Norris, 2015). Another critical driver for PA is the spread of high speed broadband into the rural community, a connection of 2 Mbps is not sufficient for downloading and uploading the volumes of data that are generated by PA and this is the norm for 60% of UK farmers, a further 13% suffer unreliability in addition to slow speeds(Norris, 2015) .

The financial benefits from adopting PA have the potential to be huge, the benefits globally could be:

<b>Precision Farming Technology Acceptance Models and potential value added</b>			
<b>Technology</b>	<b>TAM</b>	<b>Potential value added</b>	<b>Yield improvement</b>
Precision Fertiliser	\$65 billion	\$200 billion	18%
Precision planting	\$45 billion	\$145 billion	13%
Compaction reduction by using smaller tractors	\$45 billion	\$145 billion	13%
Precision spraying	\$15 billion	\$50 billion	4%
Precision irrigation	\$35 billion	\$115 billion	10%
Field monitoring, data management and other	\$35 billion	\$125 billion	

*Figure1 Table of PA potential value added*

These figures from a presentation by Goldman Sachs (Jerry Revich, et al., 2016) show the great value attached to PA, this reward is also viewed as potential revenue by organised crime and a great opportunity for disruption of an economy by state actors.

### Cybersecurity related risks in Precision Agriculture

Precision agriculture aims to reduce costs, labour and risk in producing better crops with increased yield, however there is a counter side to this with the growth in risk of cybersecurity.

The American Federal Bureau of Investigation (FBI) have issued a guide which warns of the dangers associated with the increasing use of technology in Smart Agriculture (Federal Bureau of Investigation, Cyber Division, 2016); whilst in the realm of precision agriculture the Department of Homeland Security has produced a document (Mutschler and Department of Homeland Security, 2018) which broadly details areas of risk and the dangers, with examples of hypothetical scenarios. This shows the seriousness of the risk as perceived by US government agencies. This document gives a very coherent introduction to the risks to PA., but due to its broad focus it gives little detail. It is however one of the best documents I have so far encountered for giving an introduction to the technology and the risks associated with it. The paper also includes a breakdown of the groups who are likely to be affected by PA., and so are at risk in the event of an attack. In order to demonstrate the differing types of threat, the paper gives a number of hypothetical scenarios which help to show the potential dangers of an attack on the physical and digital elements of PA.

Europe however does not appear to have a similar concern readily visible; in its paper “European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy” although many industries are mentioned as being at risk and in need of support and monitoring to ensure cybersecurity, the whole field of agriculture was missing from the report (Publications Office of the European Union, 2018b). Even the EU publication entitled “Study on risk management in EU agriculture” (Publications Office of the European Union, 2018c) does not mention PA and cybersecurity, this would appear to be a serious oversight as the effect on EU agriculture could be severe if a deliberate attack was made on PA systems.

The ISO standard ISO11783, Parts 10 & 11 (International Standard, 2015, 2011) defines how the connections are made between a tractor and machinery in agriculture, yet it makes no reference to cybersecurity and related risks. This is a critical connection between vital pieces of machinery involved in PA, yet there is no mention of requirements for physical or software security. This however is being addressed by a development of the Isobus by the Agricultural Industry Electronics Foundation (AEF) with the development of Tractor Implement Management system (TIM) which will allow bi-directional control between the tractors and the implements attached. The safety aspects of connecting devices from differing manufactures meant that a secure standard was required, this is achieved by the use of digital certificates and the exchange of a secure key. This builds on the John Deere / Pottinger version ( Tractor Implement Automation) to enable general connectivity to authorised devices (“Tractor Implement Automation and its application to a tractor-loader wagon combination,” n.d.). This however is only a small element of the issue, PA is more than just the connection between tractor and implements.

A 2013 article (Grgic et al., 2013) which does acknowledge the need for security in PA is on the subject of network connectivity using IPv6. This standard benefits from being a highly developed standard which can support large number of users; this paper looks at its use, analyses the issues and proposes a valid encryption model. The authors look at various encryption models with their pros and cons., and how they could be integrated. However researchers realise demands of such a system (power, adapting manufacturer standards) but maintain that this option is a good way of securing data collection, aggregation and routing to the base station. This paper is now 6 years old and developments in other areas such as Bluetooth and Zigbee have covered many of these issues though, it is however a very good examination of the problem faced with data collection from sensors and clear method to perform it. A paper published in 2014 (Shiravale and Bhagat, 2014) goes over the same ideas but offers no new information and just reiterates in a more general way the findings of the previous paper (Grgic et al., 2013).

Zigbee itself is not secure though, as when a new standard appears it becomes the target of persons desiring to break it. Zigbee is a low power standard for communication between IoT devices created with security in mind. But as Tobias Zillner points out (Zillner, 2015) in his paper it is employed by many companies for many implementations, it offers long life and built in security. However as he points out if the standards are not properly implemented then the security may be breached. This occurred with its implementation as seen by Phillips in its home automation products, the standard states keys should be stored securely and not transmitted unencrypted except in a few conditions. The paper details that Zigbee is susceptible to jamming also as well as key theft. It concludes by saying that the limitations are partly due to power resources and computational ability in the devices and these are fundamental flaws in designing a standard based on insufficient hardware resources. This

failing of the design is reinforced by the findings of another analysis of Zigbee security (Fan et al., 2017) by a group of students at CSAIL, MIT .

As many of the implementations in PA use similar systems to industrial systems with PLCs and sensors, similar to SCADA, it is important to consider the use of Intrusion Detection Systems in the networks to prevent unauthorised activities, this may not be practical in very small implementations of PA. However where large scale adoption occurs, for instance in networked UAV implementations this may be an important consideration (Choudhary et al., 2018). The challenges facing this are, once more though, the computational resources of the device which limit its ability to fully implement such facilities, even if they are implemented on the base station.

### Data Privacy

Precision Agriculture generates large volumes of data, and there are very large security issues associated with this. There are concerns over ownership, use of the data and how it is stored; even from the early introduction of data generating precision agricultural there have been concerns by the farmers themselves over how and where the data is stored and used. This is even though the sharing of the data and its agglomeration, potentially offers useful information to the farmers. (Fountas et al., 2008, 2005). As the data is produced it potentially can be collected by the use of Internet of Things and Cloud computing, this then will lead to the creation of a Big Data situation. The Big Data can then be analysed in many different ways to demonstrate trends, requirements, prompt on items for improvement or requiring change and aid in the decision making processes. A recent literature review (Wolfert et al., 2017) of the current situation on Big Data collection indicates that the influence of Big Data analysis goes beyond just the farmers generating it, all the way along the food chain. This means that the data becomes very valuable to large companies and others involved, however the data of the individual farmer may not hold a large amount of value in isolation: it is only when it is matched with other farm data that the volume has a significant value.

The data that will be collected will be that from devices such as sensors on machinery (flow meters, weight sensors, and optical recognition), barn and field sensors, UAV, aerial and satellite data, Real Time Kinematics (RTK) as well as farm management and financial systems. It is unlikely to be personal data from wearable sensors, as machinery will be performing the majority of tasks. There is however a case for safety in isolated regions for wearable, but this can normally be met by telephone or radio communication.

This data may be viewed by the individual farmer as being very valuable to them, but it is only when it is merged with other data from other sources that it truly becomes a high value resource. The data of many farmers when grouped together has the potential to yield large amounts of information when analysed, this Big Data though is now also a target for cybercrime who see it as a way to gain money, political or environmental groups who see it as a tool to extort or influence the populace, other companies see it as a potential information source and foreign agents see it as a means to gain leverage. This could be in the form of irrigation hacks to flood or prevent crops, over applying nitrogen or fertilisers in a fully autonomous system.

This data once it has passed out of the farmers control and onto the Cloud is now dependent on the security of the company holding it on the Cloud. If the collected farm data held by an agricultural agency was compromised by a large agricultural multinational, it could be used

to alter commodity markets by speculating; this would effectively be using the beneficial data from the farmers against themselves (Ferris, 2017). In Europe, GDPR regulation has helped to improve the situation of data management and protection unlike the USA which does not have such protections on collected data. The data collected by the farmers allows for a much more precise monitoring of their crops and resources, however the transmission and storage of the data brings about issues of ownership and rights to amend the devices (Deere and Company, 2015). The data collected on devices which are not the property of the farmer, but are provided by a 3<sup>rd</sup> party either as a leased or rented object or via Farming As A Service (FAAS) may be very useful to the farmer, but does he actually own it? Is it his property or that of the company collecting it, the company that analyse it or a combination? The data be highly sensitive containing personal details of producers and their staff, property locations and movement data of individuals. It may also contain sensitive crop yield data, spray application rates, field conditions or crop disease / growth data, furthermore from this data it may be possible to infer the financial position of the farms concerned.

One suggested solution is to use Ciphertext Policy Attribute Based Encryption (CP-ABE) (Chi et al., 2017; Helil and Rahman, 2017), this model would allow data to be selectively encrypted and transported with the recipient only able to decrypt the parts for which they are given. The data gateways would encrypt and decrypt the data going to and from recipients, and the farmer has the facility to implement access rights to the data streams. This model also deals with the issue of local storage encryption, if the store is breached the data is unintelligible and corrupt data cannot be injected as it will be immediately detected as it will be unintelligible.

Other situations might see the data used by agricultural technology providers to develop and sell new products to the very producers of the original data, this could be instances such as PA software for variable rate spraying, where the value of the land is calculated to allow a rival to approach a landlord to approach with a better offer, or the data collected about farm practices being used by government agencies against them in regulatory enforcement actions (Jacob Bunge, 2014).

The solution to the ownership of the data (at least in the USA) may lie in the way that it is treated by the producer of it, normally the farmer. The original owner of the data must be proactive in protecting his data to ensure that the Intellectual Property rights are not given away to another party (Chi et al., 2017). The method to do this may be to treat the data as a “trade secret” which will then give the farmer protection in law if his data is misused and the facility to recover damages. This could be for actual damages, reasonable data royalty rates for misappropriated data, or unjust enrichment – the unauthorised user has benefitted at the farmers expense. The obverse side to the argument about data privacy and protection is that too much of it will stifle development. It may also affect the quality of the data being collected, leading to under resourced data areas or poor quality data due to incompleteness of the supplied material.

The other area where data privacy is important is in its collection, implementation and transmission on the farm. Care should be taken that all data is protected as best as possible, this normally would mean using encryption when transmitting and storing data, but it also applies to the methods used to interchange the data – hardware and software. The hardware standards may be a universal connector to ensure that items may be easily connected without the use of multiple adaptors, whilst the software may be that data exchange protocols are

standardised and adhered to or that standard definitions are used (Nerpel et al., 2016). A study on the transport of data to the central collection point of the data streams aimed to ensure that the data transmitted and collected was authentic, so that any decisions made based upon it were valid (D. Puthal et al., 2018). In the sensor networks employed in PA, the sensitivities of differing types of sensor data may vary and this should be taken into account when encrypting data to ensure that the most sensitive data is the best protected. The system maintains intrusion detection to give a warning if the system is under attack and also used symmetric key block cyphers and multiple shared keys, these could then be maintained regardless of the load on the system. This type of encryption may well prove to be the answer to the security issues of data transmission, ensuring integrity and authenticity. It is a system like many others that is based upon the industrial security practices used in SCADA. Firewalls within the network to sub divide and protect areas is another option, but all of these impose a burden on maintenance and require additional knowledge which the average farmer does not possess.

### Aerial Drones

Aerial drones or Unmanned Autonomous Vehicles (UAV) have the potential to play a major part in PA, they can offer a cheap, effective and rapid method to obtaining data via cameras or other sensors, or delivering items to specific locations. They are cheaper to produce and operate than other aerial devices, do not require an operator to travel to all of their locations (being remotely controlled) and can be operated via commands without human intervention. However as other studies have shown there are still advantages in using other methods of reconnaissance such as planes and satellites, these may produce cheaper or better interpreted data, or may offer abilities to view from varying distances, or with differing sensors to those available on a UAV. They may also be less susceptible to atmospheric conditions or external intervention (Moran et al., 1997; Primicerio et al., 2012; Yang et al., 2006).

Although drones offer a potentially cheap method of data acquisition, due to their prevalence in military usage or the simple construction of cheap UAVs they are the subject of interest to those wishing to hack them (Mohan, 2016). Often the inexpensive and widely available drones will not incorporate strong encryption in their communications, and due to the popularity of hacking them, weaknesses are soon found. This can lead to the UAV being hijacked, its data altered or distributed to unauthorised agents (Pierluigi Paganini, 2013; Swati Khandelwal, 2015). If even military drones can be affected by malware, hacking and foreign agents such as China are known to try to use espionage to extract information (Dunn, 2013; Gorman et al., 2009), it is to be expected that PA UAVs will also be a target.

The use of commercially available components to UAV manufacturers means that the pool of components is limited, this means that it is easier for the security of a UAV to be compromised, and for this then to be used in attacks on other UAVs using the same components, and a recent study looked at how simple it was to take control of a UAV using Spektrum's DSM protocol (Bunse and Plotz, 2018). They suggest that the secret key should not be rebroadcast regularly during operations, however this then opens another method of attack for actors to replace the UAV connection to the base station with a false one – the battle for cybersecurity is a situation of fixing a problem and then facing the next. IDS is one method to combat the hijacking of UAVs, but as previously mentioned it can be computationally expensive. There has been a paper published which looks at how to detect the hijacking of a UAV, which only utilises the on-board gyroscopes and so is computationally inexpensive, this offers a potentially cheaper and faster method of detection



(Feng et al., 2018). Another research project has looked at securing the system using a set of rules of normal behaviour, which are pro-actively verified by both the UAV and base station. This has had a high level of success (93% detection, less than 3% false positives) with low communications loading, this will now be tested on a number of Parrot drones working together (these are frequently used as a cheap UAV in PA) (H. Sedjelmaci et al., 2018).

Communication security and continuity is critical in control of UAVs, it is essential that if the UAV is paired for jobs with a ground based device that this communication is uncorrupted, timely and intelligible. A study of lettuce growth shows the dependence on this (Subodh Bhandari et al., 2017), if the data was corrupted or interrupted then the ground based machine could be induced into incorrect activities. UAVs may also factor as a mobile attack point to hack into PA networks and gain control of devices.

UAVs can also be used to attack PA systems by jamming wireless networks, so in a field of sensors or where an autonomous tractor may be operating the communication signal could be jammed. The UAV could enter the location, jam the signal for long enough to cause damage or disruption and then leave, with it being very difficult to determine what the cause of the interruption to the command signal was due to. A paper into how to prevent unauthorised UAV use by jamming outlines exactly how to use this knowledge offensively (K. Pärilin et al., 2018), whilst another paper outlines the use of a UAV to jam signals of an eavesdropper on communications and leave again, this information can be used for both attacking and defending the UAV though (Li et al., 2019). Future developments of UAVs may see them controlled over cellular networks over great distances where large farms are prevalent such as in America, Canada and Australia. These will need to have security enforced over the cellular network, one such suggestion to deal with is via machine learning which from the papers results seems a promising area of development (U. Challita et al., 2019)

## Tractors

The concept of autonomous tractors is a goal for PA, along with complete automation of the crop raising process. However the issue of security is a major factor in achieving this, the devices must be deemed to be safe for humans to operate around as well as being safe to operate in the environment without damage to themselves or their surroundings. The issue of security is also a major factor in this, as are the legal aspects (Basu et al., 2018). What is the situation if an autonomous tractor is compromised and causes damage to a 3<sup>rd</sup> party or their property, on whom does the responsibility fall? The legal precedents for such an activity are unclear as yet. The legal framework for operating the tractors may allow for security breaches which may be exploited in accessing or controlling the tractors, as with everything involved in this developing field the situation needs to be reviewed as progression occurs.

However the use of autonomous devices to plant and harvest has now become a proven concept after a second year wheat harvest was successfully harvested and transported from the field autonomously (“The Hands Free Hectare project completes second harvest,” 2018). The research and development of this is ongoing, but security of the system is not seen as a major concern at the moment. Professor Simon Blackmore from Harper Adams University (HAU) and involved in this project, and that of the Small Robot Company, commented to me that:

*“As with most of our ag robot developments we use technology that has been developed outside the ag area and migrate it over as and when needed.”*

*Security has not been a hot topic at all recently as we are still getting the fundamental systems working. Mostly we just use WiFi.*

*HAU does have a research program atm exploring what 5G can do on the Hands Free Hectare.”*

This reinforces my belief that when products are being developed the desire for success, and in the case of commercial products, to reach the market are more important than the security of the products.

The autonomous vehicle on the farm will operate under its own control, and it will achieve this by utilisation of cameras, LIDAR, GPS, Radar, sensors and onboard computers. It will determine its location and where it needs to be, and then proceed there to perform its tasks. However the large numbers of sensors required make it a susceptible to attack as there are so many possible attack surface to corrupt the machine. This complex system has been investigated to try and secure it in a number of ways, especially the message authentication, communication and data storage. One topic of research is to validate the operation of the machinery with optical recognition (Jamal Raiyn, 2018), whilst such a proposal is valid in a road going autonomous vehicle, it will not work in the agricultural setting where the desire is to remove the driver. However some of the principles can be used to verify the commands for the vehicle before it begins, this would confirm the validity of the commands that the machine was to undertake.

Professor Simon Blackmore also said about the use of ISObus and TIM that:

*“ISObus is not really relevant as it only exists on the tractor. There has been talk about moving over to real-time ethernet instead. “ .*

This would once again disrupt the existing standards that have been arrived and lead to devices potentially being incompatible or insecure in their communications. Security issues which may have been resolved by the use of TIM, would now need to be revisited and secured.

The proliferation of screens in the tractors to control multiple data sources and devices (implements, sensor feeds, GPS, spray rate monitors) means that there is also a security issue in the cab with all of the data not being compatible, as well as open to misinterpretation. This is addressed in the ISO11783 standard, but has not been widely adopted but the implementation of the ISOBUS and TIM may overcome this. However there has been research done on this subject using the Virtual Terminal concept to combine these data feeds (Ham et al., 2017), this would need the manufacturing companies of PA equipment to participate in this, without their assistance this initiative will not succeed.

Many of the problems associated with UAVs and sensors, will be common to the autonomous farm vehicle. This will only be exacerbated if instead of one large vehicle, swarm machinery is used as there will be a corresponding increase in attack surfaces.

### Wireless Sensors

In the field of PA and sensors, power whether for consumption to drive the sensor or as a measure of available computing power, is critical – the more the better. This can be even more of an issue in remote sensors situated far from habitation as may occur in large farms.

Unless servicing is performed or other power sources used (e.g. solar or wind), then power consumption is a major factor. Therefore the sensors are all designed to perform as much as possible whilst consuming the minimum of power. This means that there is very little leeway to provide for security. Another aspect of this is that if a sensor network is compromised, and the sensors are power critical, it is a simple task to increase the sensor power consumption and bring down the sensors, this is the scenario which is envisaged in a report on research (Bergmann and Denzinger, 2013) which forced sensors to use processes which boosted their power consumption and thus consumed their power. This is an example of how difficult it is to protect a sensor network, as any area may be investigated to allow for exploitation.

Much is also made of the ideas of using IoT and the Cloud to operate sensor networks in agricultural environments, and research has been conducted in this area (Kim et al., 2018; Papageorgas et al., 2018) but the security aspects of such networks are completely ignored. Even where the topic of the article is concerned with security (Garcia-Sanchez et al., 2011), in this case physical and implemented by cameras, no thought is made of implementing cybersecurity to ensure the safety of the network and the data transmitted across it. Even where security of a Wireless Sensor Network (WSN) is mentioned and that Zigbee will be the technology employed (Keshtgari and Deljoo, 2012), it is in passing that Zigbee security is mentioned, after this it seems that the authors believe that security has been dealt with. This is even true in a paper in 2012 which illustrated basic guidelines for deploying WSNs in agriculture (I. Mampentzidou et al., 2012), once again cybersecurity was absent. There is literature which does include it, but these are normally articles aimed at demonstrating or implementing security in WSNs (D. He et al., 2007).

### Literature Review Conclusion

The view of cyber security in PA at the current time appears to be that it is not relevant, there is an attitude that as devices are being developed there is no requirement for immediate security. If it is required then it can be added later, but this is the thinking that has always existed in technology: find a solution and then to patch up the faults in it as they appear. A much better method is to design security into PA at the initial phases, rather than trying to add it on as an afterthought. This is always more expensive, leads to potential conflicts with existing code and practices, as well as always being not part of the structured design of a product.

There are protocols and methodologies that can be applied and many people appear to be aware of the potential risks (Mutschler and Department of Homeland Security, 2018), but the action needs to be taken now to implement these security practices and ideas.

This is a new area of technological growth and it would appear that now is the perfect time to be looking at security and its implementation, before standards are set and bolt on fixes are applied to correct the omissions that occurred in development.

## Research approach

### Background and outline

PA is based around the concept of using technology to determine the location of crops, their growth and requirements to ensure that the minimum amount of resources are expended to ensure maximal crop returns. This means using aerial imaging, GPs location and light sensors even to ensure that nutrients, water, weed control and general cultivation is only applied to the specific areas that require it and in tailored quantities. This requires a high level of technology to operate autonomously, or even as a partial farming management system.

The field of agricultural technology in precision agriculture and other associated fields is largely based on Industrial practices and those of the Internet of Things (IoT). The growing use of agricultural technology means that there is now another area for cyber-attacks, there do not appear to be any specific amendments or developments designed to cater for the agricultural environment currently. The concerns of the US government are great enough that they have produced a paper to warn of the emerging dangers, (Federal Bureau of Investigation, Cyber Division, 2016). This paper is designed to research the possible vulnerabilities and risks specific to agricultural technology, and if the vulnerabilities of the items employed from industry represent a greater risk in agriculture to those in industrial applications. The machines used may be production items (UAV drones used for imaging or herd management), or custom created machines such as the “Broccoli Bot” which utilises parts from a Microsoft Kinect (Kusuman et al., 2016) or sensor based monitoring utilising Zigbee wireless technology (Trancă et al., 2017). All of these generate valuable data flows which may be compromised in some manner.

There are also potential risks and vulnerabilities from the ownership of the very machines employed in the practices. In the USA, under Digital Millennium Copyright Act 1998, companies such as John Deere had made it illegal to repair the farm tractor as it contained code owned by John Deere under their patent application (Deere and Company, 2015). This meant that only the company can repair or modify a machine, potentially preventing a farmer using their own equipment, theoretically this could extend to other machines (this law is currently being challenged). John Deere argue that the code in their machines must be protected against hackers, third party developers looking to exploit their code.

Even water management for agriculture can be an area of risk and vulnerability. Agricultural irrigation using technology to control it, or desalination plants for water used in agriculture are potential targets; they can be attacked via SCADA methods used in other industries, as well as by conventional email or compromised PCs using social engineering. The Middle East acknowledges the dangers of water security as regional and global problem which poses as serious threat to the security of the region in a recent research paper (Swain and Jägerskog, 2016).

Legislation is another area which can have an effect on the security of Precision Agriculture. The control of a technology in an unrelated area may well affect the security of agricultural technology - the control of drone (UAV) usage may affect the use of drones in agricultural environments. This may mean that monitoring of livestock is hindered because they are not permitted in certain areas, this may impact on the welfare of the livestock.

A research project in the USA found that although precision agriculture used technology and methods common in other industries, the conversion of a highly labour intensive, mechanical industry to an electronic low labour system caused a scenario which “dramatically increasing the attack space available to threat actors. Due to this, otherwise common threats may have unique and far-reaching consequences on the agricultural industry.” (Mutschler and Department of Homeland Security, 2018).

### Research approach - overview

The research in this thesis is predominantly qualitative in nature, with a limited amount of quantitative data. This is due to the nature of the research and limiting factors such as time and access to privileged data. The project used the qualitative approach where possible in the analysis of the research of the published material on the subject and its related areas. Thus where there is a lot of published material supporting the belief that a method is insecure, then this would have greater importance than another less well detailed method. There was however, a very strong requirement to ensure that any analysis made of such situations was not just following a trend, but there was a solid reason for supporting it. Widespread belief does not make something correct, but verification of its basis may well prove it to be valid.



*Figure 2 - High level overview of the research process employed*

The research method employed has been a combination of a **literature review** and empirical data collected and analysed from **interviews** and a **survey** with companies or organisations involved in this area. The literature reviews were drawn from published academic papers, and other documents from government or industry sources. Manufacturers of PA equipment, agricultural colleges which have done previous research in these areas and other researchers that have been involved in areas of research and development that associate to the area of research have been approached for interviews and surveys. People who are involved in the development of equipment that is used in PA and associated fields, have also been contacted to gain further information. Furthermore interviews on the subject of security with the people who have been contactable and who are agreeable to being interviewed, have been performed. Due to the sensitive nature of the research, any interviewees were given the option of anonymity, this was to encourage discussion and protect their interests also.

The method used for the research was originally going to be Grounded Theory, this would test the theory against the research which has been performed. The intention had been to explore as many areas as possible that were directly connected to the area of research, extract and classify the information that could be utilised, and then use it to assist in confirming or denying the theory about PA risks and vulnerabilities. The ongoing research performed was

likely to revise the theory as the research proceeded, this would have entailed the regular revision and review of the work to reach a conclusion. However this conclusion would not be an endpoint, but merely a view at the time the research was finished; continuing changes in attack vectors and defences, technology developments and implementations mean that there can never be a definitive conclusion, only a current perspective. However due to the difficulties with securing enough interviews and survey results, this approach had to be reviewed and was changed to that of a literature review allied to interviews and surveys based upon the literature review results..

The research tried to find persons willing to participate in interviews on the subject of the thesis and to talk about the security measures that they have used to protect their developments. A brief survey was also sent to companies that may not participate in interviews to supplement the data collection. However it has proved very difficult to gain access to such data as by its nature, the manufacturers are not disposed to giving out details that could be potentially used against them by agents seeking to exploit their devices or highlight their lack of security preparation. They also are wary of giving out data that might give competitors an advantage in the market, the option of anonymity may have helped to overcome some of the resistance to participating in the research.

The method of research chosen therefore has been to undertake a literature review with this framing the questions used in the interviews and survey questions. The literature review provided a solid grounding in the many and varied areas of PA that are being addressed. It served to show where the security deficits may have been, and what the current security employed might be. In addition, the review also brought to light a number of attack surfaces that had already been identified in PA, or that could be applied to PA from other areas. This knowledge was then used to frame the initial interview and survey questions, these were then revised as more information became available both from further literature and feedback from the questions asked.

The literature review focused on the topics of the research questions but with a primary focus on agriculture in Europe, USA and Australia / New Zealand as their agriculture is broadly similar.

### Discarded research approaches

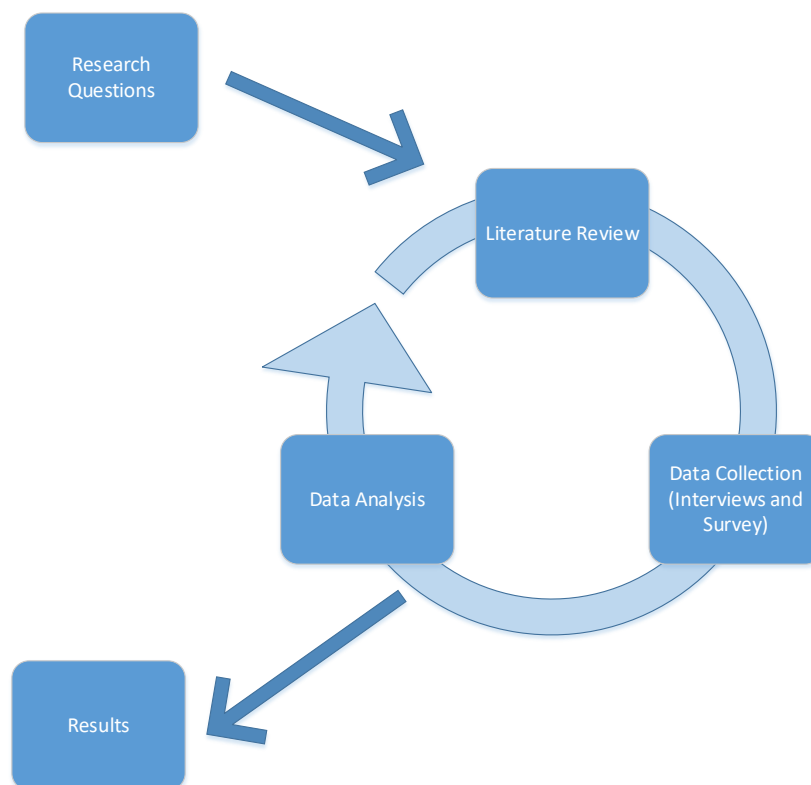
The following potential research approaches were also considered, but were subsequently discarded for use in preparing this thesis as elucidated below:

- **Grounded Practical Theory** was not an option as the research did not follow all of its aspects; whilst it looked at the problems of PA, it did not look in detail at solutions nor did it investigate the techniques and management of the issues.
- **Action Research** and **Design Research** were not applicable in this project as no artefacts were developed, but only theories based on the research. If a device had been actively developed which had a bearing on PA then these methods might have become more applicable, especially Action Research. This was because the development would have been research which was part of an active feedback loop directly attached to the development of the product “a juxtaposition of action and research, or in other words, of practice and theory.” (Marshall and McKay, 2001) .

- **Delphi** as a method of research, as well as its associated method of **Grounded Delphi** was considered; however as most of the work was derived from researching papers available on the topic with only limited number of interviews, it was decided against this method as it stands. The timescales meant that it was impractical to implement surveys, collate results, formulate a new survey and implement it a number of times. Also without a prior knowledge of this area of research it is difficult to assess how experienced, reliable and capable those replying to a survey are.

### The research process in more detail

The research process was based on a literature review used to guide the data collection, where semi-structured interviews and a survey were used. The collected data were then analysed using matrices. The research process is outlined in the figure below and the methods etc. described in further detail below that.



*Figure 3. The research process was iterative and each cycle of refinement brought a more refined result*

### Data Collection methods

Interviews – Semi-structured interviews

The interviews were conducted based upon qualitative interviewing techniques (Edwards and Holland, 2013), using a semi-structured format (Mason, 1994) – this allowed the interview to include new ideas and associated areas of discussion. There were interviews performed with 2 developers of agricultural robotic machinery, a number of farmers using PA, and 2



agricultural suppliers. Responses were also received from a Professor who heads the UK National Centre for Precision Farming and also a PA machinery developer. All of the respondents have a good knowledge of PA, but some were much less aware of the risks that it could potentially present. The interviews ranged in duration from 30 minutes to over 2 hours, the majority were conducted over the telephone or other voice communication due to mobility and location issues, however some were performed face to face. All of the respondents' views were analysed to see where commonality or differences occurred.

***The interview questions can be found in [Appendix A](#)***

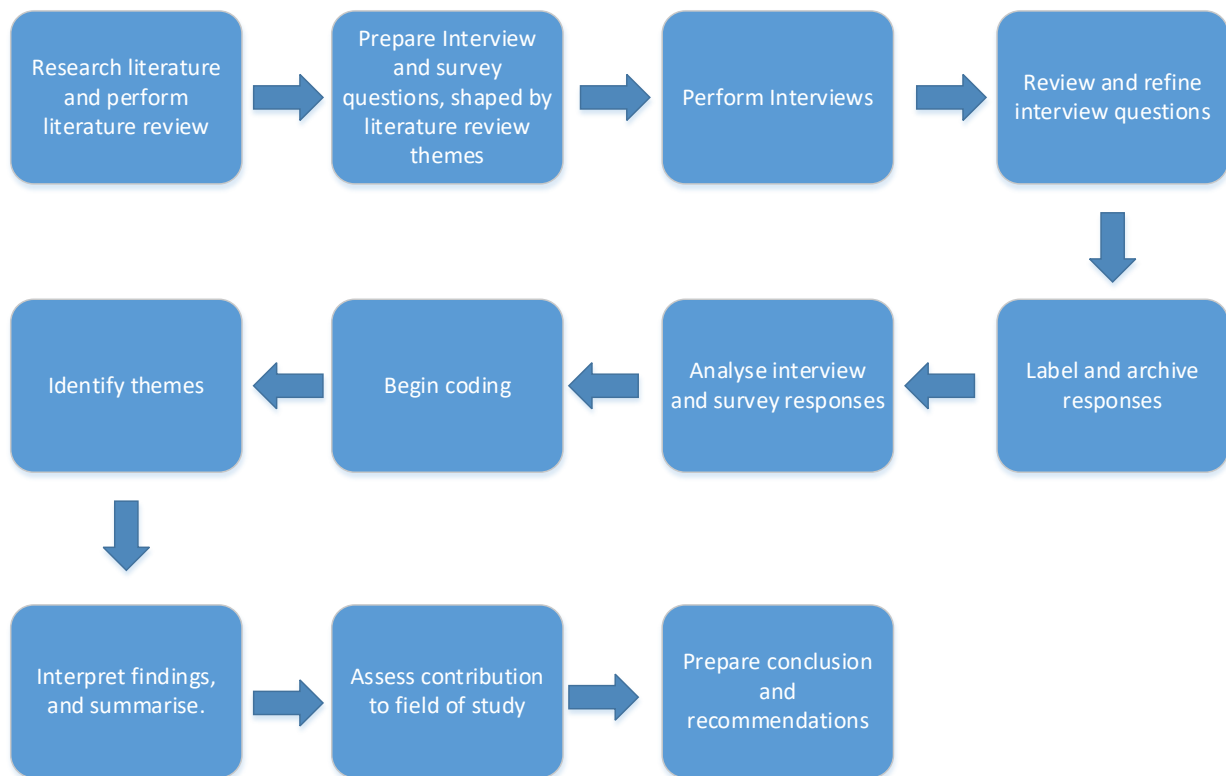
During the interviews the interviewees were asked about their understanding of PA, how did they implement it and were there any areas that they saw as potential risk areas. The reason that differing members of the PA structure were interviewed (developers, resellers and users) was so that a broad view could be gained of the subject and how the various elements viewed security.

#### Survey

A qualitative survey (Jansen, 2010; Walle, 2015) was also sent to a number of developers of PA machinery, PA start-ups and established agricultural machinery manufacturers to ascertain their attitude to security in PA. The number of questions in the survey were kept short (6 in number) in order to try and encourage responses, as well as not taking up undue amounts of time. Some guidance on the meaning and intent of the questions was given, but was phrased so as not to influence the form of the reply. The survey was sent by email to companies after they had been identified as being in the target group, this involved researching for start-up companies, UAV companies and major agricultural machinery suppliers and manufacturers. The response rate was very poor, out of 32 surveys sent out only 3 responses were received. However on following this up, two recipients gave telephone interviews. The low response was a major factor changing the research approach from Grounded Theory.

***The survey questions can be found in [Appendix B](#)***

Interviews and a survey on such a sensitive area has meant that care had to be taken not to influence any replies that were received by the questions asked or their phrasing.



*Figure 4 Data Collection and analysis process*

### Data Analysis methods

The data collected from the interviews and survey questions has been reviewed as it was collected and then used to modify the methods used for further interviews and surveys. Once this had been done it was archived (interview sheets and survey sheets stored in a binder, whilst sound recordings were transferred to computer for storage. This was then annotated separately and pertinent areas marked up via coding. The coding method used was a mixture of process coding and descriptive coding (Miles et al., 1994) as neither was a perfect fit. Descriptive coding allowed the summarisation of the data into short phrases or words when the data dealt with practices and multiple data sources (interviews, questions, surveys, informal conversations) that then allowed the development of the central themes, whilst the process coding allowed the data to be analysed in the form of interactions and processes. By combining the two methods, a practical coding method was arrived at for the limited but disparate data analysed.

Themes were then identified which appeared and the findings were summarised into a matrix display to make it easier to see the data in a coherent form (Miles et al., 1994) and then to reach a conclusion drawn from the research. In order to visualise the results, graphs and charts were used to enhance the perception of the results that were generated (Miles et al., 1994).

### Validity, reliability and generalisability

Validity is a concept that has been defined by (Drost and al., 2011), as well as being investigated by (Johnsson and Altheide, 2011) as being concerned with the meaningfulness of research components, in this case whether there is internal validity, or credibility, and external validity of the data collected.

The validity has been upheld during the data collection by talking to more than one source, in this case the data was collected from farmers, manufacturers and researchers. Furthermore, the validity has been considered during the data analysis through the coding cycles, where it is analysed and reviewed (Miles et al., 1994). The limited number of respondents (interviews and survey) has been mitigated to a degree by the fact that the responses come from across the industry – farmers as the users of the products, resellers and producers as the servicing and information source, and researchers into PA as the overarching view of the topic. The research has been limited to a small area of PA though, and research in an area where industrialised PA was prevalent may show a variance in results and a greater awareness of security issues. The dairy industry might show a more marked security awareness due to the greater spread of IT to a lower level, as might arable farming in the USA and Australia where UAVs for cultivation may become more rapidly widespread. The use of the literature reviews has also served as a check and balance on the findings of the empirical research, however the literature reviews are predominantly from an academic background and so have a bias towards theory rather than practical application.

Reliability can be seen as the ability to replicate the findings of the data collected or consistently receive the same results according to (Johnsson and Altheide, 2011). As mentioned before, security is a sensitive subject and questions about it are frequently ignored or guarded in reply. However the consistency of the replies in all areas would lead to an assumption that if the research was repeated in the same area of PA in the near future (and barring any major PA data breaches), that the results would demonstrate a similar attitude to security in PA. Agriculture is seen primarily as a technical and old fashioned industry relying on traditional knowledge, and not a technological industry, by the majority of its participants. This has meant that the majority view appears to be that technology will add to the abilities of farmers but that old fashioned knowledge can be relied upon. There does not appear to be an awareness of security risks at any point in the industry, over and above that mandated by government to conform with regulation - for example, GDPR (Publications Office of the European Union, 2016) and Health and Safety (*Health and Safety at Work etc. Act 1974*, 2019)).

Generalisability is a term which indicates if the results are transferrable from one area or context to one or more others but in quantitative research. Therefore in the instance of this being qualitative research and not quantitative research, it may be better to view reliability as the transferability of the research as defined in previous research (Jordan, 2018; Noble and Smith, 2015). However, the results in this thesis are applicable in a broad context to many areas starting to be digitalised and connected to the Internet in an industrialised/professional context using:

- IoT (i.e. sensors and actuators or other data collection devices)
- connected machines
- monitoring of machines/device/areas
- collection/storage/analytics of data in cloud services
- etc.

Examples of such areas are dairy farming, arboriculture, salmon farming, horticulture, domestic building and healthcare

.

## Empirical data collection and analysis

The collection of empirical data for this project was more difficult than had initially been envisaged. This was due to a number of factors – the topic in question (security), access to suitable candidates, timescales and ability to travel. As a result of these factors it was decided that most of the interviews would be performed by telephone for convenience and accessibility. The interview format was decided upon initially from research into the style of other interviews, however it was immediately apparent that this format was insufficient to allow for the semi-structured approach needed and so the survey questions used in [Appendix B Format 1](#)

The interviews were performed in the same manner whether it was face to face or by telephone. This was by initially introducing and explaining the purpose of the interview, which was to investigate the security used and perceived to be used in PA. The interviewee was then asked about their product/products or farming practices using the interview guide and the survey questions. This then would frequently lead to the interviewee giving more information on certain aspects of a question, and maybe none on another area as it was not relevant to them. When the farmers were interviewed they had little knowledge about the methods of communication between devices, all they wanted was for the devices to transfer data. They had no interest in the methods employed and had never given any thought to the security, validity, authenticity and confidentiality of the data transfers. The attitude assumed was that security was unlikely to be a factor in their industry as there was little perceived value in their data to other persons, and that there was no reason to try and gain access to PA systems as there was little to be gained. This view persisted across all of those interviewed and surveyed. The interviewees were all asked about the use of data by others, how they saw the security of the devices that they employed, what the potential risks were of corrupting them were and the effects that such activities might cause. They were also asked about their view of security in general in agricultural areas.

Throughout the interview I recorded the conversation (where possible) and also made notes on the interview sheet. Each interview was recorded on a unique sheet with the interviewee's name, date of interview, method (face to face /telephone), duration and location. This data was then added to an Excel spreadsheet that was maintained of all contacts.

The Excel spreadsheet was used to maintain a record of all contacts made, whether successful or not; only those where some initial contact or introduction were included. Those companies who had been contacted blind were not added to the record.

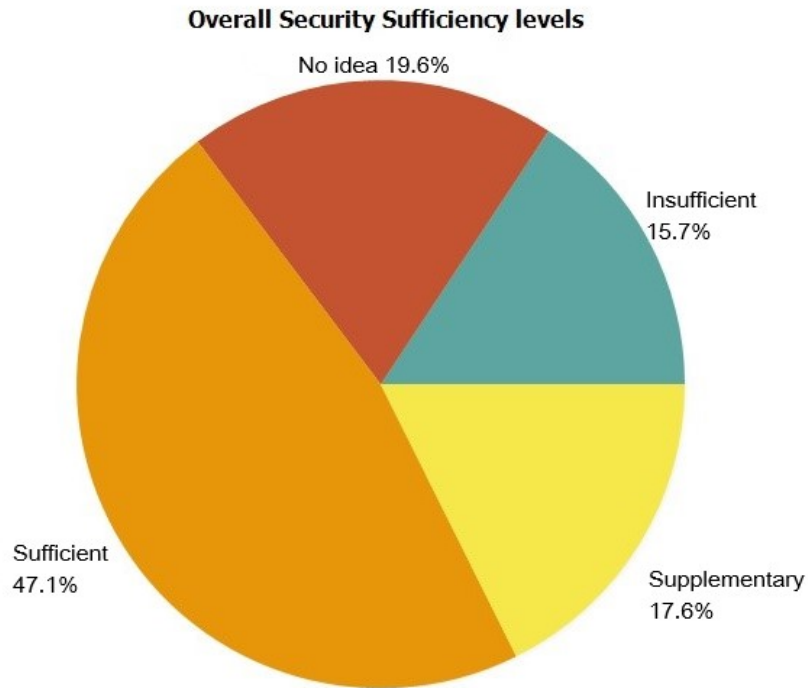
Company	Products	Contacted	Contact method	Result	Time in hours
1 Small Robot Company	Robots	07/03/2019; 08/05/19	email	Declined reply due to security - email 23/05/19	
2 Claas	Agricultural Manufacture	07/03/2019 ; 03/05/20	email	No reply	
3 Case IH	Agricultural Manufacture	07/03/2019 ; 03/05/20	email	No reply	
4 AGCO	Agricultural Manufacture	07/03/2019 ; 03/05/20	email	No reply	
5 Plymouth University	Robotics	08/05/2019	Phone ; email	Interviewed on phone 10/05/19 15:24	1.25
6 University of York	Systems Safety	08/05/2019	Phone ; email	No reply	
7 University of East Anglia	Environmental geographi	08/05/2019	Phone ; email	No reply	
8 Precision Decisions	Drones and sensors	08/05/2019	Phone ; email	Survey sheet returned - 21/05/19	
9 Martin Lishman	Sensors	09/05/2019	Phone	Interviewed on phone 09/05/19 15:49	0.5
10 Harper Adams College	Agricultural Robotics	12/03/2019	email	Email reply to marcwindow@yahoo.com 13/03/19	
11 ProAgrica	FarmPlan	15/03/2019	email	Awaiting reply - 22/05/19	
12 Tillett and Hague Technology	Automation technology	04/03/2019	email	Email reply to marcwindow@yahoo.com 05/03/19	
13 Manns / Claas	Agricultural implements	19/05/2019	Young Farmers Show	Interview 19/05/19	1
14 Does of Ulting	Agricultural implements	19/05/2019	Young Farmers Show	Interview 19/05/20	1
15 Farmer	Farmer	12/03/2019	Personal	Interview 12/03/19 12:30	1.5
16 Farmer	Farmer	03/05/2019	Personal	Interviewed on phone 03/05/19 15:49	1.5
17 Farmer	Farmer	08/05/2019	Personal	Interviewed on phone 12/05/19 15:49	1.75

*Figure 5 Companies and individuals contacted*

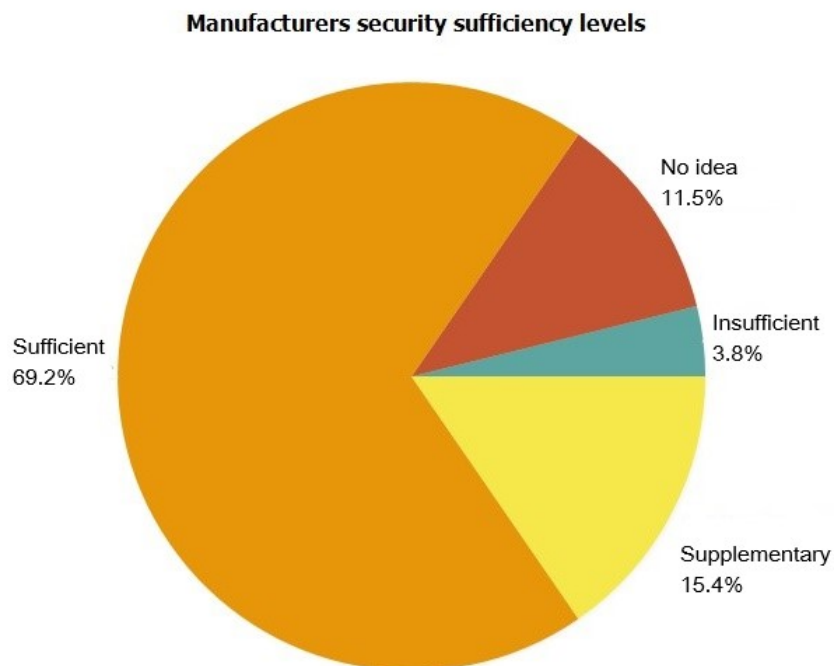
The survey questions were created based on the main areas that influenced arable PA, this was primarily the implements used, the data storage from the farm management systems and data collection, the guidance and mapping systems, the sensors employed, and general agricultural IT security awareness. The literature review provided a guide on the areas that the questions should focus on such as communication between devices, failure of communication, misuse of data, data ownership, dangers of loss of data control, awareness of general computer security and its impact on individual farming practices. The literature reviews showed that much time was spent on the creation and development of devices to aid in PA, but that little time was spent on securing such devices. The security that was in place over communication channels was normally viewed as enough to fulfil any security requirements, and passwords would protect any Internet available services. This led to the survey questions probing as to whether these levels of security were sufficient, however the questions did not ask any searching questions on the types of security employed or whether it had been compromised. The deeper research into the application, suitability, strength and trustworthiness of security methods was deemed to be too involved and time consuming to form part of this research, it would however be a good candidate for further research into the types of security required and their applicability in PA. Once I had spoken to some farmers and UAV developers informally, I saw that the questions needed to be more focused as the focus of the questioning was not fully understood. This led to the interview questions becoming much more specific in their focus, each section asked specific questions relating to that area and how security affected it. Thus in the data management section for example; after talking to farmers who said they were unaware of data security and literature reviews on items such as the John Deere right to repair and the USA's FBI paper on PA, the questions focused on ownership, encryption and communication security.

After each interview, survey or informal talk the method used to question interviewees or carry out surveys was further refined. This was true in interviews, where based on previous interviews, the focus was put on relevant topics such as awareness of the dangers of lack PC security and its ability to influence the security of the connected PA devices.

As cybersecurity is of a sensitive nature, the collected data is kept confidential and only the results of the data analysis is made public (see figures and graphs following).



*Figure 6 Security sufficiency from all respondents*

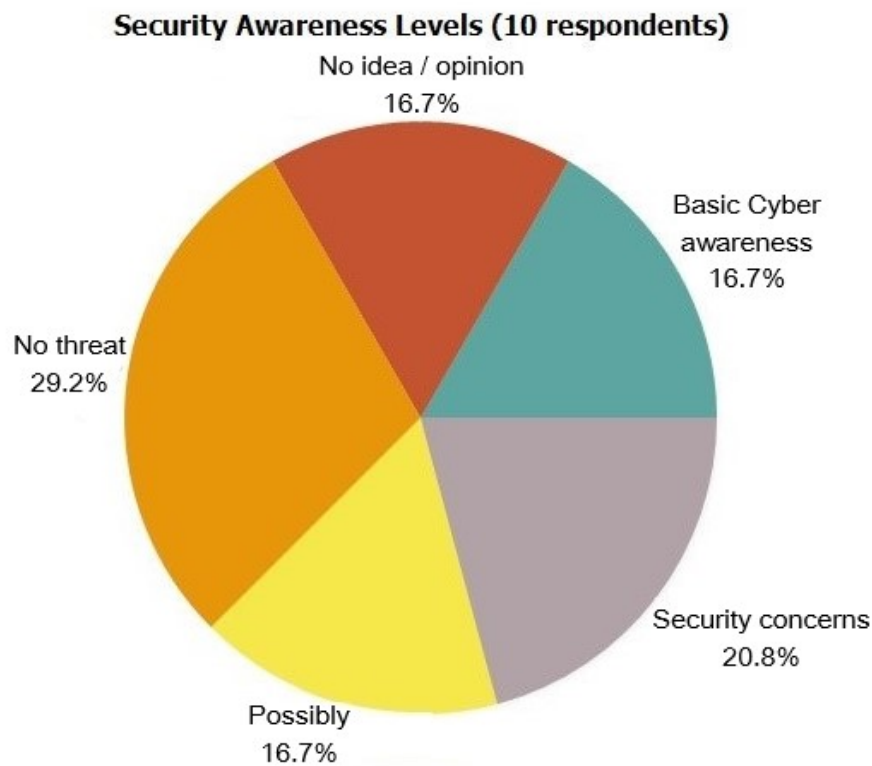


*Figure 7 Manufacturers security sufficiency*

The two charts above give a reflection of the levels of security and how sufficient they are viewed to be, the top one by all respondents and the bottom only by manufacturers and suppliers. It is apparent that that the manufacturers and suppliers are more ready to see the security measures in place as being sufficient in more cases than the users of the technology.

This view must be tempered with the knowledge that the users may be much less aware of security issues than the manufacturers. However both groups have a large area where the response is “no idea” of the sufficiency of security. This may be misleading as some of the questions may have not been in the area of expertise of the interviewee, so this causes some degree of bias.

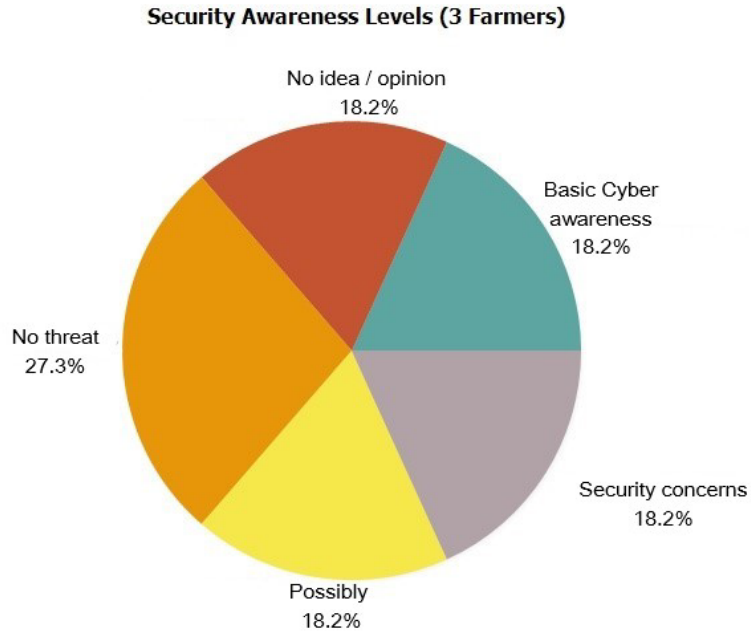
The awareness levels that were found in response to the questions on the awareness of cybersecurity in PA were also analysed. The initial analysis is of all the respondents and the frequency they responded with a reply that showed a level of cybersecurity awareness, then it was split between the 3 farming respondents and the remainder.



*Figure 8 Security awareness - all respondents*

This showed that only 1 in 5 security based questions elicited a response where there were security concerns about the current situation.

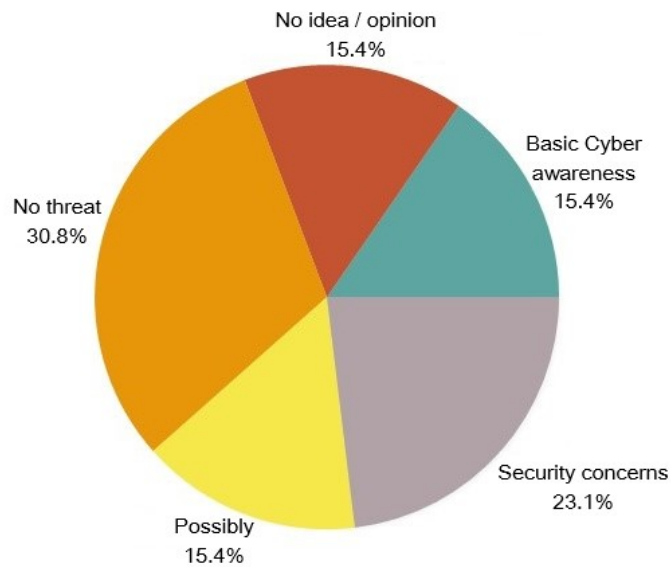




*Figure 9 Security Awareness - Farmers*

This only dropped slightly when only the farmer's replies were analysed, and only increased slightly when they were not part of the analysis.

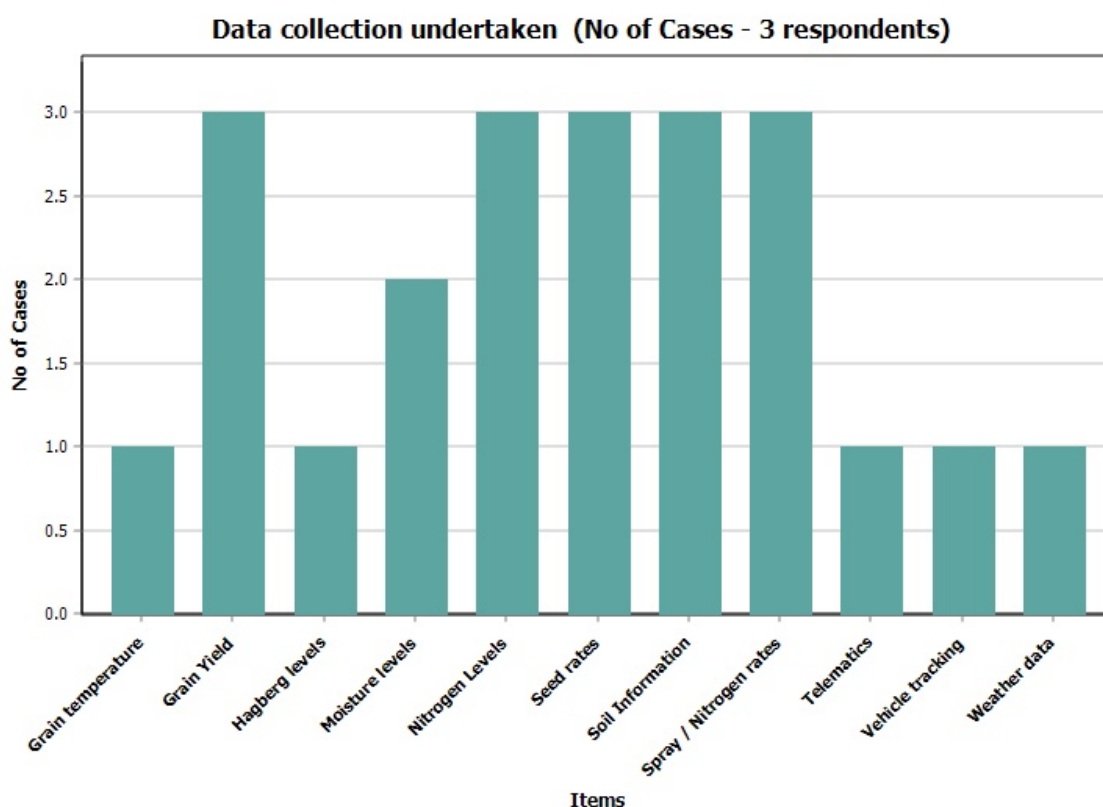
**Security Awareness Levels (7 respondents - 2 researchers, 5 Manufacturers)**



*Figure 10 Security Awareness - Researcher and manufacturers*

Although this is a very small sample, it is indicative that the attitude towards the threats in cybersecurity in PA are not viewed by the participants as being very high. They are aware of some potential threats, but do not view these as being of any need to take very large measures to combat.

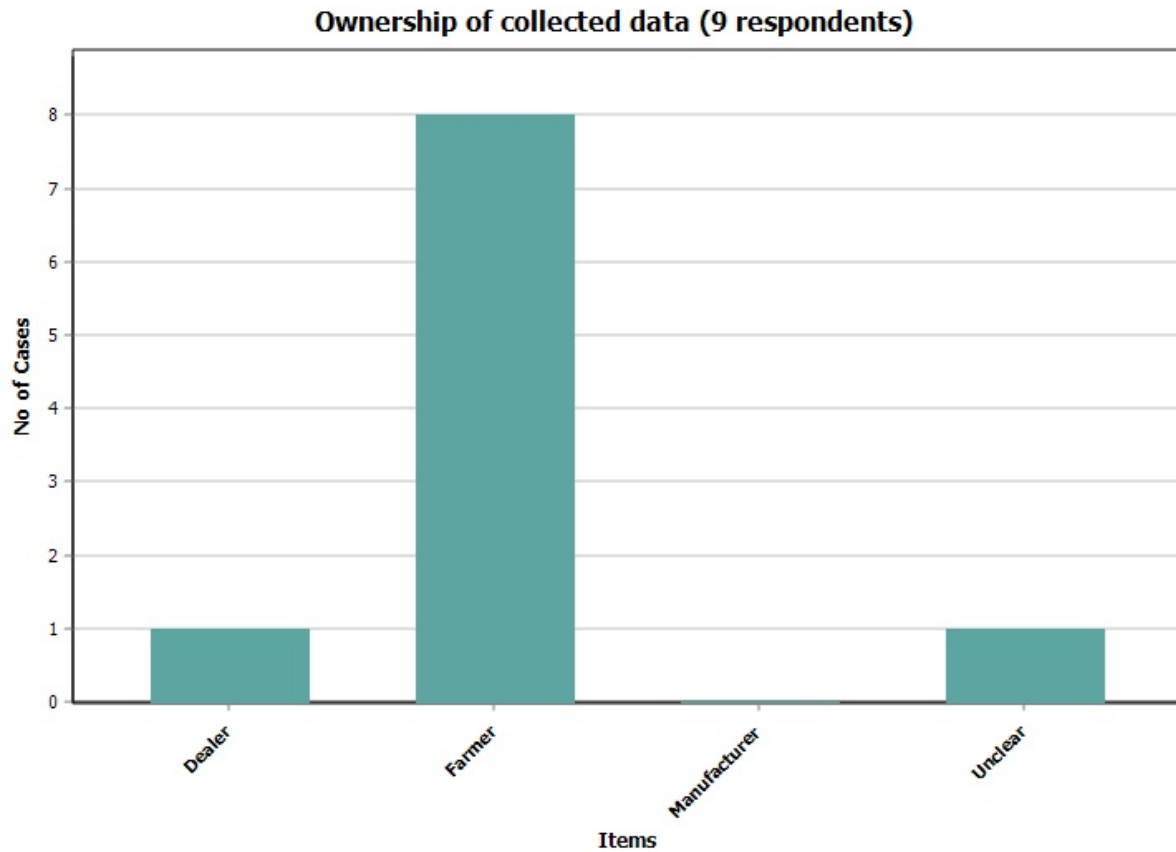
The following chart shows that the data collected by just the 3 farmers responding can be comprehensive and give a clear picture of the production and quality of a farms output, as well as giving a clear picture of the inputs used on the land and the land quality.



*Figure 11 Chart of data collection types*

In all of the cases bar one, where an answer was given (9 out of 10 cases), the farmer was seen as the owner of the data. The exception was a researcher who said that ownership could be a moot issue, as the manufacturer could claim ownership of some data that was derived from their proprietary systems as well as the farmer claiming ownership of all data. The other variable of dealer ownership data was from a machinery company who stated that the ownership of diagnostic data was theirs and not the farmers (this could potentially lead to a conflict of ownership dispute if the data was ever needed for legal disputes).

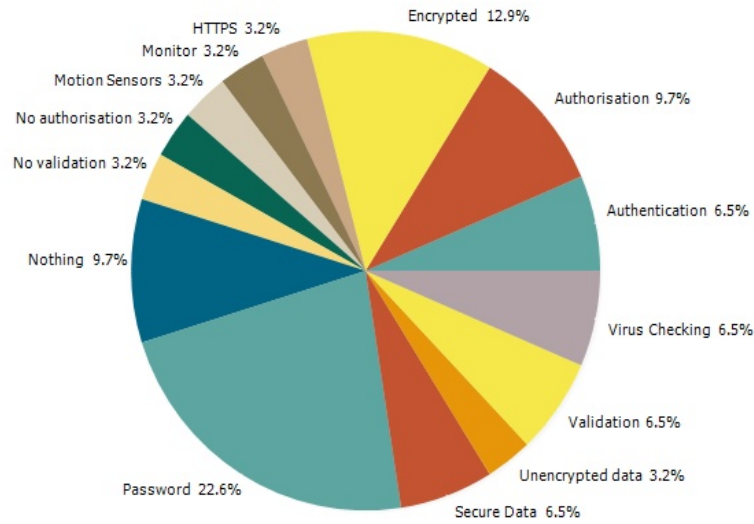
In all cases bar one where an answer was given (9 out of 10 cases), the farmer was seen as the owner of the data. The exception was a researcher who said that ownership could be a moot issue, as the manufacturer could claim ownership of some data that was derived from their proprietary systems as well as the farmer claiming ownership of all data. The other variable of dealer ownership data was from a machinery company who stated that the ownership of diagnostic data was theirs and not the farmers (this could potentially lead to a conflict of ownership dispute if the data was ever needed for legal disputes).



*Figure 12 Collected data ownership*

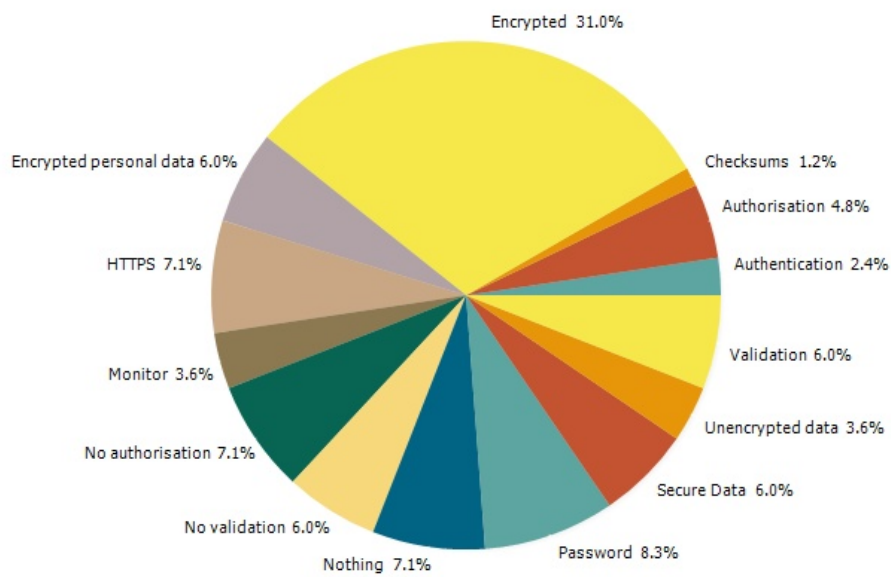
The security methods that were employed, or that it was perceived to be utilised, by respondents showed a variance between the farmers and the manufacturers/researchers. In this area of cybersecurity we can see that there is a much greater variance of views how secure the systems employed are. Whilst the farmers perceive the use of security measures implemented to protect their systems is reasonably high, they see the vulnerable areas as only being 19.3% of the areas in which they feel security measures are needed. The manufacturers view is that (28.8%) of the areas that require some form of security, do not have any form of security implemented. There is also a large variance in how the two groups see implementation of security. An example is Encrypted data and communications - Farmers see it as 12.9%, whilst the manufacturers and researchers see this figure as being 31% .

**Security methods employed ( Farmers  
based on the Frequency of responses)**



*Figure 13 Perceived Security methods employed - Farmers*

**Security methods employed ( Researchers and manufacturers  
based on the Frequency of responses)**



*Figure 14 Perceived Security methods employed - Manufacturers and researchers*

These figures may be a little misleading however as the questions are asked over a variety of subjects over which the respondent may not have a full knowledge.

Although the sample size was very small, the results appear to be fairly uniform. It would be incorrect to assume that this was a full review of the current position of cybersecurity in PA as there is no empirical data from the major manufacturers, only from the dealers for two manufacturers. This will not give a true picture as it is highly unlikely that the dealers will have knowledge of the areas of cybersecurity which may be employed by manufacturers. This could be due to the dangers of secure data of a cybersecurity / financial / commercial nature being revealed. The variance between the 3 groups involved in the sample (Farmers, Researchers and Manufacturers) reveals that the views on cybersecurity in PA are broadly similar. This is borne out to the degree that the data when analysed showed the groups to have broadly similar views. This does not mean that the findings are representative of the cybersecurity situation in PA, as a lack of knowledge on a subject by all interviewees will still not give a clear view. Furthermore where the interviewees have no knowledge of an area such as cybersecurity, there is a high probability that their answers will not give a clear picture of potential risks. The analysis was difficult to perform due to the variety of ways in which the questions were answered by varying respondents.

The coding of the responses also revealed that there was a strong belief that there was very little need for cybersecurity as the respondents believed that there was very little that required security; and that the security that was extant was sufficient, due to it being employed in other areas. At no stage was the concept of insecurity of existing security raised. An example of this was that the respondents assume that due to GSM and Bluetooth communications being readily available, that they are therefore secure. The concept of upgrading software for enhancing security against known faults was also another area in which all respondents failed to express a view.

It also showed very clearly almost all participants felt that the data collected in PA belongs to the farmer and that they should have control of how it is used and any benefits accruing from its use in all cases.

Even when companies declined to respond (an autonomous vehicle start-up), this showed that security concerns had triggered a response. Initially they had been willing to co-operate, but later decided that "because our prototype robots won't apply to the final products, and we are unsure of the security implications of sharing information." Due to prior communications, I had been aware that this had not been a concern before; therefore I would infer that the enquiries I had been making about the security which they were intending to use had prompted them to look at the security aspects of their products. Therefore although there was only limited amounts of empirical data available as well as very limited time for the research, the data analysed supports the initial theory that cybersecurity in PA is poorly implemented. In many cases the analysis supports the belief that when development of PA devices has occurred cybersecurity has not been part of the design. The use of passwords to protect website enabled services does not prove the value of this as a security measure that has been specifically included. This is because any collection of personal data requires security to be implemented to protect that data. Thus the use of an ID and password to access it is a legal minimum requirement, as well as standard when developing interactive websites. Encryption

of data does not seem to have been given any thought when developing many systems, though one developer answered that they encrypt all personal data in storage and transmissions whilst deliberately leaving the remaining data in plain text. This was due its perceived value as being minimal and therefore of no consequence to require protection.

The results of the empirical data show that the growth in use of UAVs (aerial and land based) is not viewed as a risk to cybersecurity. They are seen as a potential Health and Safety risk should they act in an uncontrolled manner and cause damage to life or property, but they are not seen as a cybersecurity risk. Their use as an entry point into a farm network of other devices is not considered, but if they are standard drones or utilise insecure properties, they present an ideal point at which to exfiltrate data, corrupt data or networks or to commence an operation to subvert other devices.

The analysis seems to further bear out the theory that the PA industry views the industry as one which has little of value to target for cybersecurity exploits. The experiences of other industries would seem to belie this, as would the increasing number of exploits involving the IoT. As the industry grows and more connectivity occurs, so will the opportunities for cyber-attacks and cyber-related incidents to increase. These may be deliberate attempts to subvert or use systems, the case of badly written code or logic causing devices to malfunction or just devices being reused for purposes for which they were not initially designed (the use of an Xbox Kinect sensor in an external, inhospitable environment to pick broccoli (Kusuman et al., 2016) ).

## Results and Analysis

A common theme throughout the whole of this research project has been the lack of awareness about cybersecurity and its part in PA (see the charts on the previous pages). This stretches from the farmer using his PC to do the farm accounts, farm management Information system and emails without a password on the computer and no anti-virus *“because it is easier that way”* through to developers of new equipment who say *“Security has not been a hot topic at all recently as we are still getting the fundamental systems working.”* Whilst the major machinery manufacturers are employing only security where there is a regulatory requirement or a financial / sales advantage. The drive to develop new products has meant that the manufacturers of devices have avoided security considerations, relying on the components they re-use for security. This may be the encryption on the GSM network used to transfer data from devices to data stores, WiFi encryption for farm based devices, or Bluetooth security. Where the manufacturers have employed some forms of security, such as in ISOBus, this use of authentication serves the primary purpose of identifying and ensuring co-operation between devices. It is not to prevent unauthorised access to devices. All of these communication methods have been breached multiple times, GSM via poor standards (A5/2) and all the weaknesses of mobile phone handsets and base stations (Souppaya and Scarfone, 2013). WiFi attacks are common and can be orchestrated from a drone or via static attack using a cracked encryption key on weak encryption (WEP) or via cloning a device. Bluetooth is easily cracked also, without the application of additional security to the communications of these devices the devices cannot be considered secure. The end users of PA (farmers) should not need to be aware of the need to additionally secure products that they use, however they should be aware of the need for security awareness in the use of the technologies in PA. The manufacturers should however be engineering in security at the design stage, rather than finding themselves in a position where it is required later and so it must be added in as an adjunct to the design. This is much harder to maintain and will need potentially more attention than designed in cybersecurity.

When data such as crop spraying data is transferred to tractors this is often done by utilising an iPad as the transfer device. Once again this relies on security over which the manufacturer and user have little or no control; worse still is the use of USB devices which are completely un-validated and secure. The user should be made aware of the dangers associated with attaching devices such as USB dongles and iPads to PA devices, this danger may appear to be insignificant but if the devices are not authenticated and their data validated then they become an obvious attack surface. The connecting of multiple devices of varying origin and use to a common network also poses large problems, such networks should ideally be broken down into smaller subnets controlled by firewalls and other industrial network monitoring devices. Unfortunately these devices need skilled installation and maintenance which is not readily available in the PA environment, also they add additional costs for little perceived result.

The storage of data by the large companies is subject to the same data breaches that any other large data store is liable to. This data may not be immediately seen as financially valuable, but it may contain data which can be data mined to give forward market information by organisations with an interest. Alternatively it may be deleted or corrupted by agents (criminal, national or malicious) to cause disturbances to PA, or it might be used to disable devices such as tractors using telematics. The data which is collected and stored should be treated with the same care that financial data is, however the information about grain yields,

nitrogen levels or tractor performance are not seen as being of such value. The rules on data storage (Publications Office of the European Union, 2016) in the EU apply to PA data in the same way that it applies to personal and financial data.

When a word cloud was created based on the frequency of code words appearing in the analysis of the collected data, the theme that is most obvious is one where the security employed is currently adequate. The most common codes are “sufficient”, “encrypted”, “no threat”, no/idea” and “manual Control”. None of the main codes are alarmist, even where “no idea / no opinion” is used this is in preference to a perceived risk. The common use of “manual control” further shows the belief that there are no hidden issues with security, because if something untoward occurs then “manual control” of the device concerned will be assumed. The industry needs to be made aware of the dangers as well as the benefits of increased use of technology in PA, the need for redundancy in operations and methods to improve the cybersecurity of PA.



*Figure 15 Word cloud of code words*



## Discussion and Conclusions

The contribution to existing literature from this thesis is difficult to quantify as there is currently little available literature specifically on the subject of cybersecurity in PA (Mutschler and Department of Homeland Security, 2018; Publications Office of the European Union, 2018c). There is a growth in interest in this subject though, as it is a part of a nation's critical infrastructure. The need to safely produce food without interruption and to optimal ability is paramount, anything that interferes with this should be investigated and acted upon.

The thesis has helped in the expansion of the awareness of the risks associated with PA. It has shown that a number of areas that had not been connected previously are connected, the IoT has allowed this connectivity to accelerate a great rate. Concepts of cross infection or control from one area to another have been highlighted in this thesis (PC – USB – UAV or aerial drone – farm network - sensors). There are many different areas of PA, even in the small area investigated in this thesis (arable farming in the UK) but there are many concepts and ideas which are applicable other areas of PA. These might be in the dairy industry with automated feeding, herd monitoring and milking; or in the horticulture industry with hydroponics, their associated highly sensor oriented activities in greenhouses. In other parts of the world, the principles of cybersecurity awareness apply to cotton growth, rice production or other cash crops. The research I conducted also showed that manufacturers and start-ups are quite prepared to use existing technologies in the production of new devices. These devices will be susceptible to the faults of their initial use, as well as any new ones from their repurposing, they may not receive upgrades and may introduce cybersecurity risks to areas which were previously unaffected. The thesis has tried to highlight just a few areas where there may be concerns over cybersecurity such as in the use of UAVs, sensors on farms, data privacy / storage / transmission / ownership, the dangers of ignoring cybersecurity in the wake of growing exploitation by criminal and nation state agencies using AI to forward their campaigns.

Further, the contribution to practice from this thesis is that a number of manufacturers have been prompted into looking into their practices and seeing that cybersecurity in PA is an area on which they need to concentrate. They had not looked at their products as being targets for cybersecurity, or as being subject to the needs of data ownership issues and data corruption or being deliberately hijacked to cause damage as in UAVs either by physical destruction or by over/under application of substances to crops. The desire of many companies not to participate in the research because it was into the security of their products may have prompted them to look at their own product's security. The withdrawal of one company from the survey process may have been a result of their desire to conceal their products security features, or conversely it may have highlighted their lack of consideration of cybersecurity in the development of a highly funded, premium UAV device.

In addition, the contribution to management from this thesis is an awareness that **cybersecurity needs to be designed in as part of the design process of a product**. In the research conducted, only one company contacted saw the dangers of failing to design security into their product from the outset. Another factor in the management of cybersecurity in PA is that although many of these attack vectors appear to be theoretical and are regarded by many in the development of products and their users as being highly unlikely to be exploited, it shows that there are very large risks involved in ignoring them. This may be because the exploitation of these risks is seen as being uncertain and difficult to execute, their perceived lack of reward or the observers ignorance of potential dangers and risks. It also helps to show

some of the areas that require further investigation, such as the collection of PA data by large companies such as John Deere, grain merchants and fertiliser companies. This large scale data collection should be viewed as any valuable resource, and so should be protected and managed carefully and its rightful owners rewarded appropriately.

The lack of cybersecurity awareness was borne out in the conversations that occurred where the interviewees were frequently dismissive of the need for the research, though they understood the concepts of cybersecurity as much as it related to hacking computer systems and phishing emails. The frequent part of any reply was that there would be no point in attacking PA as there was little to be gained,

However the 3 farming respondents' data collection details show that there is a significant amount of data collected. The respondents were two medium sized farms, one utilising the technologies of PA whilst the other felt that the technology was not cost efficient or advanced enough to justify full investment in it. The third farm was a medium to large farm, where the technology was employed where a benefit could be seen to come from implementation. Unfortunately the data from a large farmer was not available for unforeseen reasons, however the initial conversations indicated that they were much more welcoming to the technology and were employing on a much broader scale. This data has the potential to be of great value to large manufacturers and commodity dealers as it would afford a great market advantage, with the knowledge of the yield being obtained by farmers before it was available for sale it would be possible for a trader to manipulate the markets by forward purchases at a favourable price to them. This would be because of their advance notice of crop yields for that harvest period ahead of the rest of the markets. This data used in such a way would be illegal unless ownership of the data could be proved to rest with the trading company and not the farmer, or that the farmer had granted use of the data. This action would however be illegal as "insider trading" if discovered. Even if it was not used in this way, the use of large data could reveal trends which could legally be acted upon, such as high wear on engines discovered by telematics. This could be acted upon and resolved before the engine problems became publicly known as cases of engine failure. It also has the potential to be turned against farmers in an individual attack using their data to provide the basis for introducing corrupted data back into their systems. Ultimately data ownership that is collected will depend on any agreements signed or implemented when the devices are sold, as manufacturers could make it a condition of sale that they hold ownership of data (Deere and Company, 2015).

Many developers are working on PA devices and there are many devices in use, but it appears that the majority of them have taken existing technology and have reused it without consideration of any security implications. This is compounded by developers who feel that they are too busy with Research and Development to deal with the additional burden of security. The feeling that any additional security, or that PA is a potential target, is reflected across both users and manufacturers. An awareness of any potential risks is not something that has been considered as an issue by PA participants, their focus is solely on the agricultural elements.

Multi-national companies such as CASE IH, Claas, John Deere and AGCO all have large research departments which are involved in the development of integrated technological products using connectivity via various communication methods (wireless, wired and intermittent connection). These departments will have a technical knowledge, as well as a legal pressure, behind them to ensure that as far as is practical they will not have any faults in

their products. However even here there appears to be little incentive to utilise fully secure connections, data transfer and on-board storage unless it is legally mandated – otherwise the minimum cybersecurity requirements will be met. This may be due to the costs involved, user disinterest, limitations of the hardware, software or methods / protocols employed. All of these factors can compromise the cybersecurity of PA products even if there is a desire to implement a secure product. There may also be issues with data collection under the terms of GDPR (Publications Office of the European Union, 2016) as the collection of certain types of data may contravene the Act. These would be data which allows the identification of an individual or is part of a special category personal data, furthermore it could be a photographic record as recorded by a sensor. This could potentially contravene GDPR if used without consent and if it was not stored in a secure manner. This makes the collection of any data which involves human interaction much more complex. Furthermore the collection of data under GDPR must be done in such a way that all data stored is demonstrably secure, failure to do so is subject to large fines. There is also the issue that under GDPR any company developing a new product which collects data should perform a data protection impact assessment (DPIA), this constitutes additional cost. It would not apply to companies who were not developing products for use in countries covered by GDPR (e.g. USA, China) and so could give them an economic advantage in developing products over those developed in the EU for international sale.

The research approach that I adopted was flawed in its implementation, although the concept of it was sound. The literary review was highly successful in the main, and I was able to add to it as I progressed in my research. The more detailed and focused my research became the more relevant papers I discovered, this was useful in further refining my focus and my research target to a focus on just the areas covered in this thesis, rather than the broader concept of all PA elements in all areas of agriculture globally.

I concentrated very heavily on the literature review at the outset and did not do enough work on the preparation of my empirical data research. I should have been doing more research on suitable companies earlier, I should have made more use of personal contacts globally to gain access to companies who might have been more willing to impart information after a personal introduction. The need to introduce the subject of cybersecurity research to a company with no assurances of identity definitely made it harder. Companies had no reason to believe that the enquiry was not from someone wanting to obtain sensitive security data with which to compromise their product, or from a competitor looking to gain a commercial advantage by inside knowledge of a competitor's security. Once I had contacted and spoken with two respected academic individuals in the field and they had given me contact details, I was able to use this to help allay fears of the companies I contacted in many cases. This was made even easier after initial contact by being able to talk competently about both agricultural practices and cybersecurity. I believe that if I had been able to meet contacts face to face this would have been easier too, but unfortunately I was unable to travel to events which would have allowed this. Being restricted to telephone or email for contacts certainly made the research more complicated.

I also believe that it would have been easier if I had been able to secure a method of accessing research books and papers locally. As I was not located in Sweden I was unable to fully use the University's library facilities. This meant certain books and papers I wished to use for

research were not available and that I had to find alternative methods to gain access to the data which could be time consuming and difficult or locate alternative source material.

The process of coding the data collected was also much more complex than I had envisaged, I also had to try and learn a computer assisted qualitative data analysis software (CAQDAS) whilst I was learning the principles of coding and analysis. Once I had mastered the basics of the CAQDAS program that I used - QDA Miner Lite (Provalis Research, 2016). I found this a very effective program once I understood how it worked and it greatly speeded up the coding and analysis of the data.

Retrospectively another approach to the questioning would have been preferable, concentrating on the individual groups. The responses could have been analysed in groups and then the themes brought together to give more precise results. If I had been aware of the capabilities of QDA Miner Lite before I could have structured the questioning in a better manner. I would have focused more specifically on the specialities of each subject with a number of general questions common to all respondents at the end of the questions. I do believe that using the literature review to structure the questions was the correct way to approach this, as was the method of reviewing the questions in the light of each new response received. This did mean that I was able to refine my questioning in order to obtain clearer replies, without guiding the individual replying.

Research into cybersecurity is a much broader subject than I had envisioned when I began to prepare my initial thesis proposal. I had initially thought that it would just involve a few companies and farmers. Instead I now realise that the spread of PA is huge and cybersecurity is an integral part of it all. The issue is that most of the people involved in it are not aware of the dangers associated with it, as I have outlined in my thesis most of the developers are busy developing and the manufacturers are busy trying to sell. The idea of spending research time and money on preventing damage to their products and the security of their users is not a premium issue for them. The conclusion of my thesis has been that there is a need for much greater awareness of the need for cybersecurity amongst both users and developers and manufacturers of PA. There is also a need for greater care of data in all forms – creation, transmission, definition of ownership, usage and storage. A much greater awareness of the risks of interconnectivity needs to be communicated to ensure that the cybersecurity risks of PA are met. Unfortunately farmers tend to be a very traditional group who are slow to adopt new methods unless they can see a positive or financial benefit from a new development – as one farmer said about the benefits of field mapping data “It’s nice to have...and it brightens up the walls”.

I think that the areas of UAVs will increase in certain parts of PA, but in varying ways and these will be widely determined by the crops. Where arable crops are being grown, then large machines may remain to heavy duty jobs such as ploughing (if minimal cultivation is not adopted) and harvesting, however soil and field mapping may be done by aerial drones, satellites and soil sensors with small UAVs (aerial or terrestrial) weeding and applying fertilisers only to those plants requiring them. If this is to occur successfully then the needs of cybersecurity need to be impressed on developers now, and not as remedial measures once attacks on devices have begun via IoT or devices (USB devices / iPads) introducing malware directly. The costs of provisioning devices at design are likely to be substantially less than the costs of remedial cybersecurity measures, there will also be less loss in confidence in the devices if remedial action is not required. A one off design will not be enough and there

should be ways of upgrading the devices to combat innovations in cyber-attacks and faults. A method of doing this would be to look at the potential areas of high risk or high value areas at risk, then to concentrate on determining the threats to these areas. The methods that would be used to exploit these areas could then be the subject of further research and this data supplied to the manufacturers, either as a consultancy or as a benefit of co-operation in research. This would then ensure its integration into devices, whilst ensuring that development of cybersecurity continued in parallel with the development of products. All parties involved would then benefit, and if it was an open source project the common shared data would benefit all and lead to more rapid development of countermeasures and new protective practices. This could be potentially linked to work with bodies such as the Agricultural Industry Electronics Foundation (AEF) developing the ISOBus standard to greater levels of security, and compatibility. Compatibility is an area of concern in cybersecurity in PA as different manufacturers have different interpretations of the standards. These incompatibilities may lead to risks which can be exploited to circumvent the cybersecurity being employed.

Each area I have looked at is worthy of research on its own, my work has only given a very high level overview, if the areas were looked at in detail then there information produced which could be used to improve those specific areas. Although there would be levels of cross-fertilisation of ideas. It could be that the development of an aspect of cybersecurity in one area would not be applicable in another, unfortunately until the research is done this could not be ascertained as a certainty.

Regarding generalisability, the results in this thesis concerning early design incorporation can be generalised and used by any industry developing IoT or products which involve technology and connectivity. What is needed to be done to that is manufacturers need to be made aware of the costs and problems involved in developing cybersecurity after the release of a product. It is harder to update a product after it is released as you rely on customers, the development is an additional cost that must respect the existing architecture without compromising it. These are examples of some of the problems that can be experienced by failing to include cybersecurity at the design stage.

Another area which is can be generalised to apply elsewhere is the need for data control, this is already a recognised problem in many established industries and commercial activities. However in developing, new applications of technology the impact of data collection may well be overlooked. In areas where the data has high value it must be protected at all times to prevent corruption, theft, unauthorised use and disruption of the data. This involves securing the collection of it by the sensors, transmission of it, storage and ultimate use of it as information. The ownership of the data should also be established at a very early stage, as this can have a large bearing on its value and to whom the benefits of it accrue, both financially and as part of the core business .e.g. crop yield for future evaluation or telematics data.

In a conversation with an oil company executive I discovered that even though the oil refinery data has been secured in refineries, technology still played a part in extracting data for potential advantage to competitors. The deployment of aerial drones to look into storage bunkers meant that new methods had to be employed to prevent data collection through other technical methods.

A final area that is already broadly accepted as a danger in many institutions is that of device corruption and extortion, PA is also a fertile area for this to be applied as the lack of knowledge to combat this is prevalent in the PA field. This must be addressed and this will also apply to many other developing industries utilising technology, sensors, connectivity and IoT devices.

Thus, my recommendations to those involved in PA are that there is a need to look at the cybersecurity involved in PA. Even though PA has so far not been seen as a target due to perceived poor returns on investment in breaching PA cybersecurity and exploiting the devices used, this is a false view. The industry has commercial and strategic value much like many other industries that have already been subject to exploits, to ignore this is foolhardy. Pa needs to look at its cybersecurity practices now before the industry is the subject of exploits. The sheer variety of potential attack surfaces and the consequences of failing to secure them needs to be highlighted to those involved. Many people I talked to had never considered that any form of cybersecurity might be needed or that it could affect their working practices and finances.

“It is no use securing the stable door once the horse has bolted.” as the English saying goes, make cybersecurity a priority before it is required and not after.

We often think that the use of measures such as encryption, validation and other methods to secure devices makes them invulnerable, but as Cory Doctorow said of Schneier's Law: "any person can invent a security system so clever that she or he can't think of how to break it." (Cory Doctorow, 2004). An item that is secure in one application in industry, may not be secure when adapted for use in PA. In his work on PA vulnerability, West states that “there are two types of PA systems: those that have been hacked and those that will be” (West, 2018), While this may overstate the case, it does show the need for further research on this topic. By not including security in the development of products, manufacturers may well find that they are then playing a catch up game as their products are attacked and they try to find ways to protect them.

## Appendix A

### Interview Guide

The interview plan that was used for conducting interviews followed the format below to ensure consistency of information. It did however include

#### ❖ **Introduction**

- Who I am.
- Why I am doing interviews.
- Aims of research.
- How the data will be used.
- Is anonymity required?

#### ❖ **Organisation and Interviewee Information**

- Name of Organisation
- What does the Organisation do
- Name of Interviewee
- Role within Organisation
- Relevant experience/awareness to security issues, if any

#### ❖ **Products and Clients**

- What does the organisation produce?
- Who do they sell to (Industry or End user)?
- What do the products do?

#### ❖ **Product Composition**

- Are the products made utilising components from other commercially available devices?
  - Have there been any known security issues with the components utilised?
- Have there been any developments in your device to secure it from external factors?
- Does the product communicate with other?
- If so, how is communication secured?
  - Is this proprietary
    - Was security considered during development?
    - How has security been tested?
  - Commercial
    - Have all suggested security updates and upgrades been applied?
- Is there a policy to apply security/functional upgrades?

#### ❖ **Product Operation**

- Can it run autonomously?
  - What security is involved?
- Are there any failsafes?
  - Does it have backup systems
- Is it secured against interference – physical, radio-magnetic or other communication mediums?

#### ❖ **Security Issues**

- Have any security issues arisen or been addressed in development?
- What provision is there for dealing with security issues?
- If data is collected,
  - How is it secured/encrypted?

- Is it transmitted or collected internally for downloading?
- ❖ **Conclusion**
  - Thank interviewee and their company.
  - Offer to provide a copy of anonymised thesis if they would be interested.



## Appendix B

### Survey questions

These were designed to be used to supplement any interview data. There were two formats used, the first was for companies that I had spoken to or had previous contact with. The second form was sent to those companies with which I had had no prior contact with an explanatory of note.

## Format 1

### *Questions on Security in Precision Agriculture*

#### Vehicles

1. *Are communications transmitted by devices secure (encryption, validated)?*

---
2. *What methods should be employed for fault tolerance in devices?*

---
3. *How should redundancy be implemented?*

---
4. *What should occur in the event of device failure and shortfall of substitute devices?*

---
5. *Is GPS the only option, or can autonomous systems be employed (weather, dirt and irregular landscape permitting)?*

---
6. *What prevents physical interference with autonomous vehicles?*

---
7. *If the device is compromised, what effect will this have on the other devices and safety?*

---

#### Data Management and storage

8. *Has the introduction of General Data Protection Regulation (GDPR) affected data management within Precision Agriculture?*
9. *Is all data stored and communicated in encrypted forms?*
10. *Some devices have minimal computing facilities e.g. sensors, should these communicate data in clear form?*
11. *Should data be retrieved from sensors purely by connecting an ordinary device (USB, unsynchronised iPad etc.) or should authorisation required?*
12. *Should data be stored in the EU, or in data stores which may be located outside the EU?*
13. *Who should own the data generated, the farmer, services providers or equipment suppliers e.g. Claas, John Deere, Yara?*
14. *If data is moved between devices (USB, WiFi, Bluetooth, ISObus) should it be encrypted and validated?*

### GPS and RTK

15. Do you perceive any dangers from using RTK (hacking, false data, data theft)?

---

16. What happens if the RTK is corrupted or fails?

---

17. A GPS system may allow monitoring and immobilisation, what protections are there against these facilities being used for extortion, corruption or to cause damage?

---

18. What prevents field mapping data being corrupted, are checksums used to verify integrity?

---

### Sensors

19. If you use GSM communication between devices, does this offer sufficient security or is it supplemented?

---

20. If you use WiFi communication between devices, does this offer sufficient security or is it supplemented?

---

21. If you use Internet communication between devices, does this offer sufficient security or is it supplemented?

---

22. If you use a Website to control/monitor devices,

a. Do you use passwords or similar?

---

b. Does this offer sufficient security or is it supplemented?

---

c. Is the connection using HTTPS and is data held in encrypted form?

---

d. Do you monitor how / when / where logins occur?

---

e. If apps are used (IOS / Android), what security is employed?

---

23. How do sensors register with base stations, is it automatic, pre-set or manual?

---

24. What occurs in the event of a sensor failure?

---

### General

25. Is the growth of Precision Agriculture a technological security risk that is waiting to be exploited (Agriculture is listed as part of the Nations critical infrastructure, the USA has a security policy for this already)?

26. *Are there other security risks in Precision Agriculture (tractors crashing, lack of fail over in the event of a sensor failure)?*

---

27. *If a company has large amounts of farm data, which is of little use to individuals but in volume is useful to predict or manipulate markets and their prices, is this a security risk?*

---

28. *Are systems secure against activists (criminal or ideological) – hacking or physical access to systems?*

---

29. *Is user security awareness and training in Precision Agriculture needed (Malware in an email could lead to systems being corrupted or destroyed if they are connected in any way)?*

---

30. *Is the security in products adapted for agriculture (GPS, Drones, Industrial sensors etc.) sufficient or is additional security needed?*

---

*I am from a farming family in East Anglia, and I am doing a Master's thesis on the security aspects of Precision Agriculture.*

*Agriculture is seen as part of the nation's critical infrastructure, but little attention is paid to the vulnerabilities it is susceptible to in the same way as any other industry. Criminal gangs, countries security agencies and malicious hackers are all potential exploiters of technology used in agriculture.*

*All the data I collect is anonymised, and no individuals or companies named unless they specifically request acknowledgement; however I am exceptionally grateful for any replies to my queries.*

## Format 2

No.	Enquiry	Reply
1	<i>Does your device utilise components from other commercially available devices? (Please give generic device name if possible) e.g. a motion sensor from a games machine or pointing device, a flow control from an automated valve.</i>	
2	<i>Have there been any developments in your device to secure it from external factors? e.g. Bolting devices inside a secure casing, implementing software isolation.</i>	
3	<i>Does your device communicate with other devices or controllers via radio communication or other optical / audio communication methods? e.g. Bluetooth, WiFi, telephone network, infra-red sensor or audio sensor</i>	
4	<i>Are there fail safe systems in place in case of a system fault? e.g. Shutdown if communication is lost, or return to base if no input is received.</i>	
5	<i>Can the system run autonomously? e.g. without any operator input</i>	
6	<i>Are you aware of any potential security problems which you have had to address? e.g. Radio interference or password security of programs</i>	
<p><i>I am from a farming family in East Anglia, and I am doing a Master's thesis on the security aspects of Precision Agriculture.</i></p> <p><i>Agriculture is seen as part of the nation's critical infrastructure, but little attention is paid to the vulnerabilities it is susceptible to in the same way as any other industry. Criminal gangs, countries security agencies and malicious hackers are all potential exploiters of technology used in agriculture.</i></p>		

*All the data I collect is anonymised, and no individuals or companies named unless they specifically request acknowledgement; however I am exceptionally grateful for any replies to my queries.*

## Appendix C

### Initial research plan

<b>Date</b>	<b>Activity</b>	<b>Resource</b>
<b>November</b>	Prepare and submit Thesis proposal	Relevant research papers
<b>December – April</b>	Research further literature and global contacts. Perform literary reviews. Approach companies / organisations involved in relevant areas to secure interviews or further related data. Data collection.	Find further research papers, internet searches, investigation of organisations.
<b>January</b>	Investigate methods to be pursued for analysis. Decide on research method.	Utilise information from previous courses. Review research method papers
<b>January – April</b>	Perform any interviews. Review collected data.	Interact with organisations.
<b>February – April</b>	Collate data collected and rationalise it. Refine the data and review, then repeat. Ensure that analysis of data is complete, relevant and complete.	Research papers, and internet searches. Books (if accessible).
<b>May</b>	Formalise the theory. Ensure that all relevant data is included. Verify that all information to be used is correct.	
<b>Mid-May</b>	Prepare and review drafts of thesis. Finalise data and complete thesis formulation. Write final draft.	Review with colleagues
<b>Late May submission date</b>	Submit thesis for review and defence.	

## Bibliography

- Basu, S., Omotubora, A., Beeson, M., Fox, C., 2018. Legal framework for small autonomous agricultural robots. *AI Soc.* <https://doi.org/10.1007/s00146-018-0846-4>
- Bergmann, K.P., Denzinger, J., 2013. Testing of precision agricultural networks for adversary-induced problems, in: *Proceeding of The 15th Annual Conference on Genetic and Evolutionary Computation (GECCO '13)*. ACM, Amsterdam, The Netherlands, pp. 1421–1428. <http://dx.doi.org/10.1145/2463372.2463544>
- Bunse, C., Plotz, S., 2018. Security Analysis of Drone Communication Protocols, in: Payer, M., Rashid, A., Such, J.M. (Eds.), *Engineering Secure Software and Systems*. Springer International Publishing, pp. 96–107.
- Burakova, Y., Hass, B., Millar, L., Weimerskirch, A., 2016. Truck Hacking: An Experimental Analysis of the SAE J1939 Standard, in: *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association, Austin, TX.
- Capgemini Consulting, Wageninngen UR, 2016. Cybersecurity in the agrifood sector.pdf [WWW Document]. Cybersecurity Agrifood Sect. URL [https://www.wur.nl/upload\\_mm/4/6/a/f74a893e-c829-4bf3-9884-e357929ff5d6\\_Cybersecurity%20in%20the%20agrifood%20sector.pdf](https://www.wur.nl/upload_mm/4/6/a/f74a893e-c829-4bf3-9884-e357929ff5d6_Cybersecurity%20in%20the%20agrifood%20sector.pdf) (accessed 3.15.19).
- CEMA - European Agricultural Machinery, 2017. Digital Farming: What does it really mean? [WWW Document]. URL <https://www.cema-agri.org/publication/position-papers/254-digital-farming-what-does-it-really-mean> (accessed 3.17.19).
- Chae, C.-J., Cho, H.-J., 2018. Enhanced secure device authentication algorithm in P2P-based smart farm system. *Peer--Peer Netw. Appl.* 11, 1230–1239. <https://doi.org/10.1007/s12083-018-0635-3>
- Chi, H.( 1 ), Welch, S.( 2 ), Vasserman, E.( 2 ), Kalaimannan, E.( 3 ), 2017. A framework of cybersecurity approaches in precision agriculture, in: *Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017*. Presented at the Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017, Academic Conferences and Publishing International Limited, pp. 90–95.
- Choudhary, G., Sharma, V., You, I., Yim, K., Chen, I.-R., Cho, J.-H., 2018. Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey.
- Cory Doctorow, 2004. Cory Doctorow: Microsoft Research DRM talk.
- D. He, Y. Bai, Y. Wang, H. Wu, 2007. A Crop Field Remote Monitoring System Based on Web-Server-Embedded Technology and CDMA Service, in: *2007 International Symposium on Applications and the Internet Workshops*. Presented at the 2007 International Symposium on Applications and the Internet Workshops, pp. 72–72. <https://doi.org/10.1109/SAINT-W.2007.6>
- D. Puthal, X. Wu, S. Nepal, R. Ranjan, J. Chen, 2018. SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams. *IEEE Trans. Big Data* 1–1. <https://doi.org/10.1109/TBDATA.2017.2702172>
- Deere and Company, 2015. Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201.
- Drost, E.A., al., 2011. Validity and reliability in social science research. *Educ. Res. Perspect.* 38, 105.
- Dunn, J.E., 2013. Chinese Malware Targeted U.S. Drone Secrets, Security Firm Alleges [WWW Document]. CIO. URL <https://www.cio.com/article/2388604/chinese-malware-targeted-u-s--drone-secrets--security-firm-alleges.html> (accessed 3.19.19).



- Edwards, R., Holland, J., 2013. What is Qualitative Interviewing?, The “What is?” Research Methods Series. Bloomsbury Publishing.
- Fan, X., Susan, F., Long, W., Li, S., 2017. Security Analysis of Zigbee 18.
- Federal Bureau of Investigation, Cyber Division, 2016. Smart farming may increase cyber targeting against US food and agriculture sector. (Notification No. 160331–001). Federal Bureau of Investigation, Cyber Division.
- Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., yi, W., 2018. An Efficient UAV Hijacking Detection Method Using Onboard Inertial Measurement Unit. <https://doi.org/10.1145/3289390>
- Ferris, J., 2017. Data Privacy and Protection in the Agriculture Industry: Is Federal Regulation Necessary? *Minn. J. Law Sci. Technol.* 18, 309.
- Fountas, S., Blackmore, S., Ess, D., Hawkins, S., Blumhoff, G., Lowenberg-Deboer, J., Sorensen, C.G., 2005. Farmer Experience with Precision Agriculture in Denmark and the US Eastern Corn Belt. *Precis. Agric.* 6, 121–141. <https://doi.org/10.1007/s11119-004-1030-z>
- Fountas, S., Kyhn, M., Jakobsen, H.L., Wulfsohn, D., Blackmore, S., Griepentrog, H.W., 2008. A systems analysis of information system requirements for an experimental farm. *Precis. Agric.* 10, 247. <https://doi.org/10.1007/s11119-008-9098-5>
- Garcia-Sanchez, A.-J., Garcia-Sanchez, F., Garcia-Haro, J., 2011. Wireless sensor network deployment for integrating video-surveillance and data-monitoring in precision agriculture over distributed crops. *Comput. Electron. Agric.* 75, 288–303. <https://doi.org/10.1016/j.compag.2010.12.005>
- Geil, A., Sagers, G., Spaulding, A.D., Wolf, J.R., 2018. Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *Int. Food Agribus. Manag. Rev.* 21, 317–334. <https://doi.org/10.22434/IFAMR2017.0045>
- Giesler, S., 2019. Digitisation in agriculture - from precision farming to farming 4.0 - Bioeconomy [WWW Document]. *Digit. Agric. - Precis. Farming Farming 40 - Bioeconomy*. URL <https://www.biooekonomie-bw.de/en/articles/dossiers/digitisation-in-agriculture-from-precision-farming-to-farming-40/> (accessed 3.17.19).
- Gorman, S., Dreazen, Y.J., Cole, A., 2009. Insurgents Hack U.S. Drones. *Wall Str. J.*
- Grgic, K., Zagar, D., Krizanovic, V., 2013. Security in IPv6-based wireless sensor network - Precision agriculture example, in: *Proceedings of the 12th International Conference on Telecommunications, ConTEL 2013*. Presented at the Proceedings of the 12th International Conference on Telecommunications, ConTEL 2013, pp. 79–86.
- H. Sedjelmaci, S. M. Senouci, N. Ansari, 2018. A Hierarchical Detection and Response System to Enhance Security Against Lethal Cyber-Attacks in UAV Networks. *IEEE Trans. Syst. Man Cybern. Syst.* 48, 1594–1606. <https://doi.org/10.1109/TSMC.2017.2681698>
- Ham, W., Enkhbaatar, T., Luubaatar, B., Hyeokjae, K., 2017. DESIGN AND IMPLEMENTATION OF VIRTUAL TERMINAL BASED ON ISO11783 STANDARD FOR AGRICULTURAL TRACTORS 12.
- Health and Safety at Work etc. Act 1974, 2019.
- Helil, N., Rahman, K., 2017. CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy [WWW Document]. *Secur. Commun. Netw.* <https://doi.org/10.1155/2017/2713595>
- I. Mampentzidou, E. Karapistoli, A. A. Economides, 2012. Basic guidelines for deploying Wireless Sensor Networks in agriculture, in: *2012 IV International Congress on Ultra Modern Telecommunications and Control Systems*. Presented at the 2012 IV International Congress on Ultra Modern Telecommunications and Control Systems, pp. 864–869. <https://doi.org/10.1109/ICUMT.2012.6459783>

- International Standard, 2015. ISO 11783-10:2015(en), Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 10: Task controller and management information system data interchange [WWW Document]. URL <https://www.iso.org/obp/ui/#iso:std:iso:11783:-10:ed-2:v1:en> (accessed 3.17.19).
- International Standard, 2011. ISO 11783-11:2011(en), Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 11: Mobile data element dictionary [WWW Document]. URL <https://www.iso.org/obp/ui/#iso:std:iso:11783:-11:ed-2:v1:en> (accessed 3.17.19).
- Jacob Bunge, 2014. Big Data Comes to the Farm Sowing Mistrust. Wall Str. J.
- Jamal Raiyn, 2018. Data and Cyber Security in Autonomous Vehicle Networks. Transp. Telecommun. J. 19, 325–334. <https://doi.org/10.2478/ttj-2018-0027>
- Jansen, H., 2010. The Logic of Qualitative Survey Research and its Position in the Field of Social Research Methods. Forum Qual. Sozialforschung Forum Qual. Soc. Res. 11. <https://doi.org/10.17169/fqs-11.2.1450>
- Jerry Revich, Robert D. Boroujerdi, Hugo Scott-Gall, Patrick Archambault, Robert Koort, Michael Nannizzi, Mohammed Moawalla, Jesse Hulsing, Noah Poponak, Stefan Burgstaller, Yuichiro Isayama, Andrew Bonin, David Tamberrino, Jay Yang, Brooke Roach, Mathew Porat, Lincoln Kong, Deepshikha Agarwal, Gautam Pillai, Christopher Evans, Ryan Berney, Drew Cohen, Gungun Verma., 2016. Precision Farming: Cheating Malthus with Digital Agriculture 43.
- Johnsson, J., Altheide, D.L., 2011. 'Criteria for Assessing Interpretive Validity in Qualitative Research', in: Denzin, N.K., Lincoln, Y.S. (Eds.), The SAGE Handbook of Qualitative Research. SAGE, Thousand Oaks, CA, pp. 485–499.
- Jordan, K., 2018. Validity, Reliability, and the Case for Participant-Centered Research: Reflections on a Multi-Platform Social Media Study. Int. J. Hum.-Comput. Interact. 34, 913–921.
- K. Pärilin, M. M. Alam, Y. Le Moullec, 2018. Jamming of UAV remote control systems using software defined radio, in: 2018 International Conference on Military Communications and Information Systems (ICMCIS). Presented at the 2018 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–6. <https://doi.org/10.1109/ICMCIS.2018.8398711>
- Keshtgari, M., Deljoo, A., 2012. A Wireless Sensor Network Solution for Precision Agriculture Based on ZigBee Technology. <https://doi.org/10.4236/wsn.2012.41004>
- Kim, S., Lee, M., Shin, C., 2018. IoT-Based Strawberry Disease Prediction System for Smart Farming. Sensors 18, 4051. <https://doi.org/10.3390/s18114051>
- Kritikos, M., 2017. Precision agriculture in Europe: Legal, social and ethical considerations - Think Tank (No. PE 603.2017). European Parliament.
- Kusuman, K., Krajnik, T., Pearson, S., Cielniak, G., Duckett, T., 2016. Can you pick a broccoli? 3D-vision based detection and localisation of broccoli heads in the field. IEEEERSJ Int. Conf. Intell. Robots Syst. IROS.
- Li, A., Qingqing, W., Rui, Z., 2019. UAV-Enabled Cooperative Jamming for Improving Secrecy of Ground Wiretap Channel. <https://doi.org/10.1109/LWC.2018.2865774>
- Marshall, P., McKay, J., 2001. The dual imperatives of action research. Inf. Technol. People 14, 46–59. <https://doi.org/10.1108/09593840110384771>
- Mårtensson, P.-Å., Hedström, L., Sundelius, B., E. Skiby, J., Elbers, A., Knutsson, R., 2013. Actionable Knowledge and Strategic Decision Making for Bio- and Agroterrorism Threats: Building a Collaborative Early Warning Culture. <https://doi.org/10.1089/bsp.2013.0039>

- Mason, J., 1994. Linking Qualitative and Quantitative Data Analysis., in: *Analyzing Qualitative Data*. London and New York:, Lancaster U, pp. 89–110.
- Miles, M.B., Huberman, A.M., Huberman, M.A., Huberman, M., 1994. *Qualitative data analysis: An expanded sourcebook*. sage.
- Mohan, M., 2016. *Cybersecurity in drones (M.S.)*. Utica College, United States -- New York.
- Moran, M.S., Inoue, Y., Barnes, E.M., 1997. Opportunities and limitations for image-based remote sensing in precision crop management. *Remote Sens. Environ.* 61, 319–346. [https://doi.org/10.1016/S0034-4257\(97\)00045-X](https://doi.org/10.1016/S0034-4257(97)00045-X)
- Mueller, R., 2012. Robert Mueller RSA Cyber Security Speech 2012.
- Murvay, P., Groza, B., 2018. Security Shortcomings and Countermeasures for the SAE J1939 Commercial Vehicle Bus Protocol. *IEEE Trans. Veh. Technol.* 67, 4325–4339. <https://doi.org/10.1109/TVT.2018.2795384>
- Mutschler, P., Department of Homeland Security, 2018. Threats to Precision Agriculture. (6) 2018 Public-Private Analytic Exchange Program 25.
- Nerpel, D., Ellsworth, J., Hunt, A., 2016. Modus: A standard for big data, in: *Proceedings of the 13th International Conference on Precision Agriculture*. Presented at the Proceedings of the 13th International Conference on Precision Agriculture, International Society of Precision Agriculture, St. Louis, Missouri, USA, p. 4.
- Niglia, A., 2016. *Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges*, NATO Science for Peace and Security Series, D, Information and Communication Security. IOS Press, Amsterdam, Netherlands.
- Noble, H., Smith, J., 2015. Issues of validity and reliability in qualitative research. *Evid. Based Nurs.* 18, 34–35. <https://doi.org/10.1136/eb-2015-102054>
- Norris, J., 2015. Precision Agriculture: separating the wheat from the chaff | Nesta [WWW Document]. *Precis. Agric. Separating Wheat Chaff*. URL <https://www.nesta.org.uk/blog/precision-agriculture-separating-the-wheat-from-the-chaff/> (accessed 3.18.19).
- Nourian, A., Madnick, S., 2018. A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet. *IEEE Trans. Dependable Secure Comput.* 15, 2–13. <https://doi.org/10.1109/TDSC.2015.2509994>
- Papageorgas, P.G., Agavanakis, K., Dogas, I., Piromalis, D.D., 2018. IoT gateways, cloud and the last mile for energy efficiency and sustainability in the era of CPS expansion: “A bot is irrigating my farm..” Presented at the TECHNOLOGIES AND MATERIALS FOR RENEWABLE ENERGY, ENVIRONMENT AND SUSTAINABILITY: TMREES18, Beirut, Lebanon, p. 030075. <https://doi.org/10.1063/1.5039262>
- Pierluigi Paganini, 2013. *Hacking Drones ... Overview of the Main Threats* [WWW Document]. InfoSec Resour. URL <https://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/> (accessed 3.19.19).
- Pierpaoli, E., Carli, G., Pignatti, E., Canavari, M., 2013. Drivers of Precision Agriculture Technologies Adoption: A Literature Review. *Procedia Technol.* 8, 61–69. <https://doi.org/10.1016/j.protcy.2013.11.010>
- Primicerio, J., Di Gennaro, S.F., Fiorillo, E., Genesio, L., Lugato, E., Matese, A., Vaccari, F.P., 2012. A flexible unmanned aerial vehicle for precision agriculture. *Precis. Agric.* 13, 517–523. <https://doi.org/10.1007/s11119-012-9257-6>
- Provalis Research, 2016. *Free Qualitative Data Analysis Software | QDA Miner Lite*, QDA Miner Lite. Provalis Research.
- Publications Office of the European Union, 2018a. Precision agriculture and the future of farming in Europe : scientific foresight study. [WWW Document]. URL

- <https://publications.europa.eu/en/publication-detail/-/publication/40fe549e-cb49-11e7-a5d5-01aa75ed71a1/language-en> (accessed 3.17.19).
- Publications Office of the European Union, 2018b. European cybersecurity centres of expertise map : definitions and taxonomy. [WWW Document]. URL <https://publications.europa.eu/en/publication-detail/-/publication/07c5b4c0-b656-11e8-99ee-01aa75ed71a1/language-en/format-PDF> (accessed 3.17.19).
- Publications Office of the European Union, 2018c. Study on risk management in EU agriculture : final report. [WWW Document]. URL <https://publications.europa.eu/en/publication-detail/-/publication/5a935010-af78-11e8-99ee-01aa75ed71a1/language-en/format-PDF> (accessed 3.17.19).
- Publications Office of the European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.
- Shiravale, S., Bhagat, S., 2014. Wireless Sensor Networks in Agriculture Sector- Implementation and Security Measures. <https://doi.org/10.5120/16069-5217>
- Souppaya, M., Scarfone, K., 2013. Guidelines for Managing the Security of Mobile Devices in the Enterprise (No. NIST SP 800-124r1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-124r1>
- Subodh Bhandari, Amar Raheja, Robert L. Green, Dat Do, 2017. Towards collaboration between unmanned aerial and ground vehicles for precision agriculture. Presented at the Proc.SPIE.
- Swain, A., Jägerskog, A., 2016. Emerging Security Threats in the Middle East: The Impact of Climate Change and Globalization. Rowman & Littlefield.
- Swati Khandelwal, 2015. MalDrone — First Ever Backdoor Malware for Drones [WWW Document]. Hacker News — Cyber Secur. Hacking News Website. URL <https://thehackernews.com/2015/01/MalDrone-backdoor-drone-malware.html> (accessed 3.19.19).
- Sweeney, A., Allen, M., Cattanach, R., Delvo, mary K., 2016. Cyber Data Attacks: Are Farmers and Agribusiness Exempt?
- The Hands Free Hectare project completes second harvest [WWW Document], 2018. . Harper Adams Univ. URL <http://www.harper-adams.ac.uk/news/203288/the-hands-free-hectare-project-completes-second-harvest> (accessed 3.19.19).
- Tractor Implement Automation and its application to a tractor-loader wagon combination, n.d.
- Trancă, D., Pălăcean, A.V., Mihiu, A.C., Rosner, D., 2017. ZigBee based wireless modbus aggregator for intelligent industrial facilities, in: 2017 25th Telecommunication Forum (TELFOR). Presented at the 2017 25th Telecommunication Forum (TELFOR), pp. 1–4. <https://doi.org/10.1109/TELFOR.2017.8249409>
- U. Challita, A. Ferdowsi, M. Chen, W. Saad, 2019. Machine Learning for Wireless Connectivity and Security of Cellular-Connected UAVs. IEEE Wirel. Commun. 26, 28–35. <https://doi.org/10.1109/MWC.2018.1800155>
- Walle, A.H., 2015. Qualitative Research in Business : A Practical Overview. Cambridge Scholars Publishing, Newcastle upon Tyne, United Kingdom.
- Walter, A., Finger, R., Huber, R., Buchmann, N., 2017. Opinion: Smart farming is key to developing sustainable agriculture. Proc. Natl. Acad. Sci. U. S. A. 114, 6148–6150. <https://doi.org/10.1073/pnas.1707462114>

- West, J., 2018. A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. *J. Agric. Food Inf.* 19, 307–330.  
<https://doi.org/10.1080/10496505.2017.1417859>
- Wolfert, S., Ge, L., Verdouw, C., Bogaardt, M.-J., 2017. Big Data in Smart Farming – A review. *Agric. Syst.* 153, 69–80. <https://doi.org/10.1016/j.agry.2017.01.023>
- Yang, C., Everitt, J.H., Bradford, J.M., 2006. Comparison of QuickBird Satellite Imagery and Airborne Imagery for Mapping Grain Sorghum Yield Patterns. *Precis. Agric.* 7, 33–44. <https://doi.org/10.1007/s11119-005-6788-0>
- Zillner, T., 2015. ZigBee Exploited - The Good, the Bad and the Ugly. *Black HAt USA 2015* 8.