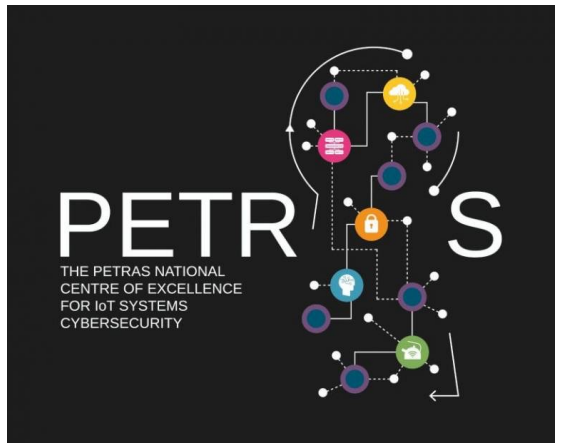
Old MacDonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming

Sharad Agarwal: sharad.agarwal@bristol.ac.uk
Awais Rashid: awais.rashid@bristol.ac.uk
Joseph Gardiner: joe.gardiner@bristol.ac.uk

University of BRISTOL
Bristol Cyber Security Group

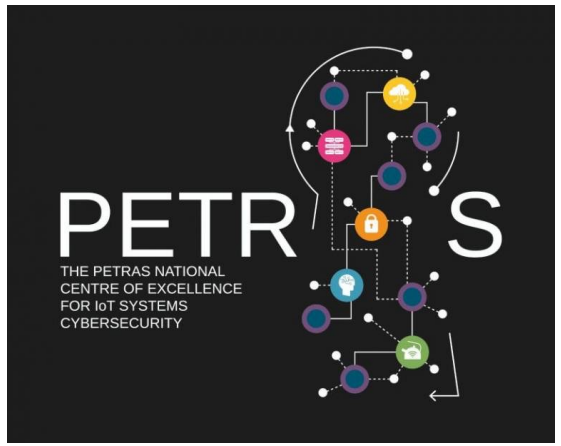
Background

- Petras National Centre of Excellence for IoT Systems Cybersecurity project
  - Cybersecurity for Food Security (CyFoo)
- Aims to study the impact of malicious actors and vulnerabilities on the food supply.
- Two approaches
  - Interview farmers about attitudes to cyber security
  - Explore security of agritech devices



Background

- Petras National Centre of Excellence for IoT Systems Cybersecurity project
  - Cybersecurity for Food Security (CyFoo)
- Aims to study the impact of malicious actors and vulnerabilities on the food supply.
- Two approaches
  - Interview farmers about attitudes to cyber security
  - **Explore security of agritech devices**



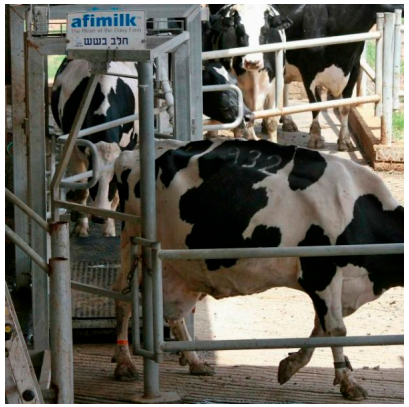
Agritech

- Agriculture is ever more reliant upon Agritech to optimise production processes.
- Increasing use across all agriculture sectors
  - Both arable and pastoral
- We focus on dairy farming

Agritech In Dairy Farming

Robotic Milking Machines

Herd Management Systems (Gates)



Cow Tracking Wearables

Barn Weather Protection and Feeding Systems

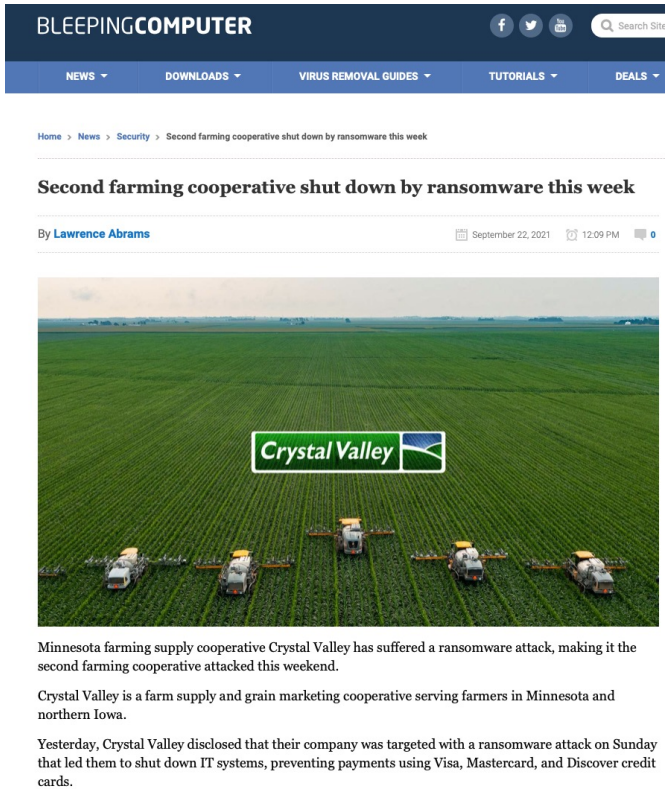
Farm Weather Stations

Camera Systems

Cloud and Smartphone Apps

What about cybersecurity?

- Farms are a critical part of a nations food supply
- Increasing reliance on smart technology and IoT provides more scope for things to go wrong
- If attackers could attack farm, could cause widespread problems.
- E.g. if milking robot is taken offline by attack:
  - Animal welfare issues - cows need to be milked!
  - Financial loss to farmers – need milk to make money
  - Disruption to food supply – people want to drink milk
- According to FBI, there have been cases of ransomware against farms in the US



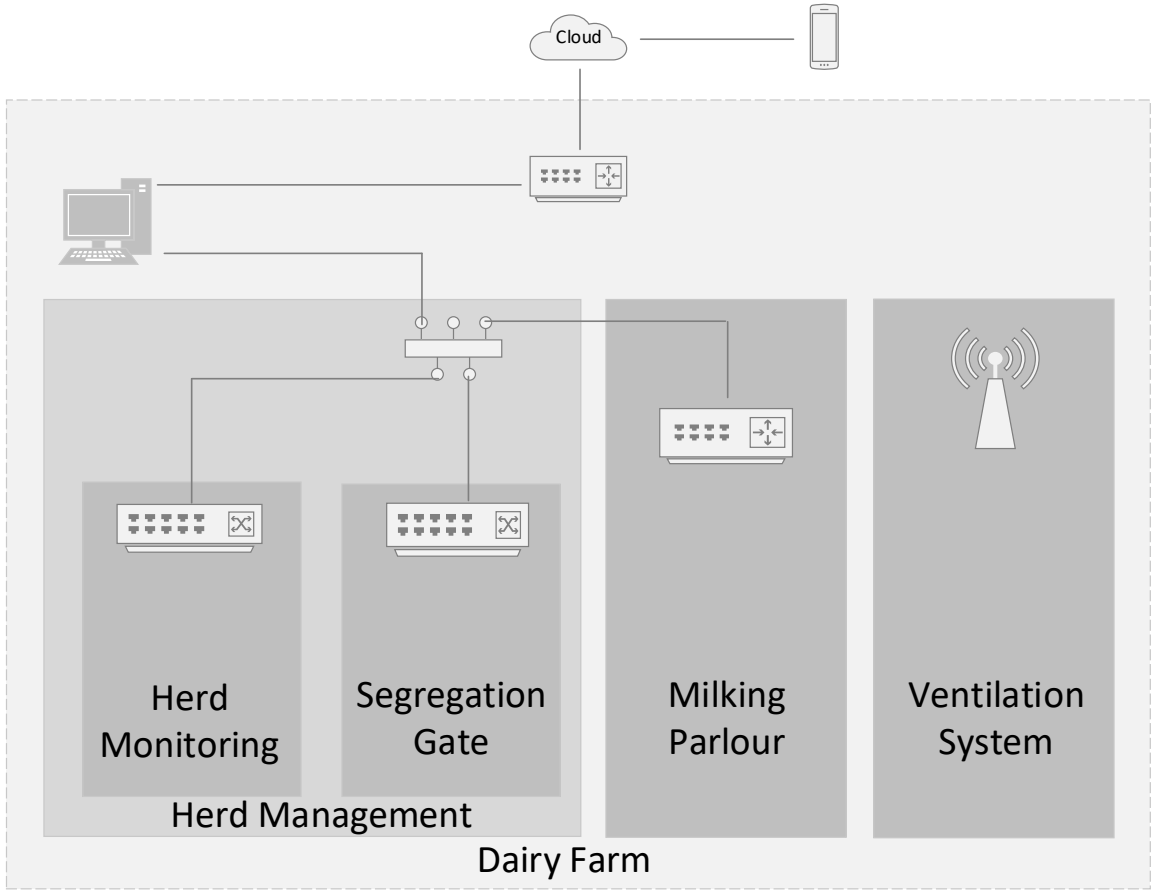
The Bristol Agritech Testbed

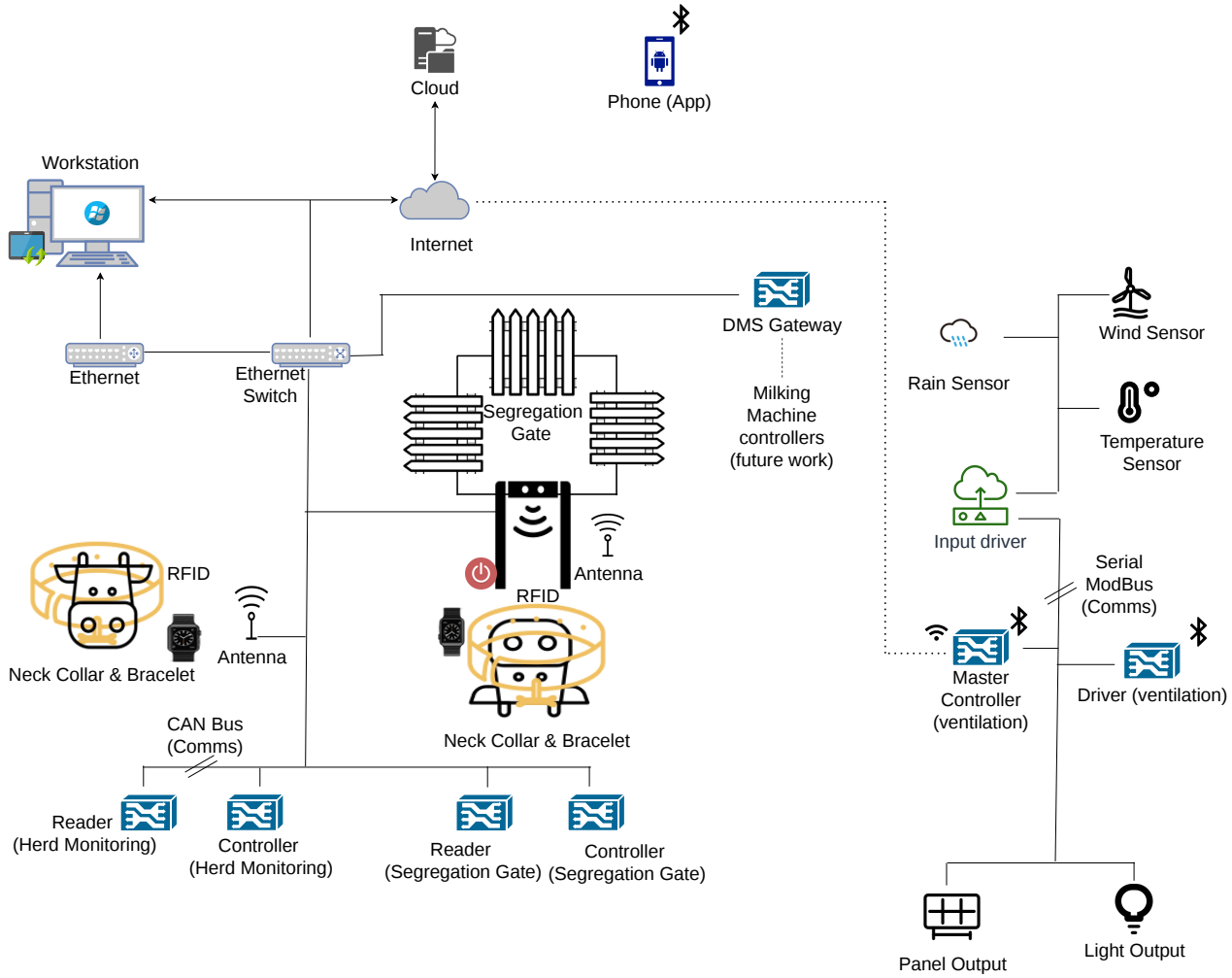
- The first testbed built to be focussed on the security of Agritech devices
- Design characteristics
  - Diversity of devices
    - Testbed consists of multiple different devices found on a smart dairy farm
  - Fidelity
    - Testbed replicates a realistic dairy farm, though no livestock
- Designed through visits to farms and interaction with vendors and stakeholders
- Procurement
  - Very difficult to buy (vendors do not want to sell at small volume and to security researchers…)
  - Cannot buy “off-the-shelf”
  - Collected devices were provided by vendors who agreed to sell at small volume, and at cost.

Use Cases

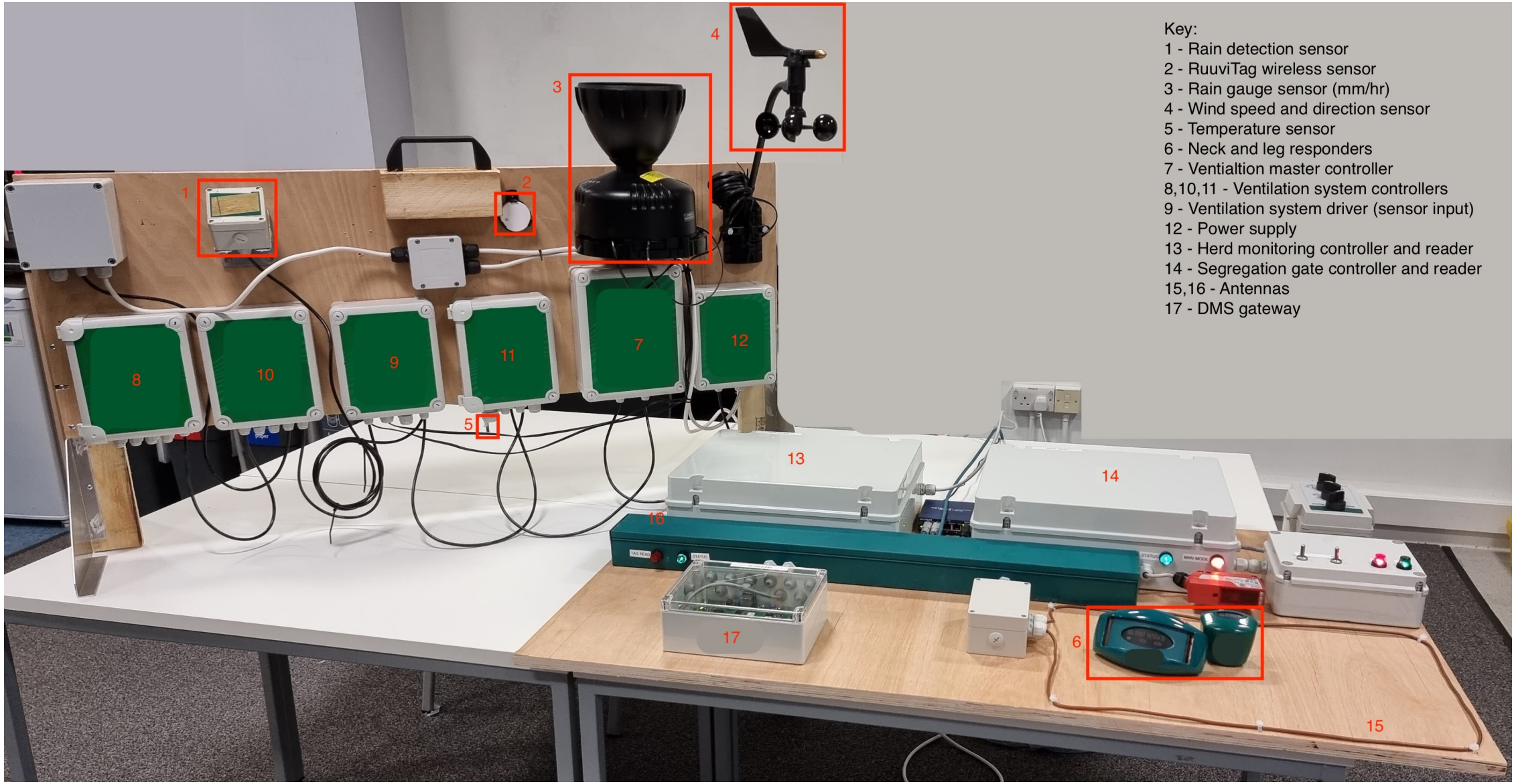
- Security analysis of devices
  - What are the vulnerabilities?
- Demonstration of attacks and implications
  - Show stakeholders what the problems are in a safe environment
- Testing of defence mechanisms
- Collaborative use
  - Testbed will be useable by vendors and other researchers

Testbed – High Level

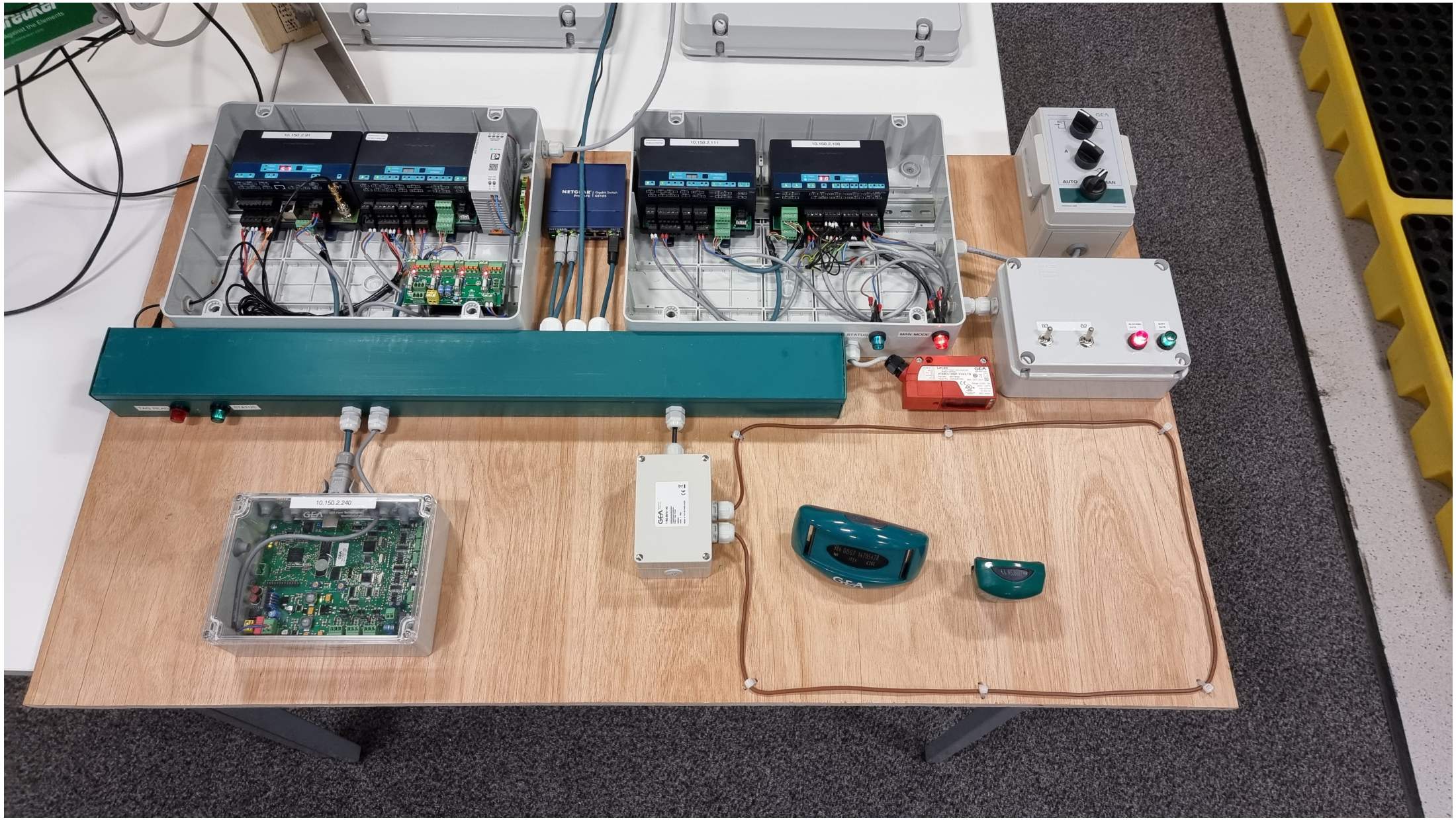




Testbed


Key:
1 - Rain detection sensor
2 - RuuviTag wireless sensor
3 - Rain gauge sensor (mm/hr)
4 - Wind speed and direction sensor
5 - Temperature sensor
6 - Neck and leg responders
7 - Ventialtion master controller
8,10,11 - Ventilation system controllers
9 - Ventilation system driver (sensor input)
12 - Power supply
13 - Herd monitoring controller and reader
14 - Segregation gate controller and reader
15,16 - Antennas
17 - DMS gateway
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17

Testbed



(Some) Early Security Findings

- No web interfaces and websites use HTTPS/TLS
- The ventilation master controller had password-less root access over SSH!
  - We reported it to vendor on a Thursday, it had been patched across all deployed systems (including ours) by the Monday
- Cow tracking collars use hardware IDs for gate access via RFID (FDX-8) – we could easily clone these to blank card using Proxmark device
- If desktop PC is turned off, segregation gates do not operate

Future Work

- Further exploration of security vulnerabilities
  - Attacking wireless signals
  - Hardware analysis
  - Build complex attack scenarios
- Exploration of security mechanisms
- Expansion of devices
  - We’re working on a milking robot (parts)!

Questions?

Sharad Agarwal: sharad.agarwal@bristol.ac.uk
Awais Rashid: awais.rashid@bristol.ac.uk
Joseph Gardiner: joe.gardiner@bristol.ac.uk

University of BRISTOL

Bristol Cyber Security Group