ITP AY 2022 T3
Security Exploits Graph Modelling Dashboard

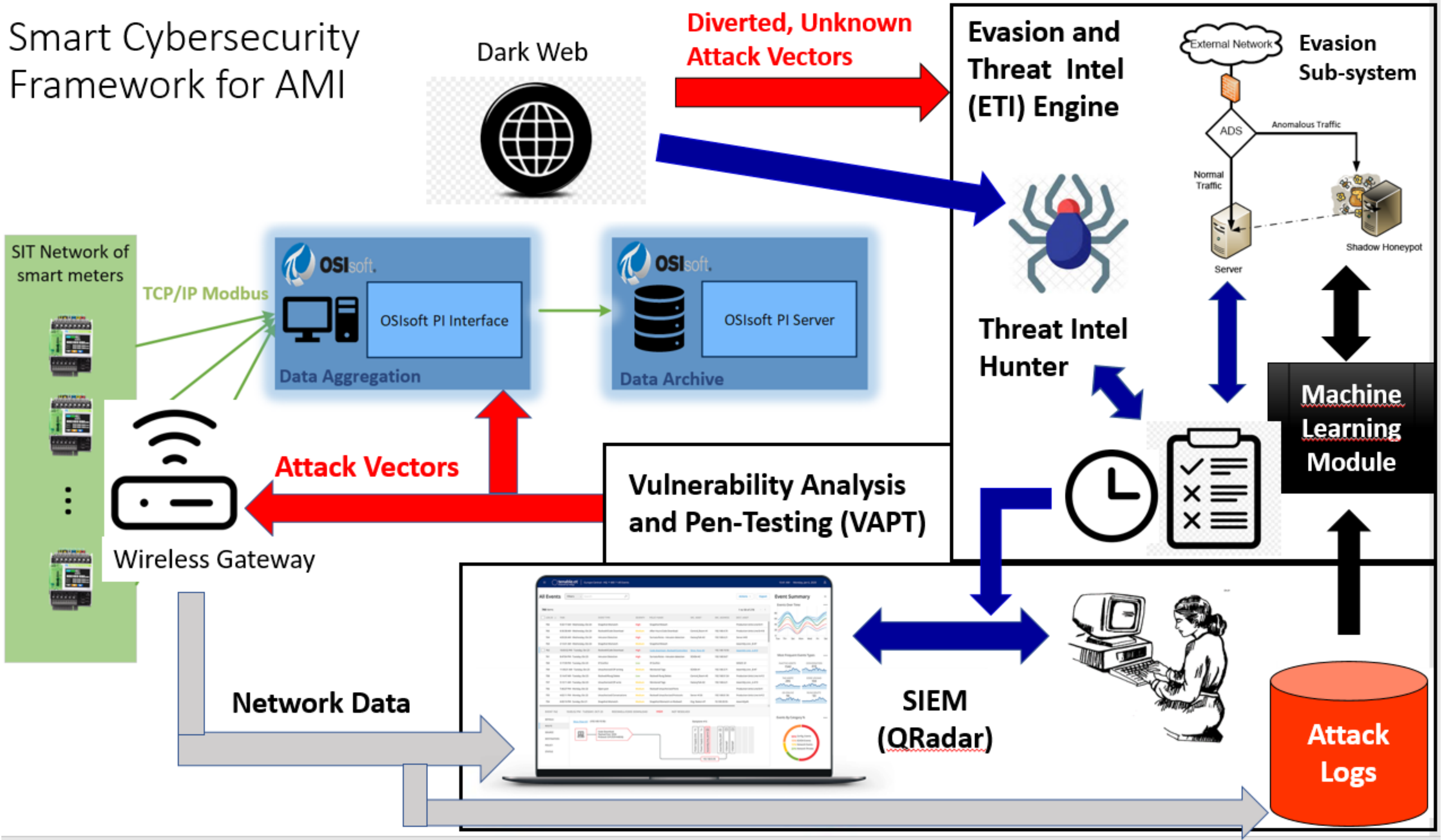
ANG WEE YI ALEX, RYAN SUAN ZHAN HUI,
SIM YU CHENG, LAW JUN HAO
IS TEAM 13

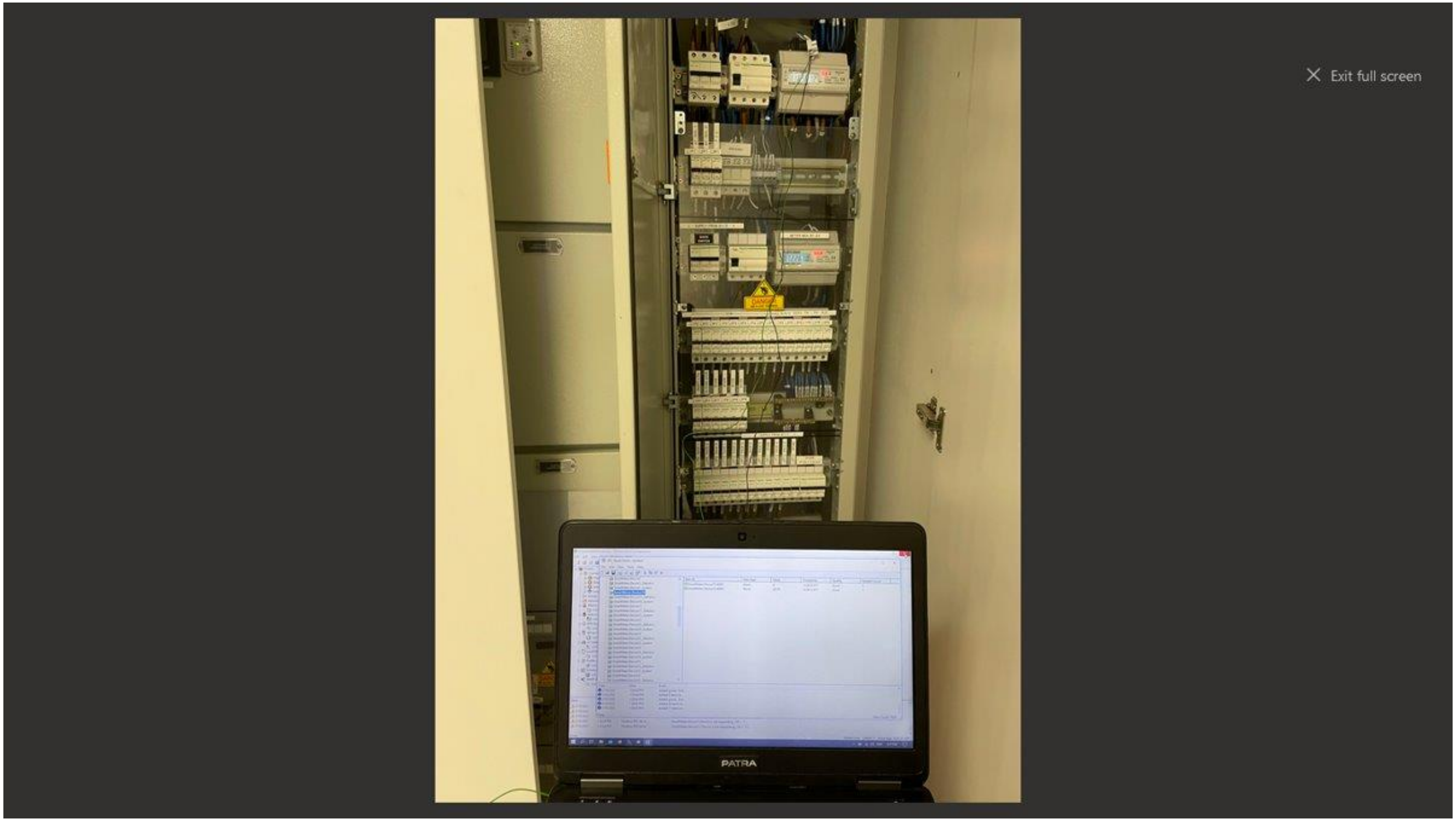
Supervisors	Organisation	Contact
James	SIT-ICT	james.ng@singaporetech.edu.sg
Peter	SIT-ICT	peter.loh@singaporetech.edu.sg

PROJECT OVERVIEW

BACKGROUND

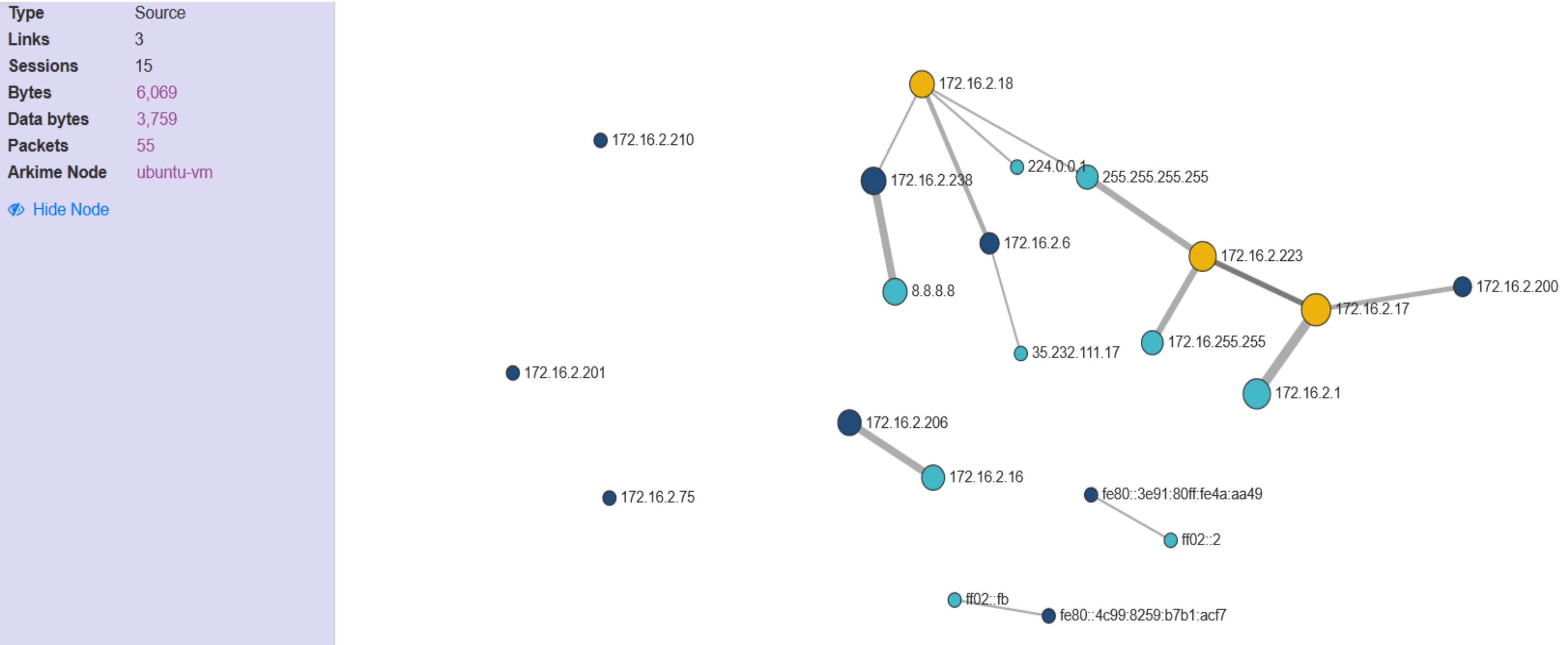
The Smart Cybersecurity Framework for Advanced Metering Infrastructure (SCFAMI) is the real-time security monitoring system we will focus on.





NYP Level 7

SCFAMI) is made up of customized open source as well as developed components. Examples include Malcolm and Arkime. Arkime is a full packet capture component with interface shown below:



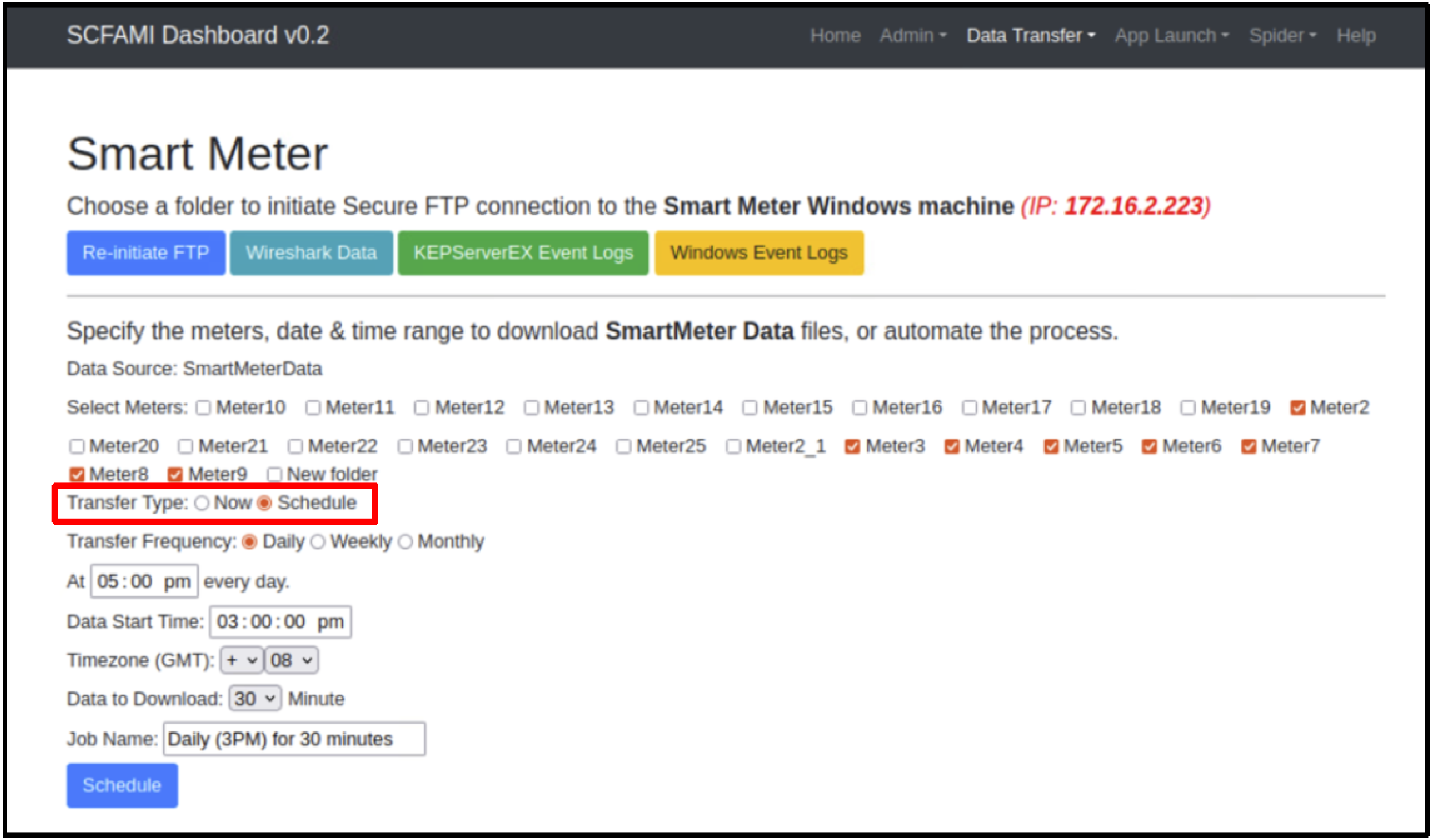
Type	Source
Links	3
Sessions	15
Bytes	6,069
Data bytes	3,759
Packets	55
Arkime Node	ubuntu-vm

Limitations: can only drag and drop

Needed: CRUD, naming functions

Approach: export generated graph (JSON?) to SCFAMI dashboard

PROJECT APPROACH



Smart Meter

Choose a folder to initiate Secure FTP connection to the **Smart Meter Windows machine** *(IP: **172.16.2.223**)*

Specify the meters, date & time range to download **SmartMeter Data** files, or automate the process.

Data Source: SmartMeterData

Select Meters: ☐ Meter10 ☐ Meter11 ☐ Meter12 ☐ Meter13 ☐ Meter14 ☐ Meter15 ☐ Meter16 ☐ Meter17 ☐ Meter18 ☐ Meter19 ☑ Meter2 ☐ Meter20 ☐ Meter21 ☐ Meter22 ☐ Meter23 ☐ Meter24 ☐ Meter25 ☐ Meter2_1 ☑ Meter3 ☑ Meter4 ☑ Meter5 ☑ Meter6 ☑ Meter7 ☑ Meter8 ☑ Meter9 ☐ New folder

Transfer Type: ○ Now ● Schedule

Transfer Frequency: ● Daily ○ Weekly ○ Monthly

At 05 : 00 pm every day.

Data Start Time: 03 : 00 : 00 pm

Timezone (GMT): + 08

Data to Download: 30 Minute

Job Name: Daily (3PM) for 30 minutes

Where should we export the graph to and how do we interact with it? -> **Design issue**

Scope of Work

1. Determine what the Arkime generated graph is used for.
2. Export generated graph to SCFAMI dashboard – where and how to display it while maintaining the user friendliness of the dashboard – DESIGN issue 1.
3. Determine additional useful interactive functions for the exported graph (CRUD, naming for nodes and edges).
4. Where to place these functions and how to invoke them – DESIGN issue 2.
5. Implement accepted DESIGN and test interactive functions systematically – TEST CASES.
6. Propose and document applications for the exported graph and new / novel functions that can enhance Arkime (see 1.).

PROJECT MANAGEMENT

Project Milestones and Deliverables

Week	Milestone / Deliverable	Start Date	End Date
1-2	Be familiarized with SCFAMI system with focus on Arkime component that generates graph model.	2 May 2023	12 May 2023
3-4	Proposed DESIGN for exported graph with additional interactive functions.	15 May 2023	26 May 2023
5-7	Implement accepted DESIGN for exported graph with additional interactive functions	29 May 2023	16 June 2023
8-10	Test and debug implementation and integrate to SCFAMI dashboard	19 June 2023	7 July 2023
11	Final test of integrated system on SCFAMI	10 July 2023	14 July 2023
12	Collect data for report and poster	17 July 2023	21 July 2023

ITP Expectations and Team Work

- Industry Innovation / Applied Research nature of project
- Open-ended, no ready solution from supervisors
- Existing students may be difficult to get hold of for reference
- No formal lectures, tutorials or labs
- Be prepared to experiment, explore and co-operate
- Pull your weight as a team member
- Progress report and meetings on weekly basis at the start
- Appraisal recognition for initiative and effort
- Absence must be accompanied by valid reason(s) eg. MC, letter or email from SWS company
- Absence must be made up for by member