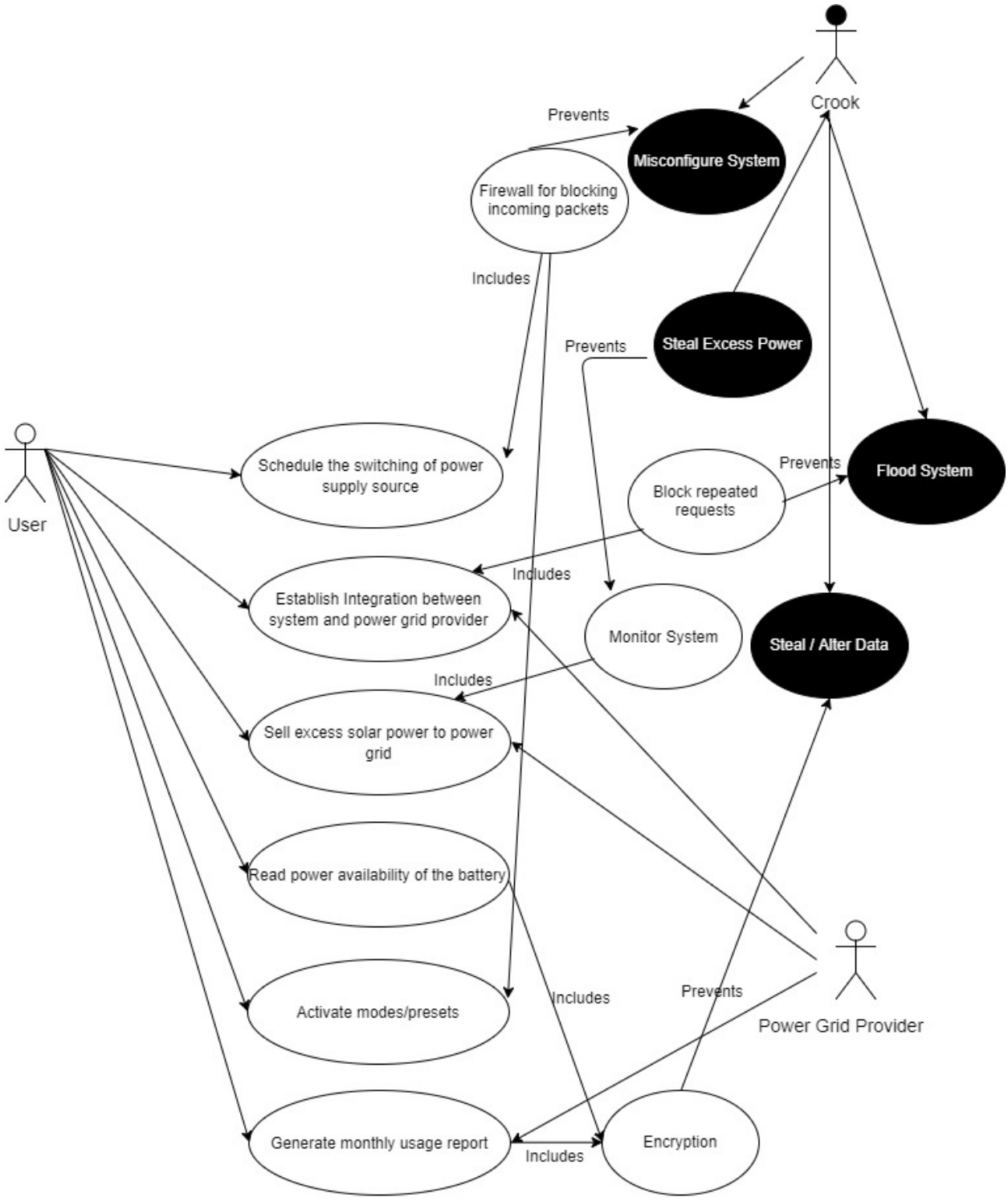
EMSS 12

SAFETY, SECURITY AND RESILIENCE

Amol Shandilya, Yanyan Jiang, Minghui Jin

The Booch Group

1. Misuse Case Diagram



2. Safety Requirements

Requirement	Description	Plan
Switch status	The switch may be faulty, unable to respond to the normal on/off operation. The system shall ensure that the switch can be controlled.	1. In the system double control switch settings, two operations, one is remote control through mobile app, the other is manually control, shall ensure the normal operation of switch. 2. The switch functionality of power supply and device status shall use diverse methods. In the stage of development, implement these methods to run successfully on both components. So, when the remote control of one switch fails, the other method shall be the backup.
Battery	Battery power detection, temperature abnormalities shall ensure that the entire system safety. Or when the battery is full, the selling operation occurs error that this operation is unavailable.	1. The battery temperature shall not be over-high. Once the temperature is over threshold, stop charging the battery and active cooling mechanism. 2. When the battery is detected as full and there is a problem with the power selling operation, stop the battery charging in case of overcharge and send an email to the developers to identify whether the transaction and authorization between the system and electricity is normally working or not.
Usage bill	The usage bill shall not make mistake, in case of loss of both the electricity providers and the users.	1. Once the system detects an abnormal total usage compared to historical usage, then send an abnormal warning notification to user and ask if the usage need to be checked. 2. If the user asked to check the usage, then check the history daily electricity data in this month to find the cause of abnormity compared to historical usage. If there is no abnormity, then check the formal specification of the bill payment. 3. If no error found, then check the bill of electricity provider provides to find if there is any update of software and the power price, and whether the update is not successfully executed. 4. If all above checked as no error, then detect whether there is any external attacks.

Abnormal working environment	Ensure your system is safe when the natural environment is abnormal.	When the house temperature is abnormal or there is smoke, turn off all the switches and issue a warning.

3. Security Requirements

Requirement	Description	Plan
Log-in access security	The hacker may log in the account and steal personal information, including home address, which is significant for the users	1. GPS location Each time the account being logged-in, the logging location shall be stored. Once the location has a big difference from normal location, then send an email to the user to ask if this is proper. 2. Device certification When the user first logs in to his account, the device shall be certified. Once an uncertified device log in the account, then send an email to the user to ask if this is correct. 3. Allow one address has multiple account, however there is only one master account, the others are slave accounts. And the slave accounts' establishment must be verified by the master. And the master shall be able to choose whether give permission to the slave account or not.
Access to device switch security	The hacker may be accessible to turn on/off the device. This is super dangerous for cameras, especially baby cameras, the air conditioner and the door alerts.	1. If the system detected an unknown access attempting to switch the device status, then immediately send a warning email to user. Do not execute the request until the user give permission. If the user denied the request and determined that this access is from unknown, then add this access to black list. Every time this access attempts to send request, ignore it. 2. Record the name and number of devices that send requests to the system in order for later check if problems happened.
Denial of switch or access	The hacker may manage to deny the user from logging in	1. When the user could not log in his account, or all his requests could not be executed, he could manually turn on/off his devices and switch the

	his account or sending requests.	power supply. Also, he shall send the error information to the system developers by help desk calls and send the error report through internet. The maintenance team shall check whether this error comes from internal or external. If external, then turn down the system until the external attacks are fixed.
Bill payment security	The hacker may steal money from users by sending fake bill to the user and add his own link in the bill to let the user payment send to his account. He could implement this by sending fake link or create a similar fake webpage.	1. Once the system detects a fake link, turn down the channel of payment, and record this fake link. 2. The system shall filter junk emails.
Database access security	The hacker may be accessible to the database which contains the history usage and personal information. He could add fake data into the usage data, which would lead to the loss of electricity provider, and he could also steal personal information.	1. The database data should have backups. 2. The user only has access to read the data from database by sending request for usage report, but no permission to write data. So, the attacker shall not have access to tamper information through the user account. 3. The access to database shall be encrypted. The managers or developers who have access to the database has a hardware, such as USB, which contains the code to decode the access. And this code shall only take effect by inserting into the server or computer. The decoding process shall be implemented by no internet involved. So, other people who do not have this hardware would no way know this code and as a result, have no access to the database.
Flood system prevention	The hacker may flood the system by sending thousands of repeated requests in a short time, such as asking usage reports a	1. Once detect that the system has received huge number of requests in a short time, then the system would block requests from the user for a time in prevention of system overload or corruption.

	hundred times in half a minute.	