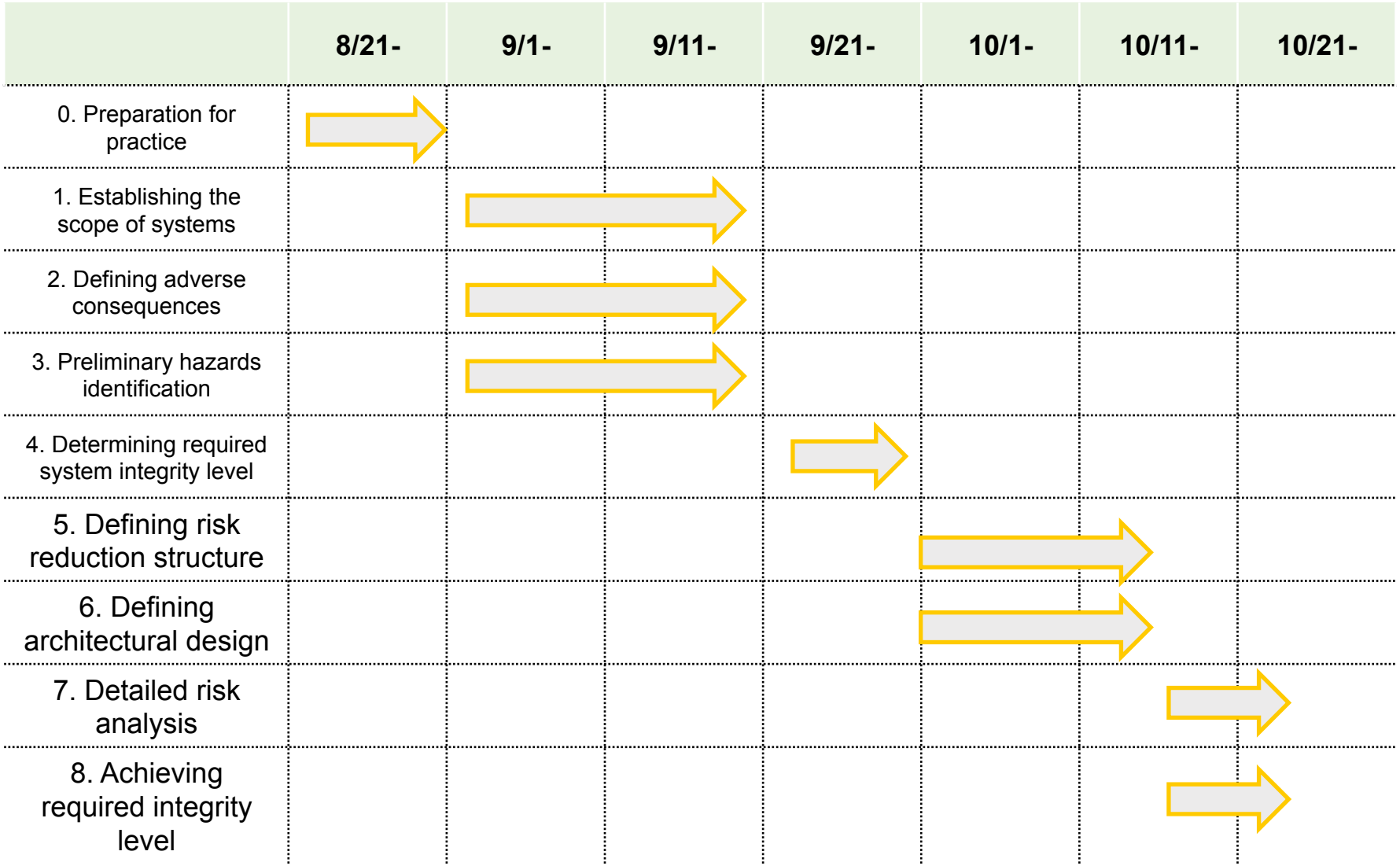
System Assurance For Smart House

Smart House Team (Nara Institute Science And Technology)

Khana Chindamaikul, Uematsu Yusuke, Jun Komeda

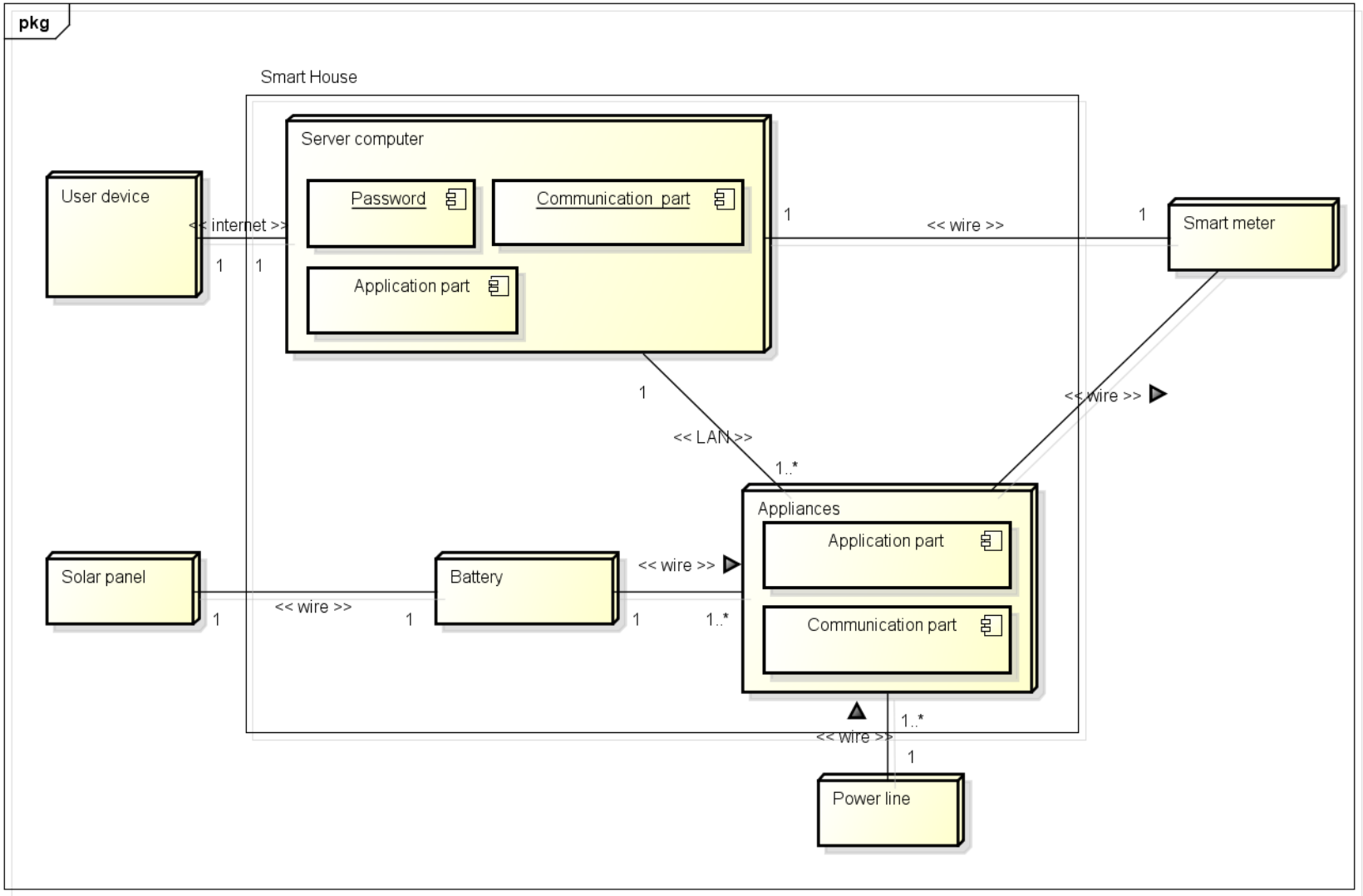
Schedule


8/21-
9/1-
9/11-
9/21-
10/1-
10/11-
10/21-
0. Preparation for practice
1. Establishing the scope of systems
2. Defining adverse consequences
3. Preliminary hazards identification
4. Determining required system integrity level
5. Defining risk reduction structure
6. Defining architectural design
7. Detailed risk analysis
8. Achieving required integrity level

Scope of systems

- **Smart House**
  - Control of appliances via smart-phone
  - Battery system using solar energy

Physical overview



General requirements

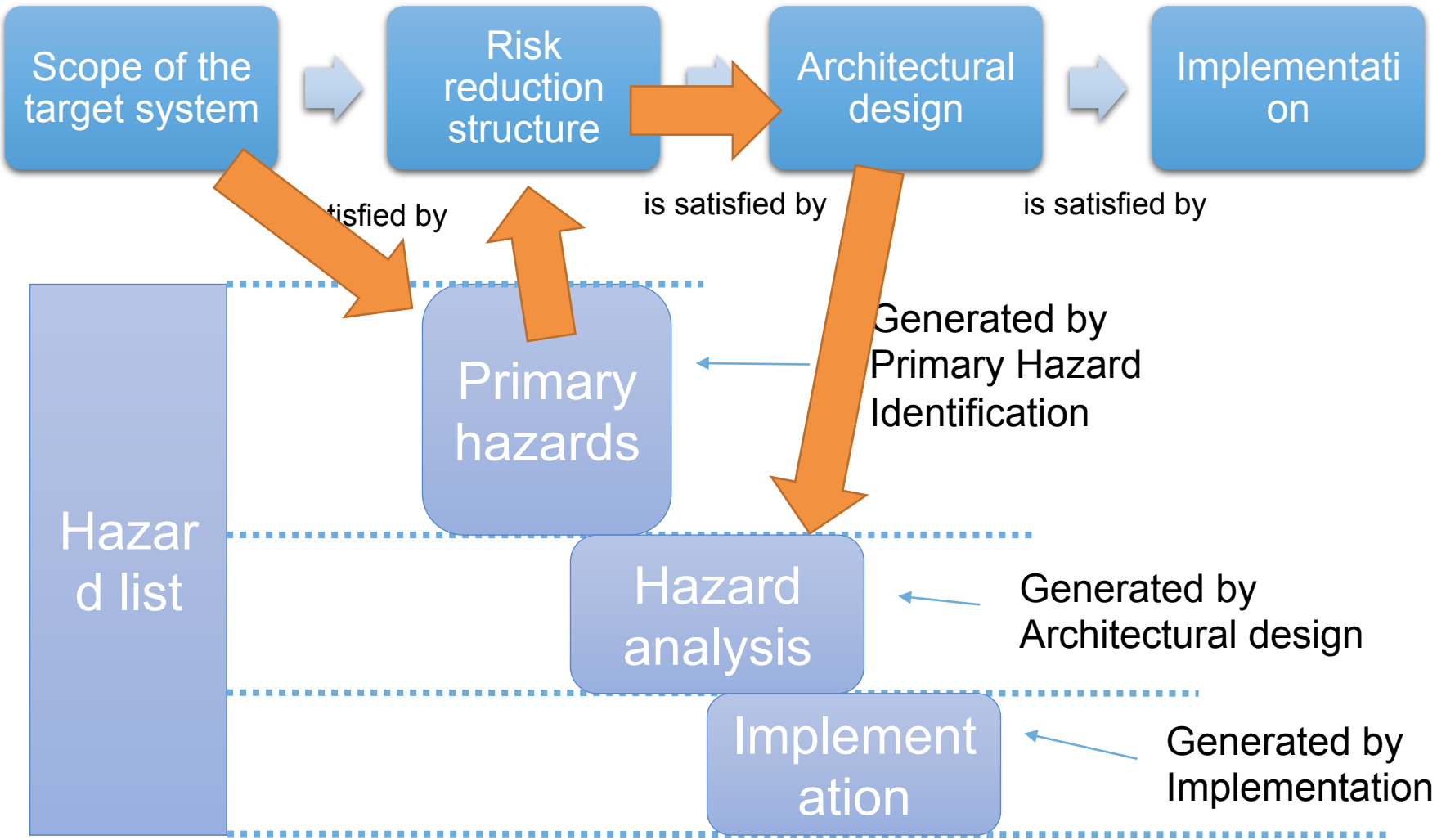
- Users' private information is protected
- Users or families and properties are protected
- The system still working even if no AC power supply
- Only owner can control appliances using mobile phone

List of obtained hazardous situations

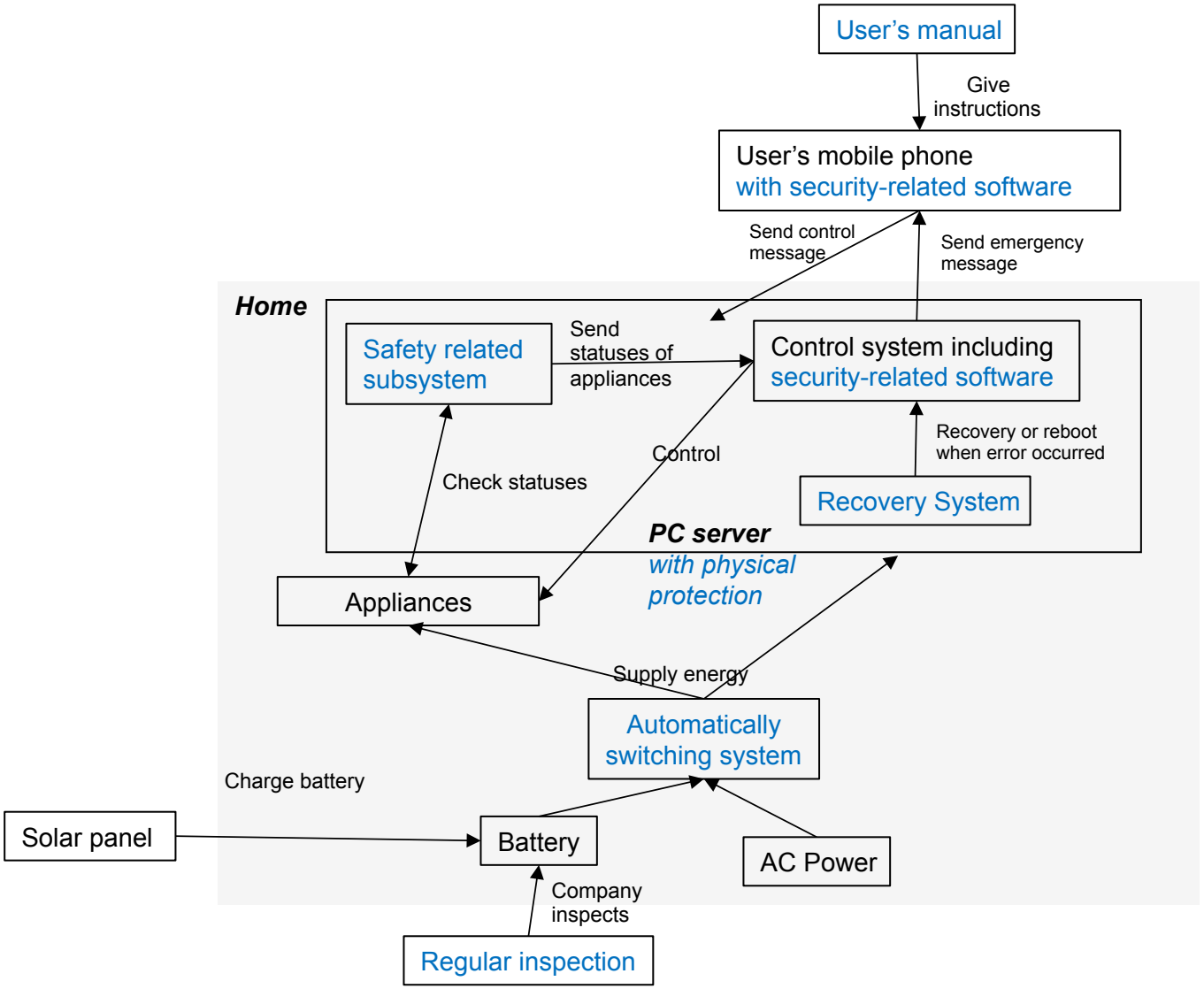
1. Man-in-the-middle-attack, for example ARP Spoofing.
2. Electric power (AC) is stopped by disaster
3. Infection with computer viruses
4. System error has occurred
5. User control appliances via mobile phone while someone in the house using it

and obtained other 7 hazards..

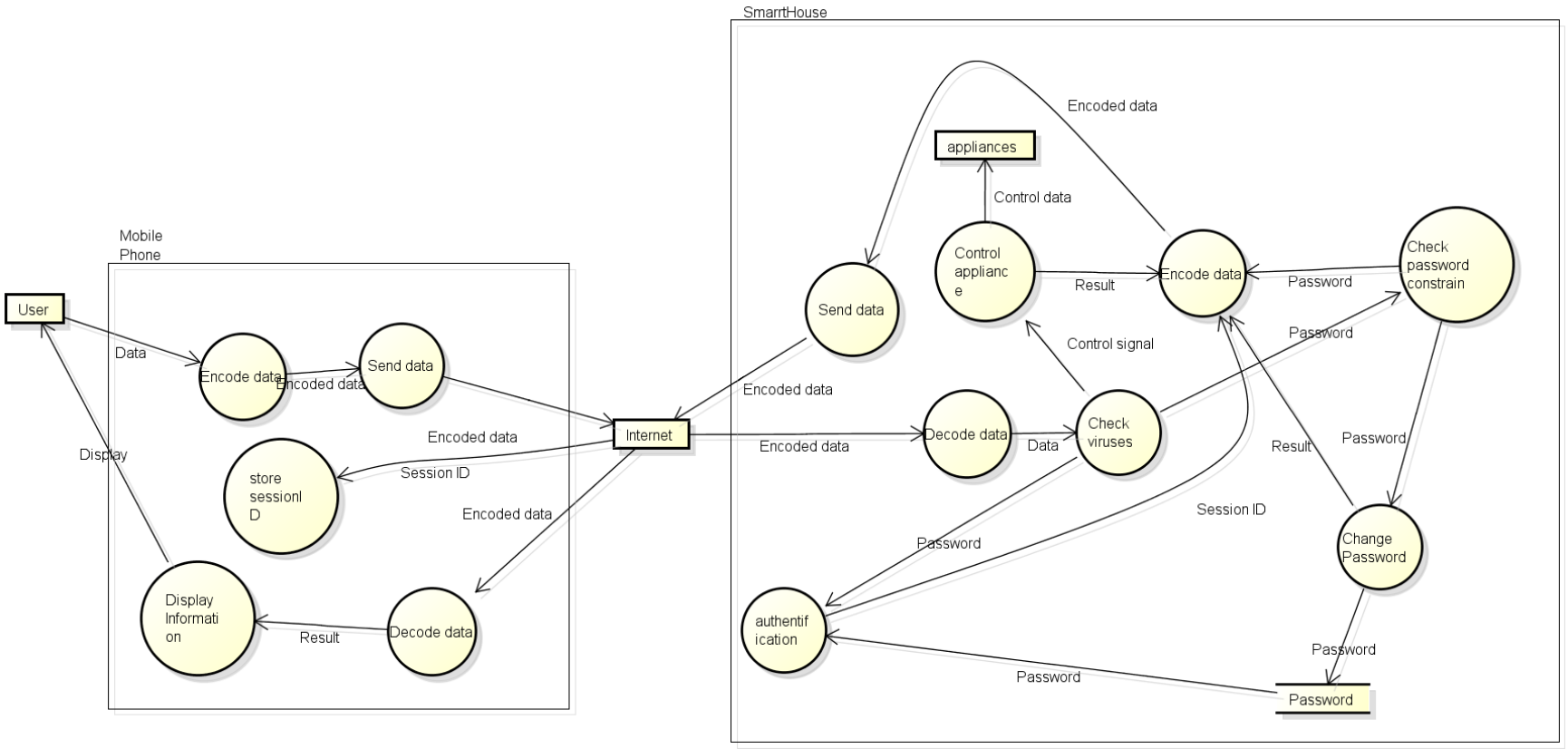
Hazard analysis based on refinement of system



Assumption of risk reduction structure

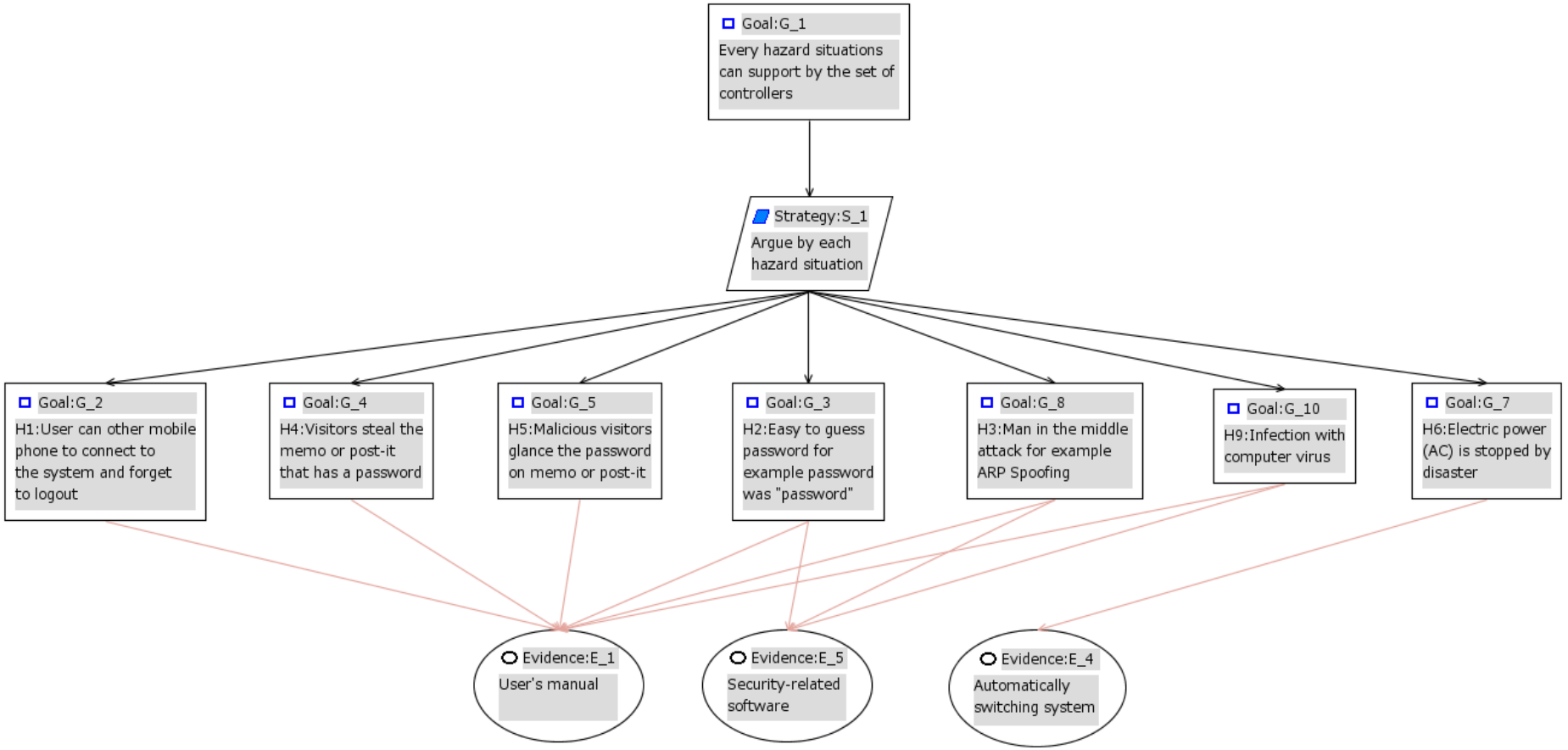


DFD as a architectural design 1 (Security-related software)

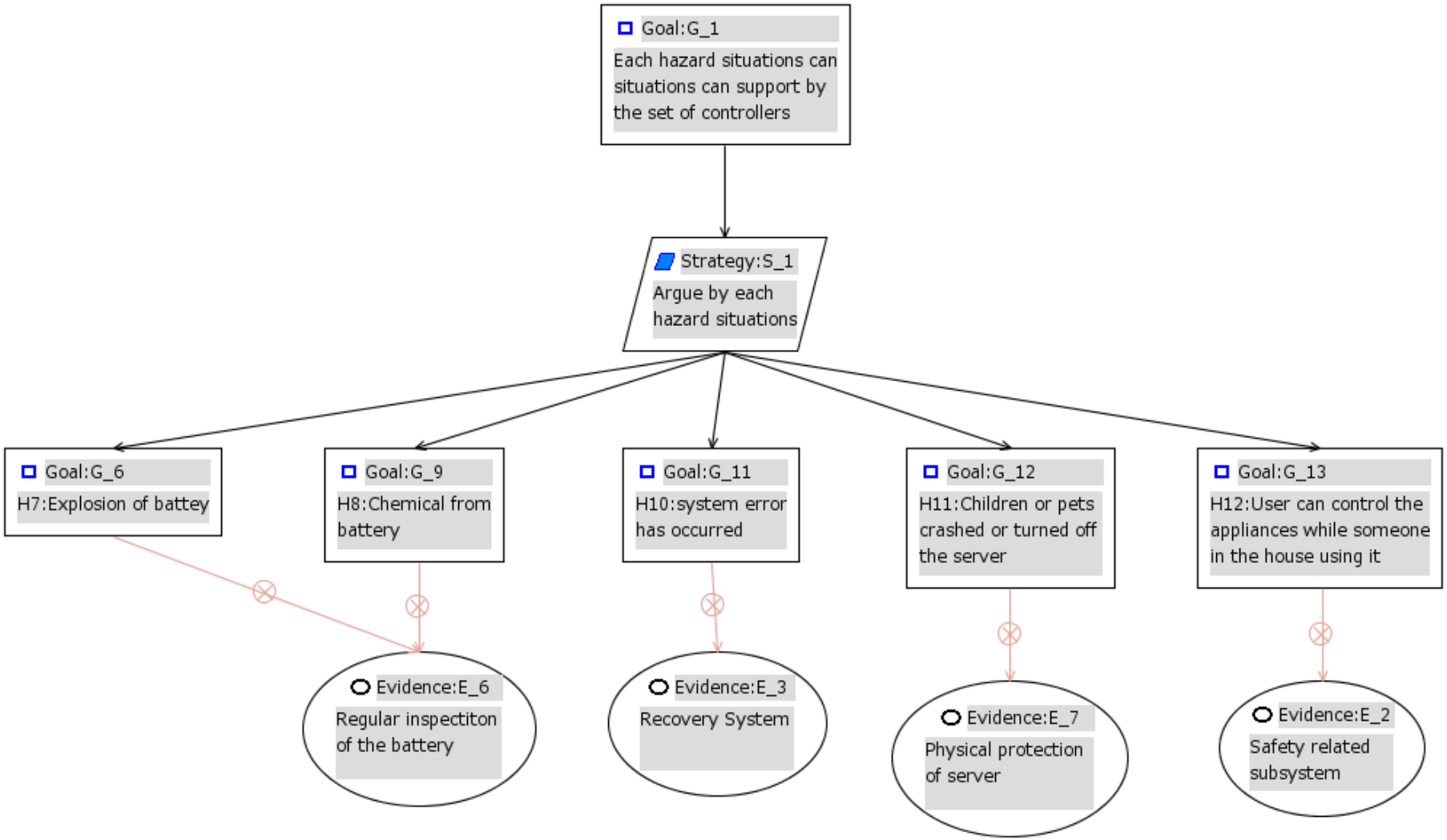


Over view of Assurance case

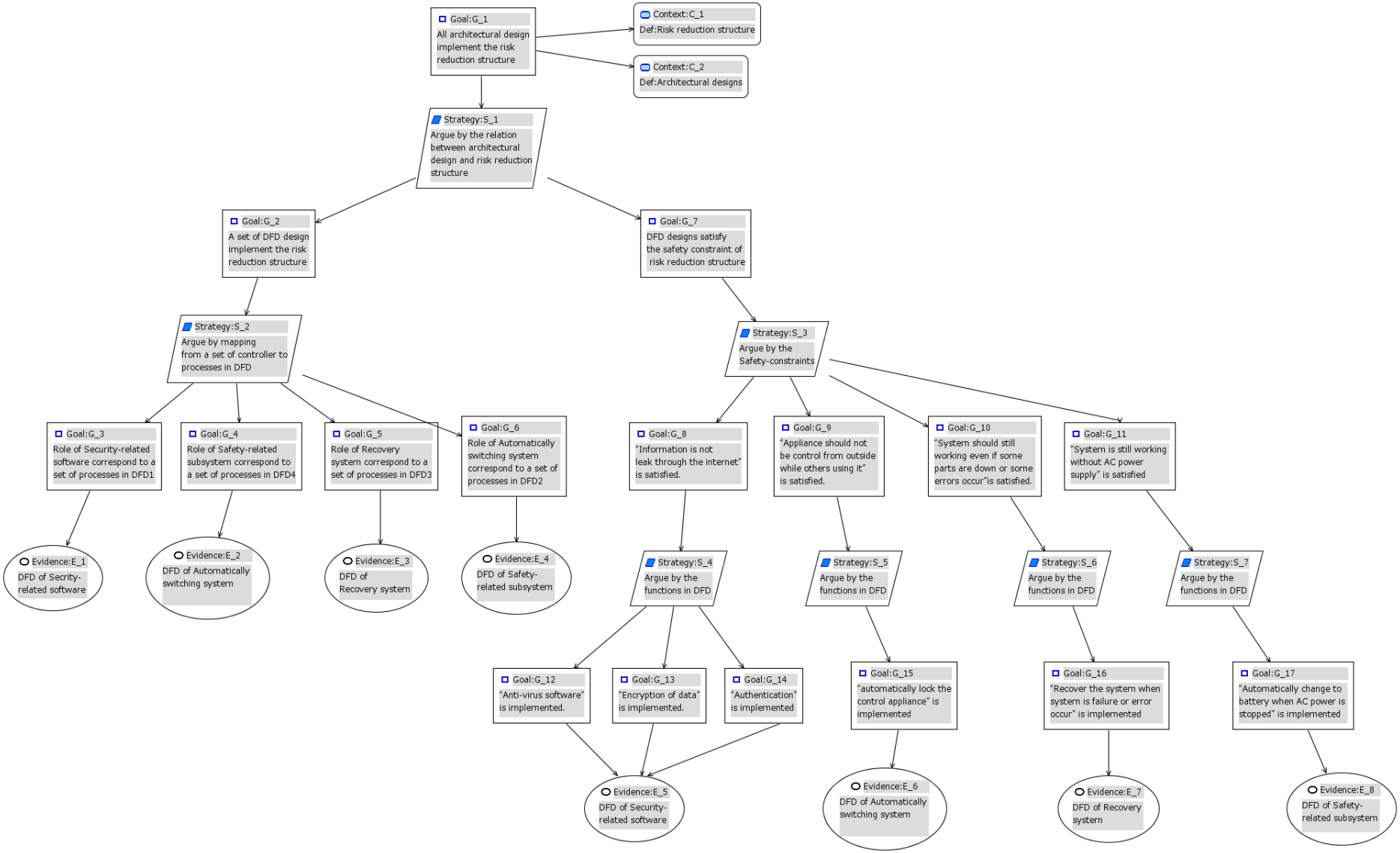
Assurance case(1)-1



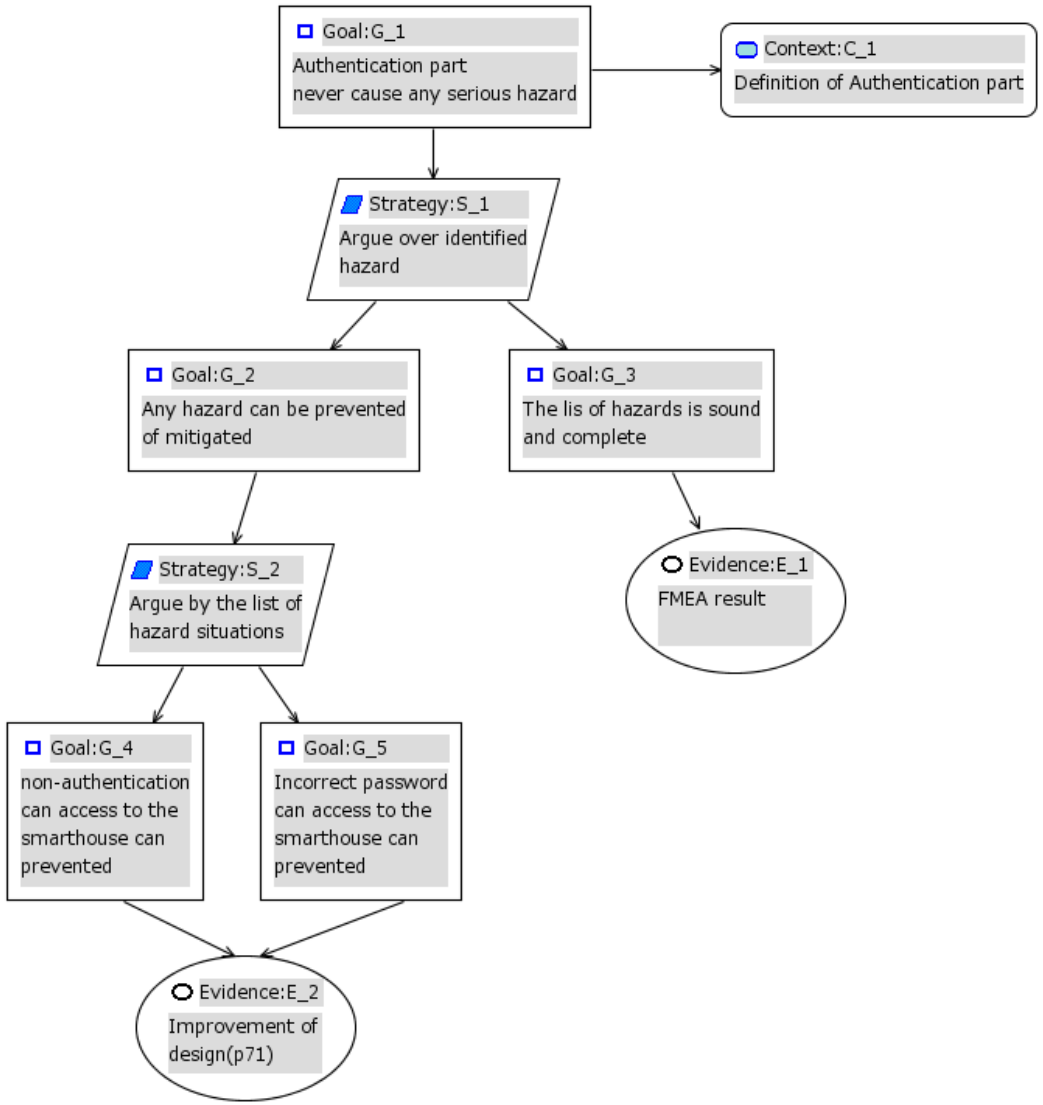
Assurance case(1)-2



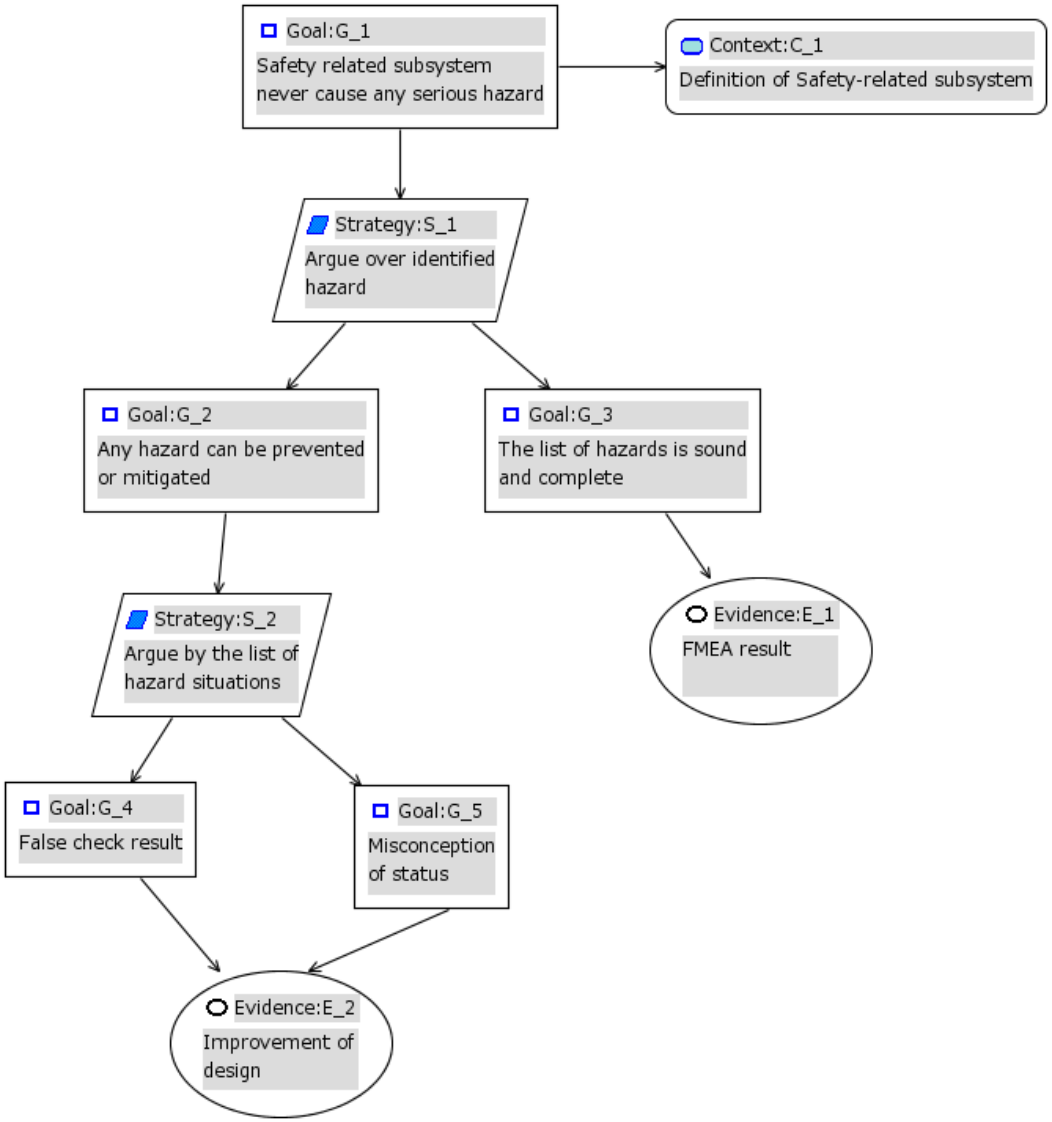
Assurance case(2)



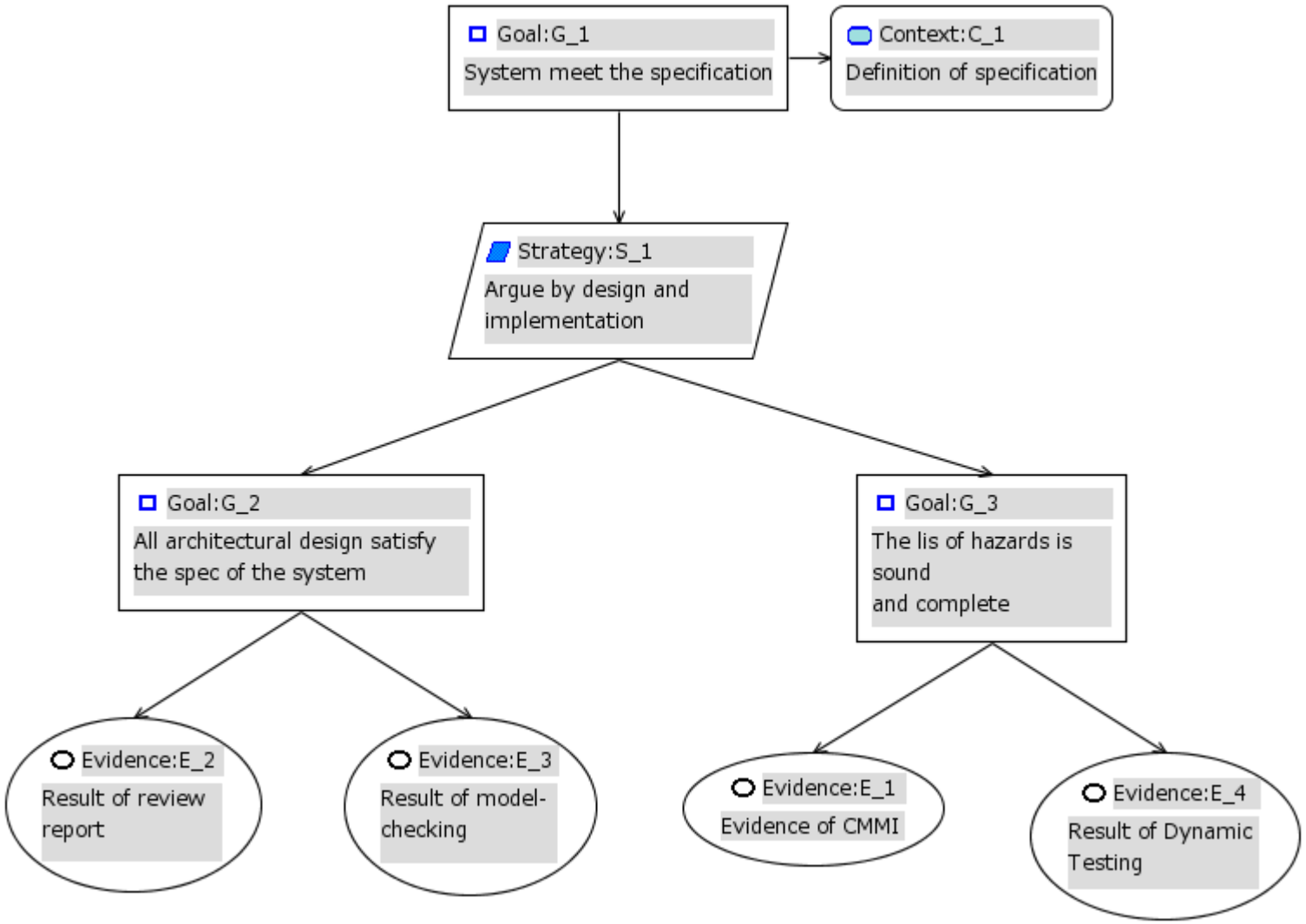
Assurance case(3)-1



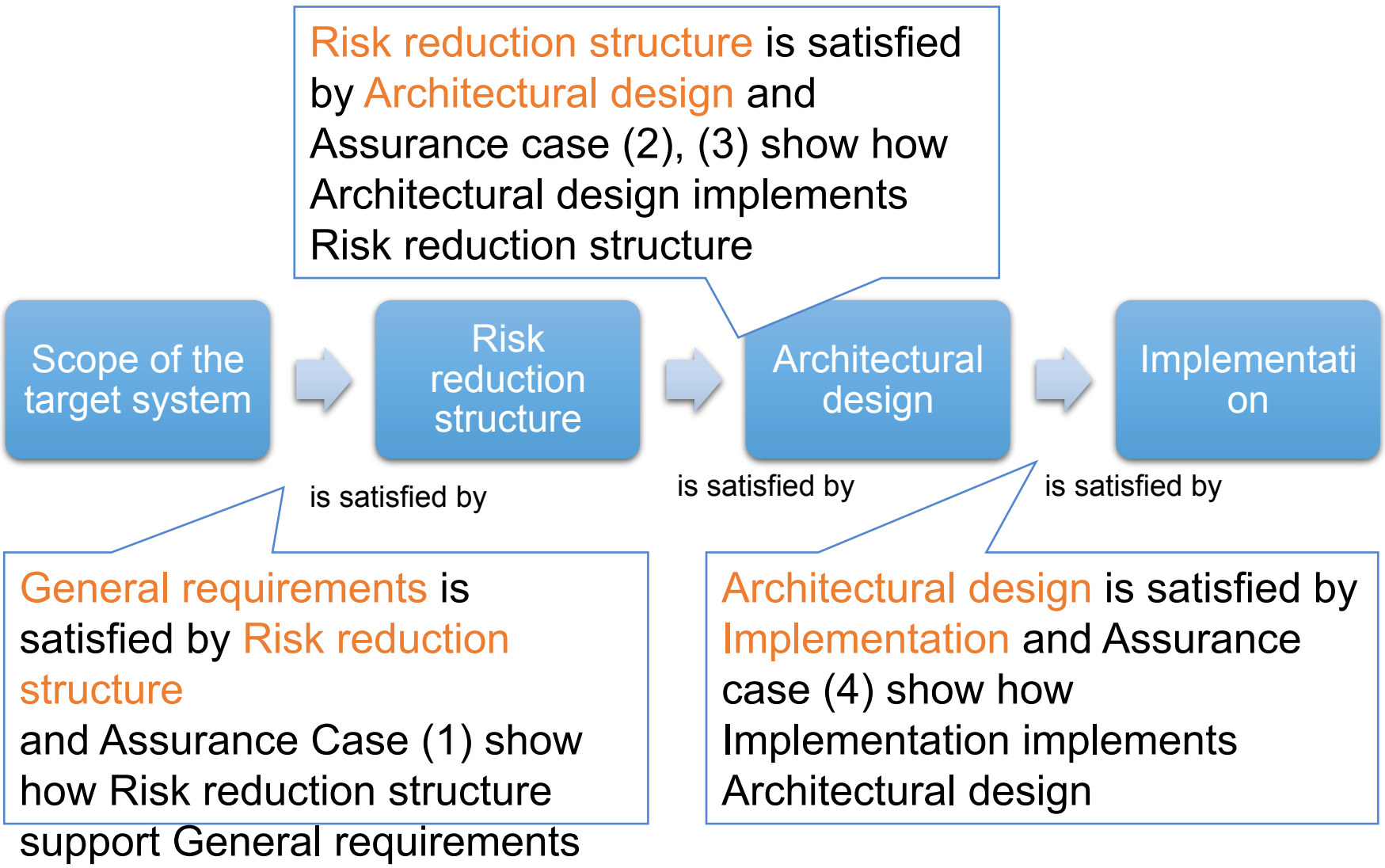
Assurance case(3)-2



Assurance case (4)



Achieving Requirement Methodology



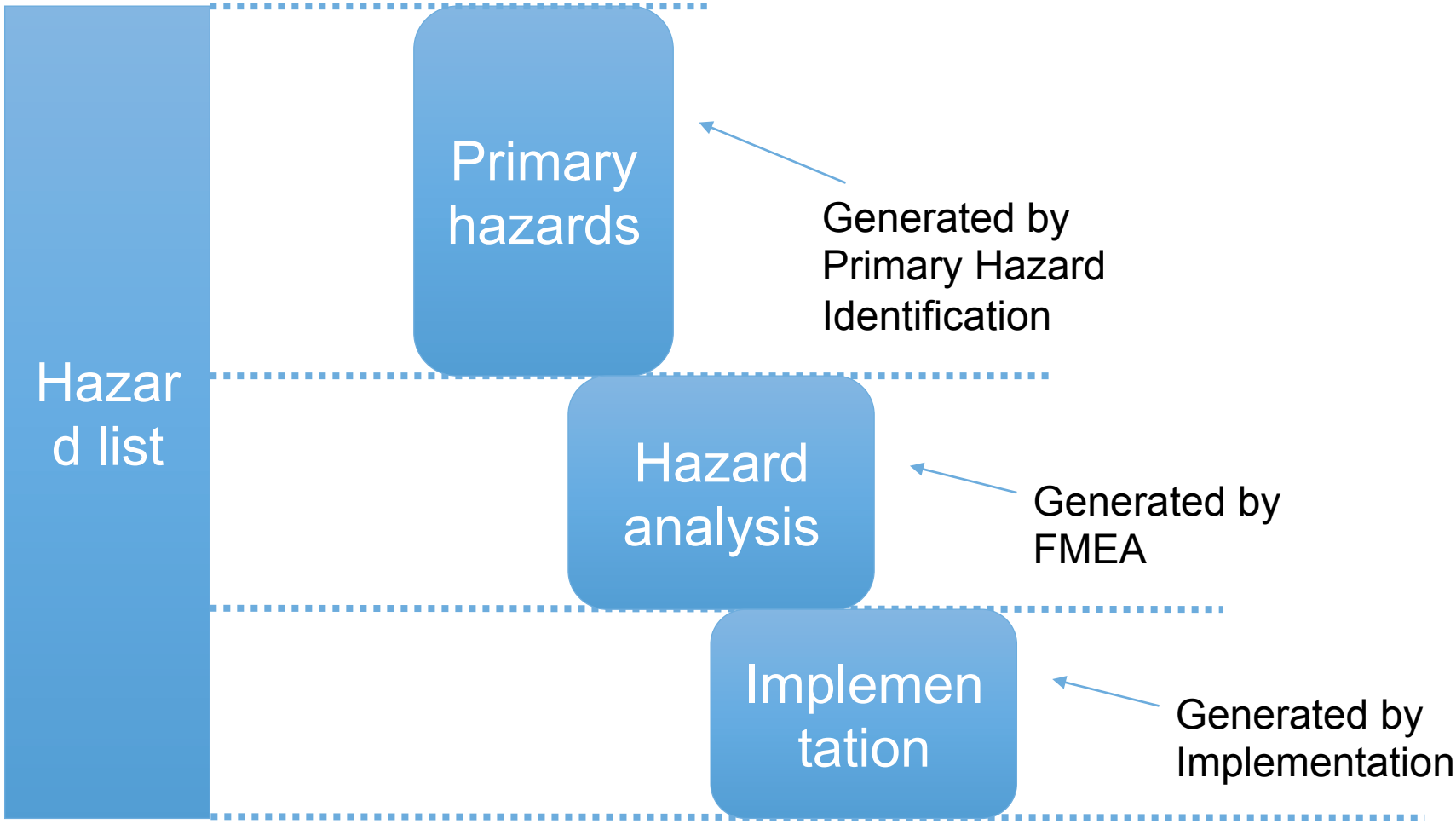
Other works

- Definition of integrity levels
- Risk analysis using FMEA
- Records of arguments using IBIS

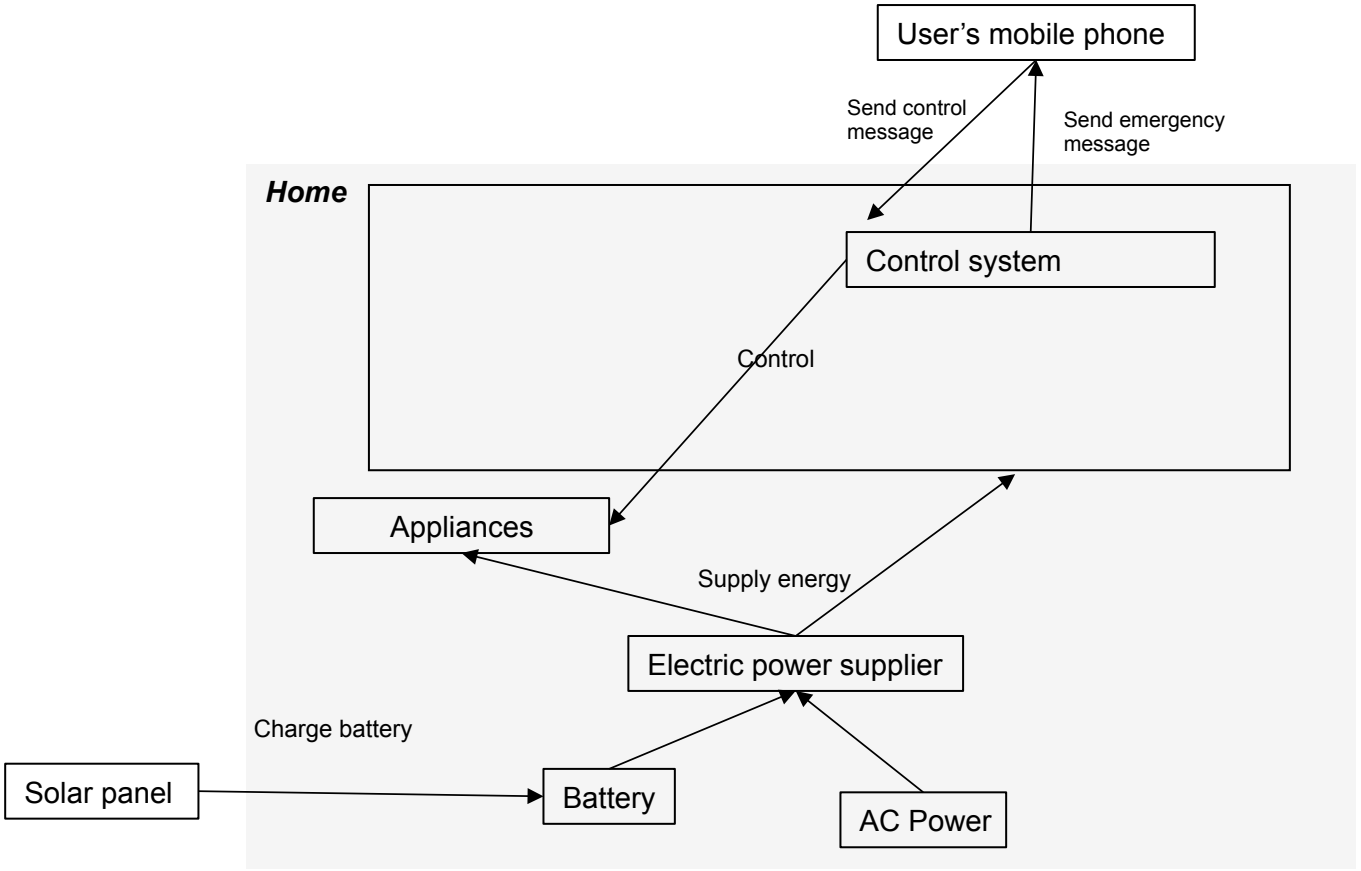
Thank you

Question and answer

Hazards mitigation

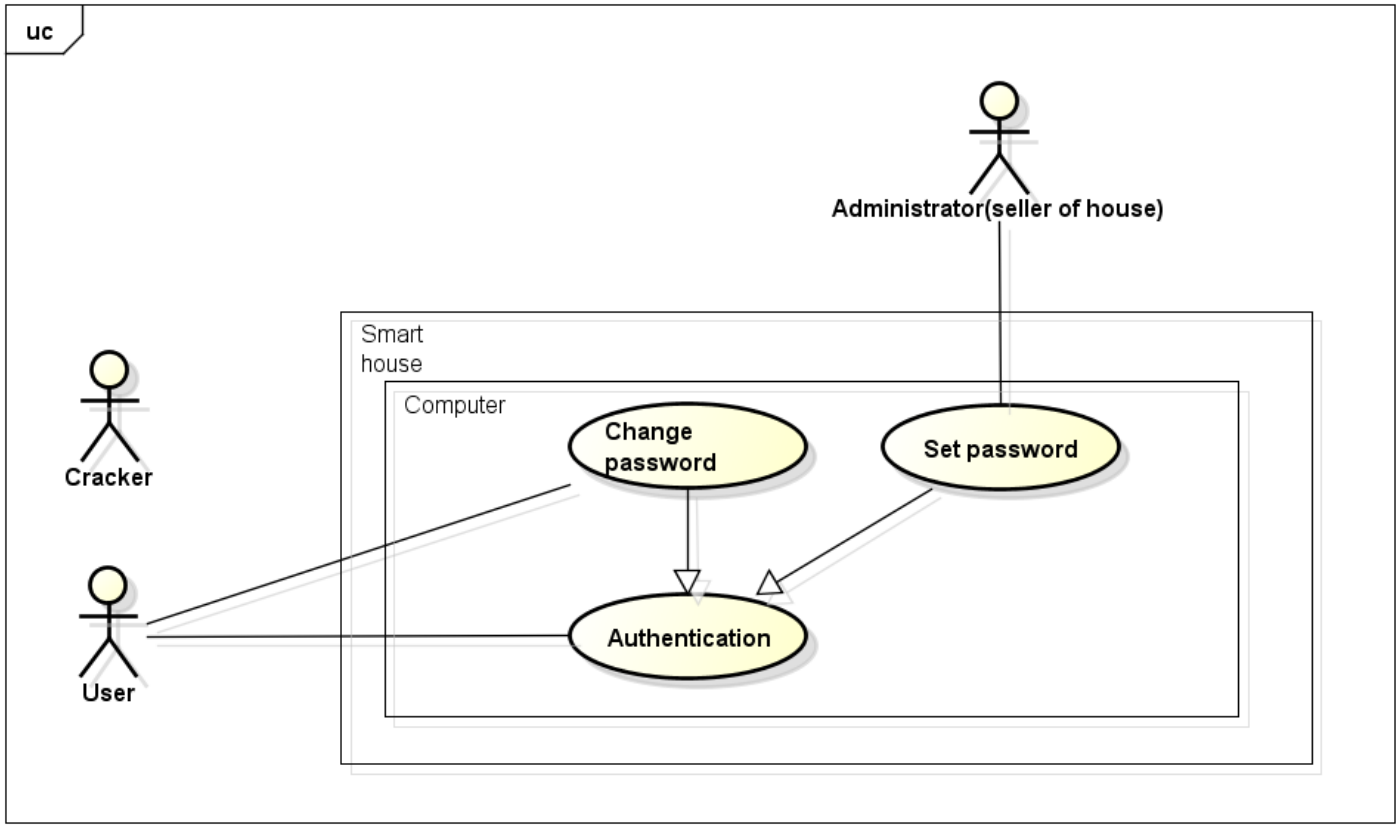


Physical overview



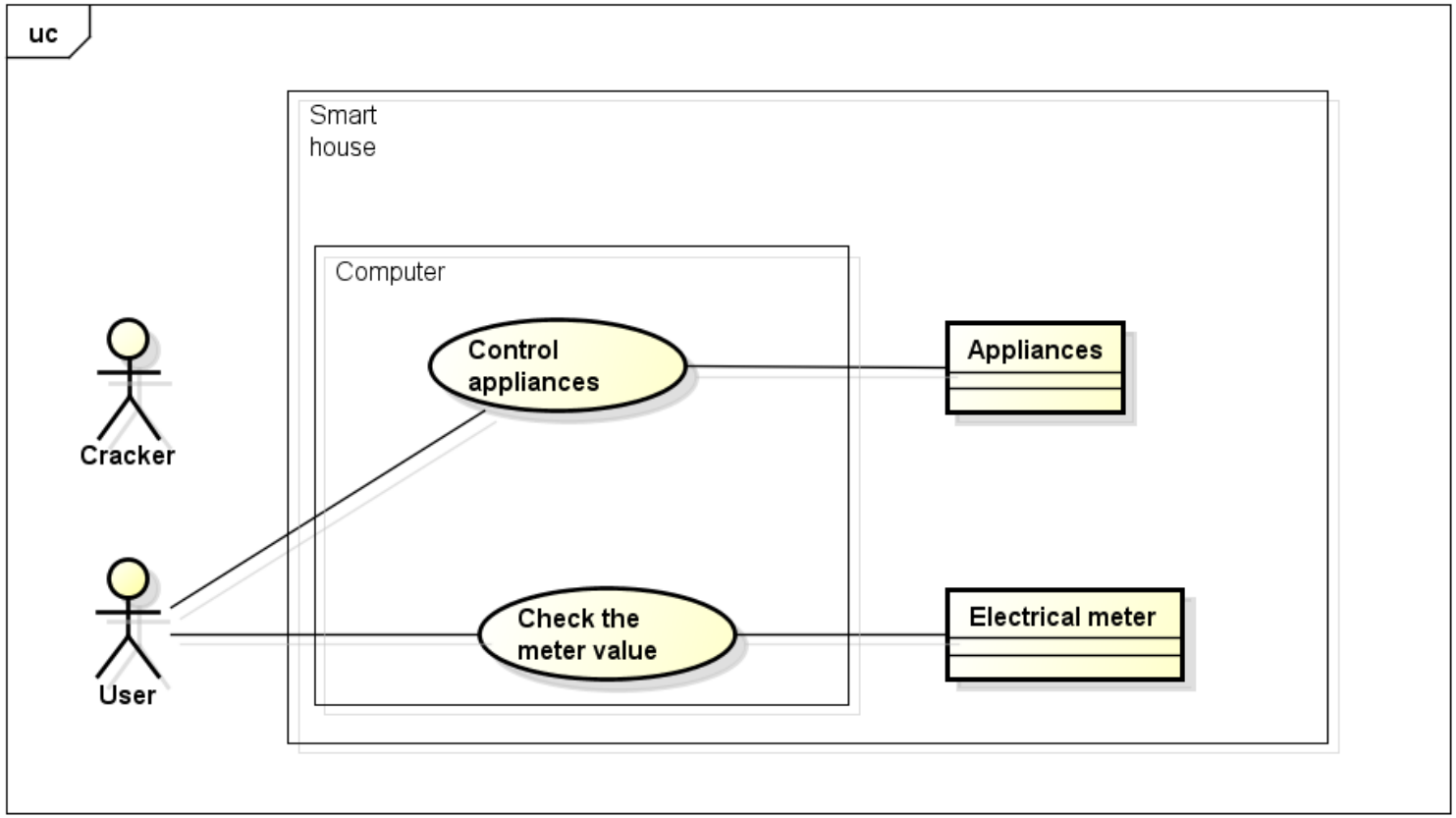
Use case 1 (Authentication and change password)

- User have to be authenticated before operating appliance, and we can change the password.



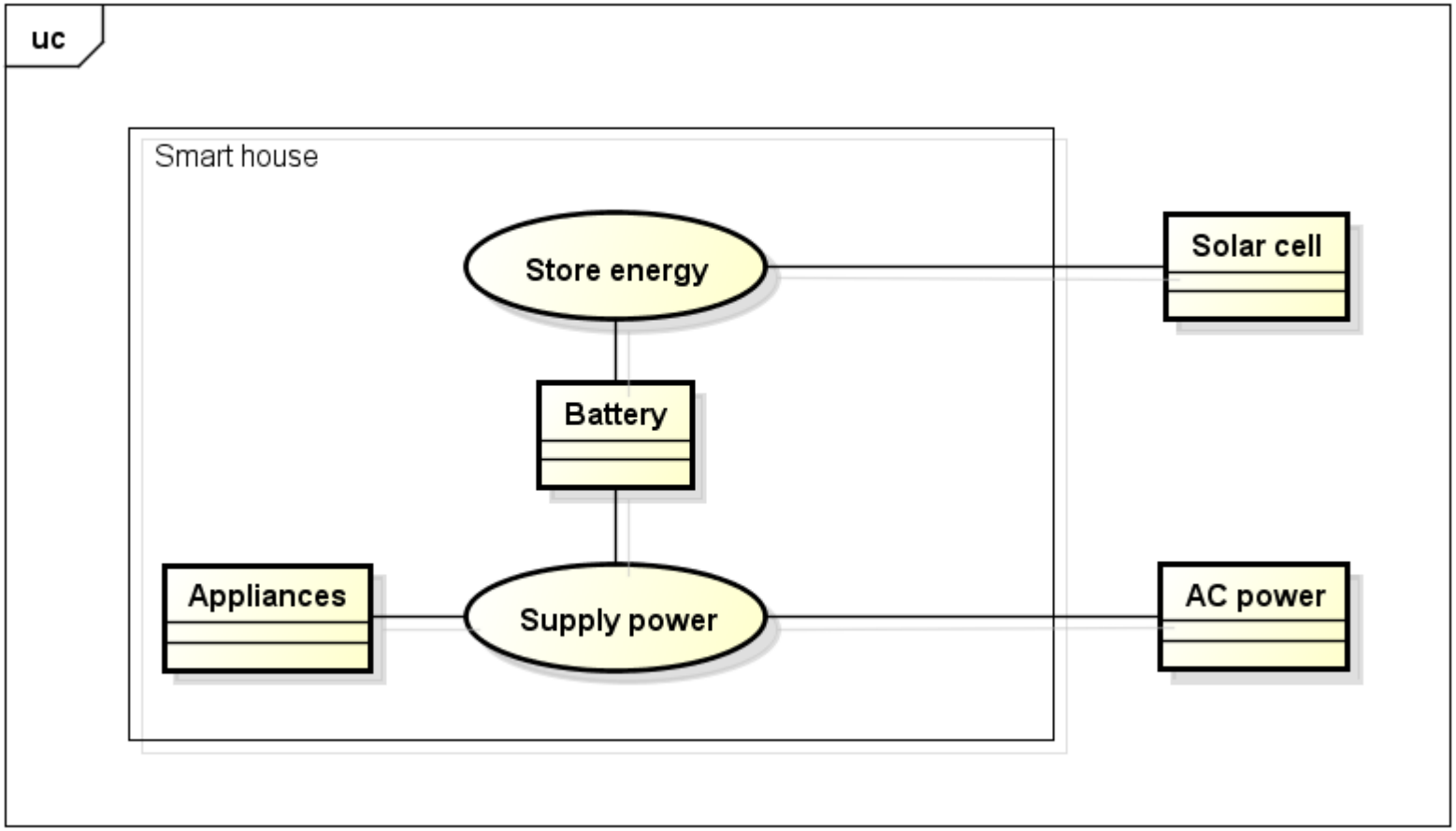
Use case 2 (Control appliances and check meter values)

- User can control appliances and check the meter values via smart-phone.



Use case 3 (Store energy and use it)

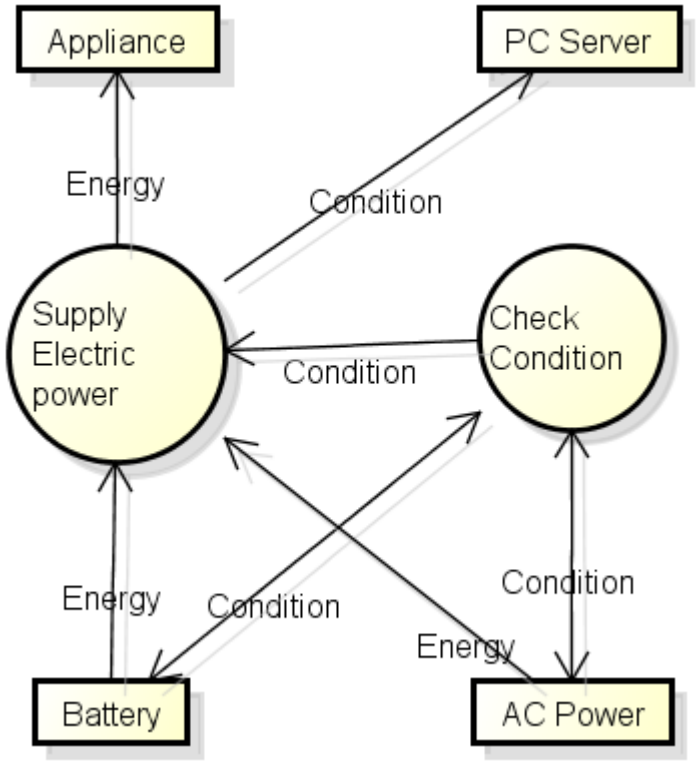
- Solar panel charge the battery and use it in accordance with situation.



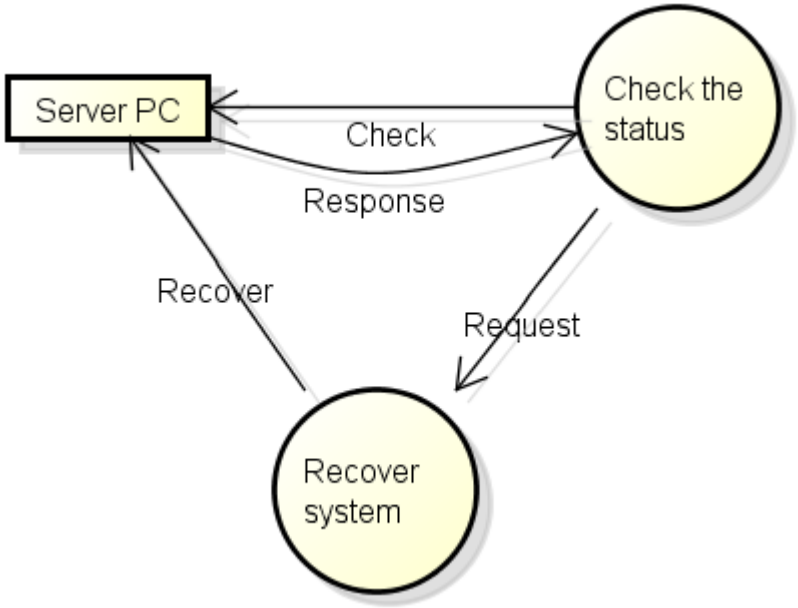
List of obtained hazardous situations

1. User use other mobile phone to connect to the system and forget to logout
2. Easy to guess password, for example password was “password”
3. Man-in-the-middle-attack, for example ARP Spoofing.
4. Visitors steal the memo or post-it that has a password
5. Malicious visitors glance the password on memo or post-it
6. Electric power (AC) is stopped by disaster
7. Explosion of battery
8. Chemical from battery.
9. Infection with computer viruses
10. System error has occurred
11. Children or pets crashed or turned off the server
12. User can control appliances while someone in the house using it

DFD as a architectural design 2 (Automatically switching system)



DFD as a architectural design 3 (Recovery system)



DFD as a architectural design 4 (Safety-related subsystem)