ITMD: 511 Application Development Methodologies

Chapters 12 & 13: Safety and Security Engineering

Exercise

1. Identify six consumer products that are likely to be controlled by safety-critical software systems. Explain your reasoning for each.

2. A software system is to be deployed for a company that has extremely high safety standards and allows for almost no risks, not even minor injuries. How will this affect the look of the risk triangle in Figure 12.3 in the textbook?

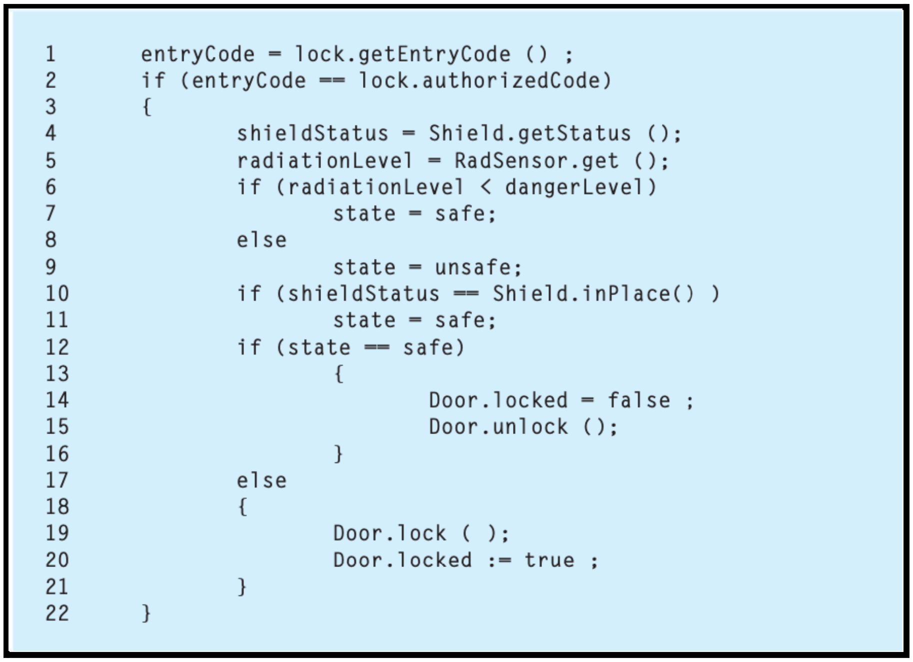
3. Explain when it may be cost-effective to use formal specification and verification in the development of safety-critical software systems. Why do you think that some critical systems engineers are against the use of formal methods?

4. List four types of systems that may require software safety cases, explaining why safety cases are required.

5. The door lock control mechanism in a nuclear waste storage facility is designed for safe operation. It ensures that entry to the storeroom is only permitted when radiation shields are in place or when the radiation level in the room falls below some given value (dangerLevel).
    a. So,
        i. If remotely controlled radiation shields are in place within a room, an authorized operator may open the door.
        ii. If the radiation level in a room is below a specified value, an authorized operator may open the door.

    iii. An authorized operator is identified by the input of an authorized door entry code.

b. The code shown below controls the door-locking mechanism. Note that the safe state is that entry should not be permitted. Using the approach discussed in this chapter, develop a safety argument for this code. Use the line numbers to refer to specific statements. If you find that the code is unsafe, suggest how it should be modified to make it safe.



```
1       entryCode = lock.getEntryCode () ;
2       if (entryCode == lock.authorizedCode)
3       {
4               shieldStatus = Shield.getStatus ();
5               radiationLevel = RadSensor.get ();
6               if (radiationLevel < dangerLevel)
7                       state = safe;
8               else
9                       state = unsafe;
10              if (shieldStatus == Shield.inPlace() )
11                      state = safe;
12              if (state == safe)
13                      {
14                              Door.locked = false ;
15                              Door.unlock ();
16                      }
17              else
18              {
19                      Door.lock ( );
20                      Door.locked := true ;
21              }
22      }
```

c.

d. Code above as a text box for editing

```
entryCode = lock.getEntryCode () ;
if (entryCode == lock.authorizedCode)
{
   shieldStatus = Shield.getStatus();
   radiationLevel = RadSensor.get();

  if (radiationLevel < dangerLevel)
  {
        state = safe;
  }

  else
  {
        state = unsafe
  }
```

```
 if (shieldStatus == Shield.inPlace())
 {
         state = safe;
 }

 if (state == safe)
 {
         Door.locked = false ;
         Door.unlock();
 }

 else
 {
         Door.lock();
         Door.locked := true ;
 }

}
```

6. Describe the security dimensions and security levels that have to be considered in secure systems engineering.

7. Explain why security is considered a more challenging problem than safety in a system.

8. Explain why it is important to log user actions in the development of secure systems.

9. Explain why it is important when writing secure systems to validate all user inputs to check that these have the expected format.

10. Suggest how you would go about validating a password protection system for an application that you have developed. Explain the function of any tools that you think may be useful.

References