# School of Information and Physical Sciences
# INFO6030 - Systems Analysis and Design

**Assignment 2 Part B: System Design (30%)**

**Due: 11:59pm Friday 2nd August (Week 12)**

**File Name: LabDay_LabTime_TeamName**

**File Type: Compressed Folder (Zip)**

**No AI tools to be utilised**

**UON Fire Management System**

## Introduction

The University of Newcastle is replacing its old fire management system for all their buildings. The fire management system is responsible not only for fire detection, but also for managing parts of the early suppression, compartmentation, and evacuation processes of the University's fire emergency response procedures as well as providing crucial information and control to fire-fighting services on-site. The fire management system (FMS) operates as a hub-and-spoke model, with a central hub managed by the University's Infrastructure and Facilities Services (IFS). The hub maintains a registry of all buildings operated by the University and connects to the local fire indicator panel (FIP, sometimes also referred to as a Fire Brigade Panel) in each registered building. The hub receives information and alerts from each FIP and can remotely issue commands and configuration updates as required. This is done via the main FIP on campus or via direct access using the IP address of registered equipment on the FMS.

Each building operated by the University has at least one FIP, usually located near the main entrance to the building. Larger buildings may have multiple FIPs located near the main entrances as well in a fire riser, if the building is equipped with one. The FIP takes input from all sensors and alarms located in the building and controls any alert and suppression equipment. Equipment differs depending on how the building is used; for example, rooms containing sensitive electrical equipment are not likely to use a sprinkler suppression system, as this is not ideal for fighting electrical fires. As a further example, food preparation areas such as staff kitchens may not be equipped with smoke detectors, opting instead for a different type of detector such as a heat detector.

Early detection of fires is crucial to an effective response. To that end, each building, and specifically, each detection zone (generally a single room or set of corridors) is equipped with detection equipment, both automated and manually triggered. This includes but is not limited to smoke detectors, heat detectors, carbon monoxide detectors, manual pull alarms, and manual break glass alarms. In some cases, a single zone may contain multiple detectors, particularly where a high rate of false alarms is likely to occur. As an example, a zone where smoke is frequently detected may still use a smoke detector, but the FIP may be programmed with a rule that will, when the detector is triggered, query a different detector in the same zone, such as a heat detector, and only enter an alarm state if the heat detector detects a temperature above a certain level.

When a fire is detected, the FIP will follow rules set by IFS, that, depending on the severity of the fire detected, may involve triggering suppression systems, evacuation, automatically contacting firefighters, and compartmentation systems. Suppression systems vary depending on how the zone is used, but may include sprinklers, gas suppression, foam suppression, and dry chemical suppression. A small fire detected in a small room with equipped sprinklers does not for example, necessarily require the entire building to be evacuated immediately. The FIP might be configured with a rule to first activate the sprinklers in the room, only triggering an evacuation if the detectors in the zone show the fire becoming worse after a set amount of time. The FIP can also shutoff building power, which may be necessary in some cases to remove a source of ignition for additional fires.

If, however an evacuation is necessary, triggered either by an automated rule, manually from the FIP or remotely from the hub, then the FIP may trigger warning systems in the building, such as sirens and strobe lights, such as from an occupant warning system and/or emergency warning and intercommunication system. The FIP may also detect conditions such as a power outage, or a high level of smoke in corridors and activate additional emergency lighting, or control dynamic emergency exit signs to activate their alarm modes with inbuilt speakers to guide people towards them, or in case an escape route is compromised, switch these signs into warning mode to alert people to seek an alternative exit. Note that not all emergency exit signs have these dynamic features included, some, including older models, may indeed not even be powered at all. As a fire grows worse, it may be necessary to attempt compartmentation of the fire. The FIP can be used to perform this task either automatically or manually, by closing fire doors, fire windows, and fire shutters within the building to delay the spread of a fire, allowing people additional time to escape. Fire doors are located at points within a building where fire resistant materials have been used in the construction of the building, and sub-divide the building into smaller sections that are typically easier for firefighters to manage.

The FIP, in addition to its automated functions, also includes an adjacent master emergency control panel in the same cabinet with indicator lights and buttons that allow authorised personnel and firefighters to quickly see the state of all connected sensors and systems, and to manually trigger or override them. It can also be used to send an all-clear signal to the system once the building is safe to re-enter, which will silence any alarms, reset detectors, and shut-off any active suppression systems. Any alerts are sent to the hub, which stores a record of any alarms, detectors triggered, suppression systems turned on, fire doors closed, firefighters contacted etc. Authorised IFS managers can generate reports of these records, which can be customized according to several parameters, for example, a list of the most frequent detectors triggered regardless of whether an alarm condition was entered (this is often used for identifying common culprits for false alarms). Another example would be a list of all recently activated suppression systems, and the amount of time they were activated for (this can be used to calculate how much water/chemical agent/foam/etc has been used and needs to be ordered to restock the relevant suppression systems).

Each building has at least one member of staff assigned to the role of evacuation warden for the building. The hub must alert these person/persons if an evacuation is triggered. Evacuation wardens can also manually trigger a building evacuation at any time. The current state of building alarms and equipment across campus are visible from the main FIP on the FMS network. To ensure that everyone can be accounted for, each building entrance is to be fitted with dual gait and facial recognition linked to the University database. If someone cannot be recognised, they should be listed as an unidentified occupant. The current building occupancy list will be stored in the hub and made available to the evacuation wardens of the building, as well as authorised IFS staff.

The hub can also send commands and configuration updates to the local FIP of each building. There are many possible ways that this could be used, for example, to trigger an evacuation of every building for a fire drill, to update the automated rules for a single building, to update the automated rules in every building for a certain type of equipment, to manually trigger compartmentation in a building if the local FIP cannot be accessed in a fire, to initiate system tests during an inspection, etc. For auditing purposes, any such use of the hub must be recorded and stored. Managers can generate reports of these records. Where commands are in conflict, the most recent command must take precedence; for example, the hub might send a remote command to close a fire door, but a person trapped in the building can still use the local FIP to temporarily open the door so that they can escape.

Both local building FIPs as well as the hub can be used to override building security systems. Areas that are usually locked by key or that require a University swipe-card to enter can be remotely unlocked in an emergency either in a single building from the local FIP or anywhere in the University from the hub. Use of this function must also be recorded for auditing purposes. It may be assumed that firefighters have their own unique code pre-programmed into every FIP that can be used to access all functionality. Additional codes to access some or all functions of an FIP, or multiple FIPs across a set of buildings may be added by IFS, either from the hub, or from the local FIP. Where added locally, the FIP will send this information back to the hub to prevent data conflict. The hub can communicate with the separate University security system for this purpose. The security system has a general override code associated with the fire management system as a whole that is used whenever the fire management system needs to override the security system. It is for this reason that the fire management system has the responsibility of associating use of this code with a specific user, or external firefighters (nominally this would be Fire and Rescue NSW) for auditing purposes.

The hub maintains all records, such as a list of buildings, equipment, configuration settings, users and their permission levels, alarms, overrides, etc. These records need to be easily searchable by IFS managers and auditors. Additional requirements for the FMS and other interconnected systems are available at https://www.newcastle.edu.au/__data/assets/pdf_file/0010/937639/UON-Fire-Services-Guiding-Principles-V1.3.pdf. Note that the scope of this project is restricted to the master control (hub) of the FMS, as other equipment comes from external suppliers according to defined standards.

## Objective of the system

The main objective is to develop an online management system for IFS that will control the hub of the fire management system. The local building FIPs are produced by other companies, but the hub needs to be able to communicate with them using their published addressable interface (IP address on the fibre FMS).

1. The manager needs all information at their fingertips to make decisions.
2. Safety is a critical aspect of this system, as failure could result in loss of life where a fire occurs.
3. The manager requires multiple types of reports, periodic each month, on-demand, and after-action reports (automatically generated after a major alarm state has been resolved).
4. Records must be kept secure, only accessed by authorised staff.
5. The system must be able to receive and report on equipment and sensor data as it comes in, that is, it must be 'live' 24/7, with reliability and uptime a priority.

The system should be online, so that, for example, IFS staff can issue commands from a mobile app outside a building in an emergency, instead of having to run to an accessible computer and login, although this should also be possible.

## Tasks

The system definition above will be used for the two assignments for this course. For this assignment, you will partially design and propose an implementation strategy for the system. You should identify system components and realize system requirements. In this assignment you will design the system according to the requirements identified in part A, map business rules to your design and construct a model of the system in UML. Specifically, you will develop sequence diagrams, interface storyboards, test plans, risk mitigation plans, and map out a class diagram for the solution domain.

There are no limits to how far the design and implementation might go. However, complexity, coverage and correctness of the elements will be taken into account in the assessment of the submitted work.

The main deliverable of this assignment is a report and Gantt Chart to be submitted via Canvas,

*Note,* your academic may also ask for a hard copy of the report and for your team to show your Gantt file in class.

For the report, you need to submit a Word or PDF document and a Gantt file in *one compressed (zip) file* containing the following:

1. **Report cover sheet containing the**
   a. Default is 5 Team members (first and last name and student numbers)
   b. Lab Day
   c. Lab Room,
   d. Lab Time and
   e. Lab academic (first name only)
2. **Introduction to the report (2.5 Marks)**
   a. What is in the report?
   b. Who is the intended audience of this report?
   c. What are the objectives of this report?
   d. How does each element of this report contribute to achieving the report objectives?
   e. https://www.monash.edu/rlo/assignment-samples/engineering/eng-writing-technical-reports/introduction
3. **Business Rules (10 Marks)**
   a. Refine business rules which you have already identified in Assignment 1 Part A. You may add on/ update your business rules as you discover more detailed requirements (as you perform iterative modelling). Your final list of business rules cannot be smaller than the requirements for part A.
   b. Explain how each business rule is captured (enforced) by your team design. This is an important part of testing your design. Remember some business rule may only be captured by human business processes. So is a business rule captured by an interface, by class data or a method etc?
   c. Use the following table format for this process

| Business Rule | System Mapping | Organisational Mapping |
|---|---|---|
| B1: Customer contact details | Data collected in the customer class and the interface | Manager notified if data is not complete by the system (not all BR will require this section) |

4. **System Design (30 Marks)**
   a. The complete subsystem specification for the system.
      i. You will need to identify the subsystems, and describe the services they each provide. (see Brugge and Dutoit Chap 6 Fig 6-29): Discussed in lecture 8 (see week 8 lab notes page 3: Fig 6-29)

    ii. Illustrate the relationships between each subsystem: Discussed in lecture 8 (see week 8 lab notes)

  b. A class diagram with all classes to be implemented (including the **Boundary** classes, **Controller** classes and **Entity** classes) and appropriate relationships between them.
  c. All attributes for each class. Include access modifiers i.e. private, public and protected for each attribute of the classes that are required for each Use Case: Discussed in lecture 7
  d. All operations/ methods, include access modifiers i.e. private, public and protected for each. You should also include input parameters and return types for each method.
  e. Your class diagram should follow principles of good system and object design as taught in lectures. Include a description explaining your design and the decisions you made.

5. **Use Case Mapping to Sequence Diagram (20 Marks)**
    a. Each team member will revise their **Use Case description** from assignment Part A (unless otherwise assigned by your academic) e.g. cannot use the logon use case.
    b. Each team member will **create a subset of the class diagram** (section 4) that shows only the part of the system required to implement their Use Case description: Discussed in lecture 7
    c. Each team member will **create a sequence diagram** (for the Use Case) that shows the relevant Boundary, Controller and Entity classes from your class diagram in section 5b.
    d. Give a short description for each diagram to briefly explain the interactions among the models to perform the use case.
6. **User Interface (10 Marks)**
    a. Each team member will develop a user **interfaces (i.e. screen design)** using your use case description, subset of the class diagram and sequence diagram (section 5) as the basis of your interface (The logon interface is not to be modeled).
    b. Use the storyboarding technique (eg Powerpoint) to illustrate each screen required by your use case, including alternate flows, and exceptions.
    c. Each interface (team style) must be consistent in appearance and visual style.
    d. Consider each user of your interface, considering accessibility and ease of use.
7. **Test Plan (5 Marks)**
    a. You are required to propose a testing strategy for the system, as well as any future modifications to the system. Your strategy should include different levels of tests:
        i. Unit tests, Integration tests, System tests, and User Acceptance tests.
        ii. For each level provide two example of white-box and two example of black-box testing (aside from User Acceptance tests, which will only have black-box tests).
        iii. Your test plan requires test cases, sample inputs, and expected outputs. Provide examples of possible defects to illustrate how your proposed testing strategy could identify a variety of faults.
8. **Risk Assessment (5 marks)**
    a. Identify a list and ranking of major and minor risks for the project.
    b. Rate the likelihood and impact of each risk to determine their severity.
    c. Risks with a high severity should include a mitigation strategy, and an updated rating before/after the strategy is implemented.
    d. To help with this you might like to consider questions such as:
        i. What is a risk matrix?
        ii. What use cases involve risk?
        iii. Are there any ethical considerations that will need to be considered – If so, what are they?
        iv. Are there any special privacy or security conditions expected by the client?
        v. The risks will include the project and your team (e.g. cost and schedule overruns).

9. **Deployment (5 Marks)**
   a. What is your team proposing for a deployment strategy?
      i. How will you address issues in data migration from the old system to the new system?
      ii. How will you handle user training?
      iii. How does your chosen strategy address the potential for system faults and bugs?
   b. Will you use a direct, pilot, parallel, or phased deployment (or a hybrid approach)?
      i. Justify your choice in comparison to the alternatives.
      ii. What are some potential disadvantages to your choice and how will these be mitigated?
   c. Have a look at the 14-2-Deployment.mp4 video link.
   d. Give an example (with inline citations and references) of a real-world situation where a similar strategy was used to support your argument.
10. **Team Management (10 Marks)**
    a. Meeting notes for at least 5 meetings and MS teams activity report
    b. Gantt Chart (MS Project)
       i. Your team will continue to refine your existing chart and show who has done what and the percentage completed for each task
       ii. This part of your assessment will be utilised if there is any issue with team management of production and team submission. Makes sure you keep copies of your individual work
    c. Self and Peer-Assessment process using TeamMates (5 marks individual, after team submission)
11. **Conclusion (2.5 Marks)**
    a. What was completed
    b. What was not completed and why
    c. How did each section of the report achieve the report objectives?
    d. What are your recommendations for the client?
    e. https://www.monash.edu/rlo/assignment-samples/engineering/eng-writing-technical-reports/conclusions-and-recommendations
12. **Reference list** (including but not limited to, any references used for the introduction and business rules sections in particular)

**Total 100 marks Final mark out of 30.**

*Self and Peer Assessment:* All team members will be individually required to complete a Self and Peer Assessment (see section 9c) within a week after the due date, this is an opportunity to reflect on how well your group performed and consider areas of improvement for future group work. The results of this assessment may be used to adjust the marks of individual members of the group where it is considered that a group member has significantly underperformed.

You will receive an email following the due date containing a link to the self and peer assessment. You will be asked to rate your own performance as well as the performance of each member of your team and give a brief comment justifying your ratings (this will be anonymous, only staff will see who gave each comment). Along with your assignment feedback, you will receive the anonymous comments from your teammates, as well as two scores: RPF (Relative Performance Factor), which is an indication of how your teammates have rated you compared to the team average; and SAPA (Self-Assessment to Peer Assessment), an indication of how you have rated yourself compared to how your teammates have rated you.