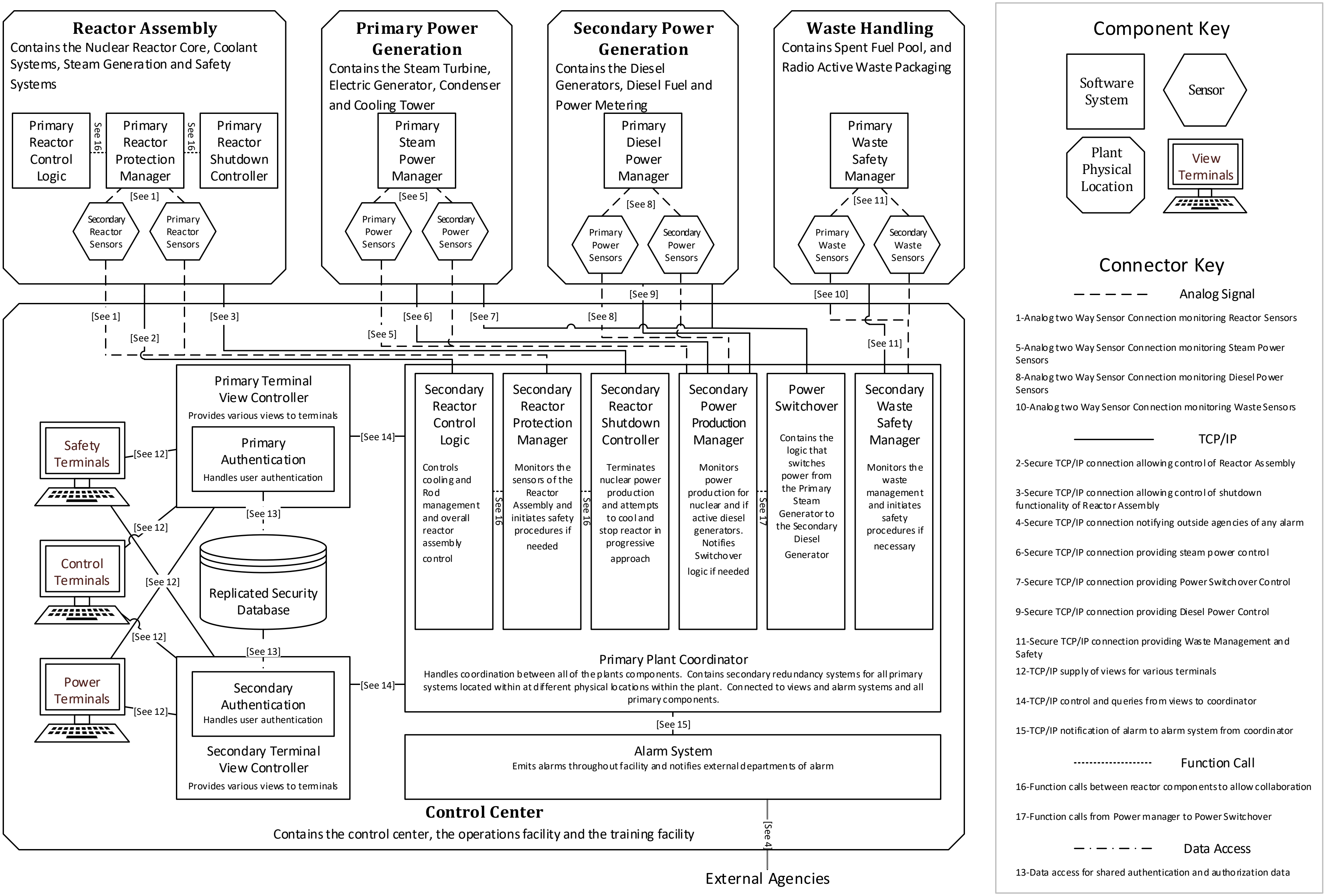
Nuclear Power Plant

High-Level Software Architecture

Tavish Burnah – CS-6500



Reactor Assembly
Contains the Nuclear Reactor Core, Coolant Systems, Steam Generation and Safety Systems

Primary Reactor Control Logic
See 16
Primary Reactor Protection Manager
See 16
Primary Reactor Shutdown Controller
[See 1]
Secondary Reactor Sensors
Primary Reactor Sensors

Primary Power Generation
Contains the Steam Turbine, Electric Generator, Condenser and Cooling Tower

Primary Steam Power Manager
[See 5]
Primary Power Sensors
Secondary Power Sensors

Secondary Power Generation
Contains the Diesel Generators, Diesel Fuel and Power Metering

Primary Diesel Power Manager
[See 8]
Primary Power Sensors
Secondary Power Sensors

Waste Handling
Contains Spent Fuel Pool, and Radio Active Waste Packaging

Primary Terminal View Controller
Provides various views to terminals

Primary Authentication
Handles user authentication

Replicated Security Database

Secondary Authentication
Handles user authentication

Secondary Terminal View Controller
Provides various views to terminals

Secondary Reactor Control Logic
Controls cooling and Rod management and overall reactor assembly control

Secondary Reactor Protection Manager
Monitors the sensors of the Reactor Assembly and initiates safety procedures if needed

Secondary Reactor Shutdown Controller
Terminates nuclear power production and attempts to cool and stop reactor in progressive approach

Secondary Power Production Manager
Monitors power production for nuclear and if active diesel generators. Notifies Switchover logic if needed

Power Switchover
Contains the logic that switches power from the Primary Steam Generator to the Secondary Diesel Generator

Secondary Waste Safety Manager
Monitors the waste management and initiates safety procedures if necessary

Primary Plant Coordinator
Handles coordination between all of the plants components. Contains secondary redundancy systems for all primary systems located within at different physical locations within the plant. Connected to views and alarm systems and all primary components.

Alarm System
Emits alarms throughout facility and notifies external departments of alarm

Control Center
Contains the control center, the operations facility and the training facility

External Agencies

Component Key

Connector Key

Analog Signal

1-Analog two Way Sensor Connection monitoring Reactor Sensors

5-Analog two Way Sensor Connection monitoring Steam Power Sensors

8-Analog two Way Sensor Connection monitoring Diesel Power Sensors

10-Analog two Way Sensor Connection monitoring Waste Sensors

TCP/IP

2-Secure TCP/IP connection allowing control of Reactor Assembly

3-Secure TCP/IP connection allowing control of shutdown functionality of Reactor Assembly

4-Secure TCP/IP connection notifying outside agencies of any alarm

6-Secure TCP/IP connection providing steam power control

7-Secure TCP/IP connection providing Power Switchover Control

9-Secure TCP/IP connection providing Diesel Power Control

11-Secure TCP/IP connection providing Waste Management and Safety

12-TCP/IP supply of views for various terminals

14-TCP/IP control and queries from views to coordinator

15-TCP/IP notification of alarm to alarm system from coordinator

Function Call

16-Function calls between reactor components to allow collaboration

17-Function calls from Power manager to Power Switchover

Data Access

13-Data access for shared authentication and authorization data

Nuclear Power Plant

High-Level Software Architecture

Tavish Burnah – CS-6500

The Nuclear Power Plant software is designed to provide a reliable, safe, and highly available system to control and monitor a nuclear power plant. The primary strategy used to offer these quality attributes is redundancy. There are 4 primary components of the system: The reactor assembly, the power generation component, the waste management component, and the control center. Each of these components makes available a commercial grade computer which runs individual systems. These systems are the primary control and monitoring systems for that component.

For example, the Reactor Assembly runs a primary reactor control logic, reactor protection management, and reactor shutdown controller systems. These systems are connected to redundant sensors. The sensors and components are then connected to a secondary coordinator within the Control Center. This coordinator hosts secondary versions of all of the systems provided within each component. These secondary systems are programmed in a different style and don't follow the same code paths as the primary systems. A discussion of how this architecture supplies the desired attributes follows.

The system is designed to be reliable. In this context, reliability means that the power provided by the plant is stable and consistent. The voltage and frequency of the power are kept within strict bounds. The plants power production is accurate and safe. Consistent power is available due to a backup, diesel powered generator. If for any reason the system is unable to generate power using the steam generator, a power switchover component will immediately start the diesel generator and continue producing power.

If an update to the steam components is required, the operators will intentionally switch over the power to the diesel generator and then shut down the steam generator and begin the update process. If a fault occurs, the safety system will shut down the steam power generation and nuclear process, yet the power will continue to flow through the diesel generator.

To keep the power consistent, both the steam and diesel power components have a Power Manager system monitoring power sensors. This system has the ability to tune the power as needed to keep the output within the specified bounds. Secondary Power Manager systems exist within the Control Center. These power systems monitor the sensors and settings as well, and if they notice that the Primary System is not making necessary changes, they will take over and force the system to make these changes.

Part of reliability is safety. This means keeping the resources of the plant from damage or harm. These resources include machinery, employees and infrastructure. Each component within the plant has a Management system that monitors sensors for detection of any safety problem. In particular, the Reactor Assembly contains a Protection Manager which monitors and reacts to any faults or problems.

A secondary protection manager exists within the coordinator in the Control Center. This system has a series of increasingly drastic steps that it can take to handle various situations. If the control rods overheat, the system will lower the rods into coolant. If the rods continue to overheat, the system will cycle the coolant through heat exchange. If overheating continues still, the system will engage the primary reactor shutdown using the component of the same name. Finally, if all else fails, a lockdown is engaged and alarms notify external agencies that drastic measures need to take place.

The system is meant to have high availability. This availability strives to minimize down time for power production. As with the components described above, the secondary power generation ability provided by the Diesel Generator allows for this high availability. A software system located within the Control Center's Plant coordinator is dedicated to this switchover. It not only performs the switch over, but routinely tests the switchover process and ensures that the diesel generator is running and in good condition.

The system is kept secure primarily by not being connected to the outside world. Despite this constraint security vulnerabilities could still be found by deep infiltration of the system. To protect against this, there are redundant authentication subsystems built into the view controllers. These subsystems give different users different views and controls based on their clearance. This ensures that a janitor won't be able to log into the system and control the rods causing a meltdown. Instead, the janitor is only given access to turn on lights or unlock certain doors.

Both of the authentication subsystems are connected to a shared, government grade, backed up and redundant database. Data stored on this database is encrypted using 512 bit encryption. Passwords to users are required to be changed monthly following strict guidelines.

The performance of the system is of the utmost importance. Sensor values provided must be real-time. Any fault scenario must be reported immediately and the appropriate alarms or status most be given. To allow for this, all sensors have a primary and secondary version. Both provide real time status using analog signals through high-quality security grade shielded cabling.

In addition to ensure high performance and awareness of problems, there is a dedicated component which is responsible for sounding any alarms. This component tests its capabilities monthly and ensures that it is in working order. The Terminal View Controllers are implemented using priority queues for messages and the highest priority messages are sent to the various terminals first.

The user interface is controlled through the Terminal View Controllers. As with other components in the system there is a secondary controller in case the primary controller fails. These controllers provide unique views for Safety, Control and Power terminals. These views are also unique per user based on permissions. The views are not meant to be pretty, but to be clear. The user should be able to quickly glance at a view and know what each symbol and component of the view means. The views also support displaying on large, wall sized panels. This allows monitoring of various systems from anywhere in the control center.