EPRI CCF Guide Chiller Controls Example

Bruce Geddes
Southern Engineering Services

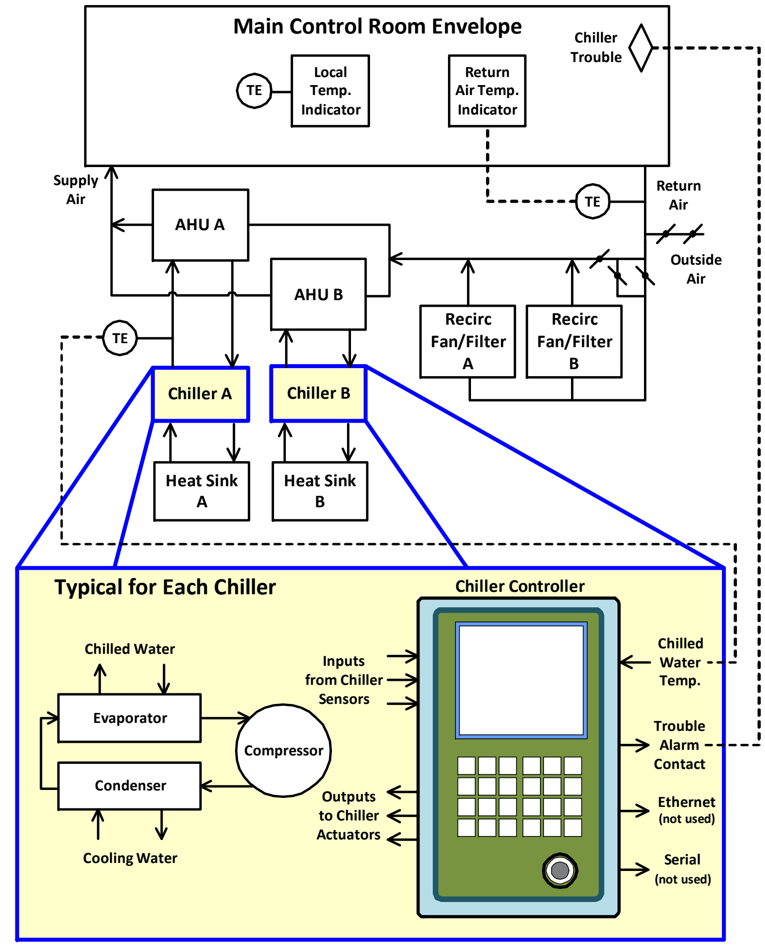
NEI / NRC "Tabletop" Meeting on CCF
11 July 2016

Tabletop Example – Chiller Controls Upgrade

The main control room envelope can be supplied with a combination of outside air and return air, and the indications and controls for the air handling units (AHU), recirculation fans & filters, and dampers are independent from the chiller controls. In addition, independent indications of MCR room temperature and return air temperature are provided in the MCR.

Each chiller is supplied with a digital controller that provides:

- Control of a variable speed drive on a centrifugal compressor
- Control of chiller auxiliaries (e.g., oil pump, water pumps, etc.)
- Monitoring and local display of controller inputs and outputs
- Menu display for changing chiller operating modes
- Menu display for changing chiller parameter values
- Dry contact output for a chiller trouble alarm
- Data communications (Ethernet and Serial) for remote indication and control (not used)

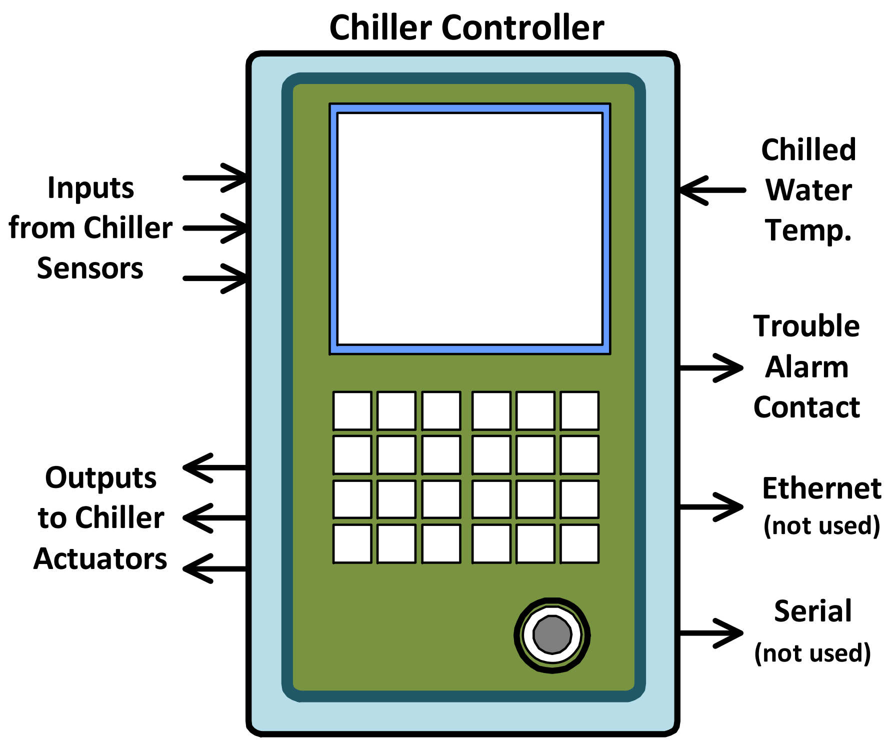


ELECTRIC POWER RESEARCH INSTITUTE

Tabletop Example – Chiller Controls Upgrade

Each digital controller is provided with some defensive measures:

- A real-time operating system that supports multi-tasking and interrupts.
- A watchdog timer that will shut it down in the event of a scan overrun.
- An identical configuration, qualified and commercial grade dedicated (CGD) by a third party.
- An operating history that shows an accumulated total of over 5000 unit-years spread over 10 years, using the same hardware and OS versions in continuous operation, with no software errors



CCF Susceptibility Analysis (1/2)

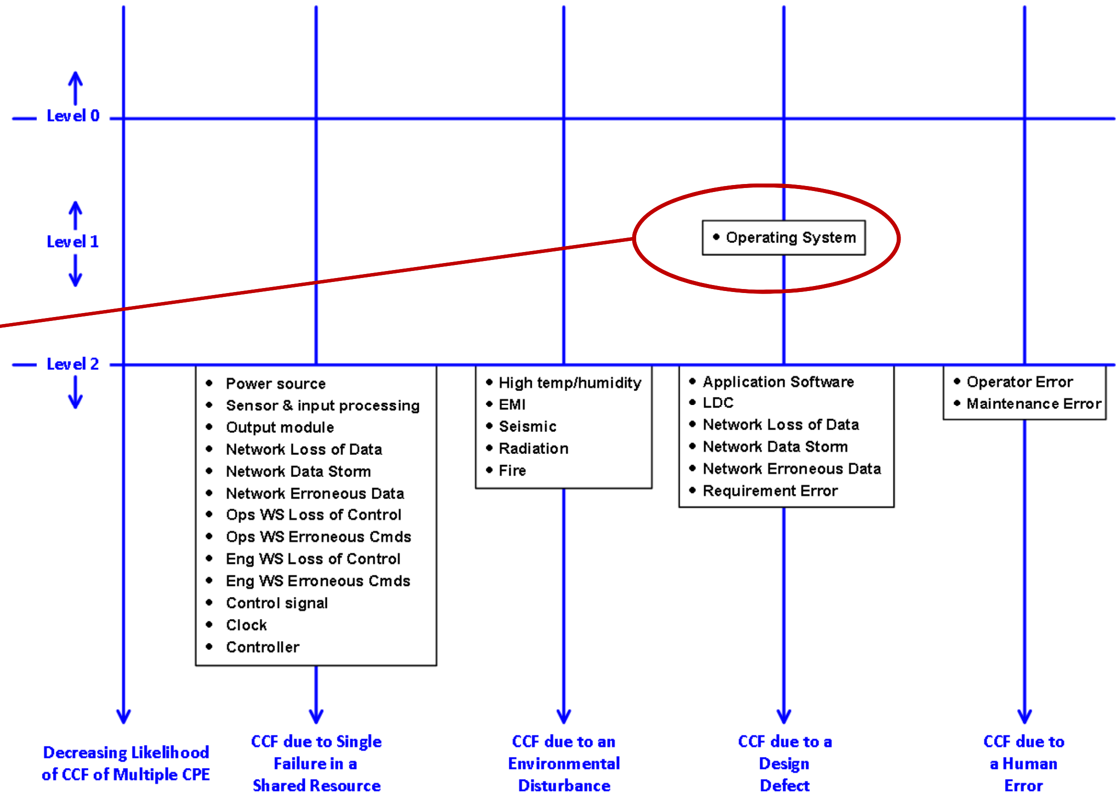
- CCF susceptibility analysis is a systematic assessment of all potential sources of CCF. In total, 26 sources of CCF are evaluated among the following 4 categories:
  - CCF Caused by a Single Random Hardware Failure in a Shared Resource
    - There are no shared resources between divisions, so the likelihood of a CCF of both chillers caused by a single random hardware failure is at Level 2
  - CCF Caused by an Environmental Disturbance
    - The designs meets all P measures for environmental disturbances, such that the equipment is qualified to its design basis environment, with adequate separation for other environment disturbances (e.g., fire). The likelihood of a CCF of both chillers caused by an environmental disturbance is at Level 2

CCF Susceptibility Analysis (2/2)

- CCF Caused by an Activated Design Defect in the Operating System
  - None of the P measures for an operating system defect are fully met. However, the commercial grade dedication of the chiller controls indicate the operating system quality is equivalent to that produced by a nuclear quality program, and a failure of a chiller controller in one division does not influence the chiller in the other division because they are physically and electrically independent.
  - Therefore, the likelihood of a CCF of both chillers due to an activated design defect is at Level 1 (much less likely than CCFs considered in the conservative safety analysis).
- CCF Caused by a Human Error
  - The P measures for a CCF caused by a human error is fully met. Therefore, the likelihood of a CCF of both chillers, caused by a human error, is at Level 2

CCF Coping Analysis (1/5)

A CCF of both chillers can result in maximum cooling by both chillers or no cooling at all by either chiller. Both scenarios are analyzed using best estimate methods because the CCF is from a Level 1 source



CCF Coping Analysis (2/5)

- Coping Analysis for a Level 1 CCF Source Employs Best Estimate Methods
  - Nominal conditions at the beginning of the transient or accident (e.g., no conservatisms with respect to initial power levels, primary coolant conditions, decay heat levels, etc.)
  - Credit for non-safety related mitigating systems and operator actions
  - Acceptance criteria similar to those accepted for PRA applications, including maintaining a coolable core geometry, and maintenance of containment integrity (e.g., containment isolated with environmental conditions less than its ultimate capacity)

CCF Coping Analysis (3/5)

- The "fail on" heat removal case has no adverse impact on MCR equipment and personnel beyond creating uncomfortably cool conditions. Heaters are provided in the MCR HVAC system for controlling humidity within limits, and the heater controls are independent of the chiller controls.

- The "fail off" heat removal case should consider eventual overheating of equipment located in the MCR envelope, including equipment required for achieving and maintaining safe shutdown. In the event that a total loss of heat removal by the chillers occurs, the control room operators will detect an increase in temperature by feel or by surveillance of MCR room temperature or MCR return air temperature indications, which are independent from the chiller controls.

CCF Coping Analysis (4/5)

- Existing calculations show that 2 hours (as indicated in the facility Technical Specifications) is enough time to begin safe shutdown from 100% power under normal conditions in the event of a total loss of MCR HVAC, before any adverse impacts on safe shutdown equipment occur caused by overheating
- Whether the plant is at power or the I&C failure is assumed to occur during a transient or accident, only the chillers are affected by the CCF that would be caused by controller failure. Air handling units and dampers remain unaffected, and are available for supplying outdoor air so that the MCR temperature is kept near the seasonal outdoor air temperature (best estimate), and one or more MCR doors can be opened to exhaust hot air.
- Operators can open safe shutdown equipment cabinet doors to reduce the local temperature rise caused by self-heating. Under these conditions, the equipment required for safe shutdown is not expected to reach their specified temperature limits (best estimate).

CCF Coping Analysis (5/5)

- No mitigating systems are affected by the loss of control room HVAC
- Control room HVAC is not a mitigating system
- Under realistic, best-estimate assumptions, radionuclide concentrations in the environment outside containment would be minimal, as many more failures beyond the control room HVAC would have had to occur in order for there to be significant fuel damage
- With adequate core cooling available, little or no fuel damage is expected, reactor vessel integrity is likely to be maintained and containment systems remain operable
- Therefore, the plant can cope with a loss of control room HVAC during postulated AOOs or PAs under best estimate conditions. Since there is no adverse impact to any systems credited for AOO/PA mitigation, this CCF is bounded by the events analyzed in the current deterministic safety analysis.

Together…Shaping the Future of Electricity

ELECTRIC POWER RESEARCH INSTITUTE