[Considerations for] Future Research on Preventing CCF

1.1.1 Preventing CCF Due to a Design Defect

In systems with a robust design process, design defects are typically the result of rare conditions that were not anticipated by the designers. Additional research should focus on the following defensive measures to prevent a CCF due to a design defect.

1.1.1.1 Simplicity – 100% Testing

BTP 7-19 requires no further consideration of a CCF due to a design defect for digital components that are sufficiently simple, as demonstrated through testing that encompasses all internal and external state combinations; this is referred to as 100% testing. But during a specific licensing review, NRC recognized that achieving this level of testing is not practical except for extremely simple devices that have very few inputs and internal states. During this review NRC relaxed their position based on the recognition that there can be untested combinations that have no bearing on the critical safety function of the device.

Future research should provide guidance for the following key "100% testing" issues:

1. Criteria for distinguishing critical safety functions from other safety functions of a device.
2. What partitions are needed between critical safety functions and other safety functions of the device to ensure there are no adverse interactions from untested functions.
3. What constitutes adequate testing to preclude further consideration of a design defect.

1.1.1.2 Simplicity – Embedded Digital Devices

Error free operating experience can be credited for I&C components with EDDs, to conclude that the component has no design defects, if the component is simple enough to correlate the operating experience to its nuclear application.

Future research should provide guidance for the following key EDD issues:

1. What simplicity attributes are necessary to ensure the nuclear application does not introduce new triggers for previously undetected design defects.
2. What configuration control attributes are necessary to ensure the I&C device applied to the nuclear application is 'the same' as the I&C devices for which the operating experience has been collected. For safety devices this configuration control is typically an element of commercial grade dedication.

1.1.1.3 Sufficient Diversity

BTP 7-19 requires no further consideration of a CCF due to a design defect for digital components that have "sufficient diversity". While this has been historically interpreted to mean different digital platforms, platform diversity is not a BTP 7-19 requirement.

Sufficient diversity, without a diverse digital platform is the basis of Strategy D in the ORNL Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, NUREG/CR-7007, ORNL/TM-2009/302. It is also the basis of NRC's approval of the Watts Bar distributed control system, described in NUREG 0847, Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Units 1 and 2. In both of these cases common digital platforms are employed, which may have a hidden design defect, but other diversities are credited to ensure concurrent triggers are avoided that could lead to a CCF.

When non-concurrent triggers are coupled with self-announcing that a defect has been triggered in one digital device, a CCF of multiple digital devices can be avoided.

Future research should provide guidance for the following key "sufficient diversity" issues to enable the use of a common digital platform:

1. What application level differences are necessary to constitute "sufficient diversity". As a minimum, this guidance should consider:
    a. Application program functions and memory load
    b. Input quantity and configuration
    c. Output quantity and configuration
    d. Digital data communication quantity and configuration
    e. Cycle times, task scheduling and CPU load
    f. Dynamic or different static memory allocation
2. What features are necessary to ensure a triggered defect is self-announcing. As a minimum, this guidance should consider:
    a. Continuous control applications (typical of reactor control systems) vs. standby control applications (typical of safety mitigation systems)
    b. Watchdog timers that detect both underrun and overrun conditions
    c. Exception handlers, such as buffer overflow detection, divide-by-zero, not-a-number