Digital protection and control systems are appearing as upgrades in older nuclear power plants (NPPs) and are commonplace in new NPPs. The hardware components of a digital system can be modeled probabilistically because they are subject to failure mechanisms similar to those of analog components, such as wear and tear, and thus can fail randomly. Software “failures” can be considered to be random, since although the way a fault is introduced into the software is not necessarily random, the occurrence of the particular context that would cause the fault to manifest into a digital system failure is random.

The models can be classified into three types: (1) models that combine hardware and software failures, e.g., a software failure is lumped together into a single event with the failure of an associated hardware component, such as a processor; (2) models where software failures are included as separate events; and (3) models where only hardware failures are considered (i.e., software failures are omitted).

There are no specific standards or guidance for modeling digital systems that a particular regulatory body has approved or endorsed.

the NRC sponsored several organizations to apply other methods to the case study of a digital feedwater control system (DFWCS). ASCA (U.S.) used the dynamic flowgraph methodology (DFM) [7,8], BNL employed a traditional Markov modeling approach [5,9],

Most organizations use failure modes and effects analysis (FMEA) with different levels of detail for hardware failures. The three exceptions are: (1) the Canadian Nuclear Safety Commission (CNSC) representative stated that identifying failure modes is not a major issue in modeling DIC systems of CANDU reactors in view of the level of detail at which they are modeled;

Usually, failure modes of software are not identified. Identification of hardware and software failure modes is an area recognized as requiring additional research.

Dependencies related to communication

Dependencies related to support systems

Dependencies related to sharing of hardware

Dependencies related to fault-tolerance features

Dependencies related to dynamic interactions

Dependencies related to common-cause failures (CCFs)

All organizations considered CCFs. The participants agreed that digital-specific CCF parameters are lacking. To evaluate their models, the participants used different approaches, such as expert judgment and the parameters of non-digital components. In general, the participants considered that the current methods for identifying and modeling dependencies are adequate, though some areas are thought to need more research (e.g., dependencies due to fault-tolerance features and dynamic interactions).

The representatives from many organizations drew an important distinction between control systems (such as a feedwater control system) and protection systems (such as a reactor protection system). They thought that dynamic methods might turn out to be useful for modeling the former, but will probably not be needed for the latter.

raw failure data; such information is scarce and sometimes unavailable.

Generic- and plant-specific data from operating experience , Plant-maintenance documentation, Licensee-event reports

gathered raw data used standard methods of reliability parameter estimation, i.e., classical and Bayesian methods.

data for fault coverage of a microprocessor of the DFWCS obtained by the method of fault injection

lack of data for quantifying probabilistic parameters of software failures,(eg probability of a software failure and CCF of software)

All organizations agreed that the impact of software failures should be accounted for in DIC system reliability models.

Digital systems are used for control and protection functions. Further, some are classified as safety-related, while others are non-safety-related.

The failure of software potentially can impact the occurrence of initiating events and the performance of mitigating systems. Software can potentially introduce some failure modes that were not considered for analog systems. There are large uncertainties in evaluating the reliability of software. Hence, quantitatively evaluating this reliability is difficult, and further research is recommended.

1)human errors associated with digital I&C systems are: An upgrade may introduce new errors into the system. due to their greater complexity and use of software

2)If the HSIs are not well designed or implemented, they are likely to increase the probability of human error during use.

that the contribution of software failures to the reliability of a DIC system should be accounted for in the models.