Digital I&C systems can be classified broadly as control systems (e.g. feedwater control system) and protection systems (e.g. reactor protection system). These systems can also be classified based on whether they are safety related or not. Digital control and protection systems are installed in new nuclear power plants (NPP) and as part of upgrades to older plants. Failures in these systems could either be in hardware or software. There could be random hardware failures, but random software faults are less likely. While hardware failures can be modeled probabilistically, software failures can also be modeled in the same way assuming that the faults caused in software are due to an underlying cause in the digital system. Some common digital system components are analog/digital (A/D) converter, microprocessor, digital/analog (D/A) converter etc. The failure of an I&C system could lead to core damage or release of radioactive substances.

A key issue of Probabilistic Risk Analysis (PRA) is to identify potential failure modes, effects and hazards of DIC systems. Failure Modes Effects Analysis (FMEA) can be used to support development of system reliability models. It aids in identifying hardware and software interactions in sufficient detail. But, there is no well established definition of a digital failure mode. Reliability is a result of features like fault tolerance, fault coverage, fail safe, redundancy, defense-in-depth and diversity of components.

Digital system reliability models either account for hardware and software failures separately or take both in to consideration in a single model. Software failures could potentially impact the performance of mitigating systems. Certain failure modes could arise due to software which was not originally considered for analog systems. Hence digital system reliability modeling is an area of research in itself. Regulatory bodies do not have standards or guidance documents exclusively on modeling these systems. The Dynamic Flowgraph Methodology (DFM) and Markov modeling method have been identified as top two methods for modeling DIC systems.

Dynamic interactions and common cause failures (CCF) must be considered in DIC reliability models. CCFs could occur either due to the operating system (OS) or the application software. While an OS failure could lead to failure of all processing computers, application software failure could affect related software functionality.CCF failure rates for reliability analysis are often subjectively assigned based on the quality of software development life cycle. Fault injection techniques have also been explored to generate failure data though these may not be as effective as field data.

Availability of raw hardware failure data is scare and hence expert judgment is often used to evaluate models with failure dependencies. Where possible, operating history, maintenance documentation and event reports are used as data sources. Classical and Bayesian techniques are used to estimate the model specific parameters. Theoretical failure rates could be gathered from design and prototype phase of hardware products.

Digital systems could fail due to human errors as well. These could be due to a software upgrade or faulty human-system interface.

Glossary:

**Fault coverage**: Percentage of faults that can be detected during testing of a digital system.

**Fault tolerance**: The ability of a system to continue operation in the event of a failure.

**Fail safe:** A feature in a digital system that minimizes harm to devices in the event of failure.