Appendix 1

DEFINITIONS

Active Safety Related System

A safety related system which actively participates in the nuclear electric generation process. Examples of active safety related systems are the Heat Transport System, which cools the fuel, and the Boiler Feed System, which maintains a heat sink in the boilers.

Availability

The fraction of time that a poised/standby system is available to perform its design function.

Atomic Radiation Worker

Any person who in the course of work, business, or occupation, is likely to receive a measurable dose of ionizing radiation from man-made source.

Barrier

A physical, administrative or people-based safeguard used to detect, prevent, discourage, terminate, or to compensate for unsafe conditions, equipment failure, or inappropriate human action.

Barrier Analysis

A root cause determination technique which examines systematically what barriers are, or should have been, in place to prevent an incident, and how and why they failed.

Bathtub Curve

The graph of failure rate versus time, whose characteristic shape is reminiscent of a bathtub in cross section. It begins with a rapidly decreasing failure rate during the so-called *infant mortality* or *burn-in* period, where failures are mainly due to manufacturing defects. Next comes a flat section during the so-called *useful life* era, where the failure rate is constant at its minimum value, and failures are random in time. Finally, the failure rate rapidly rises again, during the *wear-out* region of the curve.

Burn-in Period

See *Bathtub Curve.*

Change

In the context of NPP operations, any alteration (temporary or permanent) to systems, procedures, work practices or station organization.

Change Analysis

A root cause determination technique in which the circumstances surrounding an incident are carefully contrasted with the circumstances surrounding related successful experience.

Change Control

The process by which proposed changes are proposed, evaluated to be safe, approved, scheduled, implemented and documented.

Channelization

The provision of more than one independent means of transmitting energy or signals.

Example: Redundant and identical sets of instrument loops are provided to actuate setback, stepback and special safety systems.

Common Cause Failures (also called "Common *Mode* Failures")

Failures in more than one piece of equipment or structure due to the same external cause. Examples of ***common cause incidents*** are aircraft crashes, earthquakes, tornadoes, fires, floods, sabotage, high temperature environment, high radiation environment, steam environment, common design flaws, and common fabrication, installation, operation, or maintenance errors.

Compliance Monitoring

The monitoring of station O&M activities to ensure they are within the bounds defined by design requirements, regulatory requirements and operating procedures.

Configuration Management

The management of changes in order to keep the physical plant configuration consistent with the 'paper' plant—ie, the plant as described in the licensing documents, design manual, flow sheets, and data bases.

Conservative Decision Making

Basing decisions on the best available facts, and where facts are not available, taking the most conservative choice to protect public and staff safety.

Control Room Operator

The Operator authorized by the AECB and the Utility to operate the controls of a nuclear generating unit. Also called Authorized Nuclear Operator (Ontario Hydro), Senior Power Plant Operator (New-Brunswick Power), and First Operator (Hydro-Quebec)

Credited Mitigating Function

A credited function which serves to reduce the severity of an incident.

Critical Safety Parameters

Parameters crucial to the control of reactor power, the cooling of the fuel, and the containment of radioactivity during both normal operation and accident conditions—eg, reactor power, reactor inlet header sub-cooling margin, containment pressure, and liquid effluent radioactivity level. For comprehensive list, see station documentation.

Cross-link Failures

Related failures of more than one component or system due to a lack of physical or functional independence between the affected components or systems. An example of a cross-link failure is a contaminant in the fuel supply feeding more than one standby generator.

Defense In Depth

Defense in Depth is the principle that multiple, redundant, nuclear safety provisions are required to protect workers, the public and the environment from the radiological hazards of NPP operation.

Derived Emission Limits

Regulatory limits on chronic effluent emissions of various radionuclide groups, derived from the public dose limits.

Design Basis Accident

An accident postulated by the design process, and used to establish the functional requirements of safety related devices and systems per the Safety Report.

Design Basis Earthquake

The most severe earthquake characteristic of the geographical area of the station. DBE parameters are used to specify the seismic qualification design requirements for the group II safety related systems, which provide *control, cool* and *contain* capability during and after a DBE.

Design Criteria (System)

A clear statement of the criteria by which a system can be judged to have operated successfully. These criteria should be expressed as a set of minimum performance parameters whenever possible—eg, containment leakage rate < 1% contained mass/h at design pressure.

Design Pressure

The maximum pressure that a boiler, pressure vessel or piping system is designed to withstand safely.

Direct Component Replacement

In the context of pressure boundary work, the replacement of a component with an item that meets or exceeds the original design specifications without the requirement of welding, such as valves, strainers, pumps, and tube fittings.

Diversity

As a reliability design strategy, Diversity is variety in design, manufacture, operation and maintenance of redundant components or systems for the purpose of reducing unavailability due to common cause effects, such as design or manufacturing flaws, and operational or maintenance errors.

Dose Limits

Radiation dose limits for atomic radiation workers and members of the public, as set out by the Atomic Energy Control Board. These limits apply to the sum of doses received from all routes whether by irradiation of body tissue from internal uptakes of radionuclides, or from external radioactive sources.

Dry-out

The condition where critical heat flux is reached, and steam blanketing of the fuel occurs, resulting in a reduced heat transfer coefficient from the fuel to the coolant. Fuel failures are a likely consequence of dry-out.

Dual Failure

A serious process failure coincident with automatic shutdown by at least one of the shutdown systems, coincident with failure of either ECI or Containment to mitigate the consequences of the process failure. Failure to shut down is not considered, because coincident failure of both SDS1 and SDS2 is considered to be an incredible event, and both provide full trip coverage for all design basis accidents. Special Safety System failure in this case means inability to meet its design intent. An example of a dual failure would be a LOCA coincident with a failure (deflation) of Containment seals on both doors of an airlock.

Due Diligence

Exercising *due diligence* means taking all reasonable care and precautions to protect workers, the public and the environment.

Emission Compliance Monitoring

The measurement of radioactive environmental emissions to demonstrate compliance with the DELs and station emission targets approved by the AECB for the site.

Environmental Qualification

The process of providing documented evidence that safety related devices and systems are capable of performing their credited mitigating functions in the environments they may face following the relevant Design Basis Accident(s).

Event and Causal Factor Charting

An root cause determination technique in which the chronological sequence of events leading up to a problem, together with environmental conditions and causal factors influencing each event are displayed on a chart.

Fail Safe

A component or system performs its required function immediately and automatically as a result of a component failure--ie, component failure does not contribute to unavailability.

Fertile Substance

A substance containing isotopes which convert via neutron capture into fissionable material. For example, U-238 converts to Pu-239, and Th-232 converts to U-233. Thus naturally occurring uranium and thorium are fertile substances.

Fissile Isotope

An isotope of a substance which is fissionable by thermal neutron capture—eg, U-233, U-235 and Pu-239.

Fissionable Substance

Any substance that is capable of releasing atomic energy by nuclear fission. Naturally occurring uranium contains fissionable isotopes and is considered a fissionable substance.

Foreign Material Exclusion

The prevention of foreign material ingress to systems when they are opened for maintenance. The potential consequences of such ingress include erosion, corrosion and mechanical damage of system internals, and in the case of the Heat Transport System, a channel flow blockage, potentially resulting in fuel damage due to fretting or impaired cooling.

Guaranteed Shutdown State

A state in which enough negative reactivity has been inserted into the reactor core to ensure subcriticality in the event of any process failure, and condition guarantees are in effect to prevent net removal of negative reactivity.

Heat Removal Chain

A series of linked heat transport loops, each with its own heat sink—eg, the coolant removes heat from the fuel, the moderator removes heat from the coolant (via pressure tube, gas annulus and calandria tube), low pressure service water removes heat from the moderator (at the moderator exchangers), and the lake removes heat from the low pressure service water.

Heat Sink

A substance or a place that can absorb or utilize heat energy deposited to it. Terminal heat sinks have an essentially unlimited capacity, such as a large lake or the atmosphere.

Human Performance Enhancement System

An investigative technique developed by INPO to discover and eliminate the root causes of inappropriate human performance.

Impairment of a Safety Related System

A failure the system, such that the system would operate with a reduced redundancy or margin of safety, or would fail to meet its design intent.

Incredible Event

For purposes of limiting safety analysis to credible event combinations, an event combination is considered to be incredible if its frequency is less than 10^{-7} per annum.

Independent Verification

A personnel error reduction strategy where a second qualified individual independently verifies a critical action, or step of a critical procedure, prior to implementation.

Independence

Systems are said to be ***independent*** if a failure in one cannot cause related failures in the others. ***Independence*** is achieved by having no shared components or common services (functional separation), and by physical separation.

Infant Mortality Period

See *Bathtub Curve.*

Ionizing Radiation

Any atomic or sub-atomic particle or electromagnetic wave having sufficient energy to produce ionization when interacting with matter. Ionization occurs when an atoms or molecules become charged because of a loss or gain of electrons.

License

A document issued by a regulator, authorizing something under specified terms and conditions. In the context of this course, usually the Power Reactor Operating License issued by the Atomic Energy Control Board.

Major Work (on pressure boundary)

Repairs or modifications which require welding on systems or equipment where any of the following conditions apply:

- nuclear class 1,2 or 3 systems with design pressure > 103 kPa(g)
- gas or vapour systems with design pressure > 103 kPa(g)
- conventional liquid (not more hazardous than water) systems with design pressure > 1720 kPa(g), or normal operating temperature > 65°C
- conventional liquid (more hazardous than water) systems with design pressure > 103 kPa(g)

Margin of Safety

The difference between the conservatively established operating level of a parameter and the value where something unsafe occurs.

Margin-To-Trip

The difference between the conservatively established operating point and trip set point of a given operating parameter. It is a measure of how far the parameter must increase or decrease before a protective trip is actuated.

Maximum Individual Dose

Maximum dose to the most exposed member of the public for single and dual failures, as specified in the Siting Guide. Calculations assume an average member of the public from the most radiologically sensitive age group remains at the site boundary throughout the radioactive release. Note that the maximum individual dose for dual failures is higher than the legal annual dose limit for chronic releases.

Non Specification Component Replacement

In the context of pressure boundary work, replacement of a component with an item that does not meet or exceed the original design specification. (Requires MCCR and AECB approval.)

Non Standard Repair

In the context of pressure boundary work, a repair or modification to the pressure boundary of a system while pressurized, or a repair which cannot be performed using a standard approved repair procedure or work practice—eg, on-line leak sealing, hot tapping, peening, crimping, and bungs.

Nuclear Code Classification

For purposes of selecting welding procedures and non destructive examination test procedures, the nuclear code classification must be known. Nuclear systems are classified according to CSA standard 285.1 as NC1, NC2 or NC3, in decreasing order of criticality to nuclear safety.

Nuclear Emergency

An accident involving an environmental release of radioactive material, sufficient to trigger off-site notifications. The equivalent of a *radiation emergency.*

Nuclear Facility

In the context of NPP operations, a nuclear generating station, a heavy water plant, a tritium removal facility, or a radioactive waste disposal facility (including all associated land, buildings, and equipment).

Nuclear Safety

Nuclear safety is the protection of workers, the public and the environment from the radiological hazards arising from the operation of nuclear power plants.

Operating Experience

Experience gained from NPP operation from which can be derived lessons beneficial to the nuclear generation industry. These may be lessons as to how to achieve superior results, or lessons as to how to avoid painful losses resulting from poor performance.

Operations Manager

The person with overall responsibility for safe and efficient operation of a multi- or single-unit station. The position is authorized by the AECB. The Operations Manager may delegate his/her approval authority per the OP&P to subordinate managers, also authorized by the AECB.

Poised System

A system which is normally in a standby configuration and plays no part in the electric generation process. It remains available, ready to operate to minimize the consequences of a process system failure. All special safety systems and standby safety-support systems are classified as poised.

Pre-job Briefing

A safe work practice whereby the supervisor reviews both the conventional and radiation safety hazards of the job, and the appropriate protective measures, with the employee before dispatching the employee to the job site.

Prescribed Substance

Substance that can be used in the application of atomic energy, and is therefore controlled under the Atomic Energy Control Act—including heavy water, uranium, thorium, plutonium, neptunium, deuterium and their respective derivatives and compounds.

Pressure Boundary

An interface constructed of metal between a working fluid and atmosphere, or between two working fluids, which has a design pressure > 103 kPa(g).

Problem

A current performance of people or equipment, that is producing unsatisfactory results.

Procedural Compliance Policy

A policy mandating that workers follow approved procedures to do operations and maintenance.

Process System

A system used in the normal operation and control of plant equipment and processes for the production of power—eg, the primary heat transport system is a process system because it is continuously active in heat removal from the fuel.

Public Safety

Protection of the public from hazards associated with the generation, delivery, and customer use of electricity.

Quality Assurance

A planned and systematic pattern of actions designed to provide adequate confidence that items and services will be of the required quality.

Radiation Dose

The measure of ionizing radiation energy absorbed, in gray units (rad). Biological dose equivalent units are sievert (Rem). Unless otherwise specified, biological dose refers to *whole body* dose.

Radiation Emergency

An accident involving environmental release of radioactive material. The term preferred by civil response agencies is *nuclear emergency.*

Reactor Safety

The protection of workers, the public and the environment from radiological hazards associated with operating nuclear power plants. It includes the set of operating philosophies, management and work practices, policies, procedures, documents, equipment and systems in place to minimize the risk of serious accident involving the release of radioactive contamination to the environment.

Redundancy

The provision of components or capacity in excess of 100% of system requirements, such that failures of excess components or capacity do not disable the system function. Just as components can be redundant within a system, so systems can be redundant with each other—eg, SDS1 and SDS2 provide redundant automatic shutdown protection; auxiliary boiler feedwater, boiler emergency cooling water, and emergency water provide redundant heat sinks for decay heat removal, and so on.

Reliability

The probability that a component or system will perform its design function for a specified mission time, under specified operating conditions.

Risk

The product of the dose consequence of an effect times its frequency of occurrence.

Root Cause

A cause which, if eliminated, would prevent recurrence of an incident or problem.

Root Cause Analysis (or Determination)

An investigative process for determining the root causes of a problem, so that they can be eliminated to prevent recurrence of the problem.

Safe Operating Envelope

The set of permissible operating states which have been analyzed as safe, and described in the OP&P. The collective assembly of safety analysis assumptions about how the plant will be operated, including the numerical limits on system operating parameters.

Safe State

In the context of nuclear safety, the state or position that a component or system must be in to secure the safety of the unit—eg, when the unit is at power, the safe state for a SDS channel is in the trip condition.

In the context of work protection, the safe state is an isolated and de-energized state—eg, an isolation valve would be closed, and an electrical circuit breaker open.

Safety Culture

INSAG Definition: "That assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear power plant safety issues receive the attention warranted by their significance."

ACSNI Definition: "The safety culture of an organization is the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, an organization's health and safety management.

Organizations with a positive safety culture are characterized by communications founded on mutual trust, by shared perceptions of the importance of safety and by confidence in the efficacy of preventive measures".

Safety Related System

A broad class of systems, whose failure to perform per design intent could affect the radiological safety of the public and staff, by affecting the capability to control reactor power, cool the fuel, or contain radioactive material. For example, the moderator system is required for critical operation of the reactor, and serves as a heat sink for the fuel in the event of a severe LOCA with coincident failure of the ECIS.

Safety Support Systems

Those portions of active, common service systems such as electrical power, water supply, instrument air, that are essential for the proper operation of the Special Safety Systems. Class II power is an example. Also, those systems that support special safety system operation under accident conditions—eg, the PHTS, whose pipe work is used by the ECIS.

Seismic Qualification

The process of providing documented evidence that designated (group II) safety related components and systems are capable of performing their credited functions during and after a design basis earthquake.

Self Checking

A personnel error reduction stratagem where individual workers follow the *STAR* procedure when executing critical actions. *STAR* consists of the following steps:

- *Stop* before acting
- *Think* anticipate system response, confirm proposed action consistent with intent
- *Act* execute action
- *Review* confirm expected system response

Serious Process System Failure

Any failure of process equipment, procedure, or operator error which, in the absence of special safety system action, could lead to significant fuel failures in the reactor, or to a significant release of radioactive material from the station—eg, a loss of coolant accident.

Setback

The ramping down of reactor power set point at a specific rate by the reactor regulating system, initiated by detection of one or more designated process parameters exceeding setback limits. The reactor regulating system lowers power via normal control action using the liquid zone control system, and other reactivity mechanisms as required.

Shift Supervisor

The person (called a Shift *Superintendent* at some stations) responsible for the safe and reliable operation of the station, while acting on the duty shift crew. The SS position is authorized by the AECB. The SS is the senior supervisor, senior licensee, and senior technical resource in the shift crew.

Significant Event Report

An prompt written report produced by the SS providing details of an abnormal operating event. The criteria for determining whether an event is reportable via SER are found in station documentation.

Significant Fuel Failures

Fuel failures that significantly increase the I-131 content of the reactor coolant, typically by 500 curies or more.

Single Failure

A serious process failure for which all the special safety systems operate as designed to mitigate the consequences. An example would be a LOCA for which the shutdown, emergency coolant injection and containment systems operate as designed.

Special Safety Systems

These are the Shutdown, Containment, and Emergency Coolant Injection systems. These poised systems are designed exclusively to prevent severe fuel damage and significant releases of radioactivity to the public in the event of a serious process system failure. They play no role whatsoever in the process.

Saturation Margin

The amount by which existing coolant pressure exceeds saturation pressure at the prevailing coolant temperature.

Standby Safety Support Systems

These poised systems provide back-up electrical power and cooling water supplies when primary supplies fail—eg, emergency power system, boiler/steam generator emergency cooling system.

Stepback

A rapid power reduction initiated by the RRS (except at Darlington, where stepback is independent of the RRS) when one or more designated process parameters exceeds stepback limits. It is accomplished by dropping control absorbers (neutron absorbing rods) into the core.

Sub-cooling Margin

The amount by which existing coolant temperature is below boiling point at the prevailing coolant pressure.

Surveillance

The act of observing real-time activities or reviewing documentation to verify conformance with specified requirements and industry good practices, and to evaluate their adequacy and effectiveness.

Thermosyphoning

Circulation flow in the PHTS via natural convection, in the absence of forced circulation via pumps. Cooler, denser heavy water from the boilers 'falls' down the cold leg of the loop to the reactor, displacing the warmer, less dense heavy water and forcing it up the hot leg from the reactor to the boiler.

Unavailability

The fraction of time that a poised/standby system is not available to perform its intended design function. By definition, unavailability = 1 - availability.

Unreliability

The probability that a component or system will not perform its design function for a specified mission time, under specified operating conditions.
By definition, unreliability = 1 - reliability.

Useful Life

See *Bathtub Curve.*

Verification

The act of reviewing, inspecting, testing, or checking to determine and document that items, processes, services or documents conform to specified requirements. The verification of a document by signature means that the person is knowledgeable in detail with the contents of the document and accepts responsibility for detailed correctness of the document.

Wear-out Period

See *Bathtub Curve.*