The Certification Process for the Year 2000

Ontario Hydro Nuclear
Year 2000 Project

presented by Sig Rannem

for the OECD NEA International Workshop on
the Impact of Year 2000 on the Nuclear Industry
February 1999

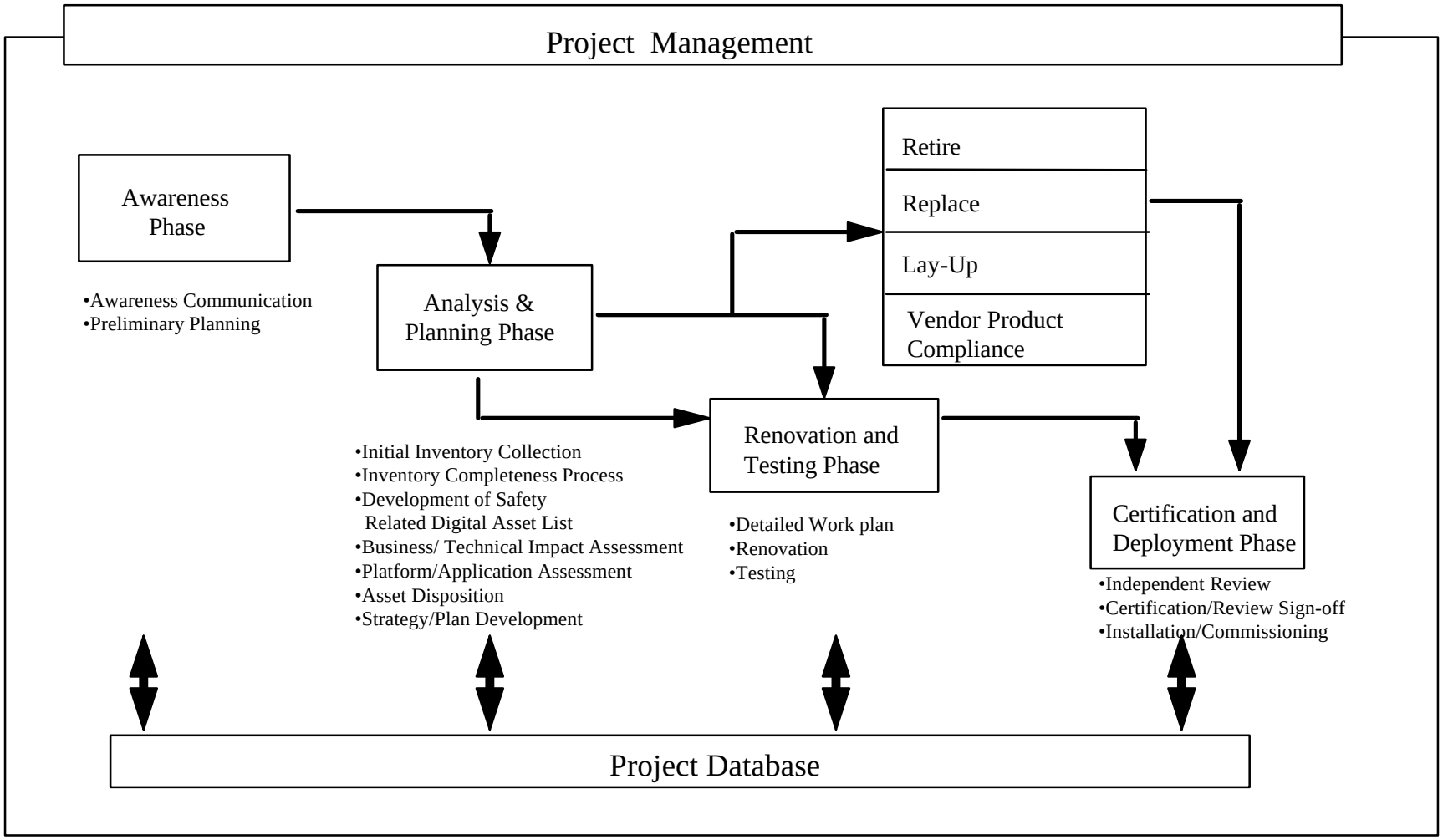
Objectives of Presentation

- Briefly describe overall Y2K certification process
- Discuss processes required for certification of nuclear safety related digital assets

Y2K Certification Process

- Certification process designed to provide assurance that:
  - digital assets deemed compliant, are compliant, and
  - for those that are non-compliant, the residual risks are identified, documented, and are acceptable to the asset owner.

OHN Y2K Process Flow



Business Impact Assessment

- Every asset is categorized according to its Business Impact
- This determines the rigour of the process to be followed

	Business Impact Rating		
Impact Factor	**High (incl. Safety)**	**Med**	**Low**
Safety	Risk of Injury/Death	Not Significant Risk	No Risk
Stakeholders	Major	Limited	None
Financial Impact	$ Millions	$ 100K+	$ 10K+
Core Product Delivery	Significant Disruption	Limited	Normal Tolerance
Environment	Impact Leading to Investigation	Not Significant	None

Safety Related Asset Categories

- Special Safety System (SSS)
- Failure Could Challenge SSS
- Other Safety Related

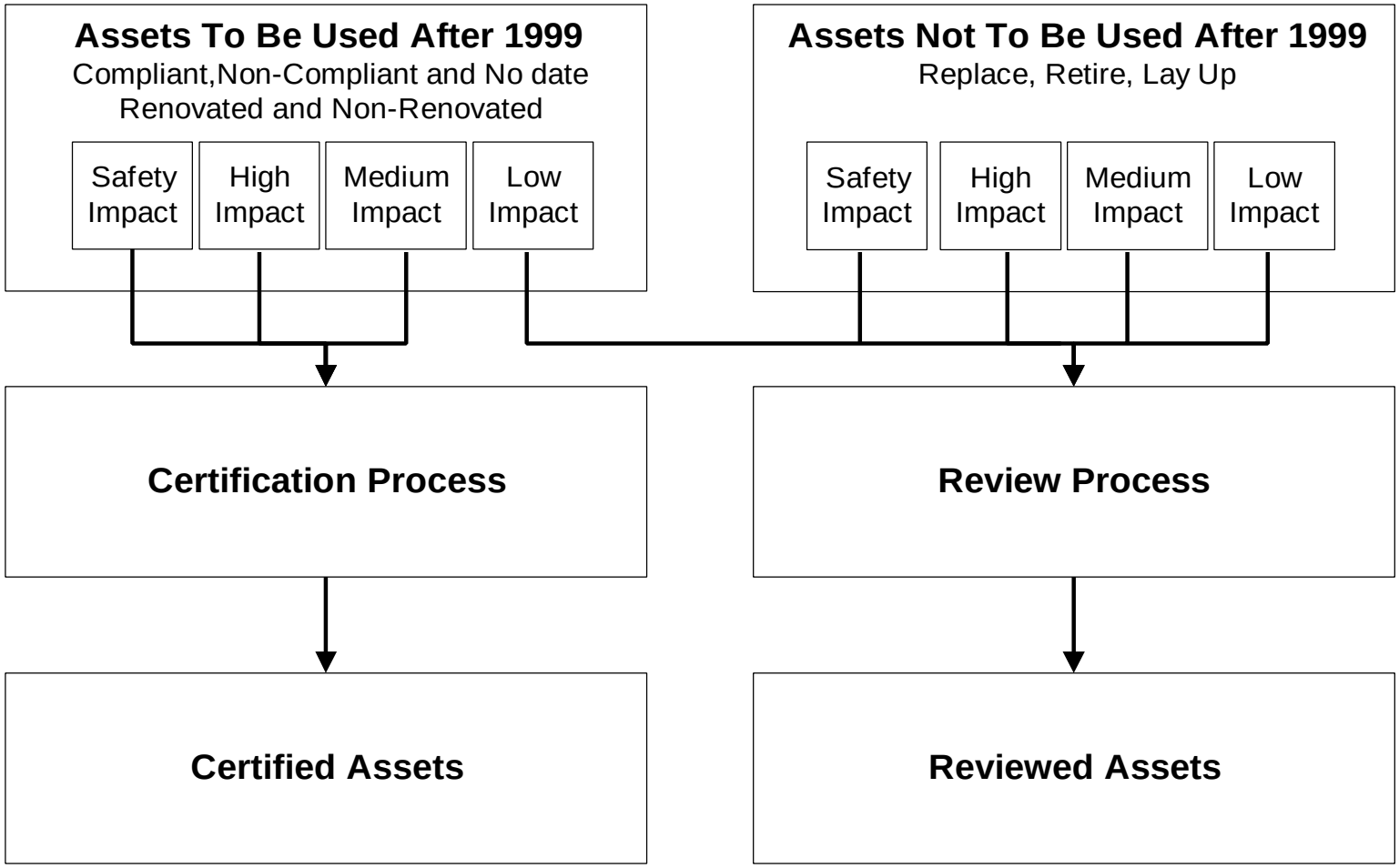
Compliance Assessment and Impact Analysis

- Y2K Compliance and Impact Assessment
  - Technical information recorded for the assets identified in the Inventory Process
  - Compliance assessments performed to establish Compliance status and determine required action
    - Technical Impact Assessment (TIA) for High & Medium assets
    - Platform & Application Assessments for Safety Related assets
- Compliance Categories:
  - No Date Capability
  - BSI Compliant
  - Compliant (life of asset + 20 years)
  - Non-Compliant

Compliance Assessment and Impact Analysis (cont.)

- Dispositions
  - Replace
  - Renovate
  - Admin. Procedure
  - Retire
  - Lay-up
  - Quarantine
  - No action required

Asset Certification and Review



Safety Related Process

- Flow Summary
  - Non-compliance of the asset identified in Platform/Application Assessment
  - Disposition established based on details of specific Y2K problems
  - PEP developed
  - Renovation performed
  - Station Change, Testing and Configuration Management Processes Applied

Safety Related Process (cont.)

- Flow Summary (cont.)
  - Y2K Test Plan and Test Cases developed (according to requirements and templates), then executed
  - Site sign-off on Certification
  - Independent Review
  - OHN Certification sign-off

Platform/Application Assessment

- Guidelines and Report Templates to ensure consistency
- Code Review Design Notes to assist in approaching the code assessment
- Platform Assessment deals with the hardware, operating system and software tools used to develop the application
- Application Assessment deals with the software application
- Investigates and documents in detail the compliance of the system and provides an auditable process of the methods used
- Explores alternatives for dealing with non-compliance

Renovation Process

- Assessments (Platform and Application) identify non-compliance of the asset.
- Asset Owner develops a Project Execution Plan (PEP) for dealing with non-compliant assets.
- Both Y2K Project Standards and Station's Normal Engineering Change Procedures combine to ensure change process is effective:
  - Normal Unit, Integration and Regression Testing are Performed
  - Normal Installation and Commissioning Workplan Developed

Y2K Testing

- Test Documentation forms an essential part of the Certification package.
- Testing Requirements Document specifies testing and test documentation requirements
- In general, an Asset's Business Impact will dictate:
  - whether Independent Testing/Review is required, and
  - the extent of Testing Documentation Required for Certification/Review
- Safety Related Assets require rigorous, independent testing, comprehensive documentation and independent review

Testing Requirements for Renovated Safety Related Assets

- Station-approved process to be followed for testing following software changes.
- Y2K Testing:
  - to cover all major systems functions, and
  - to cover all software Interfaces to Modules that have been modified

Testing Requirements for Renovated Safety Related Assets (cont.)

- Test Plan, Test Case and Procedures, Test Report produced by an individual independent of the Designer/Developer of the Y2K changes
- These documents require supervisory review
- Generally require approval of the Asset Owner
- Tester to be independent of the Designer/Developer of the Y2K changes

Independent Review

- To provide the Y2K Project Manager confidence that:
  - Assets can be OHN certified
  - Asset documentation provides an auditable trail
    - conclusions are documented
    - process for reaching conclusions is evident
    - method used is clear
  - Work is technically sound

Independent Review (cont.)

- Covers all aspects of Safety Related Digital Asset certification.
- Includes documentation, process and technical evaluation.
- Templates provided to give guidance, and promote consistency
- Reviewers to work in parallel with the site team

Independent Review (cont.)

- For due diligence purposes documents are required to be:
  - Complete
  - Consistent/Traceable
  - Correct
  - Correctly Filed and Controlled

Documents Reviewed

- Platform and Application Assessment
- Work plans
- Renovation work documents
- Testing Documents
- Site Certification Documents

Certification Sign-off

- Completes the asset certification process
- Independent Reviewer makes recommendation for Certification
- Package Reviewed by Licensing Engineer who makes recommendation for sign-off by the Y2K Project Manager