**Proceedings of IJPGC 2004**
**Power 2004**
**Baltimore, Maryland March 30-April 1, 2004**

**PWR2004-52003**

# RELIABILITY SOFTWARE TO DESIGN NEW GENERATING PLANTS

**J. K. August, PE/CORE, Inc.**
Jkaugust@msn.com (303-425-7408)

**Krishna Vasudevan/CORE, Inc.**
Kvdevan@msn.com (303-279-7170)

**W. H. Magninie/CORE, Inc.**
whmagi@cox.net (720-201-1863)

## ABSTRACT

Engineers design plants with overall income and operating cost objectives in mind. Defining system requirements, component functions, and failure modes, they discern risks that drive design. Maintenance costs get considered as an afterthought. Misunderstanding significant equipment failure modes greatly changes profitability. Improving certainty of plant economic success requires reducing the risk of unknown failures. Unanticipated operating restrictions can hobble commercial production. Avoiding unanticipated problems sustains predictable costs and operations. Relational software can reduce economic operating risk during plant design to project and control operating risks and maintenance costs.

## TERMS

ASME – American Society of Mechanical Engineers
NFPA – National Fire Protection Association
NEC – National Electric Code
NRC – Nuclear Regulatory Commission
OSHA – Occupational Safety & Heath Administration
FDA – Food and Drug Administration
EPA – Environmental Protection Agency
SOC – Safety-Operations-Cost
Failure Strategy
CMMS/EAMS – Computerized Maintenance Management System/Equipment Asset Management System
P&ID – Process and Instrumentation Drawing
TBM –Time-based maintenance
OCM – On-condition maintenance
CDM/CBM – Condition-directed maintenance
FF – Failure finding
Risk exposure classification – SOC
No (direct) risk – non-critical (X)
Failure Distribution
Safe Life Limit

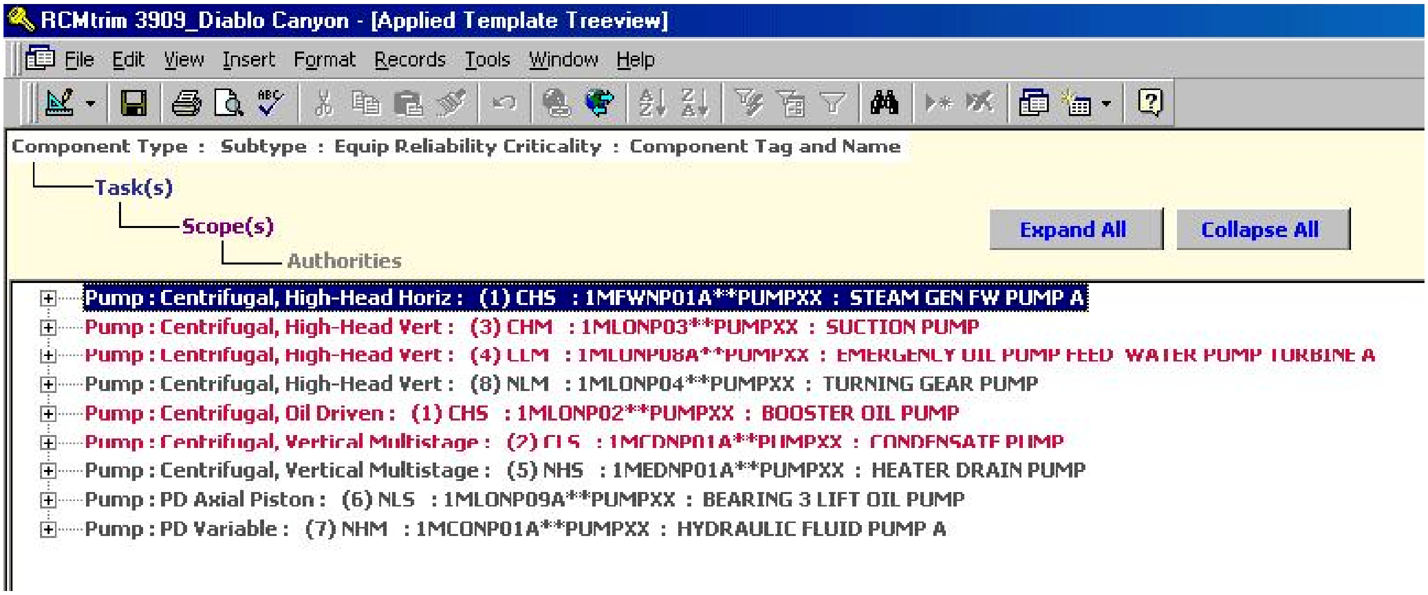
## INTRODUCTION

The purpose of any plant is to deliver a product or service. Owners establish plant production objectives before they engage an Architect Engineer (AE). The AE designs the plant to meet owner-operator's objectives. The owner engages a builder, who builds their plant to the AE's design specifications. Although responsibility for design can rest jointly among any of the three, the owners accept the final risk for plant operational success when they accept the plant.

Some production processes are inherently risky. Others pose only common everyday life risks. For example, risks associated with building occupancy occur in virtually all business. For unique and risky processes, however, codes, standards and other industry requirements may exist. Indeed, even simple commercial building design requires building code compliance. Boilers, reactors or other pressure vessel operation requires compliance with the ASME boiler and pressure vessel code as a starter. Electrical installations require NEC code compliance. Fire protection requires meeting the NFPA code. Special plants incur other codes or fall under special Federal, State, or Local statute jurisdiction. Nuclear plants comply with rules under CFR Part 50 (NRC). Emissions fall under Part 40 (EPA), food control under Part 10 (FDA), occupational safety under Part 29 (OSHA).

Regulatory agencies issue plant licenses stipulating how they must operate, defining technical specifications or other operating compliance measures that assure plant operations are safe and won't affect public health and safety in unforeseen ways. License requirements assure that plant operations are managed, controlled and maintained in ways that won’t impact the public interest. They should also help assure financial operating success, however, there is no regulatory requirement to do so. Reliability strategies are necessary, but they may not be sufficient for profitable plant operations.

**Figure 1: Risk Exposure Partition**



Component Type : Subtype : Equip Reliability Criticality : Component Tag and Name
Task(s)
Scope(s)
Authorities

Pump : Centrifugal, High-Head Horiz : (1) CHS : 1MFWNP01A**PUMPXX : STEAM GEN FW PUMP A
Pump : Centrifugal, High-Head Vert : (3) CHM : 1MLONP03**PUMPXX : SUCTION PUMP
Pump : Centrifugal, High-Head Vert : (4) CLM : 1MLONP08A**PUMPXX : EMERGENCY OIL PUMP FEED WATER PUMP TURBINE A
Pump : Centrifugal, High-Head Vert : (8) NLM : 1MLONP04**PUMPXX : TURNING GEAR PUMP
Pump : Centrifugal, Oil Driven : (1) CHS : 1MLONP02**PUMPXX : BOOSTER OIL PUMP
Pump : Centrifugal, Vertical Multistage : (2) CLS : 1MCDNP01A**PUMPXX : CONDENSATE PUMP
Pump : Centrifugal, Vertical Multistage : (5) NHS : 1MEDNP01A**PUMPXX : HEATER DRAIN PUMP
Pump : PD Axial Piston : (6) NLS : 1MLONP09A**PUMPXX : BEARING 3 LIFT OIL PUMP
Pump : PD Variable : (7) NHM : 1MCONP01A**PUMPXX : HYDRAULIC FLUID PUMP A

Plant design should also consider operating and economic risks, limiting those risks as much as practical. This is just good business practice. Although plants must produce products keeping overall operating risk acceptable, good designs mitigate operating risk. Plant operations cease when operations affect public health and safety. Shutdowns control operating risks, but at the expense of production. For safety risks, features like bermed petroleum tank farms, relief-valve protected pressure vessels, coal pile dust suppression, automatic combustible fire suppression (including offices), and excavation shoring are mandatory. Where direct safety is involved, these standards become the minimum requirements.

Operations and maintenance activities require more than safety and cost design considerations. Continuous production in an uncertain world requires online isolation for valve maintenance, filter replacement, and other routine rework. Many designs incorporate redundant design features not explicitly required by codes or licenses to assure production. These allow continued operations while servicing equipment thereby supporting safe, continuous production. Considering online maintenance during the design phase supports production by avoiding operations interruptions. Risky production activity incorporates design redundancy at two, three or even four levels. Multiple redundancy layers are common in commercial aviation, power generation, and refining operations.

## RISK DEFINITION

Risk (R) is defined mathematically as the product of probability (P) and consequence (C).

$$R = P \times C$$

Two factors drive risk – likelihood of the undesirable event, and its consequences. Assessing risk requires (1) identifying probable events, and (2) quantifying their consequences. Classifying risk by consequences provides a useful risk discrimination-ranking tool. The nuclear power industry has quantified risks from inception by law. Other industries now have risk identification processes, like process safety analysis (PSA), driven by operating events or political circumstances. (Consider, for example, Bophal, India or 9/11, for example.) **Figure 1: Risk Exposure Partition**

## RISK CONTROL STRATEGIES

Incrementally extending designs from successful "safe harbors" manages common design risk. Iterative facility design improvement introduces risk incrementally using experience. Incremental designs, however, under utilize new technology, penalizing revolutionary advances. Another strategy hinges on assessing new designs from first principles. Historically, empirical assessment has proven more uncertain. Modern industry needs assurance of success. Fortunately, risk assessment from first principles can be performed today using software.

Consider combined cycle plants. Advanced designs introduced a decade ago provided high efficiencies at the cost of increased process and material risk. Stretching the operating envelope realized dramatic efficiency increases. They came with increased operating risks and cost. Damaged, cracked and overheated turbine blades caused large production losses, leading to income loss and litigation.

New plants are only built with financial backing. To construct a new plant, the prospective owner must get financing. Bankers want assurance that a facility will be profitable; they want titles only as a last resort. To assure operations, owner-operators must completely address public safety issues. Where risky processes are involved, these typically require backup/redundant accident mitigation systems that reasonably assure public safety. Complex plants with special processes require specially trained operators. After safety, two remaining concerns assure economic viability. Economic success hinges upon certain production income and manageable operating costs. These reflect

- Availability (production and income)
- Operating costs (expenses)

Production losses occur two ways. For complex processes, loss of safety systems incurs plant shutdown for code, operating license, or other compliance reasons. Whether jet airliner, nuclear plant or chemical processing facility, loss of a significant safety system degrades the safety envelope and results in operational shutdown. Licenses may allow limited operations under higher-risk, but only to facilitate orderly shutdown. Nuclear operating licenses require shutdowns within 24-72 hours of redundant safety systems loss, and immediately when direct failure potential exists. Plant licenses don't immediately demand shutdown for safety system redundancy losses by accepting higher risk for limited periods to facilitate orderly operations. Assuring key safety systems are never lost allows uninterrupted operations. Allowing operations, however, doesn't guarantee plant economic success.

Eliminating safety system shutdown threat, the plant must still reliably generate product for income. Production is always the main plant objective. A plant must reliably support steady production, after other considerations. This establishes a hierarchy of risk – safety first, operations next, and costs last. Plant owners wisely address risks in this order for ethical reasons, and because business risks are based upon probable costs. This manages risks by type reducing operating costs.

After assuring production, reducing operating costs to maximize profit remains a practical business objective. Operating costs are driven by equipment operation and maintenance requirements. Clearing ("tagging") equipment, performing online maintenance, engaging specialty services, reworking parts, and completing outages ontime assures plant production, without operational or safety-based losses.

## MANAGING RISK

Risk management during design requires three risk-control steps: (1) providing appropriate redundancy, (2) providing effective instrumentation for process and equipment control, and (3) providing robust design for unavoidable single point failure. In short, consider:

- Process instrumentation (to alert redundancy loss and off-normal conditions)
- Redundancy (to reduce single failures)
- Robustness (to defend against unavoidable single failures).

## INSTRUMENTATION

Instrumentation extends the five senses, directly monitoring processes and alerting off-normal conditions. Where critical process parameters convey process failure conditions unambiguously, condition alerts can be provided as audible alarms, computer display alarms, flashing lights, and other warning devices to gain attention and stimulate response. Instrumentation serves two primary roles – process control and status indication. Process control, for example, controls an induction draft (ID) fan speed controller's output maintaining boiler vacuum. Status indication senses and alerts a low draft condition. Loss of status or failure-alert hidden instrumentation has no direct process effect. Their losses, however, create conditions that leave operations exposed to unacceptable risks, and must therefore be identified and controlled.

## REDUNDANCY

Redundant equipment mitigates losses that affect production. Losses can be direct – as in the case of a production component like a generator, or indirect, like the loss of a critical safety device such as an overspeed trip governor. The latter requires shutdown based upon safety consequence consideration, not actual events. Regulators and licensed operators may overlook design subtleties. While trains and skids can provide redundant configurations with moderate ease (and added cost), operating interfaces (and their redundancies) cannot. Complexities that stem from redundant designs require risk evaluation with redundancy removed, finding hidden failures to make operators aware of lost redundancy, and developing on-condition maintenance strategies in absence of self-identifying or otherwise fail-safe features. Redundancy features provide little or even negative operational value in the absence of a living maintenance strategy. Cases of supposed safety and backup systems and features that failed to operate as intended are legion in the history of modern technology.

## ROBUST DESIGN

Where redundancy has no value, the equipment itself must incorporate adequate design margin to make failure incredible. High-pressure, high-energy steam piping must have adequate structural strength to never fail over its design lifetime. Electric generator windings must never fault causing generator short to ground. Robust design features are required for process containment and production purposes. Many processes enclose high-energy fluids, high voltage, aggressive high-temperature gases, corrosives, high-pressure air, or combustibles. Handling these safely requires that they are contained under all conditions.

To manage risk, reliability engineering combines design strategies. Three risk levels – safety (to allow production), operational (for uninterrupted production), and cost (to be cost competitive) drive plant economics. All plants must manage risks on these three levels. Incremental plant designs pose low risk based upon iterative changes from established designs. Plants with completely new processes must manage risks from fundamentals. That is more demanding, fraught with larger effort to envelop all outcomes – including simple economic risks. Ultimately, all risks reduce to economics. Modern culture places tremendous value on human life, however, and strategies that assure health and safety are not just economically sound, they reflect cultural values.

## NEW DESIGNS

New facility design can manage risk by limiting new designs to variations on those already proven. Avoiding new designs avoids introducing risks inherent with new processes. However, these restrictions have consequences limiting new technology and excluding innovation from the marketplace. So although new product introduction – electricity for example – has risks, economic benefits may far outweigh those risks. Net mortality reduction from electrification over the past century far outweighed direct mortality costs, since dwelling fires declined as electricity became widely available for lighting, cooking and other purposes. Indirect technology benefits are hard to project. Risks that appear unacceptable in absolute terms can actually be favorable, relatively, culturally and socially.

Evaluating new designs requires reducing seat-of-the-pants intuition. An AE must design a plant in compliance with existing codes and standards, and develop new processes to limit the owner's risk. AE's who do this well command higher premiums, more commissions, and may well be sole sources of credible new design capability.

AE's help owners obtain financing by designing reliable operating facilities that comply with regulations. These can be insured; they operate predictably. The challenge with any new design is to assure the designed facility operates to production and reliability specifications. Where designs incrementally evolve from standard off-the-shelf designs, the AE's job is considerably simpler. Where designs are new, radically different, presenting different processes, they pose new risks and warrant different, more thorough approaches to manage risk. In both cases, quantifying and mitigating production risks rests with the AE. AE design experts anticipate failures embedded in designs, apply codes to processes and facility designs, and provide failure mitigation features. AE's design; owners operate. AE's understand process performance issues during design, but focus less on operating (including maintenance) and profitability than safety. When AE's anticipate new design operating risks, they improve outcomes. Allowing prospective owners to participate in risk assessment improves operational risk management.

## ARCHITECT ENGINEERS

AE's design the main process flows, applying codes, standards, and established risk control principles, executing design as contemporary, evolutionary or fundamentally new. The last requires most diligence considering unforeseen operating risks. Risk evaluation can include:

- Application of known experience to systems and their equipment
- Identification of credible failures at the equipment level
- Simulation of plant operational impacts for all credible equipment failures

An AE's challenge is to evaluate risks excluding incredible "meteor strike" events from the plant design basis. Able AE's perform this task more effectively, reducing the future operator-owner's risk. Conveying the analytical results to the owner's operators poses challenges, however.

Explicitly determining risk requires assessing rough draft P&ID processes to capture equipment utility and redundancies. Performing equipment level failure analysis at the design step can't be overemphasized; only the designers know equipment redundancies, monitoring instrumentation, and direct failure potential provided in the original plant design. Failure to capture design intent at this step leaves it implicit or even lost forever. Traditionally, the AE's role stopped with P&ID and associated drawing development. Removing owner-operating risk requires that designers look at the process equipment itself. This requires projecting equipment failure consequences into systems and trains, their associated plant reliability and availability impacts, and the consequent operating and maintenance costs associated with the design. This holistic design assures the owner's overall design objectives are met to a higher degree than ever possible before.

Mitigating design risk reduces to

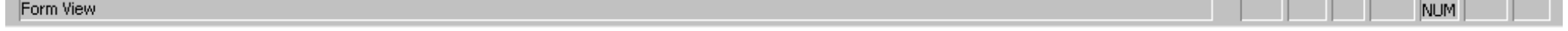
- Quantifying and reducing unknowns
- Identifying credible equipment failures to avoid
- Controlling equipment failure system impact

No owner can afford to design for virtually every failure; practically, this is unnecessary. Some failures can be mitigated through redundancy. Trains and standby equipment skids perform this role. Other failures can be mitigated with design margin. ASME pressure vessel and other codes perform this role. Primary equipment loss mitigation is the designer's role. Uncertainties of equipment service and plant longevity make assuring margin over the equipment's operating life less certain. Some failure phenomena (like fatigue) are well understood, although they exhibit considerable dispersion; others are less so. Appropriately balancing margin and cost in design assures building economic plants that still sustain long, trouble-free commercial operation. Developing more complete design bases allows the owner to review and challenge design assumptions reducing overall facility operating risk.

## PROCESS

Designing a facility while managing risk involves three major considerations, once production and its support processes are known. First, how do the functions provided by the major systems and their supporting subsystems rank based upon risk? Establishing the relative ranking determines probable safety, operations, or cost impacts (or none at all). For important equipment, failures that can actually occur drive risk. Typical equipment never experiences most failures theoretically possible, based upon failure analysis.

Second, what probable failure modes credibly drive risk? Dominant failure modes occur in the equipment because intrinsic design, use, and environmental conditions match



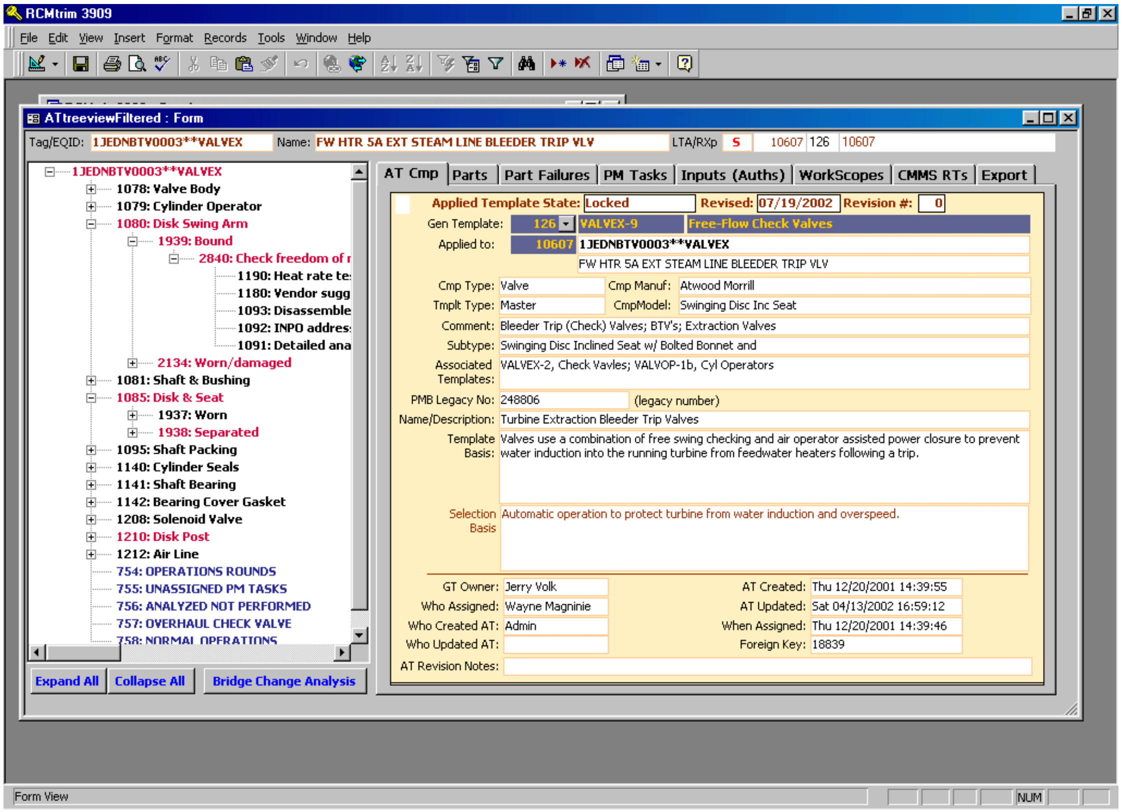
stresses against capabilities. How do we determine those equipment failure modes that really will occur? There's a bit of science and art in the answer. Science develops credible failures from first principles, comparable experience and statistics. These failure candidates warrant serious consideration, while ones that aren't likely must be removed. Failure screening reduces to a set of logical tests. Practically, failure engineers with plant maintenance experience select credible failures best. Because most generic equipment failures won't be seen in actual applications, real life criteria selection – mean age at failure, safe life limit, and failure distribution shape – require insight. Failures of interest include those with operations and cost implications. They also include cost-based or redundant equipment failures affecting safety. Knowing which is which, and why, assigns preliminary rank.

Finally, what are the total operations and maintenance plan performance costs for the resulting scheduled risk-mitigation tasks? How do these contribute to the overall cost of operations, in risk terms? What expenses are discretionary (if any) and what aren't? Ranking safety and operations first, it's easy to determine costs that will be required in a new facility under any operational scenario. The final question is what expenses facilitate production by improving cost performance. Costs are directly within plant control, have relative impact on financial performance. Those exceeding around $100,000 threshold have substantial impact on maintenance costs contribution to operations.

## DATABASE DESIGN

Design risk management software must relate failure risks with mitigation strategies. It must identify simple scheduled tasks that enable operating staff to work effectively. Software should be able to quickly reassess design risk, while the design is fluid and changing. Iterative recalculation of design process layouts, dominant failures, and probable production cost impacts must be easy. Capturing component characteristics that comprise the planned facility must be flexible, simple, and useful. Analyzed components should allow equivalent component substitution. Selection and re-selection of components, trains, suppliers and even processes for reliability, risk and cost are necessary. Assessing results optimizes the design. Iteratively "failing" equipment (e.g., resetting the operational state) while assessing train and system consequences simulates failure risk dynamically. Changing equipment operational status allows engineers to virtually assess design robustness. Simulation during the design phase identifies weaknesses before foundation concrete and steel are set – the ultimate conceptual design objective.

**Figure 2: Component Template Tasks/Workscopes**



Tag/EQID: 1JEDNBTV0003**VALVEX
Name: FW HTR 5A EXT STEAM LINE BLEEDER TRIP VLV
LTA/RXp: S 10607 126 10607

- 1JEDNBTV0003**VALVEX
  - 1078: Valve Body
  - 1079: Cylinder Operator
  - 1080: Disk Swing Arm
    - 1939: Bound
      - 2840: Check freedom of r
        - 1190: Heat rate te:
        - 1180: Vendor sugg
        - 1093: Disassemble
        - 1092: INPO addres:
        - 1091: Detailed ana
    - 2134: Worn/damaged
  - 1081: Shaft & Bushing
  - 1085: Disk & Seat
    - 1937: Worn
    - 1938: Separated
  - 1095: Shaft Packing
  - 1140: Cylinder Seals
  - 1141: Shaft Bearing
  - 1142: Bearing Cover Gasket
  - 1208: Solenoid Valve
  - 1210: Disk Post
  - 1212: Air Line
  - 754: OPERATIONS ROUNDS
  - 755: UNASSIGNED PM TASKS
  - 756: ANALYZED NOT PERFORMED
  - 757: OVERHAUL CHECK VALVE
  - 758: NORMAL OPERATIONS

Applied Template State: Locked
Revised: 07/19/2002
Revision #: 0
Gen Template: 126 VALVEX-9 Free-Flow Check Valves
Applied to: 10607 1JEDNBTV0003**VALVEX
FW HTR 5A EXT STEAM LINE BLEEDER TRIP VLV
Cmp Type: Valve
Cmp Manuf: Atwood Morrill
Tmplt Type: Master
CmpModel: Swinging Disc Inc Seat
Comment: Bleeder Trip (Check) Valves; BTV's; Extraction Valves
Subtype: Swinging Disc Inclined Seat w/ Bolted Bonnet and
Associated Templates: VALVEX-2, Check Vavles; VALVOP-1b, Cyl Operators
PMB Legacy No: 248806 (legacy number)
Name/Description: Turbine Extraction Bleeder Trip Valves
Template Basis: Valves use a combination of free swing checking and air operator assisted power closure to prevent water induction into the running turbine from feedwater heaters following a trip.
Selection Basis: Automatic operation to protect turbine from water induction and overspeed.
GT Owner: Jerry Volk
AT Created: Thu 12/20/2001 14:39:55
Who Assigned: Wayne Magninie
AT Updated: Sat 04/13/2002 16:59:12
Who Created AT: Admin
When Assigned: Thu 12/20/2001 14:39:46
Who Updated AT:
Foreign Key: 18839
AT Revision Notes:

## TEMPLATES

Templates flexibly model equipment to account for various facility contexts, improving the range of options considered before actual equipment selection and installation. Templates allow substitution of one model for another, keeping design flexible. Templates accommodate addition or deletion of specific failure modes and tasks at the equipment level. The challenge is to adjust templates from generic sources to specific applications. That requires considering symmetry and risk.

Equipment ranking importance conveys risk. Mnemonically suggesting mitigation strategies based upon redundancy, monitoring, or design margins practically ranks risk alternatives. Where unavoidable single failures compromise system design objectives, designers must provide operator warning. There should be simple means for design reviewers to validate "what if" redundancy levels, installed instrumentation and applicable standards. Where regulatory standards apply, code and register requirements should trace to federal, state and local statutes and codes as a formal design basis. Where codes and rules aren't available or known, their absence should be noted for review and consideration later should owners seek changes in tasks, risk assessment or monitoring intervals. This implicitly identifies high-risk failures and control strategies covered by oversight processes.

For economic evaluations, software must operate on several levels. Software databases must concisely present each system, train, skid and component risk profile in safety, operations and cost (SOC) risk contribution and maintenance cost terms. Strategies to maintain the facility design based should be evident. Software must support standardization and reanalysis of operations and maintenance plans to mitigate equipment failures.

Maintenance plans should discern logical equipment groups at the skid, train/loop and systems levels. Costs arise from materials and labor. The database should delineate materials and labor costs for likely operating scenarios. Equipment partitioning must extend to the replacement part level – where failure can be evaluated for detection and correction. **Figure 2: Component Template Tasks/Workscopes**

Hard time, failure finding, and on-condition task combinations provide scheduled maintenance requirements. On-condition maintenance resulting from inspections requires pre-planning based upon future performance. (This establishes maintenance costs, explicitly.) Bracketing work costs with resource estimates initiates planning, allowing critical design review, and determines future operations work performance.

Work order costs should be traceable to failure prevention value at all levels for scheduled tasks that make up workscope; no work should be based on absent, soft, or untenable value propositions. Grouping tasks into workscopes provides efficiency, identifying costs associated with the grouped tasks. Common access, trip, tool, mobilization and breakdown time costs hard to track individually, naturally spread across workscopes as common overhead. Task work selection should be based on direct value basis (for failure prevention), and workscope fit (for overall work integration synergy). Many tasks that lack value by themselves are effective with others combined into a workscope.

System-by-system, equipment tasks should be incorporated into maintenance workscopes. Equipment serving as template sources for similar equipment (based on design symmetry, application commonality, or functional role) must be suitably identified. Critical (SOC) equipment workscopes should rank all tasks' contributions by criticality (SOC), failure strategy, performance mode (on-line, outage), and skill (electrician, mechanic, fitter, etc.). Strategy and tasks should roll up to the system and plant levels developing useful statistics for maintenance performable online, total outage maintenance workhours, and so forth. Safety, operations and cost risk categories should be included by type of maintenance.

## USEFUL PERFORMANCE MEASURES

Equipment Critical/Non critical Risk (SOC/X) and Basis Workhours:

- By system
- By system classified by risk (Safety Operations Cost)
- By system and craft
- By system by strategy (TBM, FF, or OCM)

Maintenance

- By System
- By classes – Preventive (PM) vs. Corrective (CM)
- TBM, OCM, and FF PM Fractions
- Corrective Maintenance Breakdown – PM originated vs. failure originated

Practically, relational databases (RDBs) offer the best tools available to develop these requirements. Further, they offer object database compliance (ODBC) that assures their useful products (work orders) integrate with other essential business processes (the CMMS/EAMS, for example) via batch upload, multiple session data transfers, and browsing comparison between multiple applications. These features enhance the utility of CMMS/EAMS application software.

## ECONOMIC RISK ASSESSMENT

Assessing economic risks considers all likely equipment failures. Consequently, plant maintenance costs can be controlled, safety risks excluded and operational impacts kept within projected outage periods. Equipment failure evaluation assures that scheduled maintenance and consequent work performance doesn't impact outage periods, so plant production availability never shrinks below the designer's intent. Outage downtime consequently only shrinks as a fraction of total operating time over plant lifetime.

Workhours, services and materials drive maintenance expenses. Work-hours drive maintenance costs. By estimating hours using appropriate thumbrules one can estimate the total maintenance costs fairly accurately. Revising estimates based upon historical experience establishes very exact target performance values. One thumbrule is that outage-related workhour costs match service expense one-for-one. For every outage workhour, an equivalent amount is spent for services and parts, based upon cost. Services contribute heavily to total maintenance expense. Estimating outage workhours projects total outage maintenance costs with reasonable accuracy. This simplifies estimating maintenance outage hours for large overhaul work. This estimation process can be used in software databases to project overall operating costs based on workhours. The resulting cost projections provide forward-looking operating cost estimates. Once validated, adjusted, and combined with failure projection before a facility is built, they provide assurance that income and finance projections can be met.

## RISK RANKING

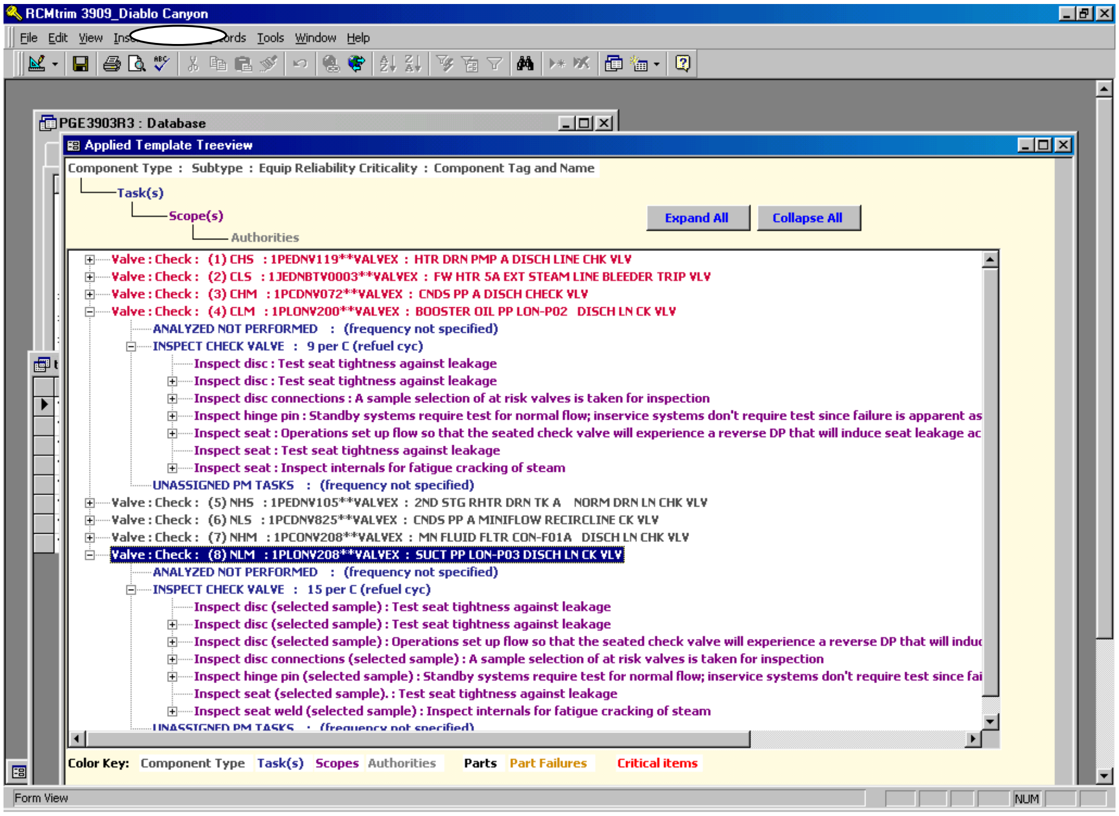
Preventive maintenance development software should facilitate rank all scheduled and on-condition work tasks by risk. Clearly ranking tasks' risk delineates the consequences of work order (WO) performance upon risk, aiding incomplete outage work assessment. Further, within a scheduled maintenance work order, the failure prevented (or targeted) by each preventive task should be identifiable by risk. Maintenance WO scopes can't always be completed as planned; this is particularly evident on large turbine or boiler work involving hundreds of tasks. Work scope breakdown helps maintenance operations establish what actual work should be performed, can be worked and actually was completed on any given large job scope. This clearly establishes risk management strategy for each failure mode, definitively, as plant operations move forward over time.

## WORKSCOPES

Facilities perform maintenance by work order. Work order scope – workscope – authorizes, summarizes, and documents maintenance work performed under a work order. Together, all scheduled maintenance work orders constitute a facility's formal maintenance strategy.

Workscopes group tasks and their associated performed workhours under one trip or tagout, by one craft for common planning and performance. By differentiating work into tasks, workscopes allow work evaluation on merit. This allows rescoping and re-evaluating large work activities like turbine overhauls as tasks (like rotor bar crack inspections) and their technology (like magnetic particle crack inspection, contrasted with metallographic replication) as it changes over time. Workscopes improve maintenance hour estimation. Techniques and technology, as well as materials, components and their parts, change in large facility operations that extend over decades of time. Evolutionary and even radical changes occur reflecting changes in these processes. Redeveloping maintenance strategy by redefining workscopes allows continuous maintenance plan update. Over time, workscopes continuously improve as a strategy for process improvement. Workscopes make it possible to relate engineering failure prevention tasks to work performance and cost. This facilitates estimating and improving maintenance based upon measurable performance-based goals.

**Figure 3: Check Valve Template Workscopes and Tasks**



```
Component Type :  Subtype : Equip Reliability Criticality : Component Tag and Name
  └──Task(s)
       └──Scope(s)
            └──Authorities

⊞ Valve : Check :  (1) CHS  : 1PEDNV119**VALVEX : HTR DRN PMP A DISCH LINE CHK VLV
⊞ Valve : Check :  (2) CLS  : 1JEDNBTV0003**VALVEX : FW HTR 5A EXT STEAM LINE BLEEDER TRIP VLV
⊞ Valve : Check :  (3) CHM  : 1PCDNV072**VALVEX : CNDS PP A DISCH CHECK VLV
⊟ Valve : Check :  (4) CLM  : 1PLONV200**VALVEX : BOOSTER OIL PP LON-P02  DISCH LN CK VLV
     ANALYZED NOT PERFORMED   :  (frequency not specified)
   ⊟ INSPECT CHECK VALVE  :  9 per C (refuel cyc)
          Inspect disc : Test seat tightness against leakage
        ⊞ Inspect disc : Test seat tightness against leakage
        ⊞ Inspect disc connections : A sample selection of at risk valves is taken for inspection
        ⊞ Inspect hinge pin : Standby systems require test for normal flow; inservice systems don't require test since failure is apparent as
        ⊞ Inspect seat : Operations set up flow so that the seated check valve will experience a reverse DP that will induce seat leakage ac
          Inspect seat : Test seat tightness against leakage
        ⊞ Inspect seat : Inspect internals for fatigue cracking of steam
     UNASSIGNED PM TASKS   :  (frequency not specified)
⊞ Valve : Check :  (5) NHS  : 1PEDNV105**VALVEX : 2ND STG RHTR DRN TK A   NORM DRN LN CHK VLV
⊞ Valve : Check :  (6) NLS  : 1PCDNV825**VALVEX : CNDS PP A MINIFLOW RECIRCLINE CK VLV
⊞ Valve : Check :  (7) NHM  : 1PCONV208**VALVEX : MN FLUID FLTR CON-F01A  DISCH LN CHK VLV
⊟ Valve : Check :  (8) NLM  : 1PLONV208**VALVEX : SUCT PP LON-P03 DISCH LN CK VLV
     ANALYZED NOT PERFORMED   :  (frequency not specified)
   ⊟ INSPECT CHECK VALVE  :  15 per C (refuel cyc)
          Inspect disc (selected sample) : Test seat tightness against leakage
        ⊞ Inspect disc (selected sample) : Test seat tightness against leakage
        ⊞ Inspect disc (selected sample) : Operations set up flow so that the seated check valve will experience a reverse DP that will induc
        ⊞ Inspect disc connections (selected sample) : A sample selection of at risk valves is taken for inspection
        ⊞ Inspect hinge pin (selected sample) : Standby systems require test for normal flow; inservice systems don't require test since fai
          Inspect seat (selected sample). : Test seat tightness against leakage
        ⊞ Inspect seat weld (selected sample) : Inspect internals for fatigue cracking of steam
     UNASSIGNED PM TASKS   :  (frequency not specified)
```

Color Key: Component Type Task(s) Scopes Authorities Parts Part Failures Critical items

## CONCLUSIONS

Developing the new facility's systems and equipment risk exposure profile predicts operational risks. Unacceptable risks are avoidable by providing design depth. Depth includes design margins, condition monitoring and alert instrumentation and equipment redundancy. Economic value comes from income; risk stems from uncertain income and costs. Designers may fail to convey design intentions to assure economic plant operations to owner-operators. Design is inexact – intent is often implied. Identification of risks, aided by the selection and application of equipment maintenance strategy templates to predict plant operating income and equipment costs assists not only designers, but lenders, regulators, and owner-operators. Risk identification at these levels assures income meets profit goals based upon production and markets.

Relational database software defines new facility risk requirements based on fundamentals using pre-developed standard equipment models – before final designs are fixed. This helps establish plant operating and maintenance strategies – and costs, before facility construction begins. Providing a new facility with complete operating and maintenance plans before startup provides many benefits. Fewer operational economic uncertainties improve financing options and ultimate commercial viability. Operators will understand plant operating assumptions and their basis in advance. Those assumptions will be retrievable on demand at any operational time in plant life. Software reliability databases advance, process understanding, and computer hardware technology make maintenance planning more feasible than ever before in conceptual plant designs. **Figure 3: Check Valve Template Workscopes and Tasks**

## ACKNOWLEDGMENTS

The authors would like to acknowledge the members of the EPRI Maintenance Rule Users Group, Brian Ramey and Steve Coppock of Arizona Public Service, and Frank Novachek of Xcel Energy for their contributions.

## REFERENCES

1. Risk-Based Methods for Equipment Life Management: A Step-by-Step Instruction Manual with Sample Applications, ASME Press, 2003
2. MSG-3, (Maintenance Steering Group) Maintenance Program Development Document, ATA 1993
3. Evaluation Criteria for Reliability-Centered Maintenance (RCM) Processes, SAE JA1011, 1999
4. RCM: How to Build a Reliable Plant Maintenance Program, August, J.K., Penn Well, 2004
5. Equipment Reliability Process Description, INPO AP 913, Institute of Nuclear Power Operations, 2001EPRI PM Basis (format), Worledge, D., Electric Power Research Institute, 1997
6. Guidelines for Application of the EPRI PM Basis, Bridges, M. and Worledge, D., Electric Power Research Institute, 2000
7. Reliability-Centered Maintenance, S. Nolan & H. Heap, United Airlines, 1978
8. CORE, Inc. *trim*™, version 3.909 (Software) ©CORE, Inc. 2004