

From ESSM to RiskVu

Richard Pullen, Ph.D.; Isograph Ltd.; Manchester, England

Abstract

The first risk monitor was installed at the Heysham 2 AGR in 1987. This innovative software, known as the Essential Systems Status Monitor (ESSM), provided on-line probabilistic safety assessments and advice to operators. The author of this article was heavily involved in the original development of the ESSM and is the principal developer of the Isograph RiskVu software. This article discusses the functionality of the original ESSM software and how modern risk monitors, such as RiskVu, can be applied in a modern computing environment.

The ESSM

In 1987 the Essential Systems Status Monitor (ESSM) was installed on a Honeywell DPS6/92 mini-computer at the Heysham 2 AGR in England. The ESSM was directly accessed by control room staff and was the earliest application of a nuclear safety risk monitor in an operational environment.

Before the ESSM was introduced to Heysham 2, operating instructions had been used to stipulate the minimum levels of redundancy required in the plant's safety systems. These documented instructions were concise and unambiguous and, due to the complexity of the safety systems, interpret requirements for minimum levels of plant in a conservative manner. The introduction of the ESSM Risk Monitor provided the ability to perform probabilistic safety assessments and allowed the plant to be operated in a less restrictive manner whilst preserving the same safety objectives.

The ESSM provided risk assessments based on fault tree methodology. The underlying fault trees modeled the effectiveness of essential safety systems to protect against a variety of initiating events leading to serious consequences. The fault trees were similar to those used in off-line probabilistic safety assessments and represented systems such as post-trip sequencing equipment, the pressure support system, the start/standby boiler feed system, the emergency boiler feed system, the essential electrical system, the decay heat boiler system, the reactor seawater system, the inlet guide vane system, the gas circulators, the circulator auxiliaries cooling system and the circulation diverse cooling system.

The analysis of fault trees representing complex nuclear safety systems had traditionally required long computing times. Reducing these computing times to provide on-line assessments in one or two minutes was probably the greatest challenge for the software development team. The fault trees representing AGR systems are particularly complex due to the high degree of system redundancy combined with the effect of common failures. In fact, common basic events were so extensive that no appreciable modularization of the trees (automatic or manual) was possible. Reducing the computing time relied heavily on developing efficient algorithms to process the system minimal cut sets using traditional Boolean Algebra methods.

ESSM Functionality

One of the principal functions of the ESSM was to perform probabilistic safety assessments for control room operators within one or two minutes. Assessments took into account current plant status (component outages due to faults or scheduled maintenance) as well as the current plant configuration. Although the ESSM performed a probabilistic assessment, the results of the assessments were provided in terms of maintenance categories that correspond to bands of failure frequencies.

Deterministic rules could also be monitored in parallel to probabilistic assessments using a special set of fault trees. Violation of such rules could also be displayed to the operator. During normal operation of the plant, however, advice displayed to the operator was provided using probabilistic criteria.

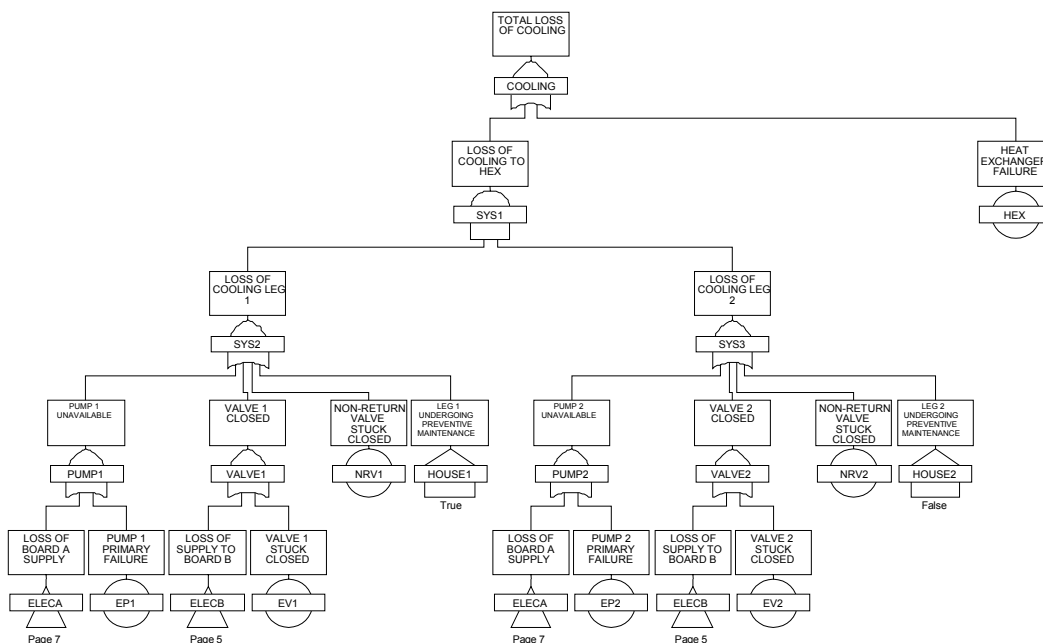
The ESSM fault trees could also be manipulated by the computer software to provide advice on how to improve the availability of the essential systems. Single items, or combinations of items, would be listed as priority maintenance candidates. These items, when restored to service, would substantially improve the availability of the essential systems.

The ESSM could also be accessed from the maintenance planning office. What-if scenarios could be investigated in an off-line environment. This allowed the effect of planned maintenance to be determined on the availability of the essential systems. The future availability of these systems could be optimized taking into account existing faults.

Adapting Fault Trees to an Operational Environment

A fault tree graphically represents the interaction of failures and other events within a system. Basic events at the bottom of a fault tree are linked via logic symbols (known as gates) to one or more TOP events. These TOP events generally represent system failure modes or hazards for which predicted reliability data is required. Basic events generally represent component failures for which a probability of failure is provided based on historical data. The traditional analysis process is to produce the system minimal cut sets, apply the basic event probabilistic data, and then determine the probability of the TOP event.

By using special events known as ‘House Events’ we can interactively modify the logic of a fault tree to take account of the real time changes in a system’s configuration and status. House events are events that have a probability of one or zero (status true or false). By switching their status we can effectively re-configure the fault tree. In addition component failures may be represented by temporarily converting a basic event to a ‘true’ house event.



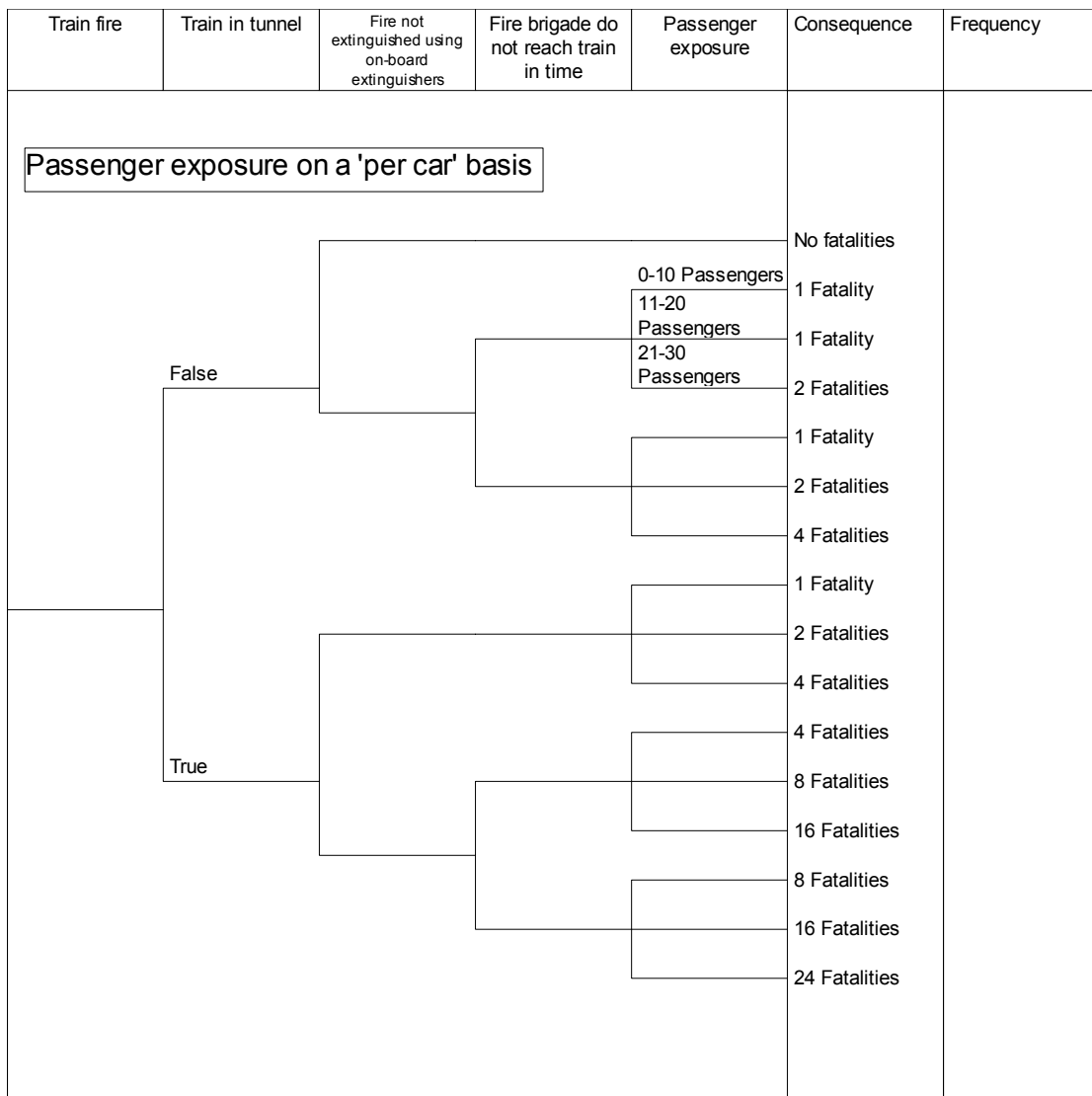
Fault tree with house events set to represent preventive maintenance being undertaken on ‘Leg 1’ of the cooling system

Re-analysis of the fault tree, taking into account the current house event settings, provides the current availability status of the system.

Quantifying Risk Using Event Trees

Event trees may be used to model the consequences of system failures after an initiating event has occurred. Examples of initiating events are 'Loss of Engine', 'Fire' and 'Pipe Break'. The likelihood of a consequence is usually expressed as a probability frequency. Each consequence may be assigned a severity according to the consequence category. For example, 'probable number of deaths' quantifies the severity arising from a safety consequence. 'Likely cost' quantifies the severity arising from a financial consequence.

Event trees are often linked to fault trees. We can include event trees in operational PSAs and model the changes in risk due to failures, the effects of scheduled maintenance and other events such as the time of day, system configuration etc.



Example event tree from the railway industry

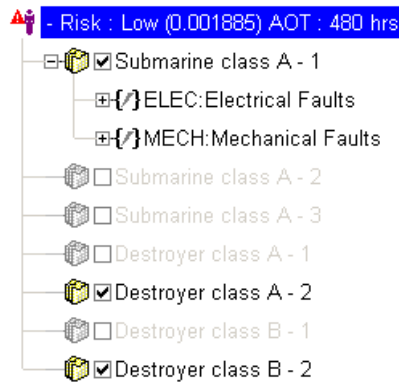
The RiskVu Risk Monitor

RiskVu V3 is an example of a modern risk monitor that may be adapted to provide on-line safety assessments or off-line comparisons of different design options. In effect it may be used as an operational aid or a management tool.

RiskVu is a ‘commercial off-the-shelf’ product that operates in parallel to the FaultTree+ computer program. FaultTree+ is widely used throughout all the major engineering industries to perform integrated fault tree, event tree and Markov analyses.

Using RiskVu as an Operational Tool

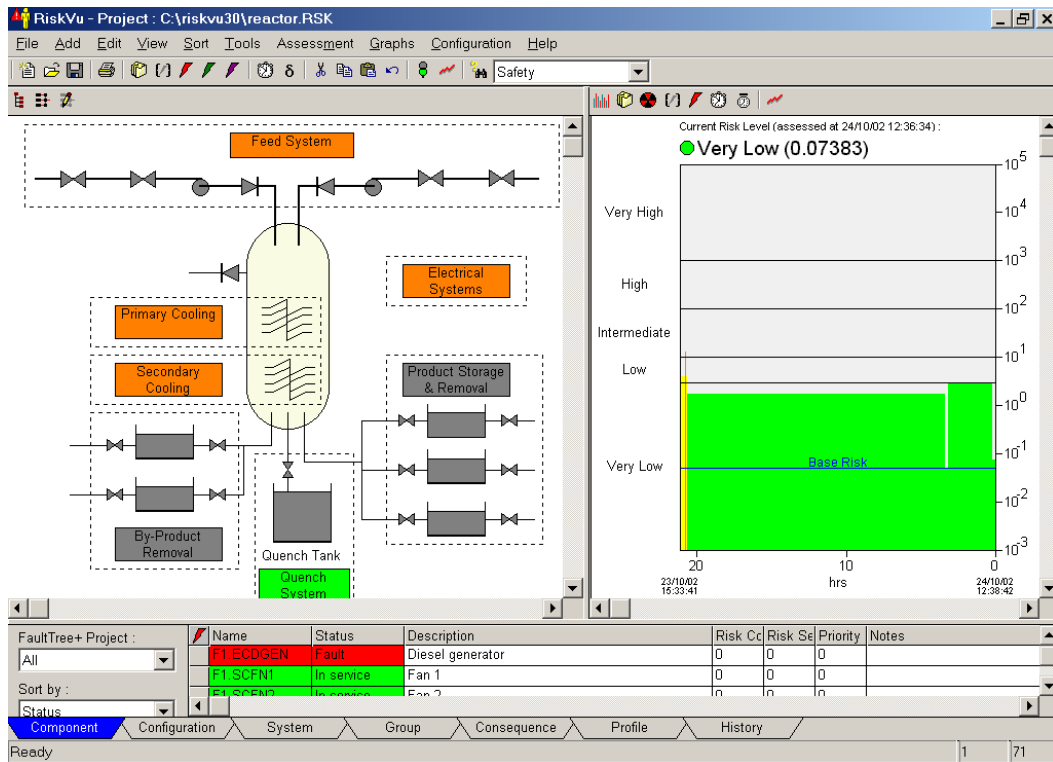
A RiskVu project is connected to one or more FaultTree+ project files. These project files might represent risk models for nuclear, aerospace, railway, process and other types of engineering systems. These project files may be temporarily disabled for any given risk assessment. This is particularly useful when modeling multiple system configurations that may vary at different times. For example, if RiskVu was being used to model the boats within a dockyard and the connected on-shore auxiliary systems, the project disable feature would allow a user to quickly indicate which classes of boats were currently in the dockyard.



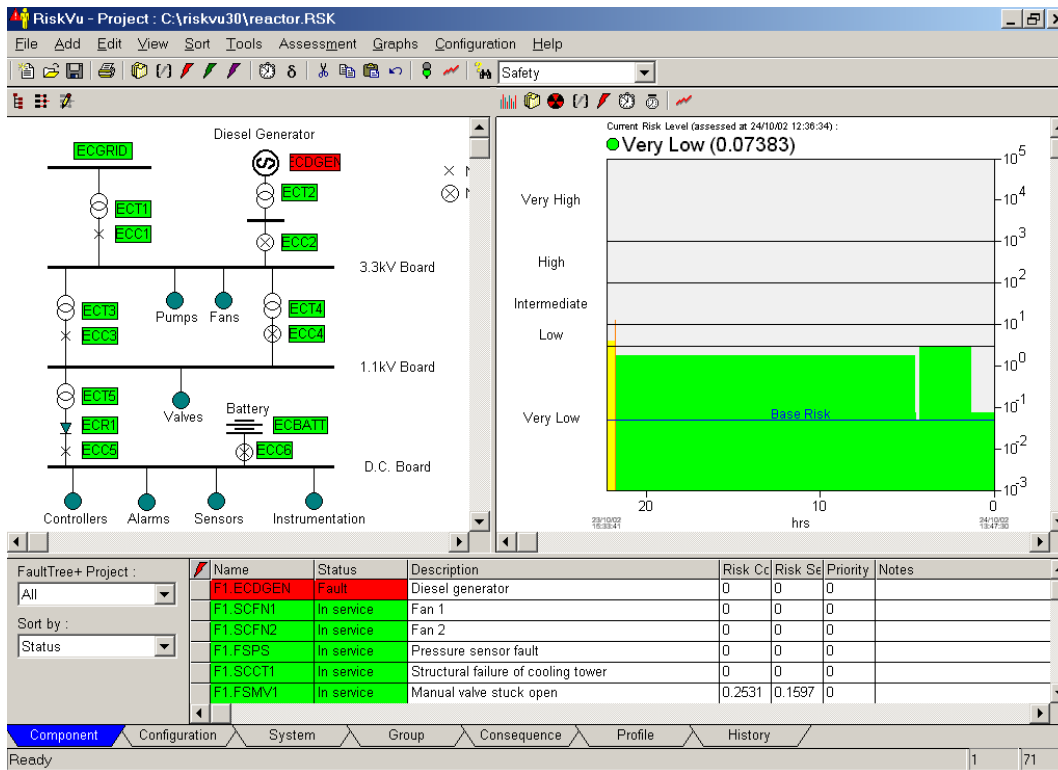
RiskVu hierarchy diagram showing enabled and disabled project elements

RiskVu allows users to provide a custom high level interface to the underlying fault tree, event tree and Markov models constructed in FaultTree+. Component and configuration events are created by the RiskVu administrator. These events are linked to primary or house events in the fault or event trees. Modification of an event’s status in RiskVu will modify the status of the primary or house events in the underlying FaultTree+ projects. The status of a component event indicates whether it is currently in service or out of service due to a fault or scheduled maintenance. A configuration event (corresponding to a house event in the fault or event tree model) has a true or false status. Component and configuration events may be grouped by an administrator.

System structures may be displayed in the form of hierarchical or schematic diagrams. Schematic diagrams may be ‘activated’ allowing users to navigate between systems, modify the status of plant items and view system degradation levels using colour codes.

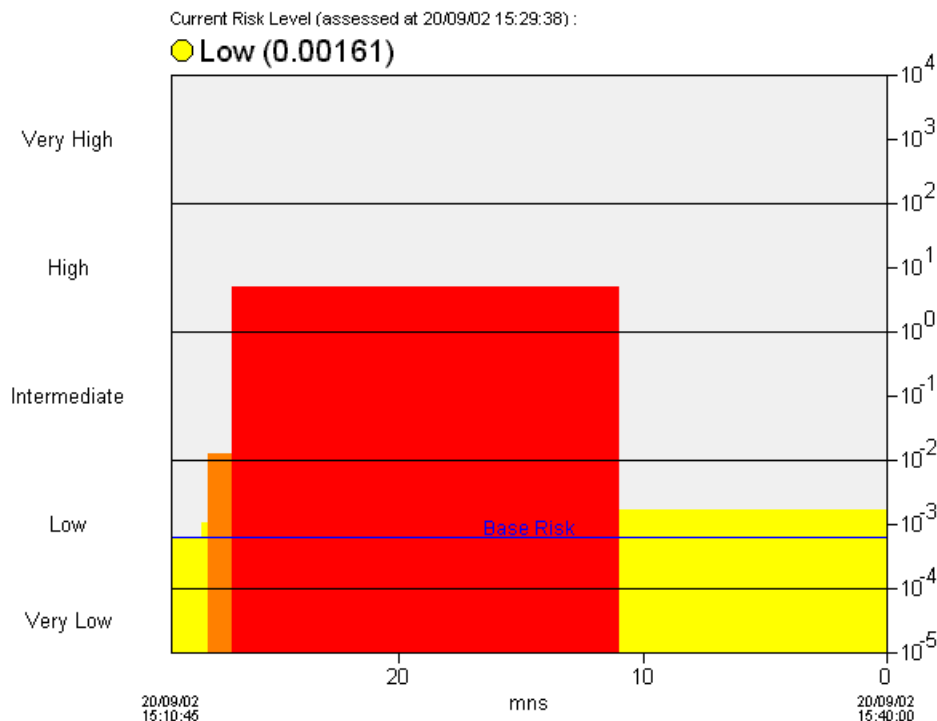


RiskVu screen display showing the current status of systems together with the history profile



RiskVu screen display showing the status of electrical items

After indicating a change of status for a component or configuration event the user may ask RiskVu to reassess the current risk level for the monitored systems and indicate any operating restrictions. Current risk levels may be compared to previous assessments in a history profile.



Example of a history profile showing the variation of risk with time

Once an assessment is performed RiskVu provides priority restoration rankings for components that are currently out of service. These rankings indicate which components will result in the largest reduction in risk if they are restored to service. RiskVu also provides importance rankings indicating which operating components would result in the highest increase in risk if they were to fail.

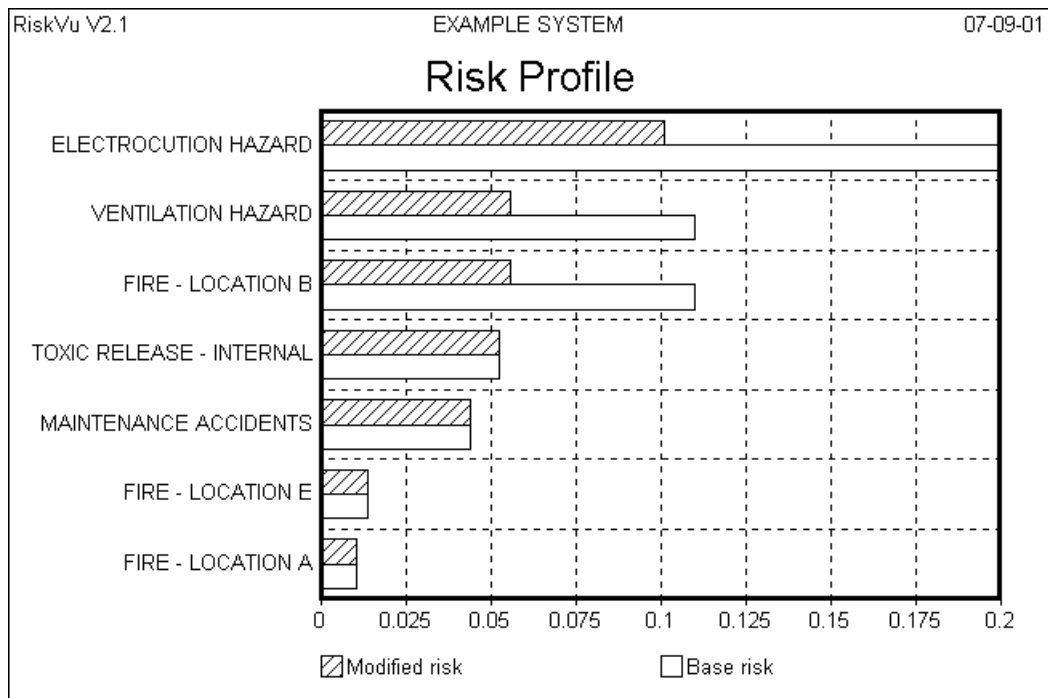
RiskVu also allows the effects of planned maintenance to be assessed. A time profile may be quickly constructed by a RiskVu user indicating at what times in the future individual components will be removed from service for scheduled maintenance. RiskVu will then assess the resultant risk levels taking into account any current outages. Alternative time profiles may be compared.

An important feature of the RiskVu risk monitor is its ability to be customized to adopt the functionality required by the user. A RiskVu project administrator (with password protection) may customize the screen interface to display only the information required by a user or operator of the system.

Using RiskVu for Design Comparisons

RiskVu may also be used as an off-line tool allowing users to assess the effects of design changes on risk or comparing the risk associated with alternative designs. Configuration events may be used to switch between different levels of redundancy and the failure rates and test intervals of component events may be temporarily changed.

In addition, the effect of different operational environments over the course of a mission may also be assessed using the time profile facility.



Risk profile comparing 'base' risk with 'modified' risk

RiskVu Summary

Use of the RiskVu risk monitor provides the answers to questions such as

- Is the plant in a safe condition to continue in operation ?
- Is it safe to start a mission ?
- What are the effects of design changes on safety ?
- What is the actual achieved availability history of the plant ?
- What are the most critical items in the system ?
- How can we optimize the planned maintenance schedule ?
- What is the effect on risk of changing test intervals ?
- What is the effect on risk of item failure rate changes ?
- What is the effect of a change of system configuration on overall risk ?
- What is the comparative risk from different design options ?

Summary

Fault and event tree analysis can be employed effectively in an operational environment to allow systems to operate in a less restrictive (and hence cost-effective) manner. Modern computers allow assessments to be performed quickly providing precise probabilistic results. These methods also allow planning to be assisted through the assessment of what-if scenarios. Users of operational PSA tools such as the ESSM or RiskVu do not need to be trained in fault tree analysis techniques. The basic fault tree models may be developed off-line by experienced reliability engineers.

Risk monitors may also be used off-line to quickly assess the effects of design changes and modifications to maintenance intervals. Operational time profiles may also be compared.

References

“ESSM gives on-line real time probabilistic reliability assessment”, Nuclear Engineering International, May 1989

“Employing PRA techniques in an operational environment”, Nuclear Engineering International, January 1986.

RiskVu V3 User Manual, Isograph, 2002.

About the Author

Richard Pullen, Ph.D., Isograph Ltd, The Malt Building, Wilderspool Park, Warrington, WA4 6HL, UK, telephone +44 1925 437000, e-mail – rpullen@isograph.com.

Dr. Pullen obtained his Ph.D. at Imperial College, London in 1981. Since then he has been involved in the development and application of reliability methods in a wide range of engineering industries. He is the principal author of the FaultTree+ and RiskVu computer programs.