LETTER TO THE EDITOR OF NUCLEAR ENGINEERING NEWS

(appeared as *Search for the Unnecessary: Letter to the Edito*r. In Nuclear Engineering International, by P.-J. Courtois, R. Bloomfield, B. Littlewood, L. Strigini January 2002, Vol 47, N° 570, p. 11)

Dear Editor,

We were very concerned to read the recent article “Search for the unnecessary” (NEI issue of October 2001, pp.24-26) which appears to suggest that BBNs (Bayesian Belief Nets) are a magic wand that can be used to reduce the cost of assessing the safety of software-based systems. The authors suggest that the IV&V of Sizewell B and perhaps of other plants was excessively expensive because no faults were found. This seems to us a mistaken view of the purpose of IV&V, which is mainly to gain justifiable confidence in a system. The fact that no faults were found in this instance does not in any way detract from the necessity of the exercise.

Whilst recognising the importance and usefulness of the Bayesian formalism for representing uncertainty (indeed, we have ourselves worked extensively in this area for many years), we believe BBNs represent just that – a helpful formalism.

The problem of safety assessment, instead, is essentially one of obtaining and marshalling appropriate evidence. In the case of software-based systems this poses difficulties that we believe to be intrinsic, and thus not open to 'magic bullet' solutions. For example:

- The relationship between the quality of software development processes and the quality of the resulting software products - particularly their dependability - is poorly understood;

- The essential discontinuity of software behaviour limits the claims that can be made about future behaviour from successful testing, and makes the effect of any changes much less predictable;

- Claims for 'complete perfection' are not believable for systems of today's complexity.

The consequence is that safety cases depend to a large extent upon marshalling and vetting highly disparate evidence, of which expert judgement forms a significant part. Bayesian probability may be of help here, by providing a formal framework for the representation of uncertainty, but it does not remove any of these difficulties. In particular, BBNs are a convenient mechanism for conducting the Bayesian computations efficiently (which is not to decry the great intellectual achievement of the enabling algorithms developed several years ago).

We feel your readers are not well served by the tone of this article, and believe that the claim that BBNs can be used to reduce significantly the effort involved in safety cases is unfounded and dangerous. If this were not serious enough, we also believe that the authors greatly underestimate the difficulty of using BBNs in this kind of situation. Some examples:

- The authors recommend the use of expert opinion to fill all probability tables. But these opinions can only be trusted if based on sufficient knowledge. Opinions about such subtle and poorly known issues as represented in the BBN can only be trusted after a great deal of (expensive) scrutiny. Using Bayesian formalism to derive the necessary implications of unfounded beliefs produces unfounded conclusions;

- The authors' BBN example has two nodes with 7 parent nodes: the notion that an expert can produce a believable 7-dimensional probability distribution, which is required to represent his/her beliefs is ludicrous;

- The authors appear to believe that, in the absence of evidence, it is natural to replace unknown frequencies of occurrences by uniform probability distributions. This is a well-known and difficult problem in Bayesian statistics for which there is no 'correct' solution;

- The authors do not address any of the difficult (and unsolved) problems concerning validation of BBNs and complex subjective beliefs. These are particularly relevant to this problem, where data are sparse and there is a large component of subjective expert judgement;

- The authors unknowingly illustrate the difficulties by not noticing mistakes in the net topology they use as an illustration: there are nodes with no parents and no children!

All in all, we feel that this article is based on a dangerous mis-interpretation and misuse of the capabilities offered by Bayesian belief networks. It makes claims that are not supported and, we believe, cannot be supported. Unfortunately, these claims are ones that could, in the hands of the ill-informed, be used to justify reductions in the effort needed to justify safety claims. Such an outcome would be dangerous. We would find it disturbing if this had already happened in the safety cases of licensed I&C systems, as the authors suggest.

SIGNED:
Professor R. Bloomfield, *Adelard, London*
Professor P.– J. Courtois, *AV Nuclear, Authorized Inspection and Licensing Body, Brussels,*
Professor B. Littlewood, *director, Center for Software Reliability, City University, London*
Professor L. Strigini, *Center for Software Reliability, City University, London*