System Design and Maintenance Modelling for Safety in Extended Life operation

John Andrews and Claudia Fecarotti
University of Nottingham

ABSTRACT
It is frequently the most cost effective option to operate systems and infrastructure over an extended life period rather than enter a new build programme. The condition and performance of existing systems operated beyond their originally intended design life are controlled through maintenance. For new systems there is the option to simultaneously develop the design and the maintenance processes for best effect when a longer life expectancy is planned. This paper reports a combined Petri net and Bayesian network approach to investigate the effects of design and maintenance features on the system performance. The method has a number of features which overcome limitations in traditionally used system performance modelling techniques, such as fault tree analysis, and also enhances the modelling capabilities. Significantly, for the assessment of aging systems, the new method avoids the need to assume a constant failure rate over the lifetime duration. In addition the assumption of independence between component failures events is no longer required. In comparison with the commonly applied system modelling techniques, this new methodology also has the capability to represent the maintenance process in far greater detail and as such options for: inspection and testing, servicing, reactive repair and component replacement based on condition, age or use can all be included. In considering system design options, levels of redundancy and diversity along with the component types selected can be investigated. All of the options for the design and maintenance can be incorporated into a single integrated Petri net and Bayesian network model and turned on and off as required to predict the effects of any combination of options selected. In addition this model has the ability to evaluate different system failure modes.

The integrated Petri-net and Bayesian network approach is demonstrated through application to a remote un-manned wellhead platform from the oil and gas industry.

Keywords
Asset management, system reliability availability, Petri nets, Bayesian networks, design, maintenance, aging systems.

1. INTRODUCTION

The performance of engineering safety systems is governed by both its initial design and also the maintenance strategy employed once it is in operation. The adequacy of any system is determined through the analysis of its predicted performance against target levels of safety and risk. The assessment process usually involves the identification of initiating events, which will produce potential hazards, and the response of the safety systems to prevent its escalation. Commonly the assessment of the system performance is carried out using an integrated combination of Event Tree Analysis [1] and Fault Tree Analysis [2-4]. The implementation of these techniques in commercial software require assumptions to

be made regarding the system characteristics. Key assumptions are that the component failure events will be independent and (in the majority of commercial codes) that failures and repairs occur with constant rates. The limited range of models used to establish the failure probability of the components also restricts the ability of the method to investigate the benefits of the complex range of options which can be employed in maintaining the system. An extension of Fault Tree to include time requirements in order to capture the dynamic behaviour of systems is the Dynamic Fault Tree [5]. Dynamic Fault Tree has been used in [6] for the dependability analysis of safety and protection systems during standby and active operation phased. The authors combine an availability analysis of the system in standby mode and a reliability analysis for the active mode within the context of Dynamic Fault Trees. Although the use of Dynamic Fault Trees enables to account for time dependencies, their analysis still remains expensive when dealing with complex systems with many components and many possible events occurring. Approaches like Semi-Markov processes [7] enable to model systems characterised by non-constant rates processes, but the state-space explosion issue when considering systems with many components and many possible states still remains.

For many industries, when systems reach the end of their intended design life, it is more cost effective to continue operating the system, controlling its state through a comprehensive maintenance strategy, than to enter a new build programme. For new systems there is a strong driver to design for longer life expectancies. To establish the most effective performance, over extended life, a whole system, whole life view is required. In this approach the system structure (obtained through design) is considered simultaneously with the maintenance strategy. To adequately model the performance of this situation the restrictions featured in the tradition risk assessment methods need to be overcome.

As systems age their components, particularly mechanical components, experience non-constant (increasing) rates of failure. Maintenance strategies are a complex activity defined by parameters which govern the inspection/testing, servicing, reactive repair on failure, component replacement on age, use or condition and sub-system renewal. Opportunistic maintenance is also a possibility where work is carried out on components when the chance presents itself due to work required by other elements in the system. This introduces dependencies between the component conditions.

In formulating a maintenance strategy, the resource utilisation needs to be directed at the elements in the system where they can achieve most benefit. It is also expected that this distribution of resources will change over the life of the system as some parts age at faster rates than others. The system lifetime can be considered as a series of discrete time phases where different maintenance strategies are applied. This concept is similar to the use of phased mission analysis where the functional requirements change as a system mission progresses [8-10]

Fault tree and event tree methods are not capable of modelling non-constant failure rates that increases over time due to wear out, dependencies between component states or complex maintenance processes. Alternative methods have features to overcome these limitations. Petri nets (PNs) [11,12] have proved very effective in modelling systems which feature non-constant deterioration rates and can be used to represent very complex asset management processes [13-15]. PNs constructed to predict the system performance based on the system structure, along with the component deterioration process and the maintenance strategy frequently feature characteristics whose solution requires the use of the Monte Carlo technique [4]. It is therefore advantageous, in the interests of efficiency, to keep the size of such models to a minimum. This can be achieved through modularisation [16] enabling the analysis to be performed in small, independent sections. Bayesian Networks (BNs) [17-19] are capable of accounting for the dependencies in the maintenance process and modularising the analysis. The conditional probability tables can be derived from the results of the PN analysis. Maintenance phases can also be accommodated in the

PN and BN methodologies. An integrated BN/PN approach, referred to as the BP-Net method, is developed in this paper and can be used to predict the system level response. An additional feature of this method is that several system failure modes can be considered in the same model.

Through setting the prior probabilities of the root nodes in the BN (to 1 and 0's) to reflect the required design and maintenance options selected, all different design and operational conditions can be investigated in a single model.

The approach is demonstrated in this paper by application to an unmanned wellhead platform used in the offshore oil and gas industry.

2. SAFETY SYSTEM MODELLING

The performance of a safety system into extended life will be dependent upon both the design and the maintenance strategy employed. Ideally the model produced to assess the system performance should be capable of incorporating all options. The options, along with a discussion on how they can be incorporated into a single model, are considered below. It is also advantageous to be able to model several different system failure modes within a single model.

2.1 Design

The design of the system will determine its structure and which of the list of potential components which perform the same function will be selected.

System structure. This will determine how vulnerable the system is to the failure of its components. For safety critical systems, it is undesirable for a single component failure to result in system failure. Redundancy or diversity in the system structure are commonly employed to ensure an adequate level of fault tolerance. In addition, where possible, the system will be made to fail safe. Duplication of the same components (redundancy) or the provision of an alternative means to achieve the same function (diversity) can be implemented in a fully redundant (parallel) structure or a partially redundant (voting) structure. When systems are analysed using a fault tree, all of these design options can be incorporated in the same analysis through the use of house events. House events are incorporated into the fault tree diagram at the base level and are set to true or false in order to represent the selected design by turning on or off the relevant sections of the tree [20]. This type of feature also works well when the fault trees are analysed utilising Binary Decision Diagrams [21-23].

Component selection. There will usually be several options as to the component type selected to fulfil a specified function. Each component selection will imply different performance metrics, maintenance requirements and costs. As with the system structure, these choices can be incorporated into a single fault tree diagram using House events as indicated in reference [20].

These design options can also be included in a PN or BN analysis of the system. This is implemented using exactly the same mechanism as for fault trees and again turn on and off features in the analysis.

2.2 Maintenance Strategy

A broad view of maintenance is taken in the context of the system modelling performed in this paper. It will have the effect of controlling the state of a system or asset once it becomes operational. Common maintenance features which need to be incorporated in the model are:

Inspection/testing this activity does not alter the state of any component. It simply reveals the component's condition and enables decisions to be made regarding the requirement to do work. For some

components, the inspection can be a visual examination. For others a test can be performed, in some instances remotely.

Servicing is carried out to reduce the rate of failure rate of a component or sub-system. This includes activities such as the replacement of lubricants and filters and the painting of metal structures.

Reactive repair on failure. All components have the potential to fail and repair of the failed component to the working condition is carried out once its state is revealed through inspection or announces itself through its impact on system performance.

Component replacement on age, use or condition. This is usually the preferred means of controlling the system state by replacing components prior to their failure. This decreases the system failure occurrences and disruptions to the functionality of the system and can be conducted at times which are convenient. The trade-off is that early replacement wastes some of the component's operational life. For items where the condition can be measured and related to its failure then condition monitoring offers an effective means on which to base decisions on early component replacement. For items whose condition cannot be measured, the creation of its unreliability function through the study of historical failures can provide a replacement time which ensures that an acceptable risk of failure is experienced.

Sub-system renewal. A whole sub-system can be renewed when maintenance becomes an ineffective means of controlling its condition.

Opportunistic maintenance can be performed on a component when the opportunity presents itself due to work being performed on another component. It could be that the component requiring attention has resulted in a system shutdown enabling access to other components which, whilst these remain functioning are in a degraded state and expected to fail in the near future. Alternatively it could be that the opportunity is presented due to the availability of specialist equipment in the locality. This type of maintenance produces dependencies between the component's conditions and cannot be adequately considered in a fault tree / event tree study.

All of the above maintenance processes have been effectively incorporated into asset management models which have been formulated using a PN. These models predict the state of any asset given a maintenance strategy [13-15]. By utilising Place Condition Transitions [13] in a PN it is also possible to specify a different maintenance strategy for different periods throughout the system life. As with the design options this has the effect of turning on and off options within the model.

3. MODELING METHODS

3.1 Petri Nets

A PN is a graphical analysis method which has been developed to model the dynamic performance characteristics of systems featured in the engineering, industrial and business sectors. The network features 'places' (indicated by circles on the diagram) which represent the possible states in which elements of the system can reside. 'Transitions' are incorporated (as represented by rectangular boxes) in order to model how the system can change between states. 'Tokens' (dots placed within places) represent the current status of the system. Arcs connect input places to a transition and transitions to output places. There are rules defined which govern how tokens are removed from input places and added into output places to simulate the dynamic behaviour of the system.

Consider the simple PN illustrated in Figure 1. Places labelled P1-P6 represent the condition of elements of a system. The transitions, labelled T1-T4, represent the four types of transition used in this study. Transition T1 is a conventional transition and associated with this will be a distribution which governs its firing time once it is enabled. A transition is enabled when the input places (P1 and P3) contain the

requisite number of tokens. If an input arc has an associated multiplicity, as in the arc from P3 to T1 (multiplicity 2), it indicates the number of tokens required in the input place to enable the transition. If no multiplicity is stated the default value is 1. When all of the input places contain at least the required number of tokens, as with T1, the transition is enabled. The transition fires after a time sampled from the associated distribution. On firing the multiplicity of tokens is removed from the input places and the multiplicity of tokens is placed in the transition output places. For transition T1 after firing P1 and P3 would contain no tokens and P2 and P4 would contain a single token each.

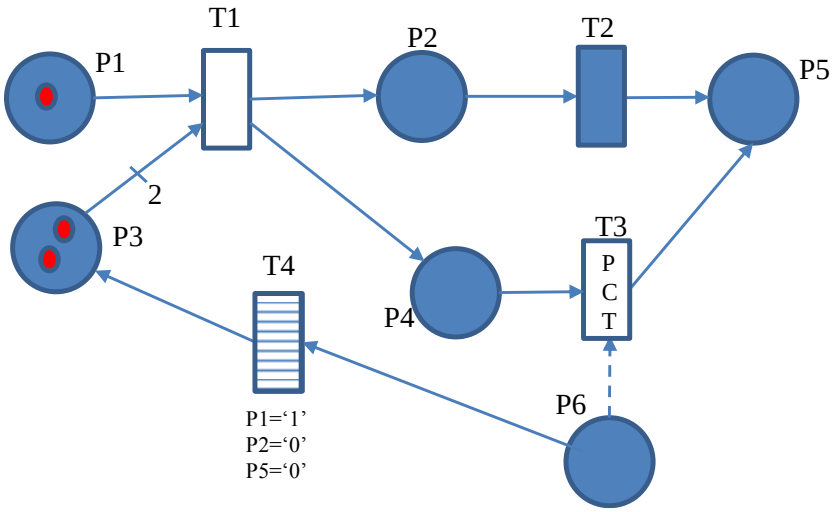

Figure 1 Petri Net Example

Transition T2 is a fixed time transition which is distinguished from transition T1 through the solid fill. A fixed time transition functions in exactly the same way as a conventional transition other than its firing time is fixed (can be zero which makes it an immediate transition) and not sampled from a distribution. T3 represents a Place Conditional Transition. The distribution law governing the transition firing time is chosen according to the number of tokens contained in the conditional place connected via a dotted line. The final transition, T4, is a reset Transition and on firing as well as moving the tokens in the traditional way it resets other places in the network. For T4, A token is placed in P1 and any tokens present in places P2 and P5 are removed.

An analysis of the PN is performed using Monte Carlo simulation, the simulations will transfer the tokens around the network. During the simulations the duration of any token's residence in a place or the number of times tokens enter a place can be logged. When convergence of the results has been obtained the system performance characteristics can be determined.

3.2 Bayesian Networks

A BN, in common with a PN, is a directed graph. In the case of the BN the graph is also acyclic and represents a probabilistic model. The direction of the arcs can be considered to represent the causality relationships between the random variables. An example of a BN is given in Figure 2 where variables represent the working (W) and failed (F) states of components in a system. In the example, the state of component C is dependent upon the condition of components A and B. Component B is also dependent upon the state of component A. Since A is a root variable its probability table contains the likelihood of it being in either of the two possible states (working and failed). The tables associated with nodes B and C are Conditional Probability Tables (CPTs) where the likelihood of these variables taking each potential value is dependent upon the states of the variables which provide inputs.

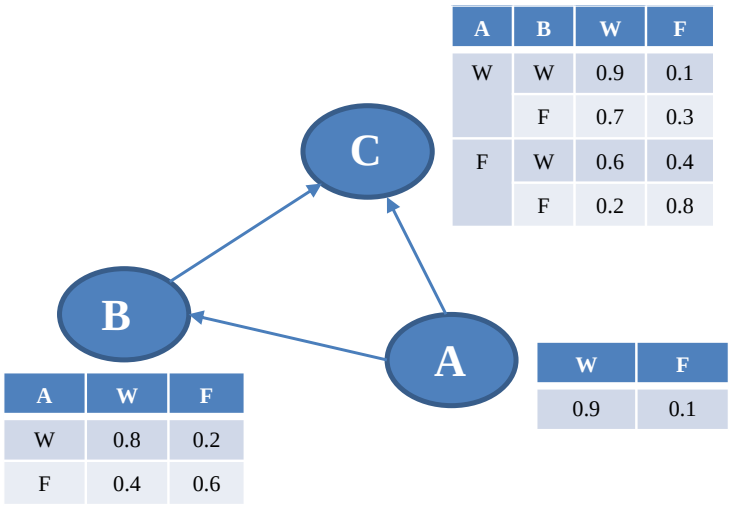

Figure 2 Bayesian Network Example

Nodes and links constitute the *qualitative part* of the network, while the *quantitative part* is represented by the conditional probabilities associated with the variables. A significant feature of BNs is that when the states of some variables in a network are known, it is possible to calculate the updated probability, given the new evidence, of all the variables in the network. Evaluating these probabilities, called *posterior probabilities*, is the main task in a BN and it is also called *inference* and is accomplished by making use of Bayes' theorem.

The structure of the BN determines the variables relationships and in the studies which follow these are established by first developing fault tree structures. The logic gates in the fault tree represent deterministic relationships and these are expressed in the BN with deterministic CPTs as defined by Bobbio [24]. Consider a BN with three nodes. Two represent component states A and B, each of which can work or fail. The state of the third variable C (which also works or fails) is dependent upon the states of A and B. In the fault tree this relationships can be represented by either an OR gate or an AND gate. The CPTs for C for each gate type are provided in Table 1 where the probabilities entered are all either 1's or 0's.

A	*B*	*Works*	*Fails*
W	W	1	0
	F	0	1
F	W	0	1
	F	0	1

OR Gate

A	*B*	*Works*	*Fails*
W	W	1	0
	F	1	0
F	W	1	0
	F	0	1

AND Gate

Table 1 OR gate and AND gate formulations for the CPTs for the Bayesian Network

4. BP-NET METHODOLOGY

The methodology developed in this paper is based on PNs and BNs and is referred to as the BP-Net method. It has the ability to incorporate the following features which advance the capability beyond the traditionally used system safety assessment methods:

- Dependencies between the component states as introduced by either the failure or repair processes.
- Any distribution of failure times and repair times.
- To analyse all alternative system designs.
- To analyse all alternative maintenance strategies.
- Incorporate a maintenance strategy which changes throughout specified life phases
- Accommodate complexity in the system structure, maintenance process or size of the analysis.
- Feature a natural modularisation process resulting from the integration of the PN and BN methods.
- Analyse all systems failure modes of interest in the same analysis.

The method lends itself to be incorporated in an optimisation framework to aid the design and maintenance decision making

The BP-Net methodology is performed in the following five stages:

1. ***Identify the system performance characteristics of concern.*** There may be several system performance measures which need to be considered. For safety systems there is the obvious undesirable failure mode where it fails to recognise and activate when the potential hazard occurs. This can be assessed through the system unavailability. However, any safety system can fail in two significant ways. In addition to failing to respond to the hazard, they can spuriously react when the hazard doesn't exist and enter the fail safe state. This will bring with it a contribution to the system down time but frequently it is the expected number of such occurrences which is a useful performance measure since it can be the nuisance value rather than the duration of the loss of system functionality which can be the main issue.
2. ***Identify where the dependencies exist in the system.*** The dependencies can occur through the operation of, for example, backup elements in warm or cold standby. They can also occur through the maintenance activities, particularly opportunistic maintenance. A list of all such dependencies, along with the components which they will affect, should be created.
3. ***Identifying the independent modules for analysis***. As a first step to identifying where the dependencies will affect elements of the system, and also providing a way in which the structure of the BN can be determined, fault trees constructed for all of the system failure modes of concern. These fault trees should be constructed for a design which, whilst not necessarily the final design, features all of the possible structures which will be present in the functional system. Having identified the component level events for which dependencies exist these events can be marked on the fault tree diagrams and algorithms such as that produced by Rauzy and Dutuit [16] can be used to identify independent modules. This algorithm will identify the gates in the fault tree which constitute independent modules. However, whilst all dependent features will be located below this gate there may still be some independent events which can be removed. To gain the greatest efficiency in the modelling the smallest independent modules are obtained by removing the

independent component failures by application of the Sun and Andrews algorithm [25] which provides an extension to that developed by Rauzy and Dutuit.

The modules which are now identified for a separate PN analysis are groups of components which feature dependencies and also individual components whose maintenance strategy or the failure / repair time distributions are too complex for their failure likelihood to be evaluated using standard formulae.

The fault trees developed are then converted to a BN. All system failure modes can be represented in a single BN by developing the appropriate logic through deterministic Conditional Probability Tables as defined in reference [24].

The likelihoods delivered from the PN models are also input to the BN model for the basic events in the fault tree. For the BN these will be dependent events whose probabilities are dependent upon the maintenance options selected. As such the failure probabilities evaluated by the PN model will be entered to the associated CPT.

4. ***Construct the module models.*** With the individual modules identified and the appropriate modelling techniques selected to efficiently analyse each according to the features of the section, the models are now constructed. These models must include all options for the potential system design and maintenance strategies which can be selected.

   Where complex degradation or maintenance processes are experienced by a component, or dependencies have been identified the modelling technique employed will be the PN formulation. The PN will have sections which model the degradation or failure process along with the inspection, servicing and repair activities.

   The system level assessment will be produced through the construction of a BN which will integrate the results obtained from the PN models of its components. The structure of the BN will follow the structure of the fault trees developed for the system. The system performance variable will be placed at the top tier of the BN structure. As the structure progresses downwards it will represent the causality of system failure through different levels of system resolution, going through variables representing the performance of the sub-systems, sections and components. The variables in the higher levels of the network will be related, as in a fault tree, through deterministic relationships. The deterministic relationships which are derived to represent the structure of the system are expressed using 0 and 1 probabilities in the CPTs (as discussed in section 3.2) which relate the lower level events with the higher level variable states in the system hierarchy. The lowest level in the main BN section will contain the variables representing the states of the system components. The performance of the components will be dependent upon the design and maintenance options selected for the system and will be obtained from the PN results which are used to populate the CPTs.

   The final layers of the BN will contain root variables which represent the design and maintenance options. The first layer in this section will contain design variables. Below these come the variables which represent the potential maintenance strategies, one layer for each maintenance phase.

Incorporation of all design options

Design options will define the system structure and component selection. It is the role of the BN in the analysis to combine the results from the analysis of the lower resolution, component failure,

events in order to make a system assessment. As such, design options which change the system structure (such as the number of levels of redundancy or the voting configuration of partially redundant sections) are best incorporated into the BN structure. They have the effect of combining the component level probabilities in different ways. Choices of component selection will change the degradation processes experienced and may change the maintenance (particularly servicing) requirements. These can be accommodated in the lower level PN models. Places can be incorporated in the network which feed into place conditional transitions (PCTs) in which the number of tokens residing in the conditional place governs the time distribution associated with a transition. For sections which model dependencies it may also be necessary to use tokens to turn on and off parts of the network to give the correct system assessment.

Figure 3 indicates how the component selection can be incorporated into the PN. For simplicity it is assumed that whichever of the two potential component types is selected it will only have two states – working and failed. Places P1 and P2 representing these states are shown on the PN section and are linked by the transition which will fire according to the failure times. The failure times will be dependent upon the component selected and so a place, P3, is included in the network which represents the component selected through the number of tokens it contains. For example, if two components, A and B can be selected, then a number of tokens in P3 is associated to each component, e.g. one token in P3 indicates that component A has been selected, while two tokens in P3 indicate that component B has been considered. Place P3 will be initialised at the start of the analysis and the number of tokens which reside there do so for the whole analysis. Transitions T1 and T2 will sample their firing times from the distribution of times to fail and times to repair corresponding to component A if P3 contains one tokens, B if P3 contains 2 tokens. The transition representing the failure process is therefore of the PCT variety where the distribution for the transition times is identified according to the marking of the conditional place (linked to the transition by a dashed line). A similar process for the repair of the selected component is adopted.

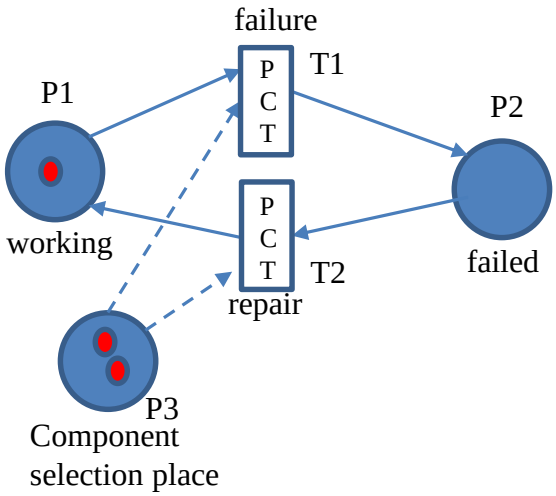

Figure 3 Component selection Petri Net

An example of how design options selected for the system structure are incorporated in the BN is shown in Figure 4. In this example the CPTs developed in section 3.2, to show how the deterministic relationships featured in fault trees are translated into a BN formulation, are extended to take into account different system structures and also different potential system states. In the

example, the lower level nodes represent the state of components A and B (working, spurious failure and dormant failure) which determine the system state, SYS, depending on the type of system selected (Series, parallel) as indicated by the Design (DES) node. Components A and B have probabilities of being in each state (if they experience complex maintenance processes these will be formulated from the PNs) entered into their probability tables. q_{dorm}, and q_{spur} are the probabilities of the components residing in the dormant and spurious failure modes respectively. The probabilities of the DES variable options are set to 1.0 and 0.0 depending on the system design selected. The state of variable SYS for every combination of the states of components A and B, and for both of the design options series (any component failing in the dormant state leaves the system un-responsive) and parallel (both components failing in the dormant state leave the system un-responsive), is shown in Table 2.

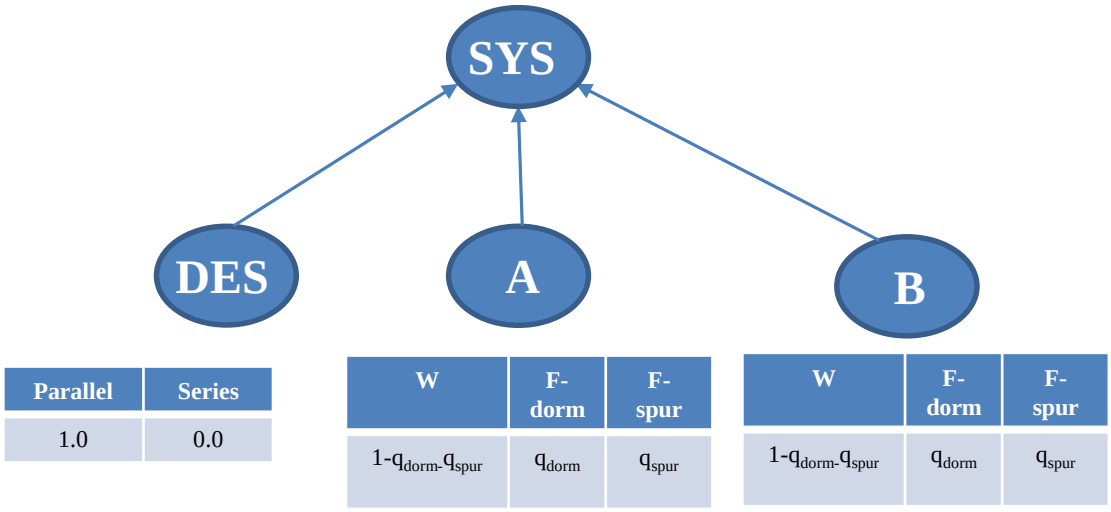

Figure 4 System Structure Selection Bayesian Network

Incorporation of all maintenance options

Variations in the maintenance strategy defined for any component can govern activities such as servicing, testing/inspection, work scheduling time and repair/replacement times. Inspection and servicing times are generally specified as a periodic variable. The selection of these can be made through a PCT where the variable representing the period selected is related to the PN transition. A PCT can also be used, as illustrated for the component degradation in figure 1, where the distribution of repair times is related to the variable representing the maintenance strategy selected.

A	B	DES	Works	DORM	SPUR
W	W	PARALLEL	1	0	0
		SERIES	1	0	0
	Dorm	PARALLEL	1	0	0
		SERIES	0	1	0
	Spur	PARALLEL	0	0	1
		SERIES	1	0	0
Dorm	W	PARALLEL	1	0	0
		SERIES	0	1	0
	Dorm	PARALLEL	0	1	0
		SERIES	0	1	0
	Spur	PARALLEL	0	0	1
		SERIES	0	1	0
Spur	W	PARALLEL	0	0	1
		SERIES	1	0	0
	Dorm	PARALLEL	0	0	1
		SERIES	0	1	0
	Spur	PARALLEL	0	0	1
		SERIES	0	0	1

Table 2 – System Performance Conditional Probability Table

5. Solution of the Models. The PN models are solved using a Monte Carlo simulation technique [4]. The simulations will record the durations that tokens spend in the critical places in the network which represent failed or deteriorated component states over the lifetime of the component. From these results the probability of being in each state can be determined and entered in to the CPTs in the system BN. These probabilities will be averaged over the number of simulations required to ensure that the PN results have converged.

The analysis of the BN is accomplished using standard commercial software such as HUGIN. The base nodes in the network represent the options for design and maintenance and are not conditional on other variables. These have prior probability tables associated with them containing probabilities set to one for each of the options selected and zero for everything else. Quantification of the BN then produces the system performance characteristics for the design and maintenance strategy selected. In order to evaluate the system performance over its lifetime, the results of the PN models are evaluated at time points throughout the system life and entered into a time point BN which contains the probabilities at that time.

5. CASE STUDY – UNMANNED WELLHEAD PLATFORM

Remote wellhead platforms are used to exploit smaller oil and gas reserves where a full processing platform cannot be justified. These smaller unmanned installations house remote wellheads. The fluids from this platform are transferred, via pipelines, for processing at a neighbouring production platform. Protection systems are incorporated onto the remote platform to prevent high pressure surges from the wells progressing to the processing equipment. If the surge is above the pressure rating of the equipment then there is a risk of hydrocarbon containment failure. In addition to the safety concerns this would also cause a major disruption to the production. An example safety system used to protect against the pressure surge, illustrated in Figure 5, is constructed of two subsystems. The first is the ESD (Emergency Shut-down) system. It features three sensors (S1-S3) which monitor the pipeline pressure. These send signals indicating the pressure to the controlling computer (COMP1). A trip is issued as soon as two out of the three sensors indicate an excessive pressure in the line. To instigate the trip the computer controller will open the vent valves (VV1, VV2) which de-pressurise the pneumatic lines to the ESD valve actuators. Since the valves are of the air-to-open type this will cause both ESD valves, ESDV1 and ESDV2, to close. As long as one valve closes it will prevent the pressure surge damaging the process equipment. The second sub-system is the HIPS (High Integrity Protection System) which, in this case, is a redundant version of the ESD sub-system.

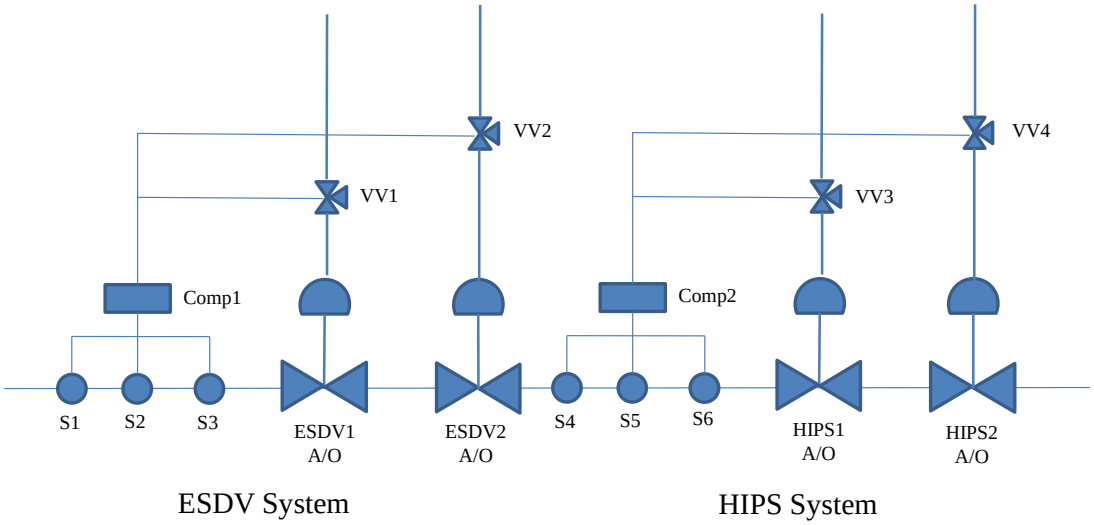

Figure 5 System Configuration

5.1 System Design Options

The system structure shown in figure 5 is a typical system configuration for such a protection system. There are many potential design variations, but to limit this to a sensible size of problem which will enable the features of the new method to be demonstrated, these will be limited to: the configuration of the sensor voting system, the types of sensor and the number of isolation valves which can be selected. Three sensors will be installed on both the ESD and HIPS systems and the design selection will choose between a fully redundant 1-out-of-3 requirement to trip configuration and a partially redundant 2-out-of-3 alternative. The first of these alternatives should have advantages from the safety point of view but would result in more spurious trips than the partially redundant alternative.

The number of isolation valves used in both the ESD and HIPS can be one or two to provide a single functioning component or to introduce redundancy into the structure. This feature need not be the same for each of the two over-pressure protection sub-systems.

For the sensors it is assumed that there are two alternative types from which the selection can be made.

5.2 System Maintenance Options

It is the nature of safety systems, such as the over-pressure protection system, that failures which render the system unable to respond to the hazard will only be revealed during testing or when a demand occurs. Testing the functionality of the system is therefore an essential part of the maintenance process. The sensors, computer control unit, and the vent valves show no measurable signs of a degradation and are simply considered to function or fail. Condition monitoring is therefore not possible for these components and the failed condition is established by a testing regime carried out at set intervals (θ_1) when engineers visit the platform. Failed items are then repaired.

The performances of the valves used for both the ESD and HIPS sub-systems, which are of an identical type, degrade as they age. The performance can be measured by the time that it takes to close from their normal, fully open, position. This time increases as the condition deteriorates and it gets closer to failure.

The valve condition can be established by remote testing. A remote closure of the valve can be instigated (at intervals of θ_2) where the duration to achieve valve closure is transmitted back to the maintenance centre. At the centre the required action can be determined. Clearly, the objective is to remove the valve from service prior to failure. In determining the maintenance strategy it has to be established at what condition (closure time) the valve is scheduled for *routine maintenance* (c_{ROUT}). If this is carried out too early in the valve life then it will discard the valve unnecessarily wasting some of the useful life remaining. If it is carried out too late in the valve life the risk of failure increases. Given that there is a substantial cost associated with sending a team out to perform maintenance on the remote platform, the condition monitoring brings about the potential for *opportunistic maintenance* where the valve will be replaced if work is to be performed on other valves and its condition, whilst better than that at which replacement would usually be triggered, is less than some threshold (c_{OPP}, $c_{OPP} < c_{ROUT}$).

Figure 6 shows the relationship between the deteriorating closure times for a valve and it's average remaining useful life. As can be seen, when functioning normally, the valve has a closure time of 10 secs. In this new condition it has a mean time to failure of 10 years. By the time the closure time has increased to 20 secs the mean time to failure has been established as 2 years. At 25 secs closure time the mean time to failure has become 1 year. This then rapidly deteriorates with the mean failure times of 6 months and 4 months respectively when the closure times reach 30 and 32 seconds.

As the systems age, the condition of some of the components will deteriorative more rapidly than others. This will be particularly evident when the systems operate beyond their originally intended life. To manage the condition of the components in the system such that acceptable performance is retained, the available maintenance resources will need to be intelligently allocated to parts of the system where it is most effective. This can be achieved by dividing the system lifetime into phases with a different maintenance strategy employed in each phase. The number of phases and the start-time of each phase will need to be defined.

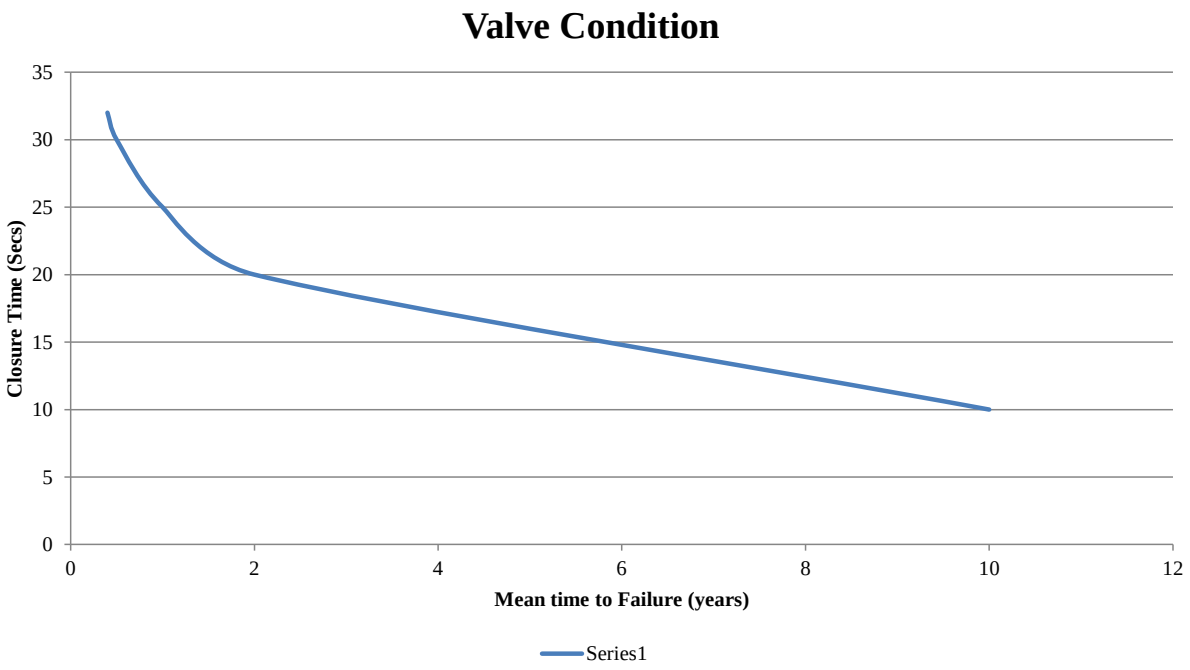

Figure 6 Valve Condition against Mean Time to Failure

5.3 Summary of the System Design and Maintenance Options

The options to be specified for the system design and maintenance strategy are listed below along with the values these variables can take:

Design

1. Sensor configuration [SenCon] (Sc): 1-oo-3 or 2-oo-3.
2. Sensor type [SenTyp] (St): type1 or type2.
3. Number of isolation valves fitted to each system [Valno] (Vn): 1 or 2.

Maintenance strategy

Two maintenance phases are assumed.

4. Start time of phase 2 [TPhase2]: 20, 30 or 40 years

Within each of the two phases the following parameters will be defined:

5. Testing interval of the components (sensor, computer, vent valve) by maintenance personnel [TIMan] (θ_1): 3, 6 or 12 months
6. Testing interval for the sub-system activation closure times [TIRemote] (θ_2): 3, 6 or 12 months
7. Closure times above which the valve can receive opportunistic maintenance [LOP] (c_{OPP}): 20 or 25 seconds or no opportunistic maintenance.

8. Closure times above which the valve will be set for routine maintenance [LR] (c_{ROUT}): 30 or 32 seconds.
9. The scheduling time for routine maintenance [STRO] ($Rout_{SHD}$): 2 or 6 months.
10. The scheduling time for revealed failure maintenance [STRE] ($\mathrm{Re}vld_{SHD}$): 1 or 2 weeks.

The scheduling time for emergency failures will also be fixed at one day due to its priority. The system life time is set at 60 years and failure rates and average repair times for the components in the sub-systems are provided in Table 3.

Component type	*Failure Mode*	*Codes*	*Failure rate (per hour)*	*Mean time to repair (hours)*
Vent Valve	Fails to open	VV1,VV2,VV3,VV4	1.0×10^{-5}	24.0
	Spuriously opens	VV1S, VV2S, VV3S, VV4S	5.0×10^{-6}	24.0
Computer Controller	Fails to detect trip condition	COMP1, COMP2	1.0×10^{-6}	12.0
	Spurious trip condition detection	COMP1S, COMP2S	1.0×10^{-6}	12.0
Pressure Sensors (type 1)	Fails to detect high pressure	S1T1-S6T1	1.0×10^{-4}	12.0
	Spurious detection of high pressure	S1T1S-S6T1S	1.0×10^{-5}	12.0
Pressure Sensors (type 2)	Fails to detect high pressure	S1T2-S6T2	5.0×10^{-4}	6.0
	Spurious detection of high pressure	S1T2S-S6T2S	1.0×10^{-4}	6.0
Shut-down valves	Fail to close	ESDV1, ESDV2, HIPS1, HIPS2	3.81×10^{-6}	24.0
	Fail closed	ESDV1S, ESDV2S, HIPS1S, HIPS2S	3.81×10^{-6}	24.0
	Fail Stuck	ESDV1St, ESDV2St, HIPS1St, HIPS2St	3.81×10^{-6}	24.0

Table 3. Component Failure and Repair Data

6. CASE STUDYANALYSIS

The details of the BP-Net methodology are demonstrated through its application to the Unmanned Wellhead Platform described in the previous section.

Each stage of the analysis process is discussed below:

1. ***Identify the system performance characteristics of concern.*** The pressure protection system is designed to respond to the occurrence of a high pressure surge in the process system and so the most important metric by which the adequacy of the system can be measured is its unavailability, Q_{avail}. This is the likelihood that the system is unable to meet its design intention and will not

respond to the pressure surge event. For the system to be unavailable it will be in the dormant failed state due to unrevealed failures which will be detected by the testing regime. A second failure event can occur when the safety system spuriously triggers and causes a process shut-down when there is no high pressure surge. This type of failure is immediately revealed but will cause an interruption to the production process while the cause(s) of the failure are corrected. For this situation both the likelihood that the process is shut-down as a consequence of the safety system failure, Q_{sd}, and the number of such occurrences, N_{sd}, are relevant factors by which to judge the adequacy of the system

2. ***Identify where the dependencies will exist in the system.*** As a first stage in this part of the process the causality of the system failure events, in terms of the component level events, needs to be established. By then considering the functional and maintenance processes, dependencies between the component level failures, the independent modules can be established and appropriate modelling techniques identified. Figure 7 illustrates the fault tree for the system dormant failure and Figure 8 the causes of system spurious failure for the HIPS (the ESD system fault trees have identical structures). The system design used to develop the failure causality logic is selected such that it contains all of the features which could influence the modelling techniques selected.

   Considering the fault tree in figure 7, the vent valves, computers and sensors all experience common inspection, maintenance scheduling and repair processes but since the failure of one component does not affect the likelihood of failure of another they can all be modelling as independent modules in the analysis. The valves however are not independent due to the occurrence of opportunistic maintenance. On either the ESDV or HIPS subsystems, when one valve requires maintenance work and the required tools, spares and maintenance personnel are transported to the remote platform, work may also be performed on the other valve (if fitted in the design) if its condition, as indicated by a remote testing strategy, is sufficiently degraded. Should two valves be fitted to either ESDV or HIPS subsystems then they need to be considered in a common model to account for the dependencies. The two sub-systems can however be considered independently.

   Considering the fault tree in figure 8, the same conclusions regarding dependencies can be confirmed.

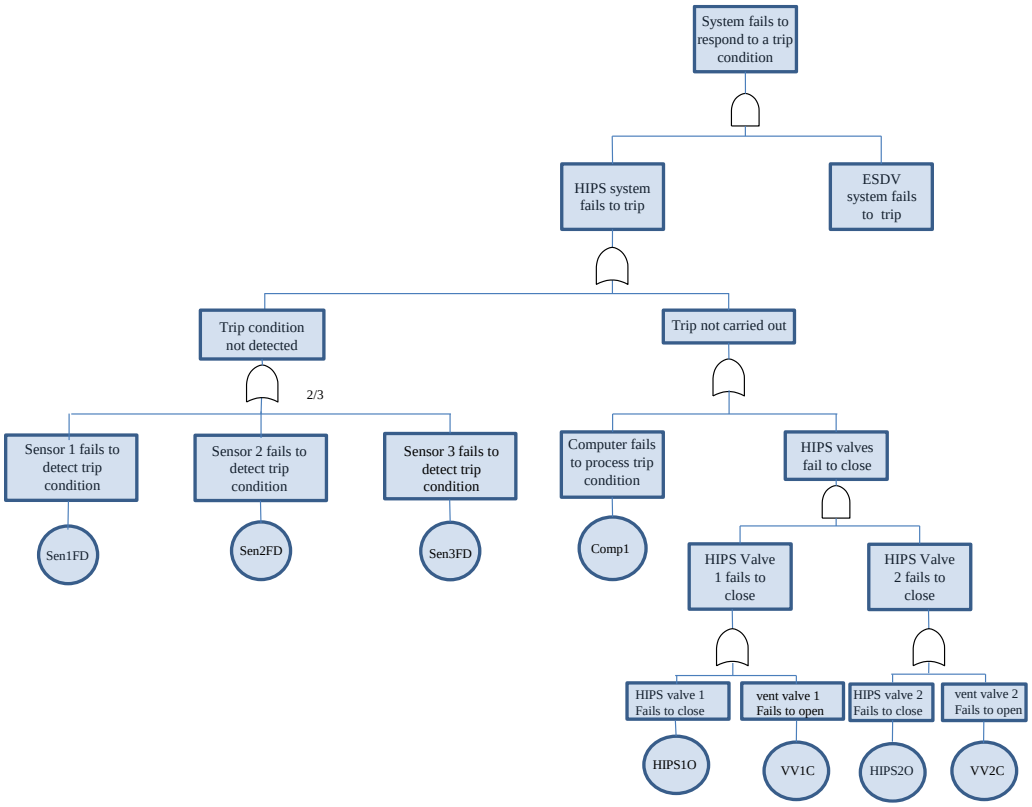

Figure 7 Fault Tree for HIPS Safety System Unavailability

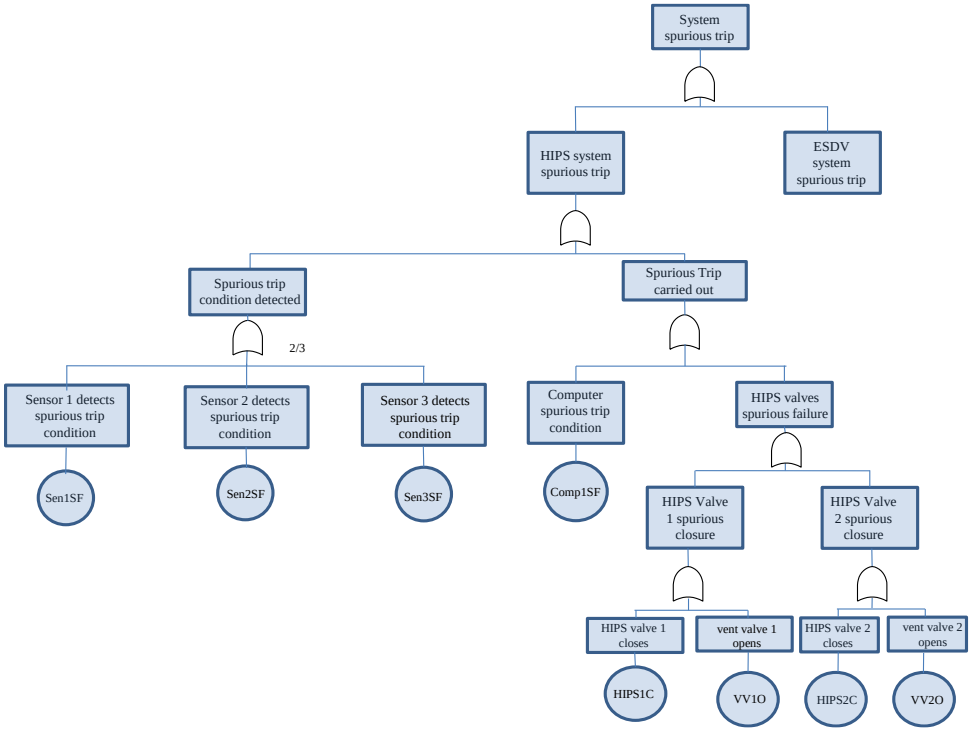

Figure 8 Fault Tree for HIPS Spurious System Failure

3. Identifying the independent modules for analysis

Through opportunistic maintenance dependent event pair (HIPS1O and HIPS2O) has been identified in the Figure 7 fault tree. Similarly ESDV1O and ESDV2O are dependent on the ESD subsystem. By applying the Rauzy and Dutuit algorithm the gate event 'HIPS valves fail to close' would be identified as the independent module. Whilst the module is independent of the rest of the fault tree it contains the component failure events VV1C and VV2C which represent the vent valves failing to open. In order to identify the smallest possible submodule for analysis these events can be removed. This refinement will result through the application of the algorithm in reference [25]. Application of the modularisation process to the fault tree for spurious system failure, shown in figure 8, results in the identification of identical component dependencies through events HIPS1C and HIPS2C. No further dependencies have been identified.

Four such models are then required to formulate the probability inputs to the system structure BN model:

i. A model of the performance of the two isolation valves featured on either the ESDV or the HIPS sub-system (both will be identical)

ii. A model of a sensor failure or functionality

iii. A model of a vent valve failure or functionality

iv. A model of a computer failure or functionality.

Whilst these models are independent they all feature complex maintenance process which include variable maintenance phase parameters, inspection, scheduling of repair and a clear dependence between the dormant and spurious failure modes. All of these independent sections will be modelled using a PN formulation. The results obtained will feed into a system level model which accounts for all possible design and maintenance options employed. This single model, based on a BN formulation, will also account for the different potential system failure modes.

4. Construct the module models

PN models will be presented for the valve section of the HIPS and also for a sensor failure. A PN model is required for the valve section to adequately account for the dependency introduced through opportunistic maintenance. For the sensor availability prediction the PN is required to model the details of the complex maintenance processes employed. The two models are presented in the sections which follow. The models required for the vent valve and computer will take the same form as the sensor model.

6.1 The HIPS Sub-system Valves Model

Sections of the PN model for the HIPS Valve sub-system are shown in Figures 9 and 10. The model for the ESDV sub-system is identical in structure and so by taking advantage of this symmetry of the problem only one model needs to be solved and the results included into the BN CPTs.

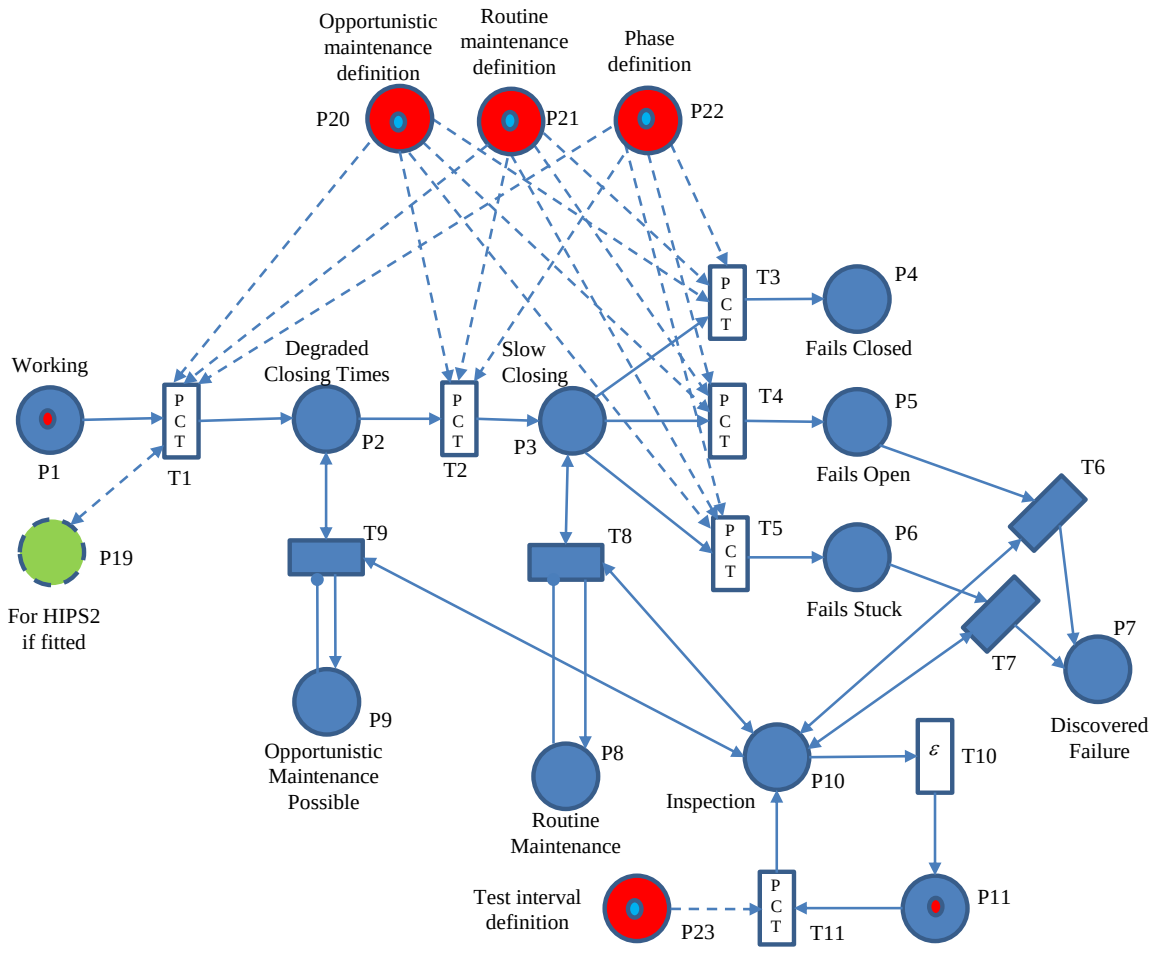

Figure 9 Petri Net for the HIPS Valve No. 1

The PN model presented in Figure 9 shows the degradation process of a single valve on the HIPS system. The valve condition can be monitored by performing a remote closure test. Depending upon the time it takes to meet full closure the condition of the valve can be established and related to it's expected remaining time to failure. This enables degraded condition states to be defined at which opportunistic or routine maintenance can be scheduled. Should the valve fail, it will fail in one of three failed states: spurious closure (the valve closes and causes the hydrocarbon flow to stop), dormant failure (the valve is stuck fully open and is incapable of closure in the event of a pressure surge) and stuck in some intermediate position (as with the dormant failure it cannot isolate the flow on the line). Since a spurious failure will cause shutdown of the process system it will be immediately revealed and due to the consequential loss of revenue its repair will be given priority. Since the other two failure modes leave the valve open and passing fluid, its normal operating state, the condition will not be revealed and has to be discovered by the testing regime. All of these failure modes are considered to be equally likely.

In the model the place labelled P1 represents the valve in good working order with no need of maintenance. In this condition the closing time will be around the 10 seconds duration expected (as shown in figure 6). Should its condition deteriorate and the closing time slow to a time where failure is thought likely to occur in the near future (place P3) then routine maintenance to replace the item prior to its failure will be

scheduled. If opportunistic maintenance is allowed then some degraded condition between the good state and the state at which routine maintenance is performed will be established (P2). In this condition it is considered to be cost effective to carry out preventive maintenance on the valve should a team be sent to the platform to carry out work on the other HIPS valve. The definitions of states P2 and P3 in terms of their closure times is a matter of selection when setting the maintenance strategy. From the state at which routine maintenance is requested, P3, continued degradation results in the spurious failure (P4), dormant failure (P5) or position stuck (P6). Since the effect of the system performance is the same for the last two of these failure modes when the condition is discovered, through the testing process, a token in either of these two states results in a token being placed in P7 indicating a discovered valve failure. The testing process is represented by the loop of P11-T11-P10-T10- P11. When the token is in P10 it indicates that a test is taking place to reveal the performance condition of the valve. This situation results from the firing of transition T11 which happens with period θ_2. On revealing the condition of a degraded but not failed performance a token will be placed in P9 indicating that opportunistic maintenance is appropriate or P8 that routine maintenance is required for the valve. This instigates the appropriate scheduling of the preventive maintenance work.

The PN in figure 9 shows the degradation and inspection processes for a single valve. If fitted, there will be another PN with the same structure as that shown in figure 9 to model HIPS2 valve. The only difference will be that there is a place (demonstrated by the dotted place, P19, which contains a token in the event that the design features a second valve). The token in P19 effectively turns on these second PN section. The inspection loop P11-T11-P10-T10-P11 will be common to both valve model sections.

The maintenance strategy will set the closure times at which the valve will be available for opportunistic maintenance (20 or 25 seconds) and routine maintenance (30 or 32 seconds). It can be seen from figure 6 that the average remaining times to failure at 20, 25, 30 and 32 seconds are 2 years, 1 year, 6 months and 4 months respectively. The expected time to failure for a new valve is 10 years. This gives the mean time for transitions between states shown in Table 4 for each of the maintenance options.

Closure time for opportunistic maintenance	*Closure time for routine maintenance*	*Average transition time for T1*	*Average transition time for T2*	*Average transition time for T3*	*Average transition time for T4*	*Average transition time for T5*
20 secs	30 secs	8 years	18 months	18 months	18 months	18 months
20 secs	32 secs	8 years	20 months	12 months	12 months	12 months
25 secs	30 secs	9 years	6 months	18 months	18 months	18 months
25 secs	32 secs	9 years	8 months	12 months	12 months	12 months

Table 4 means transition times for the valve degradation process

The number of tokens put into places P20 and P21 provide a means to define the conditions which will instigate opportunistic and routine maintenance. The selection of the maintenance options is achieved by associating to each potential strategy for opportunistic and routine maintenance, a number of tokens to mark places P20 and P21 respectively. The number of tokens in place P22 defines which maintenance phase is currently active. Specifically, a number of tokens to put into place 22 is also associated to each option related to the start time of phase 2. All three of these places feed in to the Place Conditional Transitions T1-T5 to fix the correct mean time parameter for the exponential distribution governing the degradation.

Similarly place P23 sets the remote inspection interval for the valves in Place Conditional Transition T11.

At the point of analysis of this PN the initial conditions will set tokens in places P1 and P11. It will also choose the maintenance options by placing the required number of tokens in definition places P20-23.

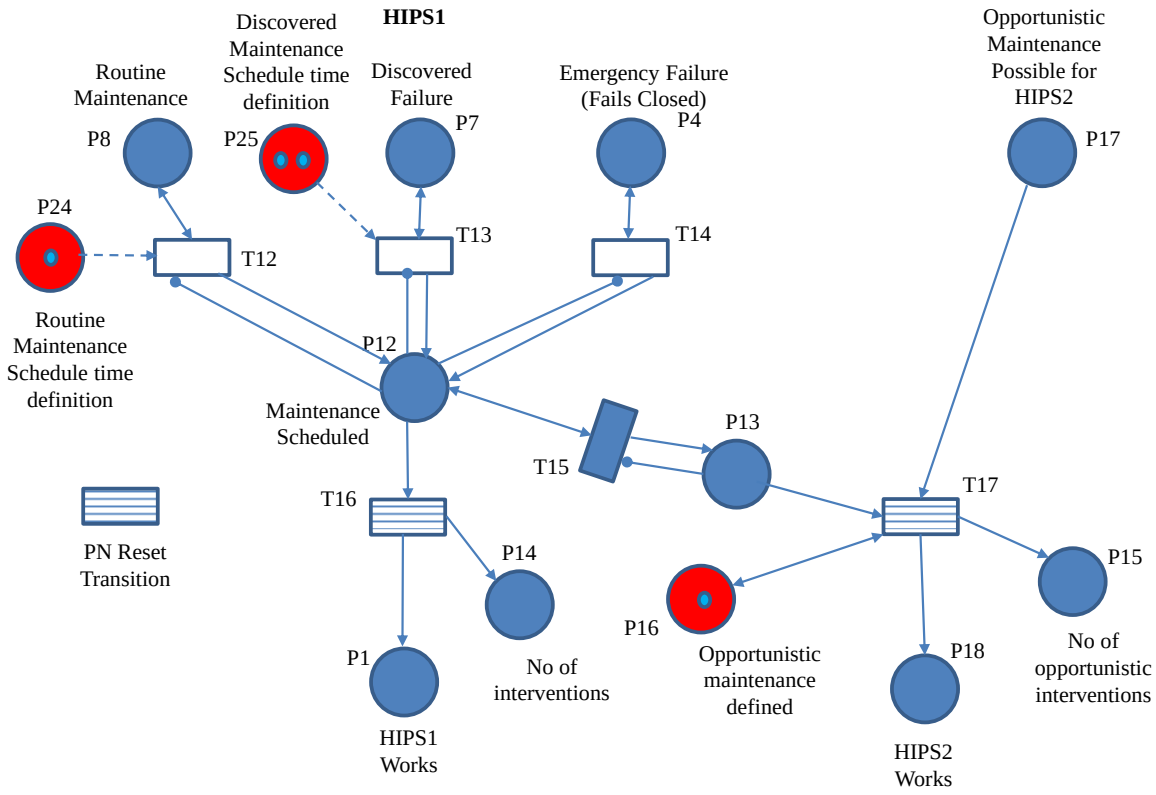

Figure 10 Petri Net for the HIPS Valve Maintenance

Figure 10 indicates the PN for the scheduling and execution of maintenance which restores the HIPS valves to the 'good' condition. States P8, P7 and P4 indicate 'routine maintenance', 'discovered maintenance' and 'emergency maintenance' respectively for valve HIPS1. When there is a token in one of these places it initiates the need for maintenance, with different priorities, to address the valve's condition. The priorities resulting from the valve condition will lead to different times in which the maintenance will be scheduled. This scheduling (making appropriate resources and transport available) has durations set by the maintenance strategy. The initial number of tokens in places P24 and P25 indicate the scheduling time for routine maintenance and revealed failure maintenance currently selected. According to such marking, Place Conditional Transitions T12 and T13 will select the appropriate time distribution governing routine (2 or 6 months) and revealed maintenance (1 or 2 weeks) respectively.

When maintenance is scheduled for the first HIPS valve this provides the opportunity for maintenance to be performed on HIPS valve 2 if it has degraded to an appropriate level (as indicated by a token in place P17). Opportunistic maintenance is selected if there is a token in definition place P16.

Note that the reset transitions initialise parts of the PN when a repair has been instigated and the valve returned to the good state. The transition times for these reset transitions is the repair time for the valves (24 hours)

Analysis of this PN will produce the probability of dormant valve failure (the sum of the probabilities of being in P5 and P6 followed by P7) or that probability that a process system shutdown exists due to the valve spurious closure (the sum of the probabilities of being in P4). These will be entered into the correct CPTs in the BN.

6.2 The sensor system sub-model

The sensor failure PN module is illustrated in Figure 11. The component has two failure modes, spurious failure (N3) which indicates high pressure surge when none is present and a dormant failure (N4) which fails to detect the high pressure condition in the process stream. The rates of failure and the repair time distributions are dependent upon the sensor type selected, which is defined through place N11. The inspection interval which will reveal the dormant failed state of the sensor is dependent upon the maintenance phase (N12) as is the repair scheduling time for such a failure.

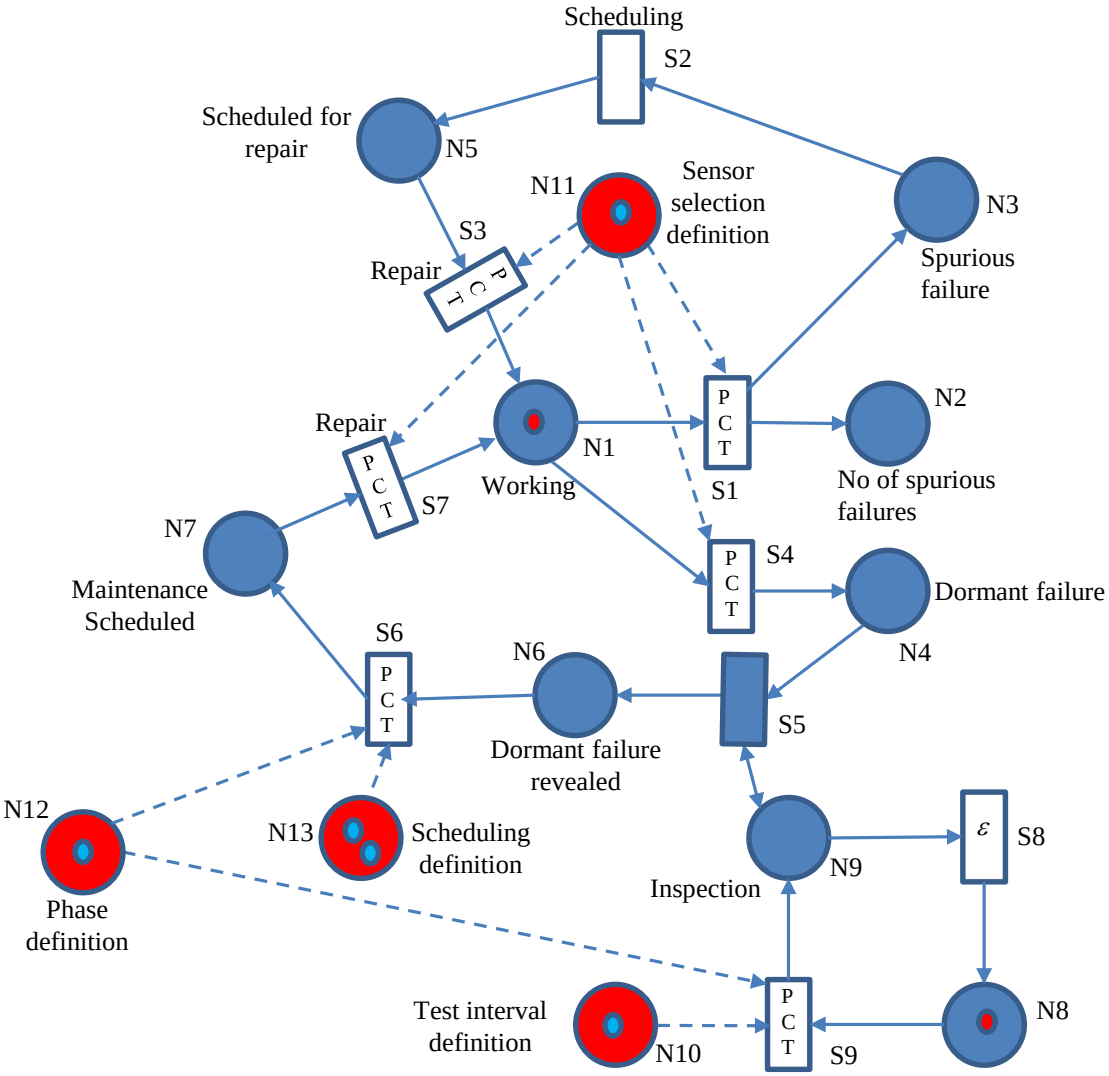

Figure 11 Sensor failure Petri Net Model

When the simulation of the sensor performance is carried out the likelihood of experiencing a dormant failure, which will be entered to the BN CPTs, is given by the sum of the probabilities of residing in states N4, N6 and N7. The likelihood of a spurious sensor failure is provided by summing the probabilities of being in states N3 and N5.

6.3 Bayesian Network System Model

The Bayesian Network to evaluate the high pressure protection system performance is illustrated in Figure 12. The structure of the network follows the fault trees developed at a prior stage. At the top of the BN diagram is a node which represents the system performance and considers three states for this variable: works, dormant (fails to respond to a high pressure surge) and Spurious (trips the process system when the pressure is normal). The causality of the system state is then represented by the dependence, at the next level of the BN (Sub-system level), upon the ESD and HIPS sub-system states. These sub-systems are in turn broken down in terms of the Sub-system activation components, i.e. the states of the valves. The states of the valves depend on the functionality and failure of the component level variables. All CPTs associated with any of the dependency relationships indicated on the BN to this point are deterministic and are derived as illustrated earlier by the CPT shown in Table 2.

Moving to the last four layers now – these represent the options which can be selected for the design and maintenance strategies. First on the design layer on the BN there are variables which represent the options for: the number of valves fitted in both the ESD and HIPS sub-systems, the type of sensor which has been fitted in the system and the redundancy configuration for the sensors.

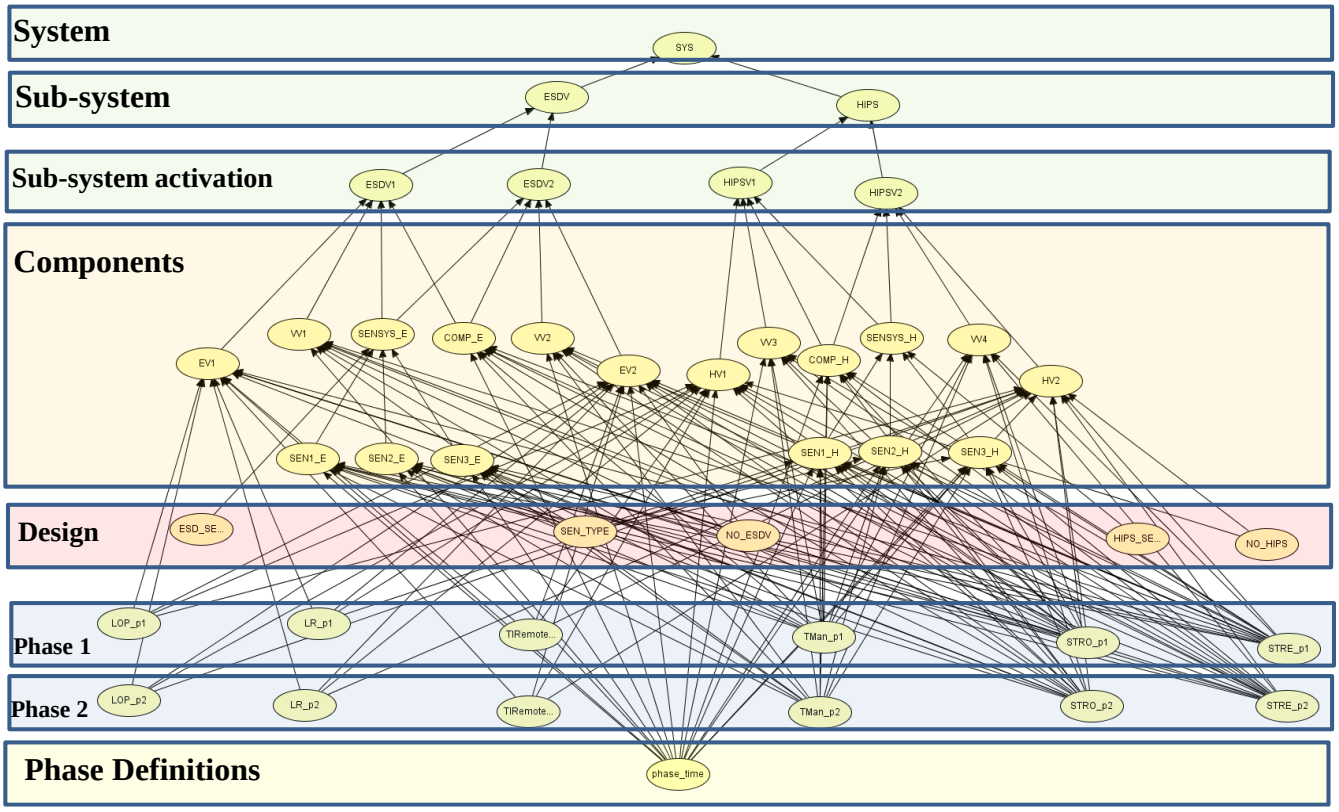

Figure 12 Bayesian Network Model

Two maintenance phases have been selected for this system example (although this too could be a variable in the analysis). On the final layer in the BN are variables representing the possible times at which phase 2 commences through the 60 year system life period. The two layers above that then have nodes which represent the maintenance options in each of the two phases. Included in this layer are variables for the inspection and testing intervals, the valve closure times which define the conditions at which the valve will be considered for routine maintenance and opportunistic maintenance and the times at which interventions of different priorities will take to be scheduled.

As indicated in the BN, the states of all components are dependent upon the types of the components selected and the maintenance strategy employed. The CPT tables which relate the design and maintenance variables with the component state are derived using the PN models. The PN for the valves, shown in Figures 9 and 10, provides the CPT for the EV1, EV2, HV1 and HV2 variables. For the sensor state variables, SEN1_E - SEN3_E, SEN1_H - SEN3_H, the PN shown in figure 11 is evaluated to produce the CPT. PNs of a similar structure to that in Figure 11 are evaluated to provide the CPTs for the vent valve variables (VV1-VV4) and the computer variables (COMP_E and COMP_H). Each PN is analysed for all the possible design and maintenance options that appear in the last four layers of the BN in Figures 12. As an example, let us consider two design options OD1 and OD2 and two maintenance options OM1 and OM2. Table 5 shows how these options are combined to obtain the probability of a component experiencing a dormant or a spurious failure, and of being in the working state conditional to the design and maintenance option selected. The probability of a dormant failure, spurious failure and working state are q_{dorm}, q_{spur}, and $q_{work} = (1 - q_{dorm} - q_{spur})$ respectively.

Design options	OD1		OD2	
Maintenance options	OM1	OM2	OM1	OM2
Dormant	$q_{dorm}^{(OD1,OM1)}$	$q_{dorm}^{(OD1,OM2)}$	$q_{dorm}^{(OD2,OM1)}$	$q_{dorm}^{(OD2,OM2)}$
Spurious	$q_{spur}^{(OD1,OM1)}$	$q_{spur}^{(OD1,OM2)}$	$q_{spur}^{(OD2,OM1)}$	$q_{spur}^{(OD2,OM2)}$
Working	$q_{work}^{(OD1,OM1)}$	$q_{work}^{(OD1,OM2)}$	$q_{work}^{(OD2,OM1)}$	$q_{work}^{(OD2,OM2)}$

Table 5 Example of conditional probabilities table.

For instance, the probability of a component experiencing a dormant failure $q_{dorm}^{(OD1,OM1)}$ when options OD1 and OM1 are selected is obtained from the PN for the component by setting the variables related to the maintenance and design options to the values corresponding to options OD1 and OM1.

By defining the states for the variables in the root layers (design, phase 1, phase 2 and phase definitions), which set the design and maintenance options of the system, the likelihood of elements on the higher levels of the BN can be evaluated. For the analysis of the BN, the probability tables of all root variables on the last four levels are set such that the option selected has a probability of 1.0 and all other alternatives are set to 0.0. Analysis of the network then provides the system performance for this particular design and maintenance option. To provide more information in assessing the adequacy of the parameters selected, a prediction of the system performance throughout its life can be delivered by the BN. For this the life period is divided into discrete times at which the BN model will be formulated. This gives a BN structure as shown in Figure 13.

In the event that the system has yet to be built then the effects of all root variable options, along with their costs, can be investigated in order to define the design and maintenance strategy which provides the best system performance into extended life. If the system is already built then the variables of the design layer

are fixed and the investigation can focus on the system performance resulting from changes to variables on the last three layers.

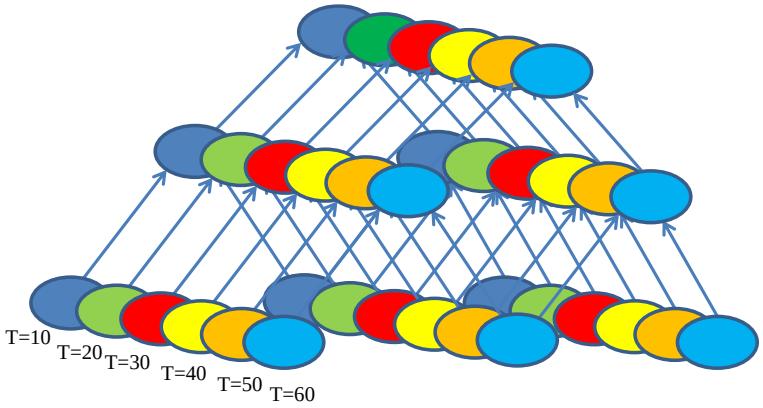

Figure 13 Dynamic Bayesian Network Structure

7. **RESULTS**

The PN models have been analysed using software written specifically for the project. It has the ability to automatically rerun the PN for all options selected for the relevant design and asset management input nodes in the 4 base layers. The probabilities obtained from the model are then used to create the entries in the CPTs for the component failure nodes. The BN analysis was carried out using the HUGIN software tool. This enables the root node design and asset management options to be selected and predicts the likelihood that the system will be in any of its three possible states: working, unable to respond to the pressure surge in the pipeline and spurious failure. The system assessment values are reported during 6 time periods over the expected 60 year system lifetime.

Petri net results

The main role for the PN analysis has been to generate probabilities for the component level CPTs in the BN. However the results from these analyses are themselves informative. During the analysis of the PNs, the number of times a token enters any place can be recorded, as can the duration of each residence time. Over the PN simulations carried out, this information can be used to form distributions of these two parameters.

Different strategies are considered for the maintenance of the components in the system. In the first a 'Base Case' selection of the possible parameters are made. In the second, the 'best' parameters are selected for each variable where everything is done as often as possible. Finally the 'worst' parameters are selected where all maintenance options are relaxed to the full extent and as little work, from among the possible selections, is carried out. The parameters selected for these three situations are shown in Table 6.

		Base Case Strategy	'Best Case' Strategy	'Worst Case Strategy
Manual test interval (Vent Valve, Computer, sensor)	TIMan (θ_1)	6 months	3 months	12 months
Remote test interval (ESD/HIPS valves)	TIRemote (θ_2)	6 months	3 months	12 months
Valve closure times for opportunistic maintenance	LOP (c_{OPP})	25 secs	20 secs	25 secs
Valve closure times for routine maintenance	LR (c_{ROUT})	32 secs	30 secs	32 secs
Scheduling time for routine maintenance	STRO ($Rout_{SHD}$)	6 months	2 months	6 months
Scheduling time for revealed failure maintenance	STRE ($Revld_{SHD}$)	2 weeks	1 week	2 weeks

Table 6 Maintenance Strategies

When the PN model was run for 500 simulations of a 60 year system life the percentage likelihoods that the components exist in the working, unrevealed and spurious failure states are provided in Table 7. As can be seen, the more intensive each of the maintenance strategies is, the better the component performance in terms of being in the working state and not being in the unrevealed, dormant, failure mode.

		Base Case Strategy	'Best Case' Strategy	'Worst Case Strategy
Sensor	Working	98.61	99.11	97.55
	Dormant	1.09	0.6	2.11
	Spurious	0.3	0.3	0.29
Vent Valve	Working	97.76	98.66	95.51
	Dormant	2.22	1.32	4.47
	Spurious	0.02	0.02	0.02
Computer	Working	99.71	99.84	99.51
	Dormant	0.29	0.15	0.49
	Spurious	0.003	0.004	0.003
Isolation Valves	Working	95.35	97.30	91.87
	Dormant	3.74	1.80	7.29

	Spurious	0.9	0.9	0.84

Table 7 Component Failure Likelihoods

Bayesian Network results

Using the results obtained from the PN modelling the CPTs of the BN can be formulated. Some of the CPT tables are large in size, for example, as can be seen from Figure 12, the isolation valves have 11 lower level variables as inputs. Taking all options that these variables can take produces a CPT with 3 x 31,104 entries. However the tables are generated automatically by the PN software and present no difficulties.

The BN has been used to test the system performance for two different designs and maintenance strategies. Both designs feature the same structure for the ESDV and HIPS sub-systems. System 1 features a 2-out-of-3 sensor configuration (type 2 sensors) and 2 isolation valves on each system. The second, System 2 has a single isolation valve on the ESDV and Hips sub-systems and a 1-out-of-3 sensor configuration (also sensor type 2). The results, reported for each 10 year period of the 60 year operational life are reported in Table 8. Three maintenance strategies made up of the parameters defined in the previous section are applied. Strategy 1 applies the 'base case' maintenance parameters throughout the 60 year life period. Strategy 2 applies the 'best' maintenance parameters for the first 40 years and then the 'worst' parameters for the reminder of the operational period. Strategy 3 reverses the contribution of the 'best' and the 'worst' parameters as used in Strategy 2. All design and maintenance options were selected by assigning a probability of 1.0 to that option in the variables in the last 4 layers of the BN in Figure 12. These designs are both robust, featuring a great deal of redundancy. As expected, System 1 performs better than System 2 for all maintenance strategies. Maintenance Strategy 2 is better than Strategy 1 which outperforms Strategy 3. Strategies 2 and 3 perform consistently over the first 40 years and change for the last 20 years.

	System 1						*System 2*					
	Strategy 1		*Strategy 2*		*Strategy 3*		*Strategy 1*		*Strategy 2*		*Strategy 3*	
10 years	99.78	W	99.90	W	99.43	W	98.06	W	98.14	W	97.81	W
	0.14	D	0.03	D	0.50	D	0.14	D	0.03	D	0.47	D
	0.08	S	0.07	S	0.08	S	1.80	S	1.82	S	1.73	S
20 Years	99.75	W	99.89	W	99.28	W	98.10	W	98.13	W	97.66	W
	0.16	D	0.03	D	0.62	D	0.17	D	0.03	D	0.65	D
	0.09	S	0.07	S	0.09	S	1.73	S	1.83	S	1.69	S
30 Years	99.75	W	99.90	W	99.24	W	98.02	W	98.20	W	97.64	W
	0.17	D	0.03	D	0.66	D	0.20	D	0.03	D	0.68	D
	0.08	S	0.07	S	0.10	S	1.78	S	1.77	S	1.69	S
40 Years	99.74	W	99.91	W	99.21	W	98.02	W	98.16	W	97.63	W
	0.18	D	0.03	D	0.70	D	0.18	D	0.03	D	0.66	D
	0.08	S	0.06	S	0.09	S	1.80	S	1.82	S	1.72	S
50 Years	99.73	W	99.68	W	99.72	W	98.02	W	98.03	W	97.97	W
	0.18	D	0.26	D	0.19	D	0.17	D	0.24	D	0.24	D
	0.09	S	0.07	S	0.09	S	1.81	S	1.72	S	1.72	S

60 Years	99.75	W	99.60	W	99.51	W	98.02	W	97.88	W	97.83	W
	0.16	D	0.33	D	0.40	D	0.17	D	0.34	D	0.41	D
	0.09	S	0.07	S	0.10	S	1.80	S	1.78	S	1.75	S

Table 8 System Assessments

8. CONCLUSIONS

An integrated Petri net and Bayesian network modelling approach has been developed for modelling the effects that the design and maintenance options have on the system performance. The method has advantages over the traditionally used methods of fault tree and event tree analysis and is capable of accounting for the following features:

i. any distribution of degradation, failure and repair time can be accommodated.

ii. dependencies between the component conditions.

iii. highly complex maintenance strategies.

iv. different design and maintenance options can be specified within a single model.

v. several system performance parameters can be predicted within a single model.

The modelling approach lends itself to integration with an optimisation process to set the design and maintenance parameters to yield the best system performance, in some sense, subject to practical limitations on the resources.

ACKNOWLEDGMENTS

John Andrews is the Royal Academy of Engineering and Network Rail Professor of Infrastructure Asset Management. He is also Director of The Lloyd's Register Foundation* Resilience Engineering Research Group at the University of Nottingham. Claudia Fecarotti is a Research Associate supported by Network Rail. They both gratefully acknowledge the support of these organisations.

* The Lloyd's Register Foundation (LRF) supports the advancement of engineering-related education, and funds research and development that enhances safety of life at sea, on land and in the air.

9. REFERENCES

[1] Andrews, J.D. and Dunnett, S.J., (2000), Event Tree Analysis Using Binary Decision Diagrams, *IEEE Transactions on Reliability*, 49(2), pp. 230-238. ISSN 0018-529.

[2] Henley, E.J. and Kumamoto H, Reliability Engineering and Risk Assessment, *Prentice-Hall, New York*, 1981.

[3] W.E. Vesely, (1970), A Time Dependent Methodology for Fault Tree Evaluation, *Nuclear Design and Engineering*, 13, pp. 337-360.

[4] Andrews, J.D. and Moss, T.R., (2002), Reliability and Risk Assessment (2nd edition), *Professional Engineering Publishing*, 540 pp, ISBN 1-86058-290-7.

[5] Dugan, J. B., Bavuso, S., Boyd, M., Dynamic fault tree models for fault tolerant computer systems. IEEE Transactions on Reliability. 41(3), pp 363- 371, 1992.

[6] Meshkat, L., Dugan, J.B. and Andrews, J.D., Dependability Analysis of Systems with On-demand and Active Failure Modes, Using Dynamic Fault Trees, IEEE Transactions on Reliability, 51(2), pp 240-251, 2002, ISSN 0018-9529.

[7] Limnios, Nikolaos, and Gheorghe Oprisan. Semi-Markov processes and reliability. Springer Science & Business Media, 2012.

[8] Esary, J.D., and Ziehms, H., Reliability Analysis of Phased Missions, *Reliability and Fault-Tree Analysis*, 1975, pp. 213-236.

[9] Prescott, D.R., Andrews, J.D. and Downes, C.G., Multiplatform Phased Mission Reliability Modelling for Mission Planning, *Proceedings IMechE Part O: Journal of Risk and Reliability Engineering*, Vol 233, Part O, 2009, pp27-39.

[10] Prescott, D.R., Remenyte-Prescott, R., Reed, S., Andrews, J.D., Downes, C.G., A Reliability Analysis Method using BDDs in Phased Mission Planning, *IMechE Part O: Journal of Risk and Reliability Engineering*, Vol 233, Part O, 2009, pp133-143.

[11] Jensen, K., (1997), Coloured Petri Nets, *Springer Verlag.*

[12] Schneeweiss, W.G., (1999), Petri Nets for Reliability Modelling, *LiLoLe Verlag Publishing Company Limited*.

[13] Audley, M. and Andrews, J.D., (2013), The Effects of Tamping on Railway Track Geometry Degradation, *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, 227)(4), pp 376 – 391.

[14] Le, B. and Andrews, J., Petri Net Modelling of Bridge Asset Management Using Maintenance Related State Conditions, *Structure and Infrastructure Engineering*, published on-line 26 June 2015 (DoI. 10.1080/15732479.2015.1043639.

[15] Andrews, J, Prescott, D. and De Rozieres, F., 2014, A Stochastic Model for Railway Track Asset Management, Reliability Engineering and System Safety, Vol 130, pp76-84.

[16] Dutuit Y and Rauzy A, A linear Time Algorithm to Find Modules in Fault Trees, *IEEE Trans Reliability*, 45, No 3, 1996.

[17] Jensen, Finn V; Nielsen, Thomas D., (2007), Bayesian Networks and Decision Graphs. I*nformation Science and Statistics series (2nd ed), New York, Springer-Verlag.*

[18] Doguc, O. and Ramirez-Marquez, J.E., (2009), A Generic Method for Estimating System Reliability Using Bayesian Networks, *Reliability Engineering & System Safety*, 94(2), pp. 542–550.

[19] Langseth., H. and Portinale, L., (2007) Bayesian Networks in Reliability, *Reliability Engineering & System Safety*, 94,(2) pp. 92-108.

[20] Pattison, R.L. and Andrews, J.D., Genetic Algorithms in Optimal Safety System Design, *Proceedings of the Institution of Mechanical Engineers*, 213(E3), 1999, pp 187-197, ISSN 0954-4089.

[21] Rauzy, A., (1993), New Algorithms for Fault Tree Analysis, *Reliab. Engng. Syst. Safety*, 40, pp. 203 - 211.

[22] Sinnamon, R.M. and Andrews, J.D., New Approaches to Evaluating Fault Trees, *Journal of Reliability Engineering and System Safety*, 58(2), 1997, pp 89- 96, ISSN 0951-8320.

[23] Sinnamon, R.M. and Andrews, J.D., Quantitative Fault Tree Analysis Using Binary Decision Diagrams, *European Journal of Automation*, 30(8), 1996, pp 1051-1071, ISSN 0296-1598.

[24] Bobbio, A., Portinale, L., Minichino, M. and Ciancamerla, E.,(2001), Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks, *Reliability, Reliability Engineering & System Safety*, 71, pp. 249-260.

[25] Sun, H. and Andrews, J.D., Identification of Independent Modules in Fault Trees which Contain Dependent Basic Events, Reliability Engineering and System Safety, 86, 2004, pp 285-296.