Value of information based inspection-strategy of a fault-tree

J. G. Norstrøm
Kongsberg Defence & Aerorospace, Section for System Safety and Reliability

R. M. Cooke
TU-Delft, Faculty of Information Technology and Systems, the Netherlands

T. Bedford
TU-Delft, Faculty of Information Technology and Systems, the Netherlands

ABSTRACT: Control software is software that receives observations from sensors such as break wires built into the satellite to timely activate actuators to trigger required functions like antenna deployment after launch and separation. Often inadvertent activation as well as a delayed response can have severe consequences. How the software monitors its sensors determines the performance of the control software. We discuss an approach that models various "design" options in detail so that the control flow can be optimised via decision theory. The example we present here uses decision analysis, statistical and mathematical properties described in Norstrøm et al (1998, 1999) to optimise the control software architecture described in Dore & Norstrøm (1996).

1 INTRODUCTION

We define *"Launch"* of a satellite as the process, carried out by e.g. the Ariane 5 rocket. The launch is characterised by the acts carried out by the launcher whose main function is to run the rocket engines to bring the satellite in orbit. Launch is completed when all rocket engines have ceased to run (booster burn out time). When the rocket engines stop running they do not start again. This is defined as *"Launch finished"*. Let T_L denote the time the launch finishes. We define *"Separated"* to be the state where the satellite is not physically attached to the rocket or other satellites. Let T_S denote the time separation occurs. Let T_F denote the time the satellite can not become operational after e.g. the satellite fail if no acts are taken by control software in the satellite before T_F (see Figure 1).

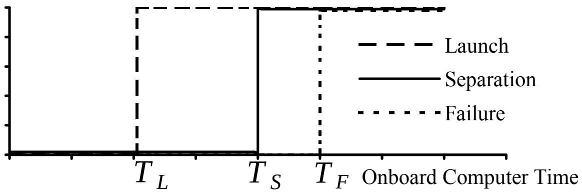

Figure 1. The launch events schedule.

1.1 Control Software Description

On top of the Ariane 5 rocket in Figure 2 there is one cargo container with an upper and a lower compartment.

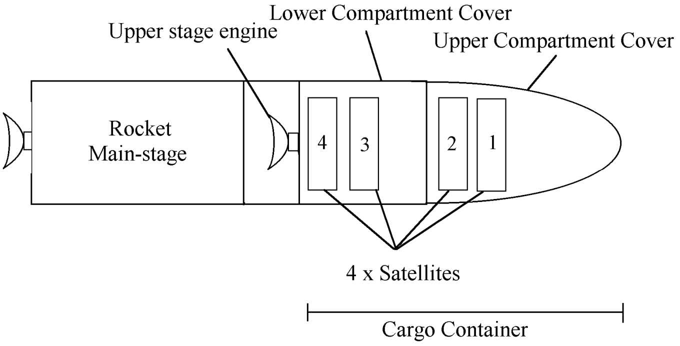

Figure 2. Rocket main-stage and cargo container.

The solid booster stages are not shown in Figure 2 since they are dropped off at a lower altitude. Only the rocket main stage, the Vulcain engine, carries the cargo out of the atmosphere. In each compartment there are two scientific satellites. Between Satellite 1 and 2 there are 5 break-wires. Similarly there are 5 break wires for satellites 3 and 4. Inside each satellite the control-software shown in Figure 6 is running. This control software steers antenna deployment. The program takes time to wait approximately to the launch finishes. Then it continuously monitors the break wire status (for example the Separation Sequence software monitors the break-wires between Satellites 1 and 2) until separation is detected. Separation is assumed when 3 of 5 break wires test broken. No time-out for the break wire monitoring is foreseen. So in any case the software will wait, until the separation is detected (i.e. 3 of 5 break wires test broken).

The use of voting logic is a popular way to take decisions under uncertainty. For example, the satellite control software acts to initiate deployment of the antenna boom if 3 out of 5 break wires test broken. Since a break wire test broken if the satellite is separated it gives information to whether a satellite is separated or not. A break wire can also show broken if shaking during launch ruptures it. Hence, when a break wire test broken we are uncertain whether the cause is separation or shaking during launch.

This paper will show how to approach this problem by using decision theory. We will use decision theory to evaluate:

i) Various control software design solutions to find the optimal break wire inspection time prior to activating the actuators that deploys antenna booms of a satellite.

ii) Estimate the control flow charter that describes how the detailed code should be coded i.e. the architectural design of the control software.

Hence, the voting logic heuristic that is normally used is not the optimal way of deciding under uncertainty.

2 DECISION PROBLEM FORMULATION

We will use the following notation:
S: Set of all relevant satellite states.
$f(t)$: Activate deploy antenna boom at time t.
F: Set of available acts $\mathrm{F} = \{f(t) \mid t > 0\}$.
$\mathrm{U}(f(t), s)$: Utility of act $f(t)$ and state $s \in \mathbf{S}$.
$X(\tau)$: Outcome of break wire test at inspection time $\tau \geq 0$, $X(\tau) \in \{0, 1, ..., 5\}$.
Mathematically define the state space **S**:

$\mathbf{S} = \{(T_L, T_S, T_F) \mid T_L < T_S, T_S \leq T_F, (T_L, T_S, T_F) =$ (Engines stop at T_L, Separation at T_S, Failure at T_F)$\}$.

The utility function defined over F × **S** is defined in Table 1. The reasoning here is based on the cost of one satellite which is $125 \cdot 10^6$\$.

	$s_1 =$ $\{t < T_L\}$	$s_2 =$ $\{T_L \leq t < T_S\}$	$s_3 =$ $\{T_S \leq t < T_F\}$	$s_4 =$ $\{T_F \leq t\}$
$f(t)$	$-500 \cdot 10^6$	$-250 \cdot 10^6$	0	$-125 \cdot 10^6$

Table 1: The utility over F × **S**.

If we deploy the antenna during launch we risk losing 4 satellites. Therefore $U(f(t), s_1 = \{t < T_L\}) = -4 \cdot 125 \cdot 10^6$. Similar after the launch ends before separation we risk loosing 2 satellites by deploying the antenna boom, hence $U(f(t), s_2 = \{T_L \leq t < T_S\}) = -2 \cdot 125 \cdot 10^6$. If the antenna is deployed at the correct time the cost is zero, $U(f(t), s_3 = \{T_S \leq t < T_F\}) = 0$. If $T_F \leq t$ we loose the satellite anyway so we use $U(f(t), s_4 = \{T_F \leq t\}) = -125 \cdot 10^6$. These values are used for illustrative purposes. Estimating the real costs would require detailed studies of the consequences involved.

The value of an act $f(t) \in$ F is to be represented by its conditional expected utility

$$v(f(t) \mid x(\tau)) = \sum_{s_j \in \mathbf{S}} \mathrm{U}(f(t), s_j) p(s_j \mid x(\tau)) \qquad (1)$$

where the uncertainty is described by a probability density function $p(\bullet)$. Taking the maximum of (1) over all accessible acts F gives the value of F as:

$$v(\mathrm{F} \mid x(\tau)) = \max_{t \geq 0} v(f(t) \mid x(\tau)) \,. \qquad (2)$$

This is the value of information given the inspection results of the break wire test $X(\tau)$. Taking the expectation of (2) with respect to $X(\tau)$ gives the expected value of F when we observe the break wire at time τ. More about decision theory can be found in Savage (1972) & De Groot (1970).

3 UNCERTAINTY MODELLING

We will assume that $T_L = \tau_L + \varepsilon_L$ where $\varepsilon_L \sim N(0, \sigma_L^2)$ and τ_L is the pre-programmed expected time of launch termination. If $t < T_L$ then the launch is not finished. T_S is the time when the separation of the satellite takes place. In Figure 1 we can see that the satellite is separated if $t \geq T_S$ and not separated if $t < T_S$. We will assume that $T_S = \tau_L + \Delta_S + \varepsilon_S + \varepsilon_L$ where Δ_S is the time we wait after the rocket engine has stopped to the separation occurs. We use that ε_S has the distribution $\varepsilon_S \sim N(0, \sigma_S^2)$. Note, we required $T_L < T_S$ in **S** which gives $\varepsilon_S > -\Delta_S$. If $t \leq T_F$ the satellite is not failed. We use $T_F = \tau_L + \Delta_S + \Delta_F + \varepsilon_S + \varepsilon_L + \varepsilon_F$ where Δ_F is the expected time we wait after separation to the satellite fail if we do not deploy the antenna. For simplicity we will assume that $\varepsilon_F \sim N(0, \sigma_F^2)$ instead of using a survival distribution. It is attractive to work with a joint normal distribution numerically. On the other hand the results later shows that the joint normal distribution gives reasonable results. We have that $\varepsilon_F \geq -\Delta_F$ since we required $T_S \leq T_F$ in **S**.

We have chosen the normal distribution mainly for illustrative purposes. The normal distribution however can be justified for the launch time since it represents launch time as the expected time of launch plus the uncertainty in time that the launch represents. The major factors that influence the launch time uncertainty are rocket engine performance, weather conditions and the launch window. A study of these factors can be used to give a distribution of the launch time. Similarly we have used the Normal distribution to model the separation time. To obtain the separation time uncertainty one should consider the separation process physically and also look at real data from previous launches. For the failure time T_F we could have used a survival distribution. We tried to use the exponential distribution and found that it did not ensure a quick enough failure of a satellite with a non-deployed antenna to give a realistic example. Another distribution more likely to work is the Weibull distribution. It is important that the failure rate quickly increases since a separated satellite without deployed antenna quickly fails or looses its mission. Finding appropriate parameters for the Normal distribution that we have used will also ensure quick failure if the antenna is not deployed.

It is important that the failure time is correlated to the separation time and launch time. For example a scenario where the launch ends too early will cause a failure much earlier than a launch where the engines run significantly longer.

We will now obtain the joint distribution of (t_L, t_S, t_F) given $\varepsilon_S \geq -\Delta_S$ and $\varepsilon_F \geq -\Delta_F$. Since we can not explain any direct linkage between the errors we will assume that ε_S, ε_L and ε_F are mutually independent. However, note although ε_S, ε_L and ε_F are mutually independent, the times T_L, T_S and T_F are not independent. If the launch duration, $t < T_F$, lasts longer we would for example also expect the separation to occur later so the two properties are positively correlated. Similarly the separation time, T_S, should be positively correlated with failure time T_F.

To obtain the conditional joint distribution of (t_L, t_S, t_F) we shall first obtain the joint-distribution of

$$\mathbf{T} = \begin{bmatrix} T_L \\ T_S \\ T_F \\ \varepsilon_S \\ \varepsilon_F \end{bmatrix} = \begin{bmatrix} \tau_L + \varepsilon_L \\ \tau_L + \Delta_S + \Delta_F + \varepsilon_L + \varepsilon_S \\ \tau_L + \Delta_S + \Delta_F + \varepsilon_L + \varepsilon_S + \varepsilon_F \\ \varepsilon_S \\ \varepsilon_F \end{bmatrix}. \qquad (3)$$

Since each of the variables are normally distributed the expectation is

$$\mathrm{E}(\mathbf{T}) = \begin{bmatrix} \tau_L \\ \tau_L + \Delta_S + \Delta_F \\ \tau_L + \Delta_S + \Delta_F \\ 0 \\ 0 \end{bmatrix}. \qquad (4)$$

Using the mutually independence of ε_S, ε_L and ε_F gives the covariance matrix

$$\Sigma = \begin{bmatrix} \sigma_L^2 & & & & \\ \sigma_L^2 & \sigma_S^2 + \sigma_L^2 & & & \\ \sigma_L^2 & \sigma_S^2 + \sigma_L^2 & \sigma_S^2 + \sigma_L^2 + \sigma_F^2 & & \\ 0 & \sigma_S^2 & \sigma_S^2 & \sigma_S^2 & \\ 0 & 0 & \sigma_F^2 & 0 & \sigma_F^2 \end{bmatrix}. \qquad (5)$$

Conditional on $\varepsilon_S > -\Delta_S$ and $\varepsilon_F \geq -\Delta_F$ the joint distribution of (t_L, t_S, t_F) is

$$f(t_L, t_S, t_F \mid \varepsilon_S > -\Delta_S, \varepsilon_F \geq -\Delta_F) = \frac{\frac{1}{(2\pi)^{5/2}\sqrt{|\Sigma\;|}} \int_{-\Delta_F}^{\infty} \int_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\varepsilon_S d\varepsilon_F}{(1-\Phi(-\frac{\Delta_S}{\sigma_S}))(1-\Phi(-\frac{\Delta_F}{\sigma_F}))}, (6)$$

where **T** is given by (3) above. In our notation we use $\Phi(x) = p(X \leq x)$ for the standard normal distribution. Since we always are given $\varepsilon_S > -\Delta_S$ and $\varepsilon_F \geq -\Delta_F$, we will simply write $f(t_L, t_S, t_F)$ instead of $f(t_L, t_S, t_F \mid \varepsilon_S > -\Delta_S, \varepsilon_F \geq -\Delta_F)$.

3.1 Parameter Specification

We will now specify the parameters in the model. This is a field where for example expert judgement can be applied. We will however use some typical values for the Ariane 5 launcher fit the model. The expected launch time is

τ_L = 26.49 min

with a variance of parameter ε_L of

Var(ε_L) = $\sigma^2{}_L$ = (8 min)^2.

The expected time for separation to be finished is τ_S = 33.30 min. Therefore the expected time between launch finished and separation is

Δ_S = 33.30 min - 26.49 min = 6.81 min.

The variance of parameter ε_S must reflect that the separation of satellites 1 and 2 takes place at approximately 28.10 min and satellites 3 and 4 at approximately 33.30 min, which suggest that the variance at least is $(5.20 \text{ min})^2$. We will use

$$\mathrm{Var}(\varepsilon_S) = \sigma^2_S = (6 \text{ min})^2.$$

The expected time from separation to failure is

$$\Delta_F = 7.70 \text{ min}.$$

We have only used this number for illustrative purposes and we will use a larger variance

$$\mathrm{Var}(\varepsilon_F) = \sigma^2_F = (10 \text{ min})^2.$$

3.2 Optimal Deployment Time

We will now find the optimal deployment time and the expected value if no inspection is carried out. Using the values in Table 1 we obtain the expected utility:

$$\begin{aligned} v(f(t)) &= -500\cdot 10^6\, p(t < T_L) \\ &\quad -250\cdot 10^6\, p(T_L \le t < T_S) - 0\, p(T_S \le t < T_F) \quad (7) \\ &\quad -125\cdot 10^6\, p(T_F \le t). \end{aligned}$$

To obtain the relevant probabilities from our probability density in (6) is just to integrate over the respective regions by using the method in Genz (1992). The optimal act is obtained by taking the best of all possible acts. This gives

$$v(\mathrm{F}) = \max_{t>0} v(f(t)). \qquad (8)$$

REMARK: In the following we use time in minutes if nothing else is specified.

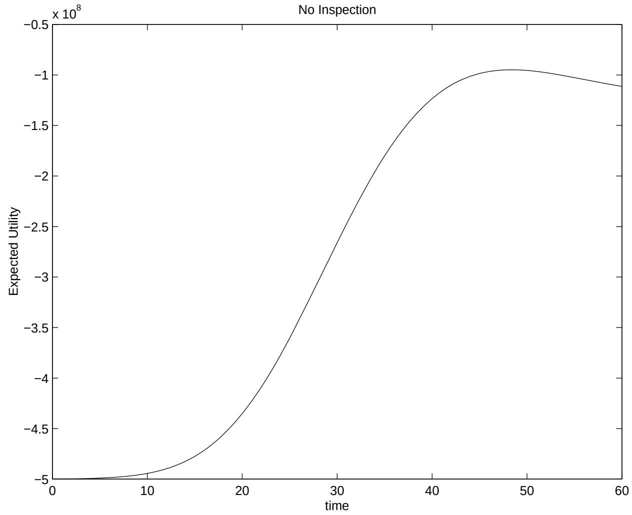

Figure 3. The expected value $v(f(t))$ as function of time t.

Figure 3 indicates that the optimal deployment time is 48 minutes with an expected utility of $-90\cdot 10^6$. Optimisation with 3 significant digits gives

$$v(\mathrm{F}) = v(f(t = 48.3)) = -94.8\cdot 10^6 \text{ \$}. \qquad (9)$$

4 THE OPTIMAL INSPECTION TIME

The number of broken break wires is described by the random variable $X(\tau) \in \{0, 1,..., 5\}$. At inspection time τ it is possible to monitor the number of wires that test broken. Conditional on the time we inspect, the break-wire test result will have different distributions. We will now define the probability distribution of the break-wire test given the four different inspection intervals (see Figure 1).

Given $\tau < t_L$ or $t_L \le \tau < t_S$ we assume that $X(\tau)$ has the binomial distribution

$$\begin{aligned} &p(x(\tau) \mid \tau < t_L \cup t_L \le \tau < t_S) \\ &\qquad = \binom{5}{x(\tau)} p(\tau)^{x(\tau)} (1 - p(\tau))^{5 - x(\tau)}. \end{aligned}$$

The binomial distribution models the break wire status before Separated it describes the break wires exposure to shocks during launch and separation. This model assumes that each wire breaks independently with probability $p(\tau)$. The probability $p(\tau)$ is a function of the accumulated stress over time and is believed to increase as a function of τ. For simplicity we will use $p(\tau) = 0.05$.

Given Separated the break-wire test can return the wrong number of broken wires due to either bit flip or transient failures in the electronic circuits. Assume that the probability of bit flip or transient errors is $\varepsilon = 0.001$ and use the distribution

$$p(x(\tau) \mid t_S \le \tau < t_F) = \begin{cases} \varepsilon \text{ for } x(\tau) \in \{0,1,\ldots,4\} \\ 1 - 5\varepsilon \text{ otherwise.} \end{cases}$$

Given failure we assume that the break-wires do not give relevant information so we use the uniform distribution

$$p(x(\tau) \mid t_F < \tau) = {}^1\!/_6, \text{ for } x(\tau) \in \{0,1 , ..., 5\}.$$

Multiply the conditional distributions above with the distribution $f(t_L, t_S, t_F)$ in (6) to obtain the joint distribution:

$$f(t_L, t_F, t_S, x(\tau)) = f(t_L, t_F, t_S) \cdot \begin{cases} \begin{pmatrix} 5 \\ x(\tau) \end{pmatrix} p^{x(\tau)} (1-p)^{5-x(\tau)} \text{ if } \tau < T_S \\ \left. \begin{cases} \varepsilon \text{ for } x(\tau) \in \{0,1,\ldots,4\} \\ 1-5\varepsilon \text{ otherwise} \end{cases} \right\} \text{ if } T_S \le \tau < T_F \\ \frac{1}{6} \text{ if } T_F \le \tau. \end{cases} \tag{10}$$

4.1 The Optimal Inspection Time

In general we have that $v(\mathrm{F}|X(\tau)) \geq v(\mathrm{F})$. Now we will obtain the conditional expectation when the break wires are observed at test time τ. Since the break-wires are observed at τ we have

$$v(f(t) \mid Breakwires) = \begin{cases} v(f(t) \mid X(t)) \text{ if } t \ge \tau \\ v(f(t)) \text{ otherwise.} \end{cases}$$

So for $t \geq \tau$ we need to compute the expected value

$$\begin{aligned} v(f(t) \mid x(\tau)) = &-500 \cdot 10^6 \, p(t < T_L \mid x(\tau)) \\ &-250 \cdot 10^6 \, p(T_L \le t < T_S \mid x(\tau)) \\ &-0 \, p(T_S \le t < T_F \mid x(\tau)) \\ &-125 \cdot 10^6 \, p(T_F \le t \mid x(\tau)). \end{aligned} \tag{11}$$

The conditional probabilities are obtained from the distribution in (10). This is however a rather complex process which is summarised in the Appendix. Optimisation over all accessible acts gives

$$v(\mathrm{F} \mid x(\tau)) = \max_{t>0} v(f(t) \mid x(\tau)).$$

For each test outcome this optimisation gives optimal deployment times. The conditional expectation is given by taking the expectation over the test-outcomes. This gives

$$v(\mathrm{F} \mid X(\tau)) = \sum_{x(\tau)} p(x(\tau)) \max_{t>0} v(f(t) \mid x(\tau)). \tag{12}$$

The numerically hardest problem is to find the optimal test time.

$$\tau = \operatorname*{argmax}_{\tau>0} v(\mathrm{F} \mid X(\tau)).$$

An overview is obtained by plotting the expected value over the interval shown in Figure 4. Figure 4 shows that the optimal inspection time is between 37 and 38 minutes. Optimisation with 3 significant digits gives

$$\max_{\tau>0} v(\mathrm{F} \mid X(\tau)) = v(\mathrm{F} \mid X(\tau = 37.5)) = -59.9 \cdot 10^6 \,\$.$$

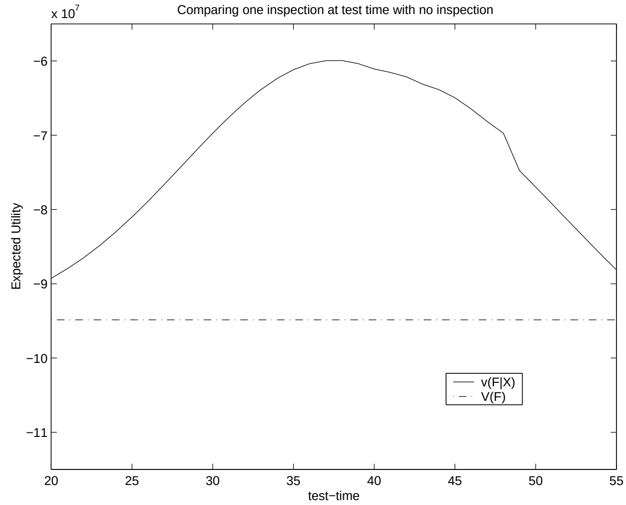

Figure 4. The conditional expected utility $v(\mathrm{F} \mid X(\tau))$ as function of test time τ.

4.2 The Optimal Control-Flow

We shall compute the optimal control flow architecture that describes how to code the control software. It describes how to implement the break wire inspection. Figure 4 shows that the optimal test-time is 37.5 minutes. For each inspection outcome $x(\tau) \in \{0, 1,..., 5\}$ we will now compute the optimal deployment time

$$t(x(\tau = 37.5)) = \operatorname*{argmax}_{t>0} v(f(t) \mid x(\tau = 37.5)).$$

From Figure 5 we can for example see that if we observe at test-time 37.5 minutes that $x(\tau = 37.5) = 0$ break wires are broken, we should deploy the antenna at 52 minutes.

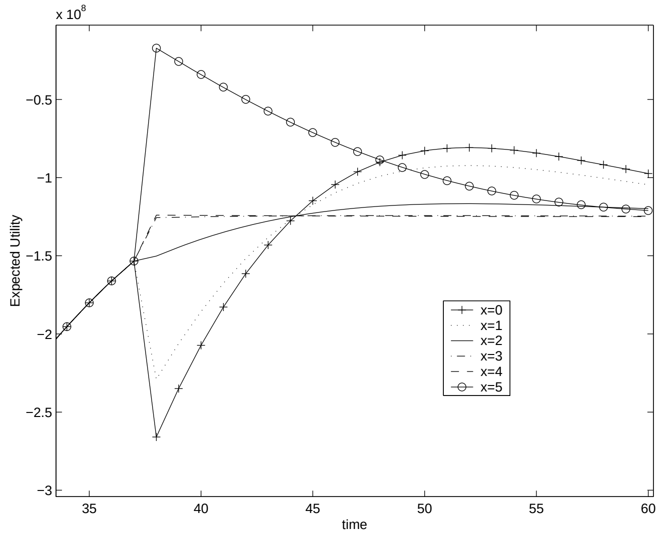

Figure 5. The conditional expected utility for the various test-outcomes.

Optimisation with 3 significant digits gives

$$t(x(\tau = 37.5) = 0) = 51.9 \qquad (13)$$

$$t(x(\tau = 37.5) = 1) = 51.9 \qquad (14)$$

$$t(x(\tau = 37.5) = 2) = 51.7 \qquad (15)$$

$$t(x(\tau = 37.5) = 3) = 48.7 \qquad (16)$$

$$t(x(\tau = 37.5) = 4) = 37.5 \qquad (17)$$

$$t(x(\tau = 37.5) = 5) = 37.5 \qquad (18)$$

In conclusion, if we have one inspection of the break wires the control software architecture should be designed so that we inspect at 37.5 minutes with the conditional deployment times given in (13) to (18). This gives the maximal value of information that can be obtained in (19) when the break wires are inspected once.

4.3 *Measuring Control Software Performance*

When we compare the expected value in Figure 4 with the optimal value in Figure 3 (see the graph labelled v(F) in Figure 4) we see that the inspection improves the expected value. The value of information is

$$v(\mathrm{F} \mid X(\tau = 37.5)) - v(\mathrm{F})$$

$$= 59.9\cdot 106 \ \$ - 94.8\cdot 106 \ \$ = 34.9\cdot 106 \ \$. \qquad (19)$$

This is a measure on how well control software inspects the break wire sensors and activates the antenna deployment.

5 CONCLUSION

In practical software engineering the use of voting logic is a popular way to take decisions under uncertainty. This paper successfully demonstrates an alternative way to design control software that decides under uncertainty. This approach utilises decision theory and has potential to formalise and improve the control software design process by optimising the control software architecture. If the control software is coded according to the optimised architecture described in Section 4.2 we can say that Bayes' Theorem is built into the software. Further, the performance of the control software architecture is measured by the value of information as shown in Section 4.3.

REFERENCES

Norstrøm, J.G. Cooke R.M. & Bedford T. 1998. Statistical methods in design of safety critical software. In Lydersen, Hansen & Sandtorv (eds), *Safety and Reliability:* 1061-1068. Rotterdam: Balkema.

Norstrøm, J.G. Cooke R.M. & Bedford T. 1999. Value of Information based inspection strategy of a fault-tree. In Kafka & Schüeller (eds), *Safety and Reliability*: 621-626. Rotterdam: Balkema.

Dore, B. & Norstrøm J.G. 1996. Pilot Application of Sneak Analysis on Computer Controlled Satellite Equipment. In P.C Cacciabue & I. A. Papazoglou (eds), *Probabilistic Safety Assesment and Management*: 1590-1596. Springer.

Genz, A. 1992. Numerical Computation of Multivariate Normal Probabilities, J. of Computational and Graphical Stat.: 1, pp. 141-149.

ESA Public Relations Division Offices: "Ariane 5 Architecture", http://www.esrin.esa.it/esa/ariane/archi.html

Ada Decision Systems 1992. DPL Advanced Version User Guide. *2710 Sand Hill Road, Menlo Park, CA94025, USA.*

De Groot, M. H. 1970. *Optimal Statistical Decisions.* New York: McGraw-Hill.

Savage L. 1972. *The Foundations of Statistics.* New York: Dover.

APPENDIX – THE PROBABILITIES

We will obtain the probabilities in (7) and (11). The difficult task is to get the integration areas correct. This is shown below.

Consider the probabilities for times greater than the inspection time, $t \geq \tau$ so the joint distribution in (10) is used. We will use

$$d\mathbf{T}' = dt_F dt_S dt_L \text{ and } d\mathbf{T} = d\varepsilon_S d\varepsilon_F dt_F dt_S dt_L .$$

The conditional probability $p(t < T_L \mid x(\tau))$ is

$$p(t < T_L \mid x(\tau)) \propto \int_{t_L = t}^{\infty} \int_{t_S = -\infty}^{\infty} \int_{t_F = -\infty}^{\infty} f(t_L, t_S, t_F, x(\tau)) d\mathbf{T}'$$

$$\propto \binom{5}{x(\tau)} p^{x(\tau)} (1-p)^{5-x(\tau)} \int_{t_L = t}^{\infty} \int_{t_S = -\infty}^{\infty} \int_{t_F = -\infty}^{\infty} f(t_L, t_S, t_F) d\mathbf{T}' .$$

Define
$A = (2\pi)^{5/2}\sqrt{|\Sigma\ \,|}(1-\Phi(-\tfrac{\Delta_S}{\sigma_S}))(1-\Phi(-\tfrac{\Delta_F}{\sigma_F}))$
and substitute $f(t_L, t_S, t_F)$ with (6) to obtain

$$p(t < T_L \mid x(\tau)) \propto \binom{5}{x(\tau)} p^{x(\tau)}(1-p)^{5-x(\tau)}$$

$$\cdot\frac{1}{A}\int\limits_{t_L=t}^{\infty}\int\limits_{t_S=-\infty}^{\infty}\int\limits_{t_F=-\infty}^{\infty}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}\,.$$

We recognise the multivariate normal distribution. The integration is solved numerically by using Genz's (1992) method. Similarly $p(T_L \le t < T_S \mid x(\tau))$ is:

$$p(T_L \le t < T_S \mid x(\tau)) \propto \int\limits_{t_L=-\infty}^{t}\int\limits_{t_S=t}^{\infty}\int\limits_{t_F=-\infty}^{\infty} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}'$$

$$\propto \binom{5}{x(\tau)} p^{x(\tau)}(1-p)^{5-x(\tau)}$$

$$\cdot\frac{1}{A}\int\limits_{t_L=-\infty}^{t}\int\limits_{t_S=t}^{\infty}\int\limits_{t_F=-\infty}^{\infty}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}\,.$$

To obtain $p(T_S \le t < T_F \mid x(\tau))$ requires more refinement. Since the distribution in (10) is differently specified for different intervals we obtain:

$$p(T_S \le t < T_F \mid x(\tau))$$
$$\propto \left[\begin{array}{l} \int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=\tau}^{t}\int\limits_{t_F=t}^{\infty} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}' \\ \quad + \int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\tau}\int\limits_{t_F=t}^{\infty} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}' \end{array}\right].$$

Use (10), (6) and substitute for $f(t_L, t_S, t_F, x(\tau))$ to get

$$p(T_S \le t < T_F \mid x(\tau)) \propto \binom{5}{x(\tau)} p^{x(\tau)}(1-p)^{5-x(\tau)}$$

$$\cdot\frac{1}{A}\int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=\tau}^{t}\int\limits_{t_F=t}^{\infty}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}$$

$$+\frac{1}{A}\int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\tau}\int\limits_{t_F=t}^{\infty}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}$$

$$\cdot\begin{cases} \varepsilon \text{ for } x(\tau) \in \{0,1,\ldots,4\} \\ 1-5\varepsilon \text{ otherwise.} \end{cases}$$

Similarly the last probability $p(T_F \le t \mid x(\tau))$ is

$$p(T_F \le t \mid x(\tau))$$
$$\propto \left[\begin{array}{l} \int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=\tau}^{\infty}\int\limits_{t_F=\tau}^{t} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}' \\ + \int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\tau}\int\limits_{t_F=\tau}^{t} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}' \\ + \int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\infty}\int\limits_{t_F=-\infty}^{\tau} f(t_L, t_S, t_F, x(\tau))d\mathbf{T}' \end{array}\right].$$

Again use (10), (6) and substitute for $f(t_L, t_S, t_F, x(\tau))$ to get

$$p(T_F \le t \mid x(\tau)) \propto \binom{5}{x(\tau)} p^{x(\tau)}(1-p)^{5-x(\tau)}$$

$$\cdot\frac{1}{A}\int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=\tau}^{\infty}\int\limits_{t_F=\tau}^{t}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}$$

$$+\frac{1}{A}\int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\tau}\int\limits_{t_F=\tau}^{t}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}$$

$$\cdot\begin{cases} \varepsilon \text{ for } x(\tau) \in \{0,1,\ldots,4\} \\ 1-5\varepsilon \text{ otherwise} \end{cases}$$

$$+{}^{1}/_{6}\cdot\frac{1}{A}\int\limits_{t_L=-\infty}^{\infty}\int\limits_{t_S=-\infty}^{\infty}\int\limits_{t_F=-\infty}^{\tau}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}\,.$$

Having worked out the probabilities for $t \ge \tau$ above we will now consider $t < \tau$. Since we consider $t < \tau$ it is sufficient to obtain the probabilities in (11) by only considering the distribution in (6). We will obtain $p(t < T_L)$.

$$p(t < T_L) = \frac{1}{A}\int\limits_{t_L=t}^{\infty}\int\limits_{t_S=-\infty}^{\infty}\int\limits_{t_F=-\infty}^{\infty}\int\limits_{-\Delta_F}^{\infty}\int\limits_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}}\Sigma^{-1}(\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}\,.$$

The second probability is

$p(T_L \le t < T_S)$

$$= \frac{1}{A} \int_{t_L=-\infty}^{t} \int_{t_S=t}^{\infty} \int_{t_F=-\infty}^{\infty} \int_{-\Delta_F}^{\infty} \int_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}} \Sigma^{-1} (\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}.$$

The third probability is

$p(T_S \le t < T_F)$

$$= \frac{1}{A} \int_{t_L=-\infty}^{\infty} \int_{t_S=-\infty}^{t} \int_{t_F=t}^{\infty} \int_{-\Delta_F}^{\infty} \int_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}} \Sigma^{-1} (\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}.$$

The last probability is

$p(T_F \le t)$

$$= \frac{1}{A} \int_{t_L=-\infty}^{\infty} \int_{t_S=-\infty}^{\infty} \int_{t_F=-\infty}^{t} \int_{-\Delta_F}^{\infty} \int_{-\Delta_S}^{\infty} \mathrm{e}^{-(\mathbf{T}-\mathrm{E}\mathbf{T})^{\mathrm{T}} \Sigma^{-1} (\mathbf{T}-\mathrm{E}\mathbf{T})/2} d\mathbf{T}.$$

Note that these probabilities are the same as the ones we need to solve (7).

APPENDIX - FIGURES

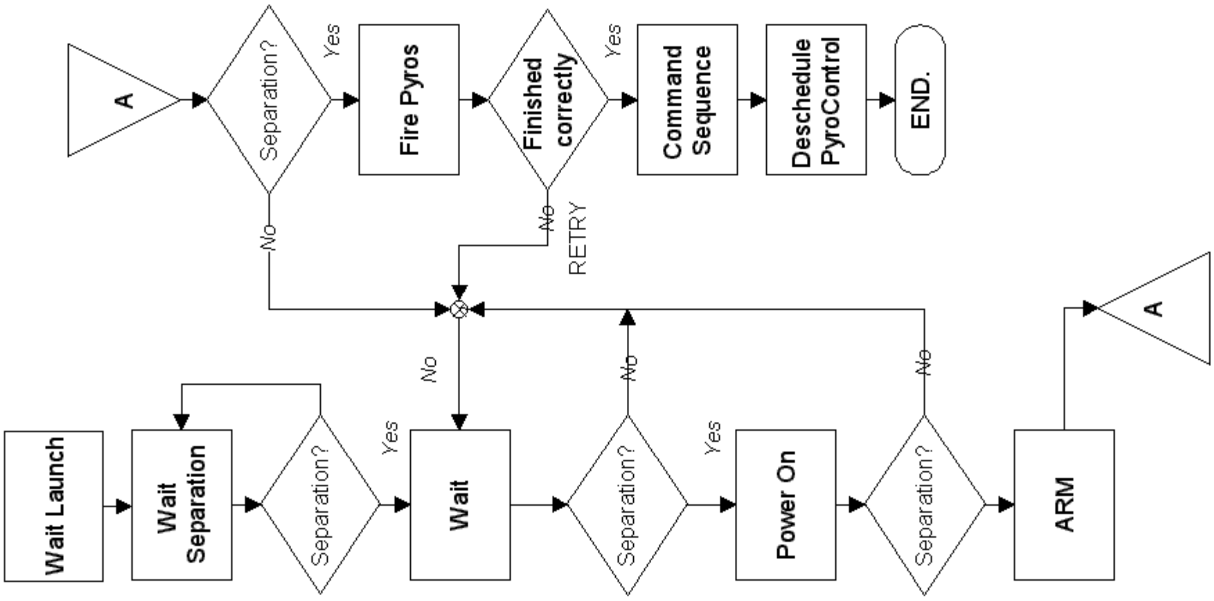

Figure 6. The required control flow of the separation sequence program (see Dore & Norstrøm (1996)).