Industrial Cost-Benefit Assessment for Fault-tolerant Control Systems

Thybo, C.; Blanke, M.

Publication date:
1998

Document Version
Også kaldet Forlagets PDF

Link to publication from Aalborg University

Citation for published version (APA):
Thybo, C., & Blanke, M. (1998). *Industrial Cost-Benefit Assessment for Fault-tolerant Control Systems*.

INDUSTRIAL COST-BENEFIT ASSESSMENT FOR FAULT TOLERANT CONTROL SYSTEMS

Claus Thybo[1], Mogens Blanke[2]

[1]Danfoss Drives A/S, Graasten, Denmark; [1,2]Department of Control Engineering Aalborg University, Denmark

ABSTRACT

Economic aspects are decisive for industrial acceptance of research concepts including the promising ideas in fault tolerant control. Fault tolerance is the ability of a system to detect, isolate and accommodate a fault, such that simple faults in a sub-system do not develop into failures at a system level. In a design phase for an industrial system, possibilities span from fail safe design where any single point failure is accommodated by hardware, over fault-tolerant design where selected faults are handled without extra hardware, to fault-ignorant design where no extra precaution is taken against failure. The paper describes the assessments needed to find the right path for new industrial designs. The economic decisions in the design phase are discussed: cost of different failures, profits associated with available benefits, investments needed for development and lifetime support. The objective of this paper is to help, in the early product development state, to find the economical most suitable scheme. A salient result is that with increased customer awareness of total cost of ownership, new products can benefit significantly from applying fault tolerant control principles.

Keywords:Fault-tolerant Control, System Development, Economy Assessment, Management of System Development

INTRODUCTION

Fault detection and isolation (FDI) based on analytical redundancy has matured over the last decade. A large number of papers have been presented, but industrial usage of the methods are still very sparse. One very promising application of FDI techniques is as part of fault-tolerant control (FTC) schemes where faults are accommodated by the control system when detected. This approach has the potential benefit of increasing plant availability and adding to total system safety. The prime reason for applying analytical redundancy instead of hardware redundancy with associated voting logics is economical based. It is cheaper to add supervisor software than to add hardware, and this is technically feasible in the majority of applications that do not require absolute fail-safe designs. Offering benefits in terms of increased availability and reduced cost over lifetime, it is striking that fault-tolerant methods have not yet penetrated into industry. One reason is natural caution and conservatism against new ideas from the scientific community, another is lack of convincing economic arguments for the technology. This paper deals with the economic aspect of the implementation of fault-tolerant control as part of new industrial development.

Several papers have been written giving an overview of available technology in fault-tolerant control. A recent overview appeared in [9], where a fault detection and isolation (FDI) communicate with a supervisor that takes care of the logics associated with re-configuration and other fault handling. A spacecraft example using this structure was presented in [6]. Earlier results include analysis of how reliability is obtained, [11]. Issues of intelligent control, including controller start-up and tuning, are dealt with in [1], and an overview of robust fault-tolerant control was given in [10]. Aiming at design optimization in industrial systems, economic relations in product development are covered in a large number of publications. Severity of faults in control applications are discussed in [2], where a list of severity levels are produced, ranging from 'No effect' to 'Hazard without notice'. In addition to the final severity level, the rapidness of fault effect appearance is also covered. This leads to useful requirements about time to reconfigure. A method for logical fault propagation analysis leading to the severity of end effects was proposed in [3] as part of a design method for fault-tolerant control. With the evolution of FTC methods, the attention of industry is increasing, but penetration into industrial applications require the methods to be compatible with the product development procedures applied by industry. The present effort has been to introduce cost/benefit analysis in FTC methods based on existing terms and relations in industrial product development.

The paper discusses the optimization of the cost/benefit ratio for systems employing FTC technology. It estimates the quantities necessary for evaluation of development and lifetime economy for a new piece of automation equipment. Particular emphasis is given to analysis of which fault modes are profitably accommodated using FTC methods. In some cases it is shown profitable to only include the fault mode in certain operational states of the product because more advanced FTC methods must be applied to cover all operational states. The assessment method is illustrated by two examples, one from mass-produced inverters for electrical induction motors, the other from a dedicated, small scale production of actuators for diesel engines. Both examples are realistic but not directly associated with current industrial production.

THE COST OF FAILURE

The cost of failures of products in daily operation at the market cause loss of profit for both manufacturers and users. Occasionally, manufacturers are forced to dramatic and economic painful retreat from a marked due to effects of product failure. Calculating the economic relations for a product at the pre-development state, it is thus very important to obtain a realistic estimate of the cost associated with different failure scenarios. Failure mode cost are considered as the total price of the fault effects witch are related to this fault mode in the products specified lifetime.

The cost can be split into a direct and indirect part, where the direct part holds cost for replacement and repair of damaged equipment, and the indirect part covers other losses, such as loss of: production, human comfort and goodwill. The precise estimate for the direct cost can be calculated, when the application is known, as repair and replacements in the application. For some general products such as PID controllers, the application is not known at design state. In these cases the repair of the application can not directly be calculated, but must rely on estimates based on typical application in the marked segment. The cost estimate for one failure mode for one product instance, C_f, can be calculated as

$$C_f = (C_{direct} + C_{indirect}) * P_f, \qquad (1)$$

where C_{direct} is the repair cost and $C_{indirect}$ is the other cost related to the failure. P_f denotes the probability of the failure occurring in a nominal lifetime of the product. Calculation of estimates of the indirect costs can be difficult because of the required application knowledge. Another problem is to assign cost to human discomfort. To evaluate the failure probability, two methods are commonly used: a component based analysis, where failure probability of individual components are used to calculate the failure mode probability, and an experienced based method, where past frequency of the failure mode in related products is used. In the sequel we will also need to express the cost of a fault

$$C_{fail} = C_{direct} + C_{indirect} \qquad (2)$$

COST WITH FTC APPLIED

Fault and failure related cost depend on how they can be accommodated. The purpose of FTC is to reduce C_f by using graceful degradation. The direct cost can be reduced by stopping the fault from developing into a system failure with more damaged equipment, but especially the indirect cost are reduced when operation breakdowns are avoided. The cost of an accommodated fault is denoted C_{acc}. The cost of a false detection is denoted $C_{false\,d}$. A FTC scheme produces a given probability of detecting a fault, P_d, and a given probability of false detections ,$P_{f\,d}$. The costs of faults vary whether they are detected or not. In the following C_{df} denotes the cost of detected, and therefore accommodated faults, and C_{udf} denotes the cost of undetected faults. The costs of undetected faults is assumed equal to the costs of fault not using FTC, whereas the costs of detected faults are assumed lower than the undetected counterpart, because of the fault accommodation. Otherwise FTC makes no sense. The cost related to a given fault mode over a nominal lifetime can be derived from the cost effect of a fault occurring multiplied with the possibility of the fault mode occurring.

$$\begin{aligned} C_{df} &= P_f * P_d * C_{acc} \\ C_{udf} &= P_f * (1 - P_d) * C_{fail} \\ C_{fd} &= P_{fd} * C_{false\,d} \end{aligned} \qquad (3)$$

Following average cost-estimates must then be produced;
C_{udf} : cost of un-accommodated faults.
C_{df} : cost of accommodated faults.
C_{fd} : cost of false detections.
The cost when FTC is not applied can be expressed as

$$C_{udf} = C_f = P_f * C_{fail}, \qquad (4)$$

hence, the optimal cost reduction for a given fault mode, when applying FTC based on one fault mode is

$$C_{ftc\,r} = C_f - C_{df} - C_{udf} - C_{fd}. \qquad (5)$$

INVESTMENTS TO IMPLEMENT FTC

When applying FTC there are some additional investments to pay. The FTC algorithm has to be developed, and it will, depended on the complexity of the methods, require more computer power. By dividing, the investment into product type investment independent of amount of products manufactured, and investment related to the individual product, an investment per product can be calculated. For each fault mode found in the FMEA analysis [2] a separate fault detection and isolation method is proposed. The product type and product investment can be calculated as

$$I_f = \frac{I_{dev}}{N_{prod}} + I_{hw} \qquad (6)$$

where I_f is the FTC investment calculated for one fault mode. I_{dev} represents the development investment and I_{hw} is the investment in additional hardware. N_{prod} is the number of products produced. The optimal selection of fault modes to include is be found by including the fault mode if the cost reduction exceeds the investment. This assumes no reuse can be used when investing in including more fault modes.

OPERATIONAL MODE DEPENDEND FTC

For some fault modes one simple FTC scheme can only detect faults in certain operational modes, whereas, other more complex schemes can detect in all operational modes. An example of operational modes where simple detection schemes often are applicable is stand-by operation, whereas operation in the saturation region can require more complex schemes. Splitting the investment and cost up into operational modes,i , with one separate detection scheme for each fault mode gives:

$$I_{f_i} = \frac{I_{dev_i}}{N_{prod_i}} + I_{hw_i} \tag{7}$$

$$C_{ftc\,r_i} = C_{f_i} - C_{df_i} - C_{udf_i} - C_{fd_i} \tag{8}$$

With the FTC scheme split up into operational modes, the selection of what to include in the FTC can be done by selecting the operational modes where the cost reduction exceeds the investment. This gives an optimal selection when no reuse of the investments in one operational mode can be used in implementing another. If the investment in FTC, for the different operational modes, can be reused, an optimal selection might include more operational modes than suggested previously.

FREQUENCY CONVERTER CONTROLLED ROCKWOOL SOLIDIFIER

Rockwoll used for house insolation, are made by melting solid rock, solidify it into thin threads, which are woven into sheets. Solidification is done by pouring the liquid rock on a fast rotating cylinder. An arm takes the warm threads and weaves them into sheets.. A production line consist typically of more identical solidifier modules. To produce a uniform quality it is important to control the speed of the process accurate. To do this, the frequency converter driving the induction motors are provided with a position encoder feedback, as shown in figure 1.

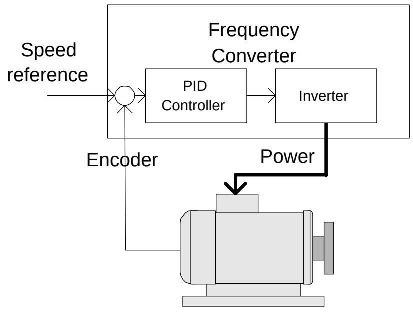

Figure 1: Inverter fed induction motor with encoder position feedback.

This example analyses disconnections in the encoder feedback. Disconnection can be caused by a cut wire, loose electrical connection or false wirering. The direct effect of the disconnection is that the motor is assumed to be at a standstill, and the PID controller propagates the effect so max speed is obtained within a few seconds. Production equipment worth approx. 5,000$ are crushed and the entire production line is down 1-2 days. In table 1 are the estimated cost for an unaccommodated fault given.

Item	Cost	Total US$
Service engineer	120 $/h	4800.-
Spare parts		5,000.-
Production losses		10,000.-
Total		**19,800.-**

Table 1: Cost of production line breakedown due to an unaccomodated encoder fault

If the fault can be detected two approaches can be selected, a controlled shutdown, or continued operation in open loop with slightly reduced quality. A controlled shutdown and repair can, when the fault is known, be completed in 3 hours. In table 2 are the estimated cost for an accommodated fault given.

Item	Cost	Total US$
Service engineer	120 $/h	240.-
Spare parts		10.-
Production losses		1000.-
Total		**1,250.-**

Table 2: Cost of controlled shut-down due to an accomodated encoder fault

Under normal operation is the speed in the range 30-90 Hz, a speed where simple slew-rate detection has proven successful. But by initiating the process, and under special operation, are the speed below the slew-rate detection range. Industrial experience says the probability of a disconnection fault is increased in a period after setup or repair, compared with continuous operation. This is explained by missing or loose connections made by the repairman. Probabilities for the fault occurring a lifetime of 15 years are estimated to; start-up:$P_{f_{startup}}$=0.03, at normal operation with high speed:$P_{f_{highspd.}}$ =0.001, and at normal operation with low speed:$P_{f_{lowspd.}}$ =0.00001. Detection of encoder faults under start-up can be done, by introducing a self-test sequence, where the speed is restricted to a range, where no damage to other equipment happens. After the sequence has been successful completed, normal operation can be initiated. The procedure is estimated to detect all encoder faults present under the self-test, $P_{d_{selftest}}$=1. The probability of false detection,$P_{fd_{highspeed}}$, is estimated zero.

In the start up mode an investment of 1.08$ can reduce the fault cost with 556.5$.

Detection of faults, when operating on high speed, can be accomplished by observing the encoder signal, and compare it with the reference. Operating on high speed, faults can be detected within a few samples, but operating on low speed faults could be un-

Item	Investment	Total US$
Analysis	2 w	7,200.-
Develop FDI	2 w	7,200.-
Implement in SW	1 w	3,600.-
Add testing	1 w	3,600.-
Documentation	2 w	7,200.-
SW over lifetime	1 m	14,400.-
Staff training	3 w	10,800.-
Total- 1000 pcs		**54,000.-**
Add hardware	0	0.-

Table 3: Additional development investment to implement FTC in the startup state

Cost and Investment	Total US$
$\bar{C}_f = P_f * C_{fail}$	594.-
$\bar{C}_{df} = P_f * P_d * C_{acc}$	37.5-
$\bar{C}_{udf} = P_f * (1 - P_d) * C_{fail}$	0.-
$\bar{C}_{fd} = P_{fd} * C_{fd}$ $\bar{C}_{ftc} = \bar{C}_f - \bar{C}_{df} - \bar{C}_{ndf} - \bar{C}_{fd}$	0.- 556.5-
$I_f = \frac{I_{dev}}{N_{prod}} + I_{hw}$	1.08-

Table 4: Cost and investment for applying FTC in the startup state

detected until the PID controller has integrated the speed into an unacceptable level. This approach will in the following be called 'simple detection scheme'. The probability of detection, when operation at high speed, is estimated to: $P_{d_{highspeed}}$=0.98. The probability of false detection,$P_{fd_{highspeed}}$, is estimated zero. The development investment is estimated to the figures given in table 5.

Item	Investment	Total US$
Analysis	1 w	3,600.-
Develop FDI	2 w	7,200.-
Implement in SW	1 w	3,600.-
Add testing	1 w	3,600.-
Documentation	1 w	3,600.-
SW over lifetime	1 m	14,400.-
Staff training	1 w	3,600.-
Total- 1000 pcs		**39,600.-**
Add hardware	0.3	0.-

Table 5: Additional development investment to implement FTC for high speed operation

Cost and Investment	Total US$
$\bar{C}_f = P_f * C_{fail}$	19.8-
$\bar{C}_{df} = P_f * P_d * C_{acc}$	1.23-
$\bar{C}_{udf} = P_f * (1 - P_d) * C_{fail}$	0.40-
$\bar{C}_{fd} = P_{fd} * C_{fd}$ $\bar{C}_{ftc} = \bar{C}_f - \bar{C}_{df} - \bar{C}_{ndf} - \bar{C}_{fd}$	0.- 18.17-
$I_f = \frac{I_{dev}}{N_{prod}} + I_{hw}$	1.09-

Table 6: Cost and investment for applying FTC in the high speed state

For the high speed mode an investment of 1.09$ can reduce the fault cost with 18.17$.
Detecting faults operating at low speed can be accomplished by a speed observer based on the electrical equations of the induction motor. Several papers has been published on open loop speed observers for induction motor drives [8] [7]. One industrial problem with the proposed speed observers is that their stability is dependent on the accuracy of the motor parameters. Hence more analysis is required before implementation in an industrial environment.. This approach will in the following be called 'advanced detection scheme'. The probability of detection is estimated to: $P_{d_{allspeed}}$=0.9, with a probability of false detections of: $P_{fd_{allspeed}}$=0.01. The development investment is estimated to the figures given in table 7.

Item	Investment	Total US$
Analysis	4 m	57,600.-
Develop FDI	3 m	34,200.-
Implement in SW	1 m	14,400.-
Add testing	2 m	28,800.-
Documentation	2 m	28,800.-
SW over lifetime	5 m	72,000.-
Staff training	3 m	34,200.-
Total- 5000 pcs		**270,000.-**
Add hardware	8	40,000.-

Table 7: Additional development investment to implement FTC for low and high speed operation

Cost and Investment	Total US$
$\bar{C}_f = P_f * C_{fail}$	21.78-
$\bar{C}_{df} = P_f * P_d * C_{acc}$	1.24-
$\bar{C}_{udf} = P_f * (1 - P_d) * C_{fail}$	2.18-
$\bar{C}_{fd} = P_{fd} * C_{fd}$ $\bar{C}_{ftc} = \bar{C}_f - \bar{C}_{df} - \bar{C}_{ndf} - \bar{C}_{fd}$	12.5- 5.86-
$I_f = \frac{I_{dev}}{N_{prod}} + I_{hw}$	13.4-

Table 8: Cost and investment for applying FTC for the full speed range

In the start up mode an investment of 13.4$ can reduce the fault cost with 5.86$. With the given estimates is not profitable. The cost of false detection, $\bar{C}_{fd}$, is very high compared with the total cost of the fault mode without FTC, $\bar{C}_f$. To be profitable with the relative high investment, the FTC scheme must lower the rate of false detections dramatically.

ACTUATOR FOR MARINE DIESEL ENGINE

The second example is a governor for marine diesel engines, where the actuator was used as an international benchmark for fault detection and isolation [4]. The marine speed governor that uses this actuator was described in [5]. The diesel actuator is a device situated at the engine driving the throttle of the engine according to command from a speed control loop. There is only one automatic device to

Item	**Cost**	**Total US$**
24 h manning	1000 $/d	5,000.-
Service engineer	120 $/h	960.-
Travel+waiting	60 $/h	1,440.-
Air fare etc		4,000.-
Spare parts		1,000.-
Total		**12,400.-**

Table 9: Cost of serious actuator fault at open sea, 5 days from port

maintain unattended operation. If a failure develops in the actuator, the result can be

- freezing of the throttle position by engagement of an electronic brake on the actuator shaft
- an over-speed of the diesel engine and an immediate shut-down by an independent safety system on the engine

Either of the two reactions limit the maneuverability of the ship since the propeller driven by the engine is needed to accelerate or stop the ship. Without propeller power, the directional maneuverability is also drastically reduced because of lack of water flow over the ships rudder and associated drop in lift forces.

The remedial action is to send a crew member down at the engine and make manual throttle control. This control task requires uninterrupted 24 hour manning of the emergency stand at the engine.

The faults considered in the benchmark could have different severity, depending on external circumstance. If a serious fault appear during manoeuvering close to a quay or to other ships, a major damage could result. It the same fault appeared amid an ocean, the cost is that of 24 hour manning of the emergency stand until the next harbor approach where the failing component can be replaced.

A cost estimate for this undramatic event is listed in Table 9. The total is US$ 11,100.-. If an accident had happened, the cost of damage repair and time where the ship is not in operation can easily sum up to a cost of 500,000.- to 1,000,000.- US$. The likelihood of such event is, however, estimated to only about 0.01 times the likelihood of the fault itself.

A development effort to implement an FTC concept where the fault detection methods from the benchmark were applied, would result in having the actuator continue running when the fault occurs but with reduced performance. The development effort is estimated to the figures given in table 10.

The FTC cost/benefit figures are, with cost in US$, and a product lifetime of 20 years

Item	**Cost**	**Total US$**
Analysis	2 w	7,200.-
Develop FDI	1 m	14,400.-
Implement in SW	2 w	7,200.-
Add testing	2 w	7,200.-
Documentation	2 w	7,200.-
SW over lifetime	2 m	28,800.-
Staff training	2 w	7,200.-
Total - 1000 pcs		**79,200.-**
Add hardware	50	59,000.-

Table 10: Additional development costs to implement FTC for selected faults on the actuator

	At sea	In harbor
P_f	0.10	0.001
P_d	0.98	0.98
$P_{f\,d}$	0.05	0.05
C_{fail}	12,400$	1,000,000$
C_{df}	1,000$	1,000$
C_{fd}	50$	50$
I_{dev}	79,200$	79,200$
N_{prod}	1,000 pcs	1,000 pcs
I_{hw}	50 $	50$

The average figures are

Average cost	**At sea**	**In harbor**
$\bar{C}_f = P_f * C_{fail}$	1000	1000
$\bar{C}_{df} = P_f * P_d * C_{df}$	49	49
$\bar{C}_{ndf} = P_f * (1 - P_d) * C_{fail}$	10	10
$\bar{C}_{fd} = P_{fd} * C_{fd}$ $\bar{C}_{ftc} = \bar{C}_f - \bar{C}_{df} - \bar{C}_{ndf} - \bar{C}_{fd}$	2.5 938	2,5 938
$I_f = \frac{I_{dev}}{N_{prod}} + I_{hw}$	129	129

The result is a net saving over product lifetime of 809 US$. This analysis is for one type of failure. Adding others of the possible failure modes, lifetime maintenance costs could obviously be significantly reduced.

DISCUSSION

Cost-benefit analysis of new product features is always difficult. The uncertainty in the estimates given are believed to be fairly large, and the confidence of our estimate of failure likelihood over lifetime, is a key to the confidence of the entire cost-benefit analysis. Historical data are useful when considering the risk factors like physical damage of cables leading to failure. With new components being applied in a development, however, standard estimation methods from reliability analysis need to be employed or physical life-time stress-tests must be made. The features gained by making such assessment is a clear potential for reduced cost over lifetime for a product, and significantly increased customer satisfaction. The latter should be considered as part of the important product image that normally enables a price differentiation and a competitive edge in professional markets.

References

[1] K. J. Åström. Intelligent control. In *Proc. First European Control Conf. ECC'91*, pages 2328–2339, Grenoble, France, July 2-5 1991. Plenary paper.

[2] George Baumgartner. Potiential failure mode and effect analysis, reference manual. Technical Report SAE J-1739, Chrysler Corporation, Ford Motor Company, General Motors Corporation, 1995.

[3] M. Blanke. Consistent design of dependable control systems. *Control Engineering Practice, Vol. 4, No. 9.*, pages 1305–1312., 1996.

[4] M. Blanke, S. A. Bøgh, R. B. Jørgensen, and R. J. Patton. Fault detection for a diesel engine actuator - a benchmark for fdi. *Control Engineering Practice*, pages 1731–1740, Dec. 1995.

[5] M. Blanke and P.B. Nielsen. The marine engine governor. In *Proc. 2nd Int. Conf. On Maritime Communications and Control. London, Soc. Of Marine Engineers*, pages 11–20, London, UK, 21-23 Nov. 1990.

[6] R. Izadi-Zamanabadi Bøgh, S.A. and M. Blanke. Onboard supervisor for the ørsted satellite attitude control system. In *5th ESA Workshop on AI and Knowledge Based Systems for Space*, pages 137–152., Noordwijk, NL, Oct. 1995. European Space Agancy.

[7] R. Blasco et. al. Speed measurement of inverter fed induction motors using the fft and the rotor slot harmonics. *5'th Int. conf. on Power Electronics and Variable Speed Drives*, 1994.

[8] O. Fenker and W. Schumacher. Control of an induction motor without shaft encode using the vecon-chip. *European Power Electronics*, 1997.

[9] M.Blanke, R. Izadi-Zamanabadi, S. A. Bgh, and C. P. Lunau. Fault-tolerant control systems - a holistic view. *Control Engineering Practice*, 5(5):693 – 702, May 1997.

[10] R.J. Patton. Robustness in model based fault-diagnosis; the 1995 situation. In *IFAC Workshop: On-line fault detection and supervision in the chemical process industriess, Newcastle upon Tyne, UK*, pages pp 55–75, June 1995.

[11] R. J. Veillette, J. V. Medanic, and W .R. Perkins. Design of reliable control systems. *IEEE Trans. Automatic Control, Vol 37. No. 3*, pages 290–304., 1992.