"Procedure for Evaluation of Control System Reliability"

A specific application in the oil-refining industry
performed during the preliminary engineering phase

Objectives:

- To provide analytical information to support decisions related to attaining desired levels of system reliability;
- Calculation of reliability parameters;
- Evaluation of system reliability in comparison to the functional specification requirements;
- Improvement of system reliability through the identification of the least reliable system elements.

For reliability evaluation, main control system functions are taken from the functional specification. These functions are used to fully define the detailed system tasks.

The following is an example of how the simulation and calculation of system reliability was applied to the control system for Kirishi Oil Refinery Shop #3 Pumping Station 910-45. Calculations were performed independently for each of 18 main functions and for the control system in total.

Example of calculations for several functions:

F-7 – pressure control;
F-8 – flow control.

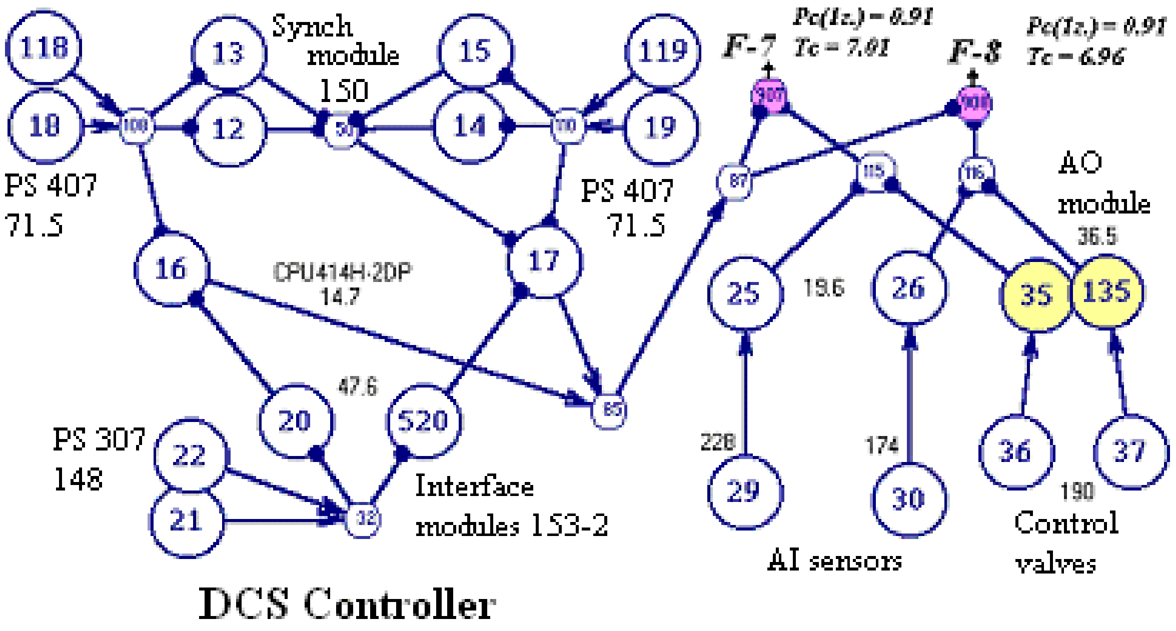

Fig-1 FIS

This functional integrity scheme (FIS) includes:

1. DCS controller.

To provide a high level of reliability of the DCS controller, redundancy of the following components was implemented:

- central processors CPU414H-2DP (nodes 16, 17)
- communication processors CP 444-1 (nodes 10, 11)
- optical communications modules OSM (nodes 7, 77)

In case of failure of the main controller line 16-10-7, automated reserve line 17-11-77 is switched-on using synchronization modules (nodes 12-15).

In compliance with functional specification requirements, controller power supplies 8, 18, 19 and 21 are redundant with (9, 118, 119 and 22). Project simulation and evaluation showed that without redundancy DCS controller reliability calculations would be:

Without restoration:
Pnon-failure operation(1year)= 0.82;
Tbefore system failure = 5.13 years

With restoration:
System availability = 0.999989;
Tbefore system failure = 5.13 years; (1)
Prestored system(1year) = 0.82.

Redundancy resulted in considerable improvement of reliability calculations as follows:

Without restoration:
Pnon-failure operation(1year)= 0.97;
Tbefore system failure = 8.18 years

With restoration:
System availability = 0.99999999989;
Tbefore system failure = 2674465.51 years; (2)
Prestored system(1year) = 0.98.

2. Two AI modules (elements 25, 26) and two AI sensors (elements 29, 30);
3. Two control valves (36, 37) and one common AO module. It is represented in Fig-1 by two multiplied nodes (35, 135) separately for each of two internal functions.

As shown in Fig-1 above and Tables 1 & 2 below differences in reliability calculations for functions F-7 and F-8 are affected by only the AI sensor parameters.

Table-1 Reliability calculations for function F-7

Calculation versions	Function size Log/probability	Calculation results	Comment
A Without restoration	12 / 20	$P_{F-7}(1_{year}) = 0.91$ T_{oF-7}= 7.01 year	Redundant power supplies 22, 118, 119
B With restoration		$K\Gamma_{F-7} = 0.999995$ $T_{HoF-7} = 11.35$ г. $P_{BF-7}(1_{year}) = 0.92$	$T_{Bi} = 0.5$ hour

Table-2 Reliability calculations for function F-8

Calculation versions	Function size Log/probability	Calculation results	Comment
A Without restoration	12 / 20	$P_{F-8}(1_{year}) = 0.91$ T_{oF-8}= 6.96 year	Redundant power supplies 22, 118, 119
B With restoration		$K\Gamma_{F-8} = 0.9999949$ $T_{HoF-8} = 11.18$ year $P_{BF-8}(1_{year}) = 0.92$	$T_{Bi} = 0.5$ hour.

After completing the reliability calculations for each control system function, an analysis of control system fault-tolerance is performed. The elements and components, whose failure or damage would be most serious, are revealed. For this a complex structure model of the control system reliability is developed which represents a logical union of all above analyzed FISs determining the conditions for the main functions realization.

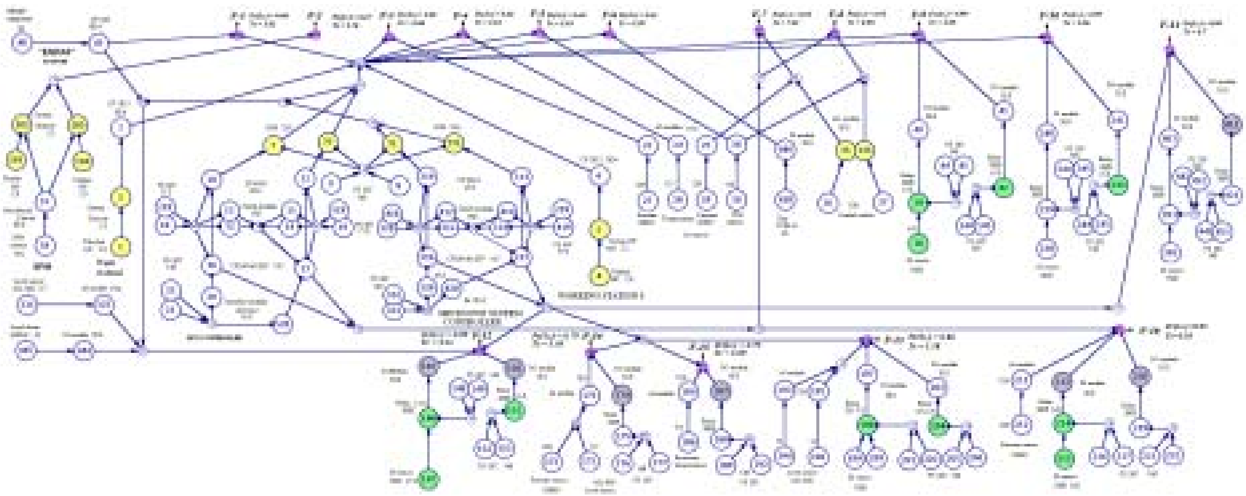

Fig-2 General FIS

Table-3 Consequences of single control system element failure

Number of the single control system elements failed	Function description which realization becomes impossible as a result of the element's failure	
47, 48	F-1	Representation of tank farm level, temperature & pressure information for the system ENRAF
56, 57	F-2	Representation of bearing status information for the system SPM
27, 23	F-3	Representation of the pump and pipeline output information
28, 24	F-4	Representation of pipeline temperature information
30, 26	F-5	Representation of pipeline water flow information
438, 440	F-6	Representation of gas content information
36, **35**, 29, 25	F-7	Pipeline pressure control
37, **35**, **30**, **26**	F-8	Oil product flow control
42, 41, 38*3, 39*3, 40	F-9	Gate valve remote control
238, 242, 239, 241, 240	F-10	Pump remote control
421, 411, 381, 391, 401	F-11	Automated ventilation switch-on
151*3, 150, 143	F-12	Shutdown system for the oil product tank farm level increase with redundancy of the ENRAF system
204, 203, 197	F-13	Shutdown system for the oil product tank farm level increase with sensor FSL-400 redundancy
175, 174, 173, 172,171	F-14	Pump emergency shutdown for input low level and output pressure
188, 187, 186, 184	F-15	Automated switch-off of oil product tank heaters
213, 219, 218, 215*2, 214*2, 212, 211	F-16	Automated switch-on of the backup pump

Analysis of Table-3:

a) Single failures of 60 out of 180 system components (33.3%) lead to the failure of only one main control system function;

b) Single failures of only 3 system components (1.67%) lead to the simultaneous failure of two main control system functions:

- Failure of the element 30 or 26 leads to the failure of functions F-5 and F-8;
- Failure of the element 35 leads to the failure of functions F-7 and F-8.

The following is an example of results for the control system reliability evaluation for Kirishi Oil Refinery Shop #3 Pump 910-45.

a) Incompliance with the functional specification, 100% redundancy of operator workstations and associated PLC communications via a ring network were utilized to provide the required level of control system functionality and reliability.

b) The control system is supplied with highly reliable components with a life expectancy greater than 10 years.

c) Elements such as controller power supplies and peripheral devices were evaluated one by one.

d) The full reliability calculation process was performed for the 18 main functions with a full set of architecture schemes, mathematical models and calculation results considered.

e) As to availability criterion (probability that the object is available at any time) the reliability of all control system functions is greater than 0.9999.

f) Average low (without restoration) and upper (with restoration) reliability for 1 year of operation for shutdown system functions (F-11 - F-16) are 0.89 ~ 0.91, and for other functions 0.76 ~ 0.93.

g) The final project design yielded almost complete elimination of main control system functions multiple failures due to single component failure.

Reliability calculations indicated that the resulting reliability and fault-tolerance levels of the main control system functions were sufficient.

Development of SPIK SZMA’s "Procedure for Evaluation of Control System Reliability.” Standard:

Based on the knowledge and experience gained from this project SPIK SZMA has developed a standardized "Procedure for Evaluation of Control System Reliability.”

To improve the quality of reliability calculations the procedure incorporates the cooperation of SPIK SZMA’s project and research department specialists. Project department specialists develop a general task foundation for reliability calculation, description and preparation of FIS versions and specification for element reliability initial parameters.

R&D specialists then provide the final FIS development and initial data entry into SC ASLS software application for automated simulation and calculation of system reliability and safety analysis. The reliability estimate results analysis, development and foundation of project design decisions, and reporting documentation preparation are finally realized through collaboration by specialists from both departments.

Based on general logic probabilistic technique, all main structural models of the system reliability such as analytical, Markov, statistical and network models can now be generated automatically.