RISK-BASED FAULT DIAGNOSIS AND SAFETY MANAGEMENT FOR PROCESS SYSTEMS

HUIZHI BAO

RISK-BASED FAULT DIAGNOSIS AND SAFETY MANAGEMENT FOR PROCESS SYSTEMS

by

Huizhi Bao

A thesis submitted to the School of Graduate Studies in partial fulfillment of the requirements for the degree of

Master of Engineering

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

March, 2010

St. John's Newfoundland

Abstract

Today, plants in chemical and process industry are becoming larger and more complex. Corollary of this trend implies that each hour of down time is more expensive. As industrial systems enlarge, the total amount of energy and material being handled increases, making fault diagnosis and safety management considerably important both from the viewpoint of process safety as well as economic loss. Therefore, seeking an effective approach to perform fault diagnosis and implement safety management is important and imperative. An innovative methodology of risk-based SPC fault diagnosis and its integration with Safety Instrumented System (SIS) is proposed in this thesis to assure the process safety.

Unlike any existing fault diagnosis and safety management approaches, the proposed methodology pioneers a brand new pathway for the fault diagnosis and safety management in process industry. This proposed methodology neither depends on any process model as model-based methods, nor depends on large amount of historical process data as conventional process history based method. Control chart technique is used to distinguish abnormal situation from normal operation based on three-sigma rule and linear trend forecast. Time series and moving average techniques are used to perform real time monitoring and noise filtering in fault diagnosis process. Furthermore, risk indicators are used to identify and determine potential fault(s) to minimize the number of false alarms.

The proposed methodology of risk-based SPC fault diagnosis and its integration with safety instrumented systems is implemented using G2 development environment. To test and verify this methodology, a tank filling system and a steam power plant system with SIS1s and SIS2s are developed in G2 environment. A technique breakthrough, from univariate monitoring to multivariate monitoring for SPC fault diagnosis has been made in the verification in the steam power plant system.

Acknowledgements

As a person who desires to dedicate herself to a research which is her dream in her life, the biggest wish for her is to have an opportunity to pursue this dream and make it true. The School of Graduate Studies of Memorial University of Newfoundland provides this opportunity to the author, so please allow the author to express her sincere appreciation to him first.

Dr. Faisal Khan and Dr. Tariq Iqbal, two of the most outstanding professors in the Faculty of Engineering and Applied Science at Memorial University of Newfoundland, provided the author with detailed guidance and also financial support for her research. Herein, please accept the thankfulness from the author's heart to them.

Appreciations are also shown to Dr. Yanjun Chang, Mr. Cen Nan and all the friends who have ever helped the author in her research and her life.

Thanks the author's family, without the understanding and support from them, the author would not have the study opportunity in Memorial University of Newfoundland.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ALARP	As Low As Reasonably Practicable
API	Application Programmer's Interface
BP	Back-Propagation
BPCS	Basic Process Control System
CA	Cumulative Average
CDF	Cumulative Distribution Function
CMA	Cumulative Moving Average
EMA	Exponential Moving Average
ESD	Emergency Shutdown
ETA	Event Tree Analysis
EUC	Equipment Under Control
FDD	First Discrete Derivative
FDI	Fault Diagnosis and Identification
GDA	G2 Diagnostic Assistant
GSI	Gateway Standard Interface
GUI	Graphical User Interfaces
GUIDE	Graphical User Interface Development Environment
ICA	Independent Component Analysis
IEC	International Electro-technical Commission
IFD	Information Flow Diagram
ISC	Intelligent Supervisory Coordinator
KBRT	Knowledge-Based Real Time
LCL	Lower Control Limit
MSPC	Multivariate Statistical Process Control
OSHA	Occupational Safety and Health Administration
PCA	Principal Component Analysis

PFD	Probability of Failures on Demand
PLC	Programmable Logic Controllers
PLS	Partial Least Squares
PSM	Process Safety Management
RI	Risk Indicator
RRF	Risk Reduction Factor
SDD	Second Discrete Derivative
SF	Safety Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SMA	Simple Moving Average
SPC	Statistical Process Control
SSD	Safety Shutdown
UCL	Upper Control Limit
UIL	User Interface Library
WMA	Weighted Moving Average

List of Symbols

C	Consequence
erf (x)	Error Function
Fnp	Unprotected Risk Frequency
Fp	Protected Risk Frequency
Ft	Tolerable Risk Frequency
P (F)	Probability of Fault
PFDavg.	Probability of Failure on Demand
S	Severity of Fault
μ	Mean
σ	Standard Deviation
ω_n	Under-damped Natural Frequency
ω_d	Damped Natural Frequency
ξ	Damping Coefficient
τ	Time Constant

List of Appendices

Chapter 1 Introduction

In 1987, Robert M. Solow, an economist at the Massachusetts Institute of Technology, received the Nobel Prize in economics for his work in determining the sources of economic growth. Professor Solow concluded that the bulk of an economy's growth is the result of technological advances (Crowl and Louvar, 2002). It is reasonable to conclude that the growth of an industry is also dependent on technological advances. This is especially true in the chemical industry, which is entering an era of more complex processes: higher pressure, more reactive chemicals, and exotic chemistry. More complex processes require more complex safety technology. Many industrialists even believe that the development and application of safety technology is actually a constraint on the growth of the chemical industry.

As chemical process technology becomes more complex, chemical engineers will need a more detailed and fundamental understanding of safety. Howard H. Fawcett said, "To know is to survive and to ignore fundamentals is to court disaster." (Fawcett and Wood, 1982). Flixborough disaster, which happened in England in 1974, was the wake-up call for the UK. The incident resulted in 28 deaths, over 100 injuries and the complete destruction of the plant. The death toll from the Bhopal accident, which happened in India in 1984, was over 2,000 at the time of the accident. Some recent reports place the estimates as high as 10,000 with over 200,000 injuries. Chernobyl accident, which happened in Soviet Union in 1986, is estimably one of the worst industrial accidents of all time. Pasadena explosion, which happened in Texas in 1989, was the wake-up call for the US with 23 fatalities and 130 injuries. Another accident in nearby Channelview killed 17 and injured over 100 less than one year later. These two accidents resulted in the Occupational Safety and Health Administration (OSHA) PSM (Process Safety Management) legislation (Gruhn, P, 1999).

As process safety incidents are still happening today and as such incidents sometimes lead to serious consequences for people, the environment and property, it is concluded that the process industry has a responsibility to further reduce occurrence of these incidents. Due to the observed changing situation in the process industry, characterized by a changing kind of incident scenarios and causes, a need exists for a changing kind of control over process safety (Knegtering and Pasman, 2009).

In an increasingly multidisciplinary engineering environment, and in the face of ever increasing system complexity, there is a growing demand for engineers and technicians involved in process engineering to be aware of the implications of designing and operating safety-related systems. Safety Instrumented Systems play a vital role in providing the protective layer functionality in many industrial process and automation systems.

1.1 Safety Instrumented System

The International Electro-technical Commission (IEC) 61508 (2000) standard defines Safety Instrumented System (SIS) as "a system composed of sensors, logic solvers and final-control elements for the purpose of taking the process to a safe state, when predetermined conditions are violated". SISs are also called emergency shutdown (ESD) systems, safety shutdown (SSD) systems, and safety interlock systems.

Safety instrumented systems (SIS) are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment (Lundteigen and Rausand, 2007). A SIS generally consists of one or more input elements (e.g., sensors, transmitters), one or more logic solvers (e.g., programmable logic controllers [PLC], relay logic systems), and one or more final elements (e.g., safety valves, circuit breakers), as shown in Fig. 1.

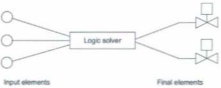

Fig. 1 Main Parts of a Safety Instrumented System

1.1.1 Process Control System and SIS

As illustrated in Fig. 2, it is generally preferable that any protection system (including a SIS) be kept functionally separate from the Basic Process Control System (BPCS) in terms of its ability to operate independent of the state of the BPCS. The operating equipment is also known as the Equipment Under Control (EUC). In essence, protection systems should be capable of functioning to protect the EUC when the process control system is in fault. Where separation is not possible because the safety functions are integral with the process control system, all parts of the system that have safety-related functions should be regarded as a SIS for the purposes of safety integrity assessment.

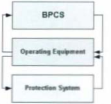

Fig. 2 Separation of BPCS and Protection System

Fig. 3 shows the basic layout of a typical SIS (in this case controlling a shutdown valve as the final control element).

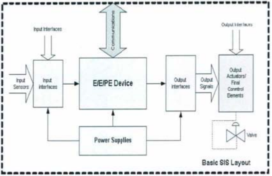

Fig. 3 Basic SIS Layout

The basic SIS layout comprises:

- Sensor(s) for signal input and power
- Input signal interfacing and processing
- Logic solver with associated communications and power
- Output signal processing, interfacing and power
- Actuators and valve(s) or switching devices to provide the final control element function.

The scope of a SIS encompasses all instrumentation and controls that are responsible for bringing a process to a safe state in the event of an unacceptable deviation or failure.

1.1.2 Risk and Risk Reduction Methods

Safety can be defined as "freedom from unacceptable risk". This definition is important, because it highlights the fact that all industrial processes involve risk. Absolute safety, where risk is completely eliminated, can never be achieved; risk can only be reduced to an acceptable level. Therefore all risks should be dealt with on the ALARP basis, i.e. the target is to ensure that risk is reduced to As Low As Reasonably Practicable. The ALARP principle provides a general objective of SIS, which is to reduce the frequency at which a hazard may occur to an acceptable or at least a tolerable level.

Process risk is defined by the frequency of the occurrence and the potential consequence severity of the process hazard (Summers, 2007). The formula for risk is:

Risk = Hazard Frequency * Hazard Consequence

To define the frequency, the initiating events are identified for each process hazard, and their frequency of occurrence is estimated. The consequence severity is the logical conclusion to the propagation of the process hazard if no protection layers are implemented as barriers to the event.

Safety Methods employed to protect against or mitigate harm/damage to personnel, plant and the environment, and reduce risk include:

- Changing the process or engineering design
- Increasing mechanical integrity of the system
- Improving the BPCS
- Developing detailed training and operational procedures
- Increasing the frequency of testing of critical system components
- Using a SIS

- Installing mitigating equipment

Fig. 4 illustrates the above measures in terms of employing protective layers to reduce risk to an acceptable level. The amount of risk reduction for each layer is dependent on the nature of the risk and the amount of risk reduction afforded by the applicable layer employed. Protective layers can be further classified as either Prevention or Mitigation layers. The former are put in place to stop hazardous occurrences and the latter are designed to reduce the consequences after hazardous events have occurred. In the case illustrated in Fig. 4, the protective layers are further sub-divided into in-plant and external areas. Methods that provide layers of protection should be independent, reliable, auditable and designed specifically for the risk involved.

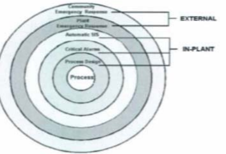

Fig. 4 Safety Protective Layers

1.1.3 Safety Function (SF)

In process industry, a safety function is defined as: A set of specific actions to be taken under specific circumstances, which will move the chemical process from a potentially unsafe state to a safe state (Marszal etc., 2003). A safety function works as a protection against a specific and identified hazardous event. It is a method to define the functional relationship between inputs and outputs in SIS. Inputs can be regarded as sensors, outputs can be regarded as final control elements and safety function can be regarded as a logic solver.

SF is able to assist SIS to reduce the risks. The amount of risk reduction can be measured based on the calculated Probability of Failures on Demand (PFD), which is the probability that SF fails to maintain safe state when predetermined safety conditions are violated. Safety function only reduces risk and will never completely eliminate the risk. However, it would be sufficient to reduce the risk to an acceptable level.

1.2 Safety Analysis

1.2.1 Risk Classification

Unlike the convenient units like volt or kilogram, there is no universal unit for risk. Scales for one industry may not suit those in another. Fortunately, the method of calculation is generally consistent and it is possible to arrive at a reasonable scale of values for a given industry. As a result, IEC have suggested using a system of risk classification that is adaptable for most safety situations. Referring to Annex B of IEC 61508 part 5, the risk classification table is provided as shown in Table 1.

Table 1: Risk Classification of Accidents: Table B1 of IEC 61508-5

Frequency	Consequences			
	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

The risk classification mentioned in Table 1 is a generalized version that works like following:

- Determine the frequency element of the EUC risk without the addition of any protective features (Fnp);
- Determine the consequence C without the addition of any protective features;
- Determine whether for frequency Fnp and consequence C, a tolerable risk level is

achieved.

If, through using Table 1, this leads to risk Class I, then further risk reduction is required. Risk class IV or III would be tolerable risks. Risk class II would require further investigation.

In practice, this Table 1 is a generic table for adaptation by different industry sectors. It is intended that any given industry sector should insert appropriate numbers into the fields of the table and hence establish acceptable norms. For example, in Table 2, some trial values have been inserted.

Table 2: Risk Classification of Accidents: Trial Values

Frequency	Catastrophic	Critical	Marginal	Negligible
	> 1 death	1 death or injuries	Minor injury	Prod loss
1 per year	I	I	I	II
1 per 5 years	I	I	II	III
1 per 50 years	I	II	III	III
1 per 500 years	II	III	III	IV
1 per 5000 years	III	III	IV	IV
1 per 50000 years	IV	IV	IV	IV

1.2.2 Risk Reduction Terms and Equations

The terms and equations that can be used to define the risk reduction are as follows (MacDonald, 2004):

Ft = Tolerable Risk Frequency

Fnp = Unprotected Risk Frequency
Fp = Protected Risk Frequency
RRF = Risk Reduction Factor
PFDavg. = Probability of Failure on Demand

RRF = Fnp / Ft (1-1)
PFDavg. = 1 / RRF = Ft / Fnp (1-2)

1.2.3 Safety Integrity Level (SIL)

SIL represents the amount of risk reduction that is required from a safety function. IEC 61508 defines SIL as "a discrete level (one of four) for specifying the safety integrity requirements of safety function." (2000). Safety integrity level 4 (SIL4) is the highest level and safety integrity level 1 (SIL1) is the lowest one.

SIL has become increasingly part of the design and operation of safety instrumented system (Kirkwood and Tibbs, 2005). Companies are now specifying SIL based on the amount of risk reduction that is required to achieve a tolerable risk level. The SIS is designed to meet or exceed this level of performance.

How do we decide when to use a safety instrumented system and how good must it be? The answer is: it depends on the amount of risk reduction required after the other devices have been taken into account. The measure of the amount of risk reduction provided by a safety system is called the Safety Integrity, and it is illustrated by Fig. 5 from IEC.

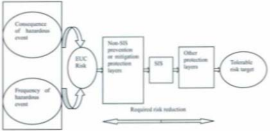

Fig. 5 Risk Reduction

This diagram defines safety integrity as applicable to all risk reduction facilities. When it is applied to the safety instrumented system, however, it becomes a measure of the system's performance.

In order to scale the performance, safety integrity levels or SILs are used. The SILs are derived from earlier concepts of grading or classification of safety systems. The principle is illustrated in Fig. 6 where the layer of protection provided by an SIS is quantified as a risk reduction factor (RRF), which can be converted into a PFDavg and referenced to an SIL table.

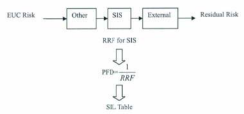

Fig. 6 Determination of SIL

Essentially the SIL table provides a class of safety integrity to meet a range of PFDavg values. Hence, the performance level of safety instrumentation needed to meet the SIL is divided into a small number of categories or grades.

The IEC standard provides the following table for SILs.

Table 3: Definitions of SILs for demand mode of operation from IEC 61511-1

SIL	Range of Averaged PFD	Range of RRF
4	10^{-5} <= PFD < 10^{-4}	100,000 >= RRF > 10,000
3	10^{-4} <= PFD < 10^{-3}	10,000 >= RRF > 1000
2	10^{-3} <= PFD < 10^{-2}	1000 >= RRF > 100
1	10^{-2} <= PFD < 10^{-1}	100 >= RRF > 10

An SIL 1 system is not as reliable in providing risk reduction as SIL 2; an SIL 3 is even more reliable. Once we have the SIL, we will know what quality, complexity and cost are going to consider.

1.2.4 Event Tree Analysis (ETA)

An event tree is a graphical logic model that identifies and quantifies possible outcomes following an initiating event (Ghodrati etc., 2007). Event trees begin with an initiating event and work toward a final result. This approach is inductive. The method provides information on how a failure can occur and the probability of occurrence. When an accident occurs in a plant, various safety systems come into play to prevent the accident from propagating. These safety systems either fail or succeed. The event tree approach includes the effects of an event initiation followed by the impact of the safety systems.

The typical steps in an event tree analysis are:

1. Identify an initiating event of interest,
2. Identify the safety functions designed to deal with the initiating event,
3. Construct the event tree, and
4. Describe the resulting accident event sequences.

If appropriate data are available, the procedure is used to assign numerical values to the various events. This is used effectively to determine the probability of a certain sequence of events and to decide what improvements are required. An example of event tree analysis is shown in Fig. 7.

Initiating event	Start of fire	Sprinkler system does not function	Fire alarm is not activated	Outcomes	Frequency (per year)

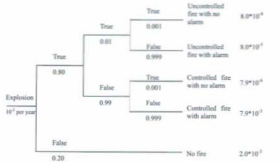

Fig. 7 An Example of Event Tree Analysis

The initiating event is usually a failure/undesired event corresponding to a release of failure/hazard. In the above example, the initiating event is "Explosion", and the frequency of this incident is 10^{-2} per year. The safety functions are actions or barriers that can interrupt the sequence from an initiating event to a failure/hazardous outcome. In the above example, the safety functions are sprinkler system functions and activating the fire alarm. The outcomes in the above example are "Uncontrolled fire with no alarm" with frequency $8.0*10^{-8}$, "Uncontrolled fire with alarm" with frequency $8.0*10^{-5}$, "Controlled fire with no alarm" with frequency $7.9*10^{-6}$, "Controlled fire with alarm" with frequency $7.9*10^{-3}$, and "No fire" with frequency $2.0*10^{-3}$.

1.3 Statistical Process Control

1.3.1 Introduction

Statistics is a mathematical science pertaining to the collection, analysis, interpretation or explanation, and presentation of data (Moses etc., 1986). Statistical Process Control is defined as a system that uses statistics to identify special causes of variation in a process (Leonard, 1996). Statistical Process Control (SPC) was pioneered by Walter A. Shewhart in the early 1920s. W. Edwards Deming later applied SPC methods in the United States during World War II, thereby successfully improving quality in the manufacture of munitions and other strategically important products. Deming was also instrumental in introducing SPC methods to Japanese industry after the war had ended. In 1989, the Software Engineering Institute introduced the notion that SPC can be usefully applied to non-manufacturing processes, such as software engineering processes. Through surveys and researches, I deeply believe that SPC method can be applied in the process industry, that is, to be utilized in my development for the fault diagnosis and real time monitoring of the process system.

Statistical Process Control (SPC) is an effective method of monitoring a process through the use of control charts. Control charts enable the use of objective criteria for distinguishing background variation from events of significance based on statistical techniques. Much of its power lies in the ability to monitor both process center and its variation or deviation about that center. By collecting data over time at various points within the process, variations or deviations in the process can be detected and clearly displayed. If the deviation exceeds thresholds predefined, then a fault probably occurs. In this research, SPC will be used as a fault diagnosis method to perform fault diagnosis function to the process systems.

1.3.2 Control Chart

A control chart is a statistical tool used to distinguish between variation in a process resulting from common causes and variation resulting from special causes. It presents a graphic display of process stability or instability over time.

Every process has variation. Some variation may be the result of causes which are not normally present in the process. This could be special cause variation. Some variation is simply the result of numerous, ever-present differences in the process. This is common cause variation. Control Charts differentiate between these two types of variation.

In general, control chart contains a center line that represents the mean value for the in-control process. Two other horizontal lines, called the upper control limit (UCL) and the lower control limit (LCL), are also shown in Fig. 8. These control limits are chosen so that almost all of the data points will fall within these limits as long as the process remains in-control. If a single quality characteristic has been measured or computed from a sample, the control chart shows the value of the quality characteristic versus the sample number or versus time.

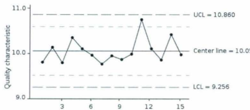

Fig. 8 An Example of Control Chart

The purpose in adding warning limits or subdividing the control chart into zones is to provide early notification if something is amiss. Instead of immediately launching a process improvement effort to determine whether special causes are present, the quality engineer may temporarily increase the rate at which samples are taken from the process output until it's clear that the process is truly in control.

One goal of using a Control Chart is to achieve and maintain process stability. Process stability is defined as a state in which a process has displayed a certain degree of consistency in the past and is expected to continue to do so in the future. This consistency is characterized by a stream of data falling within control limits based on plus or minus 3 standard deviations (3 sigma) of the centerline (Wheeler and Chambers, 1992).

1.3.3 Time Series

In statistics, signal processing and financial mathematics, a time series is a sequence of data points, measured typically at successive times spaced at uniform time intervals. Examples of time series are the daily closing value of the Dow Jones index or the annual flow volume of the Nile River at Aswan. Time series analysis comprises methods for analyzing time series data in order to extract meaningful statistics and other characteristics of the data. Time series forecasting is the use of a model to forecast future events based on known past events: to predict data points before they are measured. An example of time series forecasting in econometrics is predicting the opening price of a stock based on its past performance.

An example of time series for random data plus trend, with best-fit line and different smoothing is shown in Fig. 9.

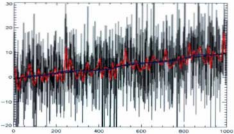

Fig. 9 Time Series: random data plus trend, with best-fit line and different smoothings (en.wikipedia.org)

Time series data have a natural temporal ordering. This makes time series analysis distinct from other common data analysis problems, in which there is no natural ordering of the observations. Time series analysis is also distinct from spatial data analysis where the observations typically relate to geographical locations. A time series model will generally reflect the fact that observations close together in time will be more closely related than observations further apart. In addition, time series models will often make use of the natural one-way ordering of time so that values for a given period will be expressed as deriving in some way from past values.

1.3.4 Moving Average Techniques

Moving average technique will be utilized in my development. In statistics, a moving average, also called rolling average, rolling mean or running average, is a type of finite impulse response filter used to analyze a set of data points by creating a series of averages of different subsets of the full data set. A moving average is commonly used with time series data to smooth out short-term fluctuations and highlight longer-term trends or cycles. The threshold between short-term and long-term depends on the application, and the parameters of the moving average will be set accordingly. For example, it is often used in technical analysis of financial data, like stock prices, returns or trading volumes. It is also used in economics to examine gross domestic product, employment or other macroeconomic time series. Mathematically, a moving average is also similar to the low-pass filter used in signal processing.

An example of Moving Average of stock price chart is shown in Fig. 10.

Fig. 10 An example of Moving Average of Stock Price Chart (stockcharts.com)

Followings are various types of Moving Average techniques:

1. Simple Moving Average (SMA)

A simple moving average (SMA) is the unweighted mean of the previous n data points. For example, a 10-day simple moving average of closing price is the mean of the previous 10 days' closing prices. If those prices are P_M, P_{M-1}, ..., P_{M-9}, then the formula is:

$$SMA = \frac{p_M + p_{M-1} + \cdots + p_{M-n}}{10} \qquad (1\text{-}3)$$

When calculating successive values, a new value comes into the sum and an old value drops out, meaning a full summation each time is unnecessary,

$$SMA_{today} = SMA_{yesterday} - \frac{p_{M-n}}{n} + \frac{p_M}{n} \qquad (1\text{-}4)$$

In technical analysis, there are various popular values for n, like 10 days, 40 days, or 200 days. The period selected depends on the kind of movement one is concentrating on, such as short, intermediate, or long term.

2. Cumulative Moving Average (CMA)

In some data acquisition systems, the data arrives in an ordered data stream and the statistician would like to get the average of all of the data up until the current data point. For example, an investor may want the average price of all of the stock transactions for a particular stock up until the current time. As each new transaction occurs, the average price at the time of the transaction can be calculated for all of the transactions up to that point using the cumulative average. This is the cumulative average, which is typically an unweighted average of the sequence of i values $x_1, \ldots, x_i$ up to the current time:

$$CA_i = \frac{x_1 + \cdots + x_i}{i} \qquad (1\text{-}5)$$

The brute force method to calculate this would be to store all of the data and calculate the sum and divide by the number of data points every time a new data point arrived. However, it is possible to simply update cumulative average as a new value x_{i+1} becomes available, using the formula:

$$CA_{i+1} = \frac{x_{i+1} + iCA_i}{i+1} \qquad (1\text{-}6)$$

where CA_0 can be taken to be equal to 0.

The derivation of the cumulative average formula is:

$$CA_{i+1} = CA_i + \frac{x_{i+1} - CA_i}{i+1} \qquad (1\text{-}7)$$

Thus the current cumulative average for a new data point is equal to the previous cumulative average plus the difference between the latest data point and the previous average divided by the number of points received so far. When all of the data points arrive ($i = N$), the cumulative average will equal the final average.

3. Weighted Moving Average (WMA)

A weighted average is any average that has multiplying factors to give different weights to different data points. Mathematically, the moving average is the convolution of the data points with a moving average function; in technical analysis, a weighted moving average (WMA) has the specific meaning of weights that decrease arithmetically. In an n-day WMA the latest day has weight n, the second latest $n - 1$, etc, down to zero.

$$WMA_M = \frac{np_M + (n-1)p_{M-1} + \ldots + 2p_{M-n+2} + p_{M-n+1}}{n + (n-1) + \ldots + 2 + 1} \qquad (1\text{-}8)$$

The denominator is a triangle number, and can be easily computed as $\frac{n(n+1)}{2}$.

When calculating the WMA across successive values, if we denote the sum $p_M + \ldots + p_{M-n+1}$ by $Total_M$, then

$$Total_{M+1} = Total_M + p_{M+1} - p_{M-n+1} \qquad (1\text{-}9)$$

$$Numerator_{M+1} = Numerator_M + np_{M+1} - Total_M \qquad (1\text{-}10)$$

$$WMA_{M+1} = \frac{Numerator_{M+1}}{n+(n-1)+\ldots+2+1} \qquad (1\text{-}11)$$

Fig. 11 shows how the weights decrease, from highest weight for the most recent data points, down to zero.

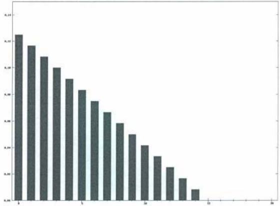

Fig. 11 WMA Weights (n=15)

4. Exponential Moving Average (EMA or EWMA)

An exponential moving average (EMA), sometimes also called an exponentially weighted moving average (EWMA), applies weighting factors which decrease exponentially. The weighting for each older data point decreases exponentially, giving much more importance to recent observations while still not discarding older observations entirely. Fig. 12 shows an example of the weight decrease.

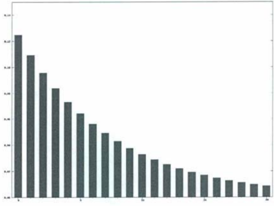

Fig. 12 EMA Weights

The degree of weighing decrease is expressed as a constant smoothing factor α, a number between 0 and 1. The formula for calculating the EMA is:

$$EMA_{today} = EMA_{yesterday} + \alpha \times (price_{today} - EMA_{yesterday}) \qquad (1\text{-}12)$$

Expanding out $EMA_{yesterday}$ each time results in the following power series, showing how the weighting factor on each data point p1, p2, etc, decrease exponentially:

$$EMA = \alpha \times (p_1 + (1-\alpha)p_2 + (1-\alpha)^2 p_3 + (1-\alpha)^3 p_4 + \ldots) \qquad (1\text{-}13)$$

This is an infinite sum with decreasing terms.

SMA technique is intuitive and simple. CMA technique is not as intuitive and simple as SMA, but it is more efficient in detecting small shifts. EWMA technique is used for detecting small shifts, like 0.5σ to 2σ in the process mean.

1.4 Objectives of this Research

As process industrial systems become larger and more complex, the total amount of energy and material being handled increases, making fault diagnosis and safety management considerably important both from the viewpoint of process safety as well as economic loss. There exist various kinds of methods to do the fault diagnosis and safety management to the industrial processes. However, due to the limitations in various methods, the effects for fault diagnosis and safety management are not that desirable. For this reason, Venkatasubramanian etc. (2003) even proposed to develop hybrid systems to overcome the limitations of individual solution strategies.

Motivated by the desire of seeking an effective approach to perform fault diagnosis and implement safety management in process systems, and by the current situation for solving this problem in academia, an innovative methodology of risk-based SPC fault diagnosis and its integration with Safety Instrumented System is proposed in this thesis. To verify this methodology, G2 development software from Gensym Corporation is utilized in this research.

The overall objectives for this research are as follows:

- To propose an innovative methodology of risk-based SPC fault diagnosis and its integration with SIS to solve the fault diagnosis and safety management problem in process engineering.
- Using G2 development environment, to implement and verify the proposed methodology in a tank filling system developed with G2 software.
- Realizing a technique breakthrough, from univariate control to multivariate control for SPC fault diagnosis, in process fault diagnosis field.
- Simulating a real process system, the steam power plant system, in G2 development environment, to testify the proposed methodology.

1.5 Organization of this Thesis

Six chapters are included in this thesis. In Chapter 1, the knowledge of SIS, safety analysis and statistical process control are introduced. The objectives of this research are also presented in this chapter. In Chapter 2, the existing fault diagnosis methods are first reviewed. Then, an innovative methodology of fault diagnosis and safety management for process system is proposed and verified theoretically. At last, the G2 development environment is introduced. In Chapter 3, the proposed methodology is implemented and verified in the G2 development environment through developing a tank filling system. Meanwhile, the proposed methodology is testified that it neither depends on any model, nor depends on large historical data. To demonstrate the advantages of the proposed methodology, a comparison between the tank filling system developed with the proposed methodology and a traditional design for the same system is held. In Chapter 4, the proposed methodology is further implemented and verified in the G2 development environment through developing another process system, the steam power plant system. In the meantime, a technique breakthrough is made in this chapter. At the end of this chapter, a comparison between the steam power plant system developed with the proposed methodology and the traditional expert systems method for the same system is held. In Chapter 5, the ten characteristics of the proposed methodology are listed. In Chapter 6, conclusion for this proposed methodology is made, and the future works for this research are presented.

Chapter 2 Methodology of Risk-based SPC Fault Diagnosis and Safety Management for Process System

2.1 Review of Existing Fault Diagnosis Methods

In the area of process fault diagnosis, the term fault is generally defined as a departure from an acceptable range of an observed variable or a calculated parameter associated with a process (Himmelblau, 1978). This defines a fault as a process abnormality or symptom, such as high temperature in a reactor or low product quality and so on. The underling cause(s) of this abnormality, such as a failed coolant pump or a controller, is (are) called the basic event(s) or the root cause(s). The basic event is also referred to as a malfunction or a failure. Early detection and diagnosis of process faults while the plant is still operating in a controllable region can help avoid abnormal event progression and reduce productivity loss.

From a modeling perspective, there are methods that require accurate process models, semi-quantitative models, or qualitative models. On the other hand, there are methods that do not assume any form of model information and rely only on historical process data. We broadly classify fault diagnosis methods into three general categories. They are quantitative model-based methods, qualitative model-based methods, and process history based methods (Venkatasubramanian et al., 2003). The classification of fault diagnosis methods are shown in Fig. 13.

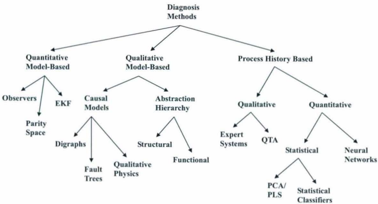

Fig. 13 Classification of Diagnostic Algorithms (Venkatasubramanian et al., 2003)

There are abundant literatures on process fault diagnosis approaches which range from analytical redundancy to knowledge-based systems and neural networks. Ghetie et al. (1998) propose a fault diagnosis approach using balance equations methods and the algorithmic redundancy. In this approach, they illustrate the algorithmic redundancy concept using two representative fault detection and isolation methods based on balance equations. An approach of model-based fault diagnosis using knowledge base and fuzzy logic technique is presented by Mohamed et al. (2002). The input/output measurements are used to generate analytic symptoms. Heuristic symptoms observed by the operator or based on the process history are another source for fault diagnosis. Lo et al. (2006) develop an intelligent supervisory coordinator (ISC) for process supervision and fault diagnosis in dynamic physical systems. A qualitative bond graph modeling scheme, integrating artificial-intelligence techniques with control engineering, is used to construct the knowledge base of the ISC. The model type which the analytical approaches can handle is limited to linear, and in some cases, to very specific nonlinear models. For a general nonlinear model, linear approximations can prove to be poor and hence the effectiveness of these methods might be greatly reduced. Model-based fault diagnosis requires accurate process models, while the computational complexity in real-time fault diagnostic systems and the difficulty in developing accurate process models make this approach impractical in real industrial processes. Albazzaz and Wang (2004) propose a monitoring and fault diagnosis method for process by deriving SPC charts based on ICA (Independent Component Analysis). He et al. (2006) present a novel process fault detection and diagnosis technique based on principal component analysis (PCA). The proposed method reduces the dimensionality of the original data set by the projection of the data set onto a smaller subspace defined by the principal components through PCA. A major limitation of PCA-based monitoring is that the PCA model is time invariant, while most of the real processes are time-varying. Hence the PCA model should also be recursively updated. Simani and Fantuzzi (2000) propose a FDI (Fault Diagnosis and Identification) methodology. This FDI methodology consists of two stages. In the first stage, the fault is detected on the basis of residuals generated from a bank of Kalman filters; in the second stage, fault identification is obtained from pattern recognition techniques implemented by Neural Networks. To enhance fault diagnosis reliability, Zhang (2006) proposes a technique where multiple neural networks are developed and their diagnosis results are combined to give the overall diagnosis result. Ma et al. (2009) propose a new fault diagnosis approach with fault gradation using BP (back-propagation) neural network group consisting of 3 sub BP neural networks. According to the hazard extents and the occurrence frequencies of different faults, the faults are divided into different grades. Neural network based fault diagnosis systems are easy to develop and can cope with nonlinearities. However, a single neural network can lack robustness, especially when the data available for training the network are not abundant.

Most of the quantitative model based approaches are based on general input-output and state-space models. One of the major advantages of the quantitative model-based fault diagnosis approach is that we can control the behavior of the residuals. However, due to system complexity, high dimensionality and process nonlinearity, it is impractical to develop an accurate mathematical model for the process system. This has limited the application of this approach in real industrial processes. Qualitative model based approaches are usually developed based on some fundamental understanding of the physics and chemistry of the process. An important feature of this approach is that qualitative models do not require detailed process information, and the qualitative behavior can be derived even if the accurate mathematical model cannot be developed. The main disadvantage is qualitative model based method generates spurious solutions when reasoning with qualitative models. From industrial application viewpoint, the maximum number of fault diagnostic applications in process industries are based on process history based approaches. Among the process history based approaches, statistical approach seems to have been well studied and applied (Venkatasubramanian et al., 2003). Unlike model-based approaches, process history based methods do not require a priori quantitative or qualitative knowledge about the process. However, the conventional process history based methods need a large amount of historical process data. For these above reasons, Venkatasubramanian et al. even propose to develop hybrid systems to overcome the limitations of individual approach. As they said, "*One realizes that no* *single method has all the desirable features one would like a diagnostic system to possess. It is our view that some of these methods can complement one another resulting in better diagnostic systems. Integrating these complementary features is one way to develop hybrid systems that could overcome the limitations of individual solution strategies.*"

In this situation for fault diagnosis in process engineering and the aforementioned (in Chapter 1) safety incidents happened in process industries that lead to the serious consequences for people, the environment and property, it is important and imperative for our researchers to find an effective method to perform the fault diagnosis and safety management to the process system. These factors motivated the proposal of an innovative methodology of risk-based SPC fault diagnosis and its integration with SIS for process systems in this research.

2.2 Proposed Methodology

Since there are various bewildering fault diagnosis approaches in process engineering, and for the existing methods, quantitative model-based methods, qualitative model-based methods and process history based methods, each of them has its limitations, it is not an ideal solution for us to follow one branch in the classification of diagnostic algorithms shown in Fig. 13, nor the hybrid systems solution proposed by Venkatasubramanian et al.. Statistical approach is easy to build and it performs considerably well on fast detection of abnormal situations, and it has been successfully implemented in industrial applications, but it belongs to the conventional process history based method, that means it needs a large amount of historical process data. If we cut the dependence between statistical and a large mount of historical process data which are required by the conventional process history based method in Fig. 13, and we do not use any branches below statistical method, i.e., PCA/PLS or Statistical Classifiers, then this brand new approach is desired to be an ideal solution for this process fault diagnosis problem, because it will neither depend on a large amount of historical process data, nor have the limitations from PCA/PLS or Statistical Classifiers methods. Based on these thoughts, an innovative methodology, risk-based Statistical Process Control (SPC) fault diagnosis and its integration with SIS for process system, has been proposed. The pathway of the proposed approach for fault diagnosis in the classification of diagnostic algorithms is shown in Fig. 14.

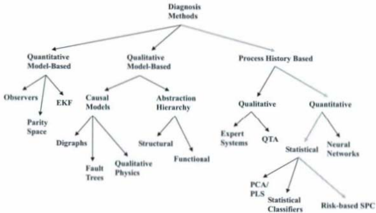

Fig. 14 Pathway of Proposed Methodology in the Classification of Diagnostic Algorithms

The flow chart of the proposed risk-based SPC fault diagnosis and its integration with SIS for process systems is shown in Fig. 15.

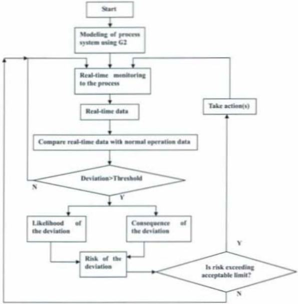

Fig. 15 Methodology of the Risk-based Fault Diagnosis and Safety Management for Process Systems

2.3 Verification of Proposed Fault Diagnosis Methodology

In order to theoretically verify the proposed risk-based SPC fault diagnosis methodology, historical data from Thermodynamics and Fluids Lab in Faculty of Engineering and Applied Science at Memorial University of Newfoundland will be used in this analysis. These historical data are the steam pressures of the steam power plant in the Thermodynamics and Fluids Lab. Historical data obtained during 12:49 p.m. through 12:58 p.m. on July 13, 2006 are taken to do the verification. The steam pressure data in normal operation are shown in Table 4 (normal situation). A fault event is simulated in this time period, and the corresponding data are shown in Table 5 (abnormal situation).

Table 4: Steam Pressure Data for the Steam Power Plant (Normal Situation)

Time	12:49-12:53	12:54-12:58
	678	673
	656	679
	638	658
	633	639
	645	643

Table 5: Steam Pressure Data for the Steam Power Plant (Abnormal Situation)

Time	12:49-12:53	12:54-12:58
	678	673
	656	700
	638	730
	633	639
	645	643

In this risk-based SPC fault diagnosis methodology, moving average technique will be utilized. To increase the sensitivity of the risk-based SPC fault diagnosis method to the fault event, the number of data points, 3, is chosen to do the moving average calculation. The steam pressure data obtained for normal situation and abnormal situation are shown in Table 6 and Table 7.

Table 6: Moving Average Steam Pressure Data for the Steam Power Plant System (Normal Situation)

Time	12:49-12:51	12:50-12:52	12:51-12:53	12:52-12:54	12:53-12:55	12:54-12:56	12:55-12:57	12:56-12:58
	678	656	638	633	645	673	679	658
	656	638	633	645	673	679	658	639
	638	633	645	673	679	658	639	643
Xbar	657.3	642.3	638.7	650.3	665.7	670	658.7	646.7

Note:

The normal steam pressure is 640 kPa, and the maximum steam pressure is 690 kPa.

Table 7: Moving Average Steam Pressure Data for the Steam Power Plant System (Abnormal Situation)

Time	12:49-12:51	12:50-12:52	12:51-12:53	12:52-12:54	12:53-12:55	12:54-12:56	12:55-12:57	12:56-12:58
	678	656	638	633	645	673	700	730
	656	638	633	645	673	700	730	639
	638	633	645	673	700	730	639	643
Xbar	657.3	642.3	638.7	650.3	672.7	701	689.7	670.7

2.3.1 Fault Diagnosis Principle

Three-sigma Rule:

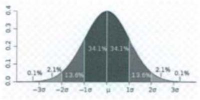

Fig. 16 Standard Deviation Diagram

In statistics, for a normal distribution, nearly all (99.7%) of the values lie within 3 standard deviations of the mean (or between the mean minus 3 times the standard deviation and the mean plus 3 times the standard deviation). Statisticians use the following notation to represent this: $\mu \pm 3\sigma$.

For the steam power plant system, the normal steam pressure is 640 kPa. This value will be the mean, i.e., μ, in later fault diagnosis analysis. The maximum steam pressure is 690 kPa. This value will be the mean plus 3 times the standard deviation, i.e., $\mu + 3\sigma$, the upper control limit (UCL) in the control chart. Then the value of 3σ is 50, and we can obtain the mean minus 3 times the standard deviation, i.e., $\mu - 3\sigma$, the lower control limit (LCL) in the control chart. This LCL value is 590 kPa. According to the three-sigma rule, in normal situation, the data of the moving averages of the steam pressures should fall into the [LCL, UCL], i.e., [590kPa, 690kPa]. If there is a data which falls outside of this range, then a fault could occur. In this system, when the data exceeds the upper control limit, 690 kPa, it could be a fault.

2.3.2 SPC Fault Diagnosis

1. Normality Test to the Moving Average Steam Pressure Data

In order to test if the moving average steam pressure data are normally distributed, the normality tests in Minitab 15 are conducted. The results are shown in Fig. 17 and Fig. 18.

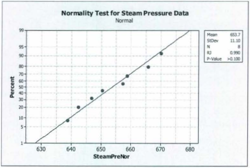

Fig. 17 Normality Test for Steam Pressure Data in Normal Situation

Fig. 17 is the normality test for the moving average steam pressure data in the Steam Power Plant System in normal operation. From Fig. 17, we can see that: The P-Value >0.100 (that is, P-Value>0.05); RJ=0.990, is very close to 1. So the moving average steam pressure data are normally distributed.

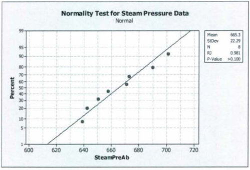

Fig. 18 Normality Test for Steam Pressure Data in Abnormal Situation

Fig. 18 is the normality test for the moving average steam pressure data in the Steam Power Plant System in abnormal situation. From Fig. 18, we can see that: The P-Value > 0.100 > 0.05; RJ=0.981, is very close to 1. So the moving average steam pressure data are still normally distributed.

2. SPC Fault Diagnosis Results

If the process is in normal operation, according to the three-sigma rule, the moving average steam pressure data points should fall into the [LCL, UCL], i.e., [590kPa, 690kPa]; otherwise, there could be a fault event. Plotting the moving average steam pressure data in Excel 2003, the following results are obtained, as shown in Fig. 19 and Fig. 20.

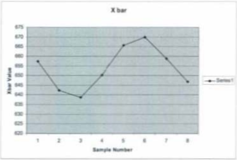

Fig. 19 Line Chart for Moving Average Steam Pressure Data in Normal Situation

From the above chart, we can see that the moving average steam pressure data points fall into the [590, 690], so the process is in normal situation.

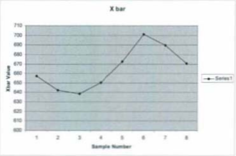

Fig. 20 Line Chart for Moving Average Steam Pressure Data in Abnormal Situation

From the above chart, we can see that the sixth data point falls outside the [590, 690], so the process is suspected to be abnormal, i.e., there could be a fault.

2.3.3 Risk-based SPC Fault Diagnosis

To minimize the number of false alarms, risk or risk indicator concept is introduced into the proposed fault diagnosis methodology to identify and determine potential fault(s). Risk is estimated for each deviation in the predicted values of control variables, using probability of the deviation and its associated severity. The probability of the fault is assessed using three-sigma rule, whereas the severity is assessed using the deviation from the predefined threshold value(s).

1. Risk Calculation Analysis

According to the definition to the process risk, the calculation of the risk of a fault in this research is as follows,

$$RI = Risk = P(F) * S \qquad (2\text{-}1)$$

Where,

RI indicates Risk Indicator.

P (F) is the probability of fault. $P(F) = \phi[\frac{x-(\mu+3\sigma)}{\sigma}]$

S is the severity of fault. $S = 100^{P(F)}$ (2-2)

While,

$$P(F) = \phi[\frac{x-(\mu+3\sigma)}{\sigma}] = \int_{-\infty}^{x} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(t-\mu)^2}{2\sigma^2}} dt \qquad (2\text{-}3)$$

Where,

$\mu' = \mu + 3\sigma$

From equation 2-3, we can see: in order to obtain P (F), we need to do the above integral. However, in G2 development environment, the Integrator block passes on the Euler integral of the block's history of values.

The two types of Euler integrals in mathematics are:

(1). the Beta function

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\,dt = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)} \qquad (2\text{-}4)$$

(2). the Gamma function

$$\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\,dt \qquad (2\text{-}5)$$

Obviously, this is not suitable for the risk calculation in this research. To be able to develop this risk-based fault diagnosis method in G2 environment, the author solved this problem through using mathematical trarsformation as follows,

From equation 2-3, as can be seen, the Cumulative Distribution Function (CDF) is not a standard form; therefore, an error function, erf (), is introduced to standardize the P (F) function.

2. Error Function:

In mathematics, the error function (also called the Gauss error function) is a special function (non-elementary) of sigmoid shape which occurs in probability, statistics, materials science, and partial differential equations. It is defined as (en.wikipedia.org):

$$erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \qquad (2\text{-}6)$$

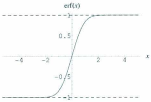

Fig. 21 Error Function

The integrand $f = \exp(-z^2)$ and $f = \mathrm{erf}(z)$ are shown in the complex z-plane in Fig. 22 and Fig. 23.

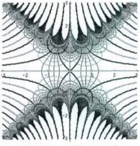

Fig. 22 Integrand $f = \exp(-z^2)$

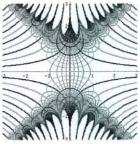

Fig. 23 erf (z)

The error function is an entire function; it has no singularities (except that at infinity) and its Taylor expansion always converges. The defining integral cannot be evaluated in closed form in terms of elementary functions, but by expanding the integrand into its Taylor series and integrating term by term, we can obtain the error function's Taylor series as:

$$erf(z) = \frac{2}{\sqrt{\pi}} \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{n!(2n+1)} = \frac{2}{\sqrt{\pi}} (z - \frac{z^3}{3} + \frac{z^5}{10} - \frac{z^7}{42} + \frac{z^9}{216} - \cdots) \qquad (2\text{-}7)$$

which holds for every complex number z. The denominator terms are sequence A007680 in the OEIS.

In order to apply this error function in G2 development environment, we use the approximation with elementary functions to error function:

$$erf^2(x') \approx 1 - \exp(-x'^2 \frac{4/\pi + ax'^2}{1 + ax'^2}) \qquad (2\text{-}8)$$

Where,

$$a = -\frac{8(\pi - 3)}{3\pi(\pi - 4)}$$

From above equation 2-8, we can obtain the calculation of $erf(x')$:

When $x' \geq 0$,

$$erf(x') \approx \sqrt{1 - \exp(-x'^2 \frac{4/\pi + ax'^2}{1 + ax'^2})} \qquad (2\text{-}9)$$

When $x' < 0$,

$$erf(x') \approx -\sqrt{1 - \exp(-x'^2 \frac{4/\pi + ax'^2}{1 + ax'^2})} \qquad (2\text{-}10)$$

3. Risk Calculation

First, we perform the standardization to the above P (F):

$$z = \frac{X - \mu'}{\sigma}$$

Let $x' = z$,

Then, we can obtain:

$$P(F) = \phi(x') = \frac{1}{2}[1 + erf(\frac{x'}{\sqrt{2}})] \qquad (2\text{-}11)$$

From equation 2-9, equation 2-10 and equation 2-11, we can obtain the value of P (F), correspondingly, the risk value:

$$RI = Risk = P(F) * S = P(F) * 100^{P(F)} \qquad (2\text{-}12)$$

Through the above calculation, the risk value for the predicted values of control variables will be obtained. Corresponding to the upper control limit of the control variable, there is a risk extreme limit. Besides, we can also define other risk limits or ranges for different systems to take some specific actions, like popping up warning messages, raising an alarm or shutting down the system, as will be described in detail in subsequent chapters.

In the safety management strategy to the process systems, two protection layers, i.e., Safety Instrumented System SIS1 and SIS2 to the Basic Process Control System (BPCS), are proposed to be implemented into the processes. When any disturbance causes the monitored variable to deviate away from the threshold(s) for normal operation, SIS1 will detect this deviation, evaluate its risk, and then take corresponding action(s) to maintain the safety of the process system. In SIS1, the deviation of the controlled variable must have happened in the processes. To ensure the safety of the process system, SIS2 is implemented into the system development. In SIS2, before a deviation occurs, SIS2 can detect this deviation in advance, and evaluate its risk, then take corresponding action(s) promptly. After implementing the proposed strategy of SIS1 and SIS2, the Safety Integrity Level (SIL) of the safety system has upgraded from SIL1 to SIL3.

2.4 G2 Development Environment

For complex industrial processes, such as chemical, oil, and gas processes, consistently achieving quality and safety targets is a major challenge for process engineers. The heart of the challenge is to measure the quality accurately and to make effective process control and safety management decisions in real time. G2 software from Gensym Corporation provides services for mission-critical solutions that automate decisions in real time. G2 software applies real-time rule technology for decisions to optimize operations and to detect, diagnose, and resolve costly problems.

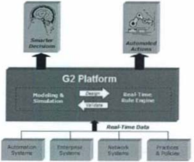

Fig. 24 G2 Platform from Gensysm Corporation

G2 is a complete development environment for creating and deploying intelligent real-time applications. With the flexibility of G2 software, it can be used in the following complex situations:

- Monitoring, diagnosis, and alarm handling.
- Supervisory and advanced control.
- Process design, simulation, and re-engineering.
- Intelligent network management.
- Decision support for enterprise-wide operations.

G2 development environment is a graphical environment. Almost everything in G2 has a graphical representation. The system-defined display items in G2 can show the state of the application as it changes over time, and the system-defined buttons can be used to send commands to G2 or the outside world. Besides, G2 uses a structured natural language in programming statements. The G2 language is similar to ordinary human language, so the application development programmed with G2 language is easier to read.

G2 offers Gateway Standard Interface (GSI) network and interfacing capability. The G2 Gateway Standard Interface (GSI) is a network-oriented toolkit used for developing software interfaces, or bridges, between G2 and other, external systems. G2 Gateway allows KBs to exchange various types of data between a G2 process and the bridge.

GDA, the G2 Diagnostic Assistant, is a layered product built on top of G2. GDA is a visual programming environment for developing intelligent applications that monitor and control real-time processes. A GDA application contains schematic diagrams that

- Acquire data from real-time processes.
- Make inferences based on the data.
- Take actions based on the inference values, such as raising alarms, sending messages to operators, or concluding new setpoints.

The principal component of the GDA is a graphical language that lets you express complex diagnostic procedures as a diagram of blocks, also called an Information Flow Diagram (IFD). These blocks are connected by paths that show how data flows through the diagram.

GUIDE, the G2 Graphical User Interface Development Environment, is a development tool that enables users to create graphical user interfaces (GUI's) for G2 applications. A G2 GUIDE user interface can be constructed by using the graphical components called UIL (User Interface Library) controls. GUIDE/UIL provides an application programmer's interface (API) to procedures that control dialogs and other elements of a graphical user interface. GUIDE supports different classes of UIL controls for different purposes:

- Some classes of UIL controls, such as edit boxes, buttons, and scroll areas, enable users to view and edit the data stored in object attributes. The different classes are suitable for viewing and editing different types of data.
- Other classes of UIL controls, such as borders and separators, enable users to organize a user interface visually.

In this research, integrated G2 development environment, i.e., the integration of G2& GDA & GUIDE, is used to develop application systems including the Tank Filling System and the Steam Power Plant System, and is also used to verify the proposed methodology of risk-based SPC fault diagnosis and safety management for process system. Recently, most fault diagnosis using G2 software employ the expert system approach. To demonstrate the advantages of the proposed methodology over expert system, a comparison will be held between these two approaches in Chapter 4.

Chapter 3 Implementation and Verification of the Proposed Methodology in G2 Development Environment — Tank Filling System

In order to testify the proposed methodology of risk-based SPC fault diagnosis and safety management for process system, from this chapter to next chapter, two process systems are built in G2 development environment. The first process system is a tank filling system, a tank level monitor, in process industry, as will be described and studied in this chapter. The second process system is a steam power plant system located in Thermodynamics and Fluids Lab in Faculty of Engineering and Applied Science building at Memorial University of Newfoundland, as will be described and studied in Chapter 4.

In this chapter, the proposed methodology is implemented and verified in the G2 development environment through developing a tank filling system. Meanwhile, the proposed methodology is testified that it neither depends on any model, nor depends on large historical data. At the end of this chapter, to demonstrate the advantages of the proposed methodology, a comparison between the tank filling system developed with the proposed methodology and a traditional design for the same system is held.

3.1 Requirements to the Tank Filling System

In this chapter, a tank filling system, i.e., a tank level monitor, is to be developed in G2 development environment. In this system, tank is filled with inflow liquid through a manual valve. The basic process control to this filling system is to maintain the controlled variable, the tank level, at some desired value, i.e., the set point. If some disturbance causes the tank level deviate away from its set point, some protection layers, i.e., safety instrumented systems, should be added into this system to ensure system safety. The tank filling system to be developed should have the following functions:

- Popping up warning message when tank level reaches some limit;
- Raising alarm when tank level exceeds upper control limit;
- Raising alarm when there is a fault and then shut down the system;
- Raising alarm and shut down the system immediately when there is an excessive deviation in inflow.

According to the requirements to the tank filling system to be developed, three development stages will be conducted and studied in three subsequent sections. These three development stages are deterministic stage, SPC stage and risk-based SPC stage.

In deterministic stage, the console for the tank filling system containing basic process control system BPCS, protection layer SIS1 and protection layer SIS2 is built in G2 development environment, and the basic functions for this filling system are provided.

In SPC stage, statistical technique of moving average is used to filter out the noise disturbances. Statistical technique of control chart is used to monitor the tank level in the whole process of the tank filling system. Besides, to ensure an event is a fault, the fault is defined as three successive data points of tank level exceed the upper control limit 6 m. In risk-based SPC stage, risk indicator is introduced into the methodology to reduce the number of false alarms, real time monitoring to the process is performed, and forecast function to the fault event is conducted.

3.2 Deterministic Development Stage

1. The Console Construction of the Filling System

The purpose of a BPCS is to maintain the controlled variable at its set point. In this tank filling system, the controlled variable is the tank level. The set point for the tank level is set to 5 m. Other parameters of the tank are set as follows: The area of the tank is 100 m^2, the maximum level is 20 m, the upper extreme level is 6 m, and the lower extreme level is 4 m. According to the requirements, the tank filling system with BPCS is designed as Fig. 25.

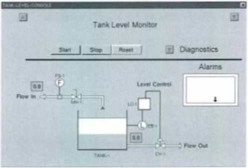

Fig. 25 Console of the Tank Level Monitor with BPCS

In Fig. 25, the liquid flows into tank through a manual valve MV-1, and the inflow rate is measured by a flow sensor FS-1. The BPCS is composed of a level sensor LS-1, a proportional controller LC-1 and a control valve CV-1. The purpose of BPCS is to maintain the tank level at its set point 5 m.

If any disturbance causes the tank level deviates from its set point, it is dangerous some time in process engineering, some protection layer must be added into this system to ensure system safety. Fig. 26 shows the filling system with adding one protection layer of safety instrumented system SIS1.

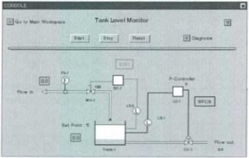

Fig. 26 Console of the Tank Level Monitor with BPCS & SIS1

In SIS1 in Fig. 26, the SIS1 is composed of a level sensor LS-2, a controller SC-1 and the manual valve MV-1. If any disturbance causes the tank level deviates away from its set point 5 m, the SIS1 will perform its safety function and take some actions to bring the system to a safe state. In this development for SIS1, the sensor LS-2 detects the current tank level, if the tank level exceeds set point, i.e., a fault event happens, a warning message will pop up to warn the operator. If the tank level exceeds the upper extreme limit 6 m, an alarm will be raised to alert operator to shut down the system, and if the operator fails to shut down the system in specified time period, the manual valve MV-1 will be shut down automatically by the controller SC-1.

In SIS1, the effects of a disturbance must propagate through the process before some actions are taken, that means a fault evert must have occurred. From safety point of view, it is not an ideal approach to ensure system safety. The best strategy for process safety is to take action(s) before a fault happens. That is the reason for adding protection layer SIS2 in this filling system as shown in Fig. 27.

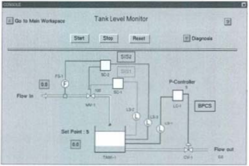

Fig. 27 Console of the Tank Level Monitor with BPCS & SIS1 & SIS2

In Fig. 27, SIS2 is added into the filling system to ensure the system safety. SIS2 is composed of a level sensor LS-3, a controller SC-2, a flow rate sensor and the manual valve MV-1. In SIS2, the controlled variable is still tank level, the manipulated variable is the inflow rate, and what is concerned more herein is the inflow volume in one unit of sample time. If we calculate the coming tank level exceeds the upper limit 6 m through using the current inflow volume in one sample time period and the current tank level, then some actions can be taken before the fault event happens, i.e., the tank level exceeds the upper limit 6 m. Therefore, by using SIS2 in the development system, the fault event can be detected and identified in advance, and this has greatly improved the system safety and reliability.

2. SIL Evaluation

SIL is defined as a relative level of risk-reduction provided by a safety function. According to the IEC61511, the SIL of the developed tank filling system is evaluated in Table 8. In Table 8, SILs can be evaluated by using event tree analysis.

Table 8 Safety Integrity Level (SIL) Evaluation to the Tank Filling System

System Composition	PFDavg	Risk Reduction	SIL
BPCS	10^{-1} to 10^{-2}	10 to 100	SIL1
BPCS+SIS1	10^{-2} to 10^{-3}	100 to 1000	SIL2
BPCS+SIS1+SIS2	10^{-3} to 10^{-4}	1000 to 10,000	SIL3

From Table 8, we can see: After applying two protection layers, SIS1 and SIS2, the system safety integrity level has upgraded from SIL1 to SIL3.

3. The Functions Realized in Deterministic Stage

- Popping up warning message when tank level exceeds set point 5 m;
- Raising alarm when tank level exceeds upper limit 6 m;
- Raising alarm when tank level is out of control and then shut down the system in specified time period (in SIS1);
- Popping up dangerous warning message, raising alarm and shutting down the system immediately when there is an excessive deviation in the inflow (in SIS2).

3.3 SPC Development Stage

In the deterministic development stage, only a set of deterministic results can be obtained, there are not noise filtering technique applied to the filling system to filter out noise disturbances which could lead to false alarms, and the developed fault diagnosis function cannot perform real time monitoring to the whole process. In addition, the determination of the fault is that one data point of tank level exceeds the upper limit 6 m, then the actions like raising alarm and shutting down the system will be taken, which will increase the probability of false alarms. Therefore, SPC fault diagnosis and safety management (SIS1 & SIS2) method is introduced to overcome the aforementioned disadvantages in deterministic development stage.

In SPC development stage, statistical technique of moving average is used to filter out the noise disturbances. Statistical technique of control chart is used to monitor the tank level in the whole process of the tank filling system. Besides, using control chart and three-sigma rule, if three successive data points of tank level exceed the upper limit 6 m, then this is defined as a fault event.

1. The Developed Control Chart

The developed control chart for the tank filling system is shown in Fig. 28.

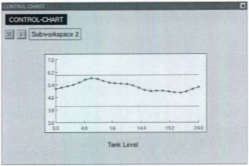

Fig. 28 Control Chart for the Tank Filling System

2. The Functions Realized in SPC Stage

- Popping up warning message when tank level exceeds set point 5 m;
- Raising alarm with severity 1 when tank level exceeds upper limit 6 m;
- Raising alarm with severity 2 when three successive data points of tank level exceed upper limit 6 m;
- Raising alarm with severity 3 when tank level is in range [6.1, 6.2], then shut down the system in specified time period (in SIS1);
- Popping up dangerous warning message, raising alarm with severity 4 and shut down the system immediately when there is an excessive deviation in the inflow (in SIS2).

3.4 Risk-based SPC Development Stage

Although in SPC development stage, the developed fault diagnosis and safety management system overcomes the disadvantages existing in deterministic stage, there is not forecast capability in the SPC fault diagnosis and safety management stage. Forecast capability is a very important characteristic for a fault diagnosis and safety management system. Using forecast capability, potential risks of the industrial processes can be identified and corrected, thus it can reduce the hazards to people, property and environment. Another drawback in SPC stage is the number of the alarms is still high. Besides, in SPC stage, real time monitoring function has not been implemented.

In order to minimize the number of alarms, perform real time monitoring to the processes and conduct forecast function to the fault event, the methodology of risk-based SPC fault diagnosis and its integration with safety instrumented system SIS1 & SIS2 is introduced in this stage. The developed console for the tank filling system is shown in Fig. 29. Since this risk-based SPC fault diagnosis and its integration with safety instrumented system SIS1 & SIS2 is the finalized proposed methodology, it will be described in detail as below.

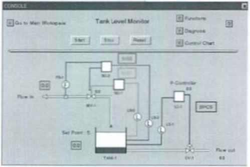

Fig. 29 Risk-based SPC Fault Diagnosis and SISs for Tank Filling System

3.4.1 Characteristic Functions and Fault Definition

1. The Implementation of Risk Calculation in G2 Development Environment

According to the risk calculation analysis in Chapter 2 for risk-based SPC fault diagnosis, the equations are obtained as follows:

When $x^{'} \geq 0$,

$$erf(x^{'}) = \sqrt{1-\exp(-x^{'2}\frac{4/\pi + ax^{'2}}{1+ax^{'2}})} \qquad (3\text{-}1)$$

When $x^{'} < 0$,

$$erf(x') = -\sqrt{1-\exp(-x'^2 \frac{4/\pi + ax'^2}{1+ax'^2})} \qquad (3\text{-}2)$$

Where,

$$a = -\frac{8(\pi-3)}{3\pi(\pi-4)}$$

$$P(F) = \phi(x') = \frac{1}{2}[1 + erf(\frac{x'}{\sqrt{2}})] \qquad (3\text{-}3)$$

$$RI = Risk = P(F) * S = P(F) * 100^{P(F)} \qquad (3\text{-}4)$$

Note:

1. Risk calculation for the tank filling system is shown in the Table 11 in APPENDIX I.
2. The graphs of risk values with base 100 and with base e are shown in Fig. 56 and Fig. 57 in APPENDIX I.

To realize the calculation of the risk for the forecasted data points, related parameters, rules and functions are defined in the Procedure Definition workspace, Rule workspace and Function workspace in G2 development environment separately, and realized corresponding risk calculation through programming. Considering the transplant capability for the development, standardization and modularization designs are utilized. A rule definition added in the Rule workspace is shown in Fig. 30.

```
whenever stand-mov-ave receives a value
  and when stand-mov-ave > 0.0 then
  conclude that err-func = error-
  function(0.7071 * stand-mov-ave)
```

Fig. 30 An Example of Rule Definition in Tank Filling System

2. The Development of Forecast Function

To perform the best linear trend forecast, the previous three data points are used to do the best fit for a line, so we can obtain the best fit value for the third point and the rate of change, i.e., the slope, of the best fit line. With this best fit line, we can predict the value of next (fourth) data point. The data points of tank level moving average and their forecasted data points are shown in Fig. 31. Since what we concern in this filling system is whether the tank level exceeds the upper limit, only the upper control limit is drawn in the figure.

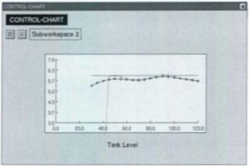

Fig. 31 Data Points in Time Order

In this chart, X axis is time, and Y axis is tank level. The red line is the upper control limit, corresponding to the tank level value 6 m. The black line with data points is the real tank level moving average value curve. The green line with data points is the predicted tank level moving average value curve.

3. Fault Definition in Risk-based SPC Development Stage

Fault is defined as three successive data points exceed some limit(s). In these three data points, two successive data points are the real values of the moving average of controlled variable, and the third successive data point is the predicted value of the moving average of controlled variable. For SIS1, when two successive real data points of the moving average of controlled variable exceed the upper control limit, and the third successive predicted data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, this event is defined as a fault. For SIS2, when two successive real data points of controlled variable are above the mean value, and the third predicted data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, this event is defined as a fault. For example, in SIS1 of the tank filling system, when two successive real data points of tank level moving average exceed the upper control limit 6 m, and the third successive predicted data point exceeds the upper control limit 6m, this event is defined as a fault, as shown in Fig. 32.

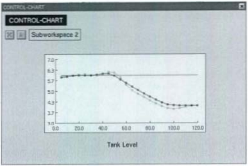

Fig. 32 Risk-based Tank Level Control Chart

In the charts in Fig. 31 and Fig. 32, the data points are in time order, but the time is not real time. To perform the real time monitoring to the processes, trend chart is introduced into the development to the tank filling system to display the results for SIS1 and SIS2.

3.4.2 The Development of SIS1

1. Fault Diagnosis for SIS1

In SIS1, to detect fault and take corresponding actions, the tank level data are measured by LS-2. After filtered out noise by using moving average technique with sample size 3, these tank level data become tank level moving average data. Then through performing linear trend forecast with sample size 3 and time horizon 5 seconds, the predicted tank level values can be obtained from these real data of tank level moving average. Later, through doing risk calculation to the predicted tank level data, we can obtain the values of risk indicator, and then take corresponding actions like raising alarm or shutting down system according to the risk values.

2. The Results of the Fault Diagnosis for SIS1

The results of fault diagnosis in SIS1 are shown in Fig. 33 and Fig. 34.

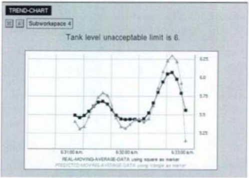

Fig. 33 Risk-based Tank Level Trend Chart – SIS1

In Fig. 33, X axis is the real time, and Y axis is tank level. The black curve is the real tank level moving average curve. The green curve is the predicted tank level moving average curve. We can see from this chart: when three successive data points of tank level exceed the upper control limit, that is, two successive real data points of tank level moving average exceed the upper control limit 6m, and one predicted tank level for the third data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, the system will be shut down.

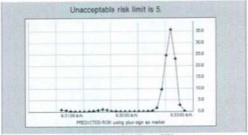

Fig. 34 Predicted Risk Chart – SIS1

In Fig. 34, X axis is the real time, and Y axis is the risk value. The black curve is the predicted risk curve for the predicted tank level. From this chart, we can see: when there is a fault, there will be a very sharp top in the curve.

3. The Realized Functions in SIS1

The realized functions in SIS1 are as follows:

- Popping up warning message when risk value for the predicted tank level is in range 1-5;
- Raising alarm with severity 2 when risk value exceeds 5, i.e., the predicted tank level exceeds upper control limit 6 m;
- Raising alarm with severity 3 when the real tank level exceeds upper control limit 6 m;

- Raising alarm with severity 4 when a fault happens, shutting down the system and highlighting the valve MV-1 in green.

3.4.3 The Development of SIS2

1. Fault Diagnosis for SIS2

In SIS2, to detect fault and take corresponding actions, the inflow rate is measured by FS-1. After filtered out noise by using moving average technique with sample size 3, these inflow rate data become inflow rate moving average data. Then through performing linear trend forecast with sample size 3 and time horizon 5 seconds, the predicted tank level values can be obtained from these real data of tank level moving average. Using the predicted tank level, the current outflow rate and the current tank level, we can obtain the predicted tank level. Later, through doing risk calculation to the predicted tank level data, we can obtain the values of risk indicator, and then take corresponding actions like raising alarm or shutting down system according to the risk values.

2. The Results of the Fault Diagnosis for SIS2

The results of fault diagnosis in SIS2 are shown in Fig. 35 and Fig. 36.

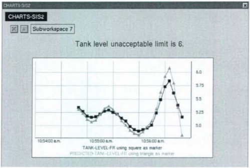

Fig. 35 Risk-based Tank Level Trend Chart – SIS2

In Fig. 35, X axis is the real time, and Y axis is tank level. The black curve is the real tank level curve, and the green curve is the predicted tank level curve (**Note:** The predicted tank level point is aligned with real tank level point by time, i.e., at the same time, the black point is the current level, and the green point is the predicted level). From this figure, we can see: when two successive real tank level data points are above mean value 5 m, and the third predicted data point exceeds the upper control limit 6 m, corresponding to the unacceptable risk limit 5, the system will be shut down.

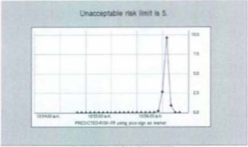

Fig. 36 Predicted Risk Chart – SIS2

In Fig. 36, X axis is the real time, and Y axis is the risk value. The black curve is the predicted risk curve for the predicted tank level. From this chart, we can see: when there is a fault, there will be a very sharp top in the curve.

3. The Realized Functions in SIS2

The realized functions in SIS2 are as follows:

- Raising alarm with severity 4 when there is an excessive deviation in inflow, shutting down the system and highlighting the valve MV-1 in red.

3.4.4 Discussion

In SIS2, the ideal situation is when two successive real data points of tank level are above the mean value 5 m and below the upper control limit 6 m, and the third predicted data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, the system will be shut down. However, there exists another scenario for this situation, that is, when the previous two successive real tank level points are above mean value 5 and below upper control limit 6, and the third predicted tank level is below the second data point and of course also below the upper control limit 6 m, then the next real tank level data point will occur, this real point value has the possibility of exceeding the upper control limit 6 m, as shown in Fig. 37. However, the likelihood of this situation is very low and the risk for this situation is acceptable.

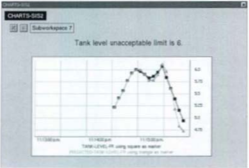

Fig. 37 Risk-based Tank Level Trend Chart – SIS2

3.4.5 Comparison with Cen Nan's Work

To demonstrate the advantages of the proposed methodology of risk-based SPC fault diagnosis and its integration with SISs, a comparison between the author's work and the previous developer Cen Nan's work (Nan et al., 2008) for the same tank filling system is held as follows.

The tank filling system developed by Cen Nan is shown in Fig. 38.

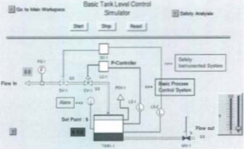

Fig. 38 Console of the Tank Filling System in Cen Nan's Work (Nan et al., 2008)

In this design shown in Fig. 38, there is one BPCS and one SIS. The BPCS is composed of a level sensor LS-1, a proportional controller LC-1 and a control valve CV-1, and it maintains the tank level at set point 5 m. The SIS is composed of a level sensor LS-2, a controller SC-1 and a manual valve SV-1. When the tank level exceeds the upper extreme value 6 m, which will raise an alarm to the operator, if the operator fails to close the SV-1 in some period, the SIS will close the SV-1 automatically. The fault diagnosis functions developed by Cen Nan are: when tank level exceeds upper extreme value 6 m, an alarm with severity 1 will be raised. When tank level is out of control, an alarm with severity 5 will be raised and system will be shut down.

In the tank filling system developed by Cen Nan, there are one BPCS and one protection layer SIS1, and the SIL for the developed system is SIL2. While in author's work for same system, there are one BPCS and two protection layers, i.e., SIS1 and SIS2. The SIL of the system developed by the author has reached SIL3.

Real time monitoring and forecast functions are essential to the fault diagnosis in process systems. In these two developed systems, both have real time monitoring function. However, there is not any chart in Cen Nan's system for visual display, and there is not forecast function in Cen Nan's system either. While in the author's system, we can perform the best linear trend forecast to the controlled variable, the tank level, and trend chart is used to display the real data points and the predicted data points in real time.

The fault diagnosis in Cen Nan's system is in deterministic mode, and there are not SPC fault diagnosis development and risk-based SPC development, so the number of false alarms is very high. In author's system, SPC control chart technique is used to distinguish abnormal situation from normal situation, and risk indicator is introduced into the fault diagnosis to minimize the number of false alarms.

The comparison between author's work for the tank filling system and Cen Nan's work is shown in Table 9.

Table 9: Comparison to Cen Nan's Work for the Tank Filling System

Characteristics	Cen Nan's System	Huizhi Bao's System
BPCS	Yes	Yes
SIS1	Yes	Yes
SIS2	No	Yes
Real Time Monitoring	Yes	Yes
Trend Chart	No	Yes
Forecast Capability	No	Yes
Deterministic Development	Yes	Yes
SPC Development	No	Yes
Risk-based Development	No	Yes
Noise Filtering	Yes	Yes
Additional Hardware for Noise Filtering	Yes	No
SIL	2	3

Chapter 4 Implementation and Verification of the Proposed Methodology in G2 Development Environment — Steam Power Plant System

The conventional SPC control chart method, which belongs to process history based method because a large amount of historical data are needed, was introduced into the process fault diagnosis in 1931 as the Shewhart control chart, and followed by others such as the cumulative sums chart in 1954. As the demand for product quality and process reliability is growing, the conventional SPC charts have been extensively used in industrial processes. Although the conventional SPC method is still valid now, it has vital limitation that the conventional SPC chart is a univariate control chart, and it can not handle multivariate processes and the correlation among controlled variables, thus MSPC techniques are extensively studied and used in industrial processes. Another vital limitation for the conventional SPC method is in the data acquisition technology. These two reasons are why the SPC method is not written into any branch in Fig. 13.

In this chapter, the proposed innovative methodology of risk-based SPC fault diagnosis and its integration with SIS is further implemented and verified in the G2 development environment through developing another process system, the steam power plant system. In the meantime, a technique breakthrough, from univariate monitoring to multivariate monitoring for SPC fault diagnosis, is made in this chapter. To demonstrate the advantages of the proposed methodology over other traditional methods, at the end of this chapter, a comparison between the steam power plant system developed with the proposed methodology and the traditional expert systems method for the same system is held.

4.1 Requirements to the Steam Power Plant System

The steam power plant is located in Thermodynamics and Fluids Lab in Faculty of Engineering and Applied Science building at Memorial University of Newfoundland, as shown in Fig. 39.

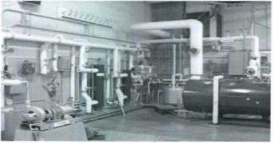

Fig. 39 Steam Power Plant in Thermodynamics and Fluids Lab

The schematic diagram of this steam power plant is shown in Fig. 40. This steam power plant is composed of a boiler, two superheaters, a turbine, a condenser, a condensate tank, a pump and other components like pressure sensors, temperature sensors etc. Steam is generated in the boiler, after flowing through two superheaters, it reaches and drives the turbine to produce electricity. This electricity will power ten electric bulbs. Flowing out turbine, the steam is condensed into water by condenser, and then flows into condensate tank to prepare to be pump into boiler together with the city water for later use.

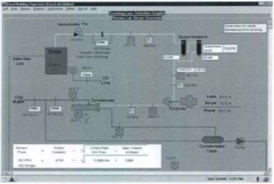

Fig. 40 Schematic Diagram of the Steam Power Plant

The development works for this steam power plant system include:

- Constructing the console of the steam power plant in G2 development platform;
- Modeling and simulating the entire process for the steam power plant in G2 environment;
- Designing BPCS, SIS1 and SIS2 to the controlled variables. In this development system, the controlled variables are three parameters of the boiler, that is, the steam flow rate, the steam pressure and steam temperature;
- Realizing a technique breakthrough, from univariate control to multivariate control for SPC fault diagnosis, in process fault diagnosis field.
- Applying the proposed methodology of risk-based SPC fault diagnosis and its integration with SIS into the developed steam power plant system.

The set points and maximums of the three parameters of the boiler are as follows: the set point and the maximum of the steam flow rate are 160 Kg/H and 166 Kg/H separately. For the steam pressure, they are 640 kPa and 690 kPa separately. For the steam temperature, they are 219 °C and 239 °C separately. When a fault event happens in any individual controlled variable, safety system SIS1 should pop up a warning message. When any risk of the three controlled variable is greater than 20, the SIS1 should raise an alarm of shutting down the system with severity 4. When the overall risk for the three parameters is in range 5-10, safety system SIS2 should pop up a warning message. When the overall risk is in range 10-20, the SIS2 should pop up a severe warning message. When the overall risk is greater than 20, the SIS2 should raise an alarm of shutting down the system with severity 4.

4.2 Console Construction in G2 Environment

According to the description to the steam power plant system, the developed console for this system is shown in Fig. 41 on next page.

In this console, there are mainly seven subworkspaces. They are Procedure, Function, Rule, Diagnosis, Charts, Assumption and GDA Interface subworkspaces. The Procedure workspace contains all the procedure, method and parameter definitions used in this development. All the functions used in this system are defined in the Function workspace, and all the rules are defined in the Rule workspace. The functions of fault diagnosis and safety management SIS1 & SIS2 are implemented in the Diagnosis workspace. The Charts workspace provides the real time trend charts and risk charts for the three controlled variables of the boiler in the steam power plant system. In the Assumption workspace, some assumptions about this system are listed, and in the GDA Interface workspace, some source signals are provided. In the steam power plant system, the three controlled variables are the steam flow rate, the steam pressure and steam temperature of the boiler. The BPCS for the steam flow rate consists of a flow sensor SG-FS-1, a controller SG-PC-1 and a control valve SG-CV-1. The BPCS for the steam pressure consists of a pressure sensor SG-PS-1, a controller SG-PC-2 and a control valve SG-CV-2. The BPCS for the steam temperature consists of a temperature sensor SG-TS-1, a controller SG-PC-3 and a control valve SG-CV-3.

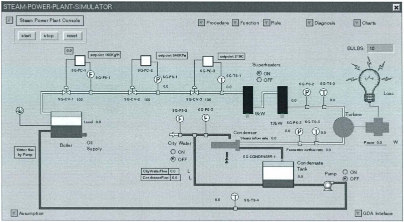

Fig. 41 Console of the Steam Power Plant System

4.3 System Modeling

During the development of the steam power plant system, many historical data records are collected from the Thermodynamics and Fluids Lab in the Engineering building in Memorial University of Newfoundland, and from the previous developer, Cen Nan, for this system.

According to the data records, we can obtain the historical data chart for the boiler steam pressure in the steam power plant system, as shown in Fig. 42.

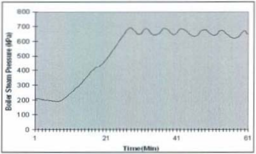

Fig. 42 Historical Data Chart for the Boiler Steam Pressure

As we can see in Fig. 42, from 200 kPa, the boiler steam pressure starts to rise and reaches the steady state (oscillation state) at about 700 kPa. Comparing this procedure with the characteristic of a second-order system of under-damped response shown in Fig. 43:

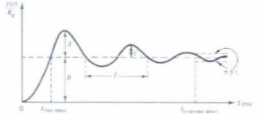

Fig. 43 Characteristics of an Under-damped Response

We can see that the historical data chart of the boiler steam pressure is very similar to the latter system, so we can model the boiler steam pressure with the second-order system of the under-damped response, that is:

$$f(t)=1-\frac{e^{-\xi\omega t}}{\sqrt{1-\xi^2}}\sin(\omega_d t+\tan^{-1}\frac{\sqrt{1-\xi^2}}{\xi})$$

Where,

$\omega_n =$ under-damped natural frequency

$\omega_d =$ damped natural frequency

$\xi =$ damping coefficient

Through analyzing the historical steam flow rate data, steam temperature data, steam pressure data and Control & Electrical data, and together with analyzing the physical process of the steam power plant system, other parameters or components can be modeled with the response of the first-order system, that is:

$f(t)=K(1-e^{-t/\tau})$ Where, τ = time constant

4.4 The Implementation of the Proposed Methodology

The proposed methodology of risk-based SPC fault diagnosis and its integration with SIS is implemented in G2 development environment in two stages, that is, SPC stage and risk-based SPC stage. These two development stages will be conducted and studied in two subsequent sections. In SPC development stage, control chart is used to distinguish abnormal situation from normal variation of controlled variable based on three-sigma rule and linear trend forecast. To minimize the number of false alarms, in risk-based SPC development stage, risk indicators are used to identify and determine potential fault(s).

In the steam power plant system shown in Fig. 41, the controlled variables are three parameters of the boiler, that is, the steam flow rate, the steam pressure and steam temperature. In normal situation, the corresponding BPCS maintains individual controlled variable at its set point. When there is a fault or the risk value exceeds some limits, safety instrumented systems should provide warning messages or raise alarms of shutting down the system.

4.4.1 SPC Development Stage

In SPC development stage, control chart of the individual controlled variable is developed. To illustrate this development stage, one of the controlled variables, the boiler steam pressure, is chosen to conduct the procedure. In this stage, all the functions that Cen Nan's system has have been completed. To demonstrate the effectiveness of this SPC fault diagnosis system, an experiment is held in this stage.

1. Fault Diagnosis in SPC Stage

In the fault diagnosis module, the main task is to construct and develop the control charts for the process variables. Control chart is used to distinguish abnormal situation from normal variation of controlled variable based on three-sigma rule.

2. The Development of Control Chart

The developed control chart for the steam pressure of the boiler in the steam power plant system is shown in Fig. 44.

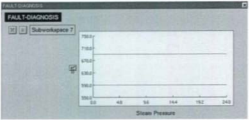

Fig. 44 Control Chart of the Steam Pressure in Steam Power Plant System

Fig. 44 indicates two control limits, the upper control limit 690 kPa and the lower control limit 590 kPa for the steam pressure using two red lines. In normal situation, real time data of the steam pressure moving average should fall into the [590 kPa, 690 kPa], the range between two red lines as shown in Fig. 45. If there is a real time data which falls outside of this range as shown in Fig. 46, then a fault could occur. In this system, when the real time data exceed the upper control limit 690 kPa, there could be a fault.

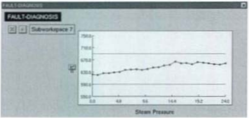

Fig. 45 Control Chart of the Steam Pressure in Steam Power Plant System (Normal Situation)

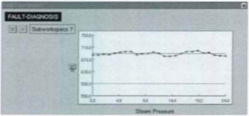

Fig. 46 Control Chart of the Steam Pressure in Steam Power Plant System (Abnormal Situation)

To ensure the aforementioned event is a fault, the number of successive values that exceed the upper control limit is set to 3. That means an alarm will be raised if there are more than 3 times (inclusive) that the successive monitored value exceeds the upper control limit. Besides, to detect and predict the fault event, another condition for raising recurring alarm is set. The condition is if there are more than 3 times (inclusive) that the monitored value exceeds the upper control limit in an hour.

3. An Experiment for Effectiveness Demonstration

To demonstrate the effectiveness of the developed SPC fault diagnosis system with traditional fault diagnosis systems, the developed SPC fault diagnosis module was put into the same steam power plant system developed by Cen Nan whose fault diagnosis method is knowledge-based real-time approach, which belongs to the Expert Systems branch in Fig. 13 and is abbreviated to KBRT approach in later description, as shown in Fig. 47.

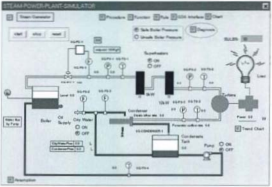

Fig. 47 Cen Nan's Steam Power Plant System + Huizhi Bao's Diagnosis Module

Through the assumptions made in Assumptions workspace in Cen Nan's system (Same assumptions are made in author's development), as shown in Fig. 48, the SPC

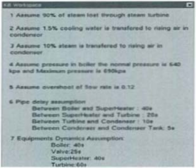

Fig. 48 Assumptions in Cen Nan's Steam Power Plant System

fault diagnosis module detected the following problems that exist in Cen Nan's system with KBRT fault diagnosis module:

(1). Raising false alarms when the steam pressure data are still safe.

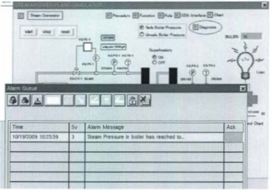

Fig. 49 False Alarm in Cen Nan's Steam Power Plant System

From 310 kPa for the steam pressure when in heating period, the system keeps raising alarms with the Alarm Message **Steam Pressure in boiler has reached to an unsafe point, Pls be careful**.

(2). Raising false alarms when the steam pressure is still in safe range, i.e. [590 kPa, 690 kPa].

At 645 kPa and 669 kPa, the system raised alarms with the Alarm Message **Steam Pressure in boiler has reached to a critical point, Pls be report to an engineer**.

From the point of the kb file capacity, the kb file developed by Cen Nan using KBRT fault diagnosis approach is 957 KB, while the kb file using SPC fault diagnosis approach is 431 KB.

From this experiment, we can see the SPC fault diagnosis is more effective and accurate in fault diagnosis in process system. Using control chart, the controlled variable is monitored and displayed clearly. This feature makes the SPC fault diagnosis approach more intuitive. In addition, the SPC fault diagnosis approach is more compact than the traditional knowledge-based real time (KBRT) approach, i.e., the traditional expert systems approach.

4.4.2 Risk-based SPC Development Stage

In SPC development stage, there is not forecast capability in the steam power plant system, the number of the alarms is still high, and the function of real time monitoring has not been implemented. In order to minimize the number of alarms, perform real time monitoring to the processes and conduct forecast function to the fault event, the methodology of risk-based SPC fault diagnosis and its integration with safety instrumented system SIS1 & SIS2 is introduced in this stage. A technique breakthrough, from univariate monitoring to multivariate monitoring for SPC fault diagnosis, is made in this stage, and so is the correlation problem among multiple variables. The developed console for the steam power plant system is shown in Fig. 38. Since this risk-based SPC fault diagnosis and its integration with safety instrumented system SIS1 & SIS2 is the finalized proposed methodology, it will be described in detail as below.

4.4.2.1 Characteristic Functions and Fault Definition

1. The Implementation of Risk Calculation in G2 Development Environment

According to the risk calculation analysis in Chapter 2 for risk-based SPC fault diagnosis, the equations are obtained as follows:

When $x^{'} \geq 0$,

$$erf(x') \approx \sqrt{1-\exp(-x'^2 \frac{4/\pi + ax'^2}{1+ax'^2})} \qquad (4\text{-}1)$$

When $x' < 0$,

$$erf(x') \approx -\sqrt{1-\exp(-x'^2 \frac{4/\pi + ax'^2}{1+ax'^2})} \qquad (4\text{-}2)$$

Where,

$$a = -\frac{8(\pi-3)}{3\pi(\pi-4)}$$

$$P(F) = \phi(x') = \frac{1}{2}[1 + erf(\frac{x'}{\sqrt{2}})] \qquad (4\text{-}3)$$

$$RI = Risk = P(F) * S = P(F) * 100^{P(F)} \qquad (4\text{-}4)$$

Note:

1. Risk calculation for the steam power plant system is shown in the Table 12 in APPENDIX II.
2. The graphs of risk values with base 100 and with base e are shown in Fig. 58 and Fig. 59 in APPENDIX II.

To realize the calculation of the risk for the forecasted data points, related parameters, rules and functions are defined in the Procedure Definition workspace, Rule workspace and Function workspace in G2 development environment separately, and realized corresponding risk calculation through programming. Considering the transplant capability for the development, standardization and modularization designs are utilized. A rule definition added in the Rule workspace is shown in Fig. 50.

```
whenever stand-pred-val-f receives a value
    and when stand-pred-val-f > 0.0 then
    conclude that pred-err-func-f = error-
    function-f(0.7071 * stand-pred-val-f)
```

Fig. 50 An Example of Rule Definition in Steam Power Plant System

2. The Development of Forecast Function

To perform the best linear trend forecast, the previous three data points are used to do the best fit for a line, so we can obtain the best fit value for the third point and the rate of change, i.e., the slope, of the best fit line. With this best fit line, we can predict the value of next (fourth) data point.

3. Fault Definition in Risk-based SPC Development Stage

Fault is defined as three successive data points exceed some limit(s). In these three data points, two successive data points are the real values of the moving average of controlled variable, and the third successive data point is the predicted value of the moving average of controlled variable. In SIS1, when two successive real data points of the moving average of controlled variable exceed the upper control limit, and the third successive predicted data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, this event is defined as a fault.

In SPC stage, the monitoring to the controlled variable is not in real time. To perform real time monitoring to the processes, trend chart is introduced into the development to the steam power plant system to display the results for SIS1 and SIS2.

4.4.2.2 The Development of SIS1 & SIS2

1. Fault Diagnosis for SIS1 & SIS2

In this stage, there are three controlled variables in the steam power plant system, they are the steam flow rate, the steam pressure and steam temperature of the boiler. The fault diagnosis procedure for every controlled variable is same with the description for the controlled variable of tank level in SIS1 of the risk-based SPC stage in the tank filling system. When two successive real data points of the moving average of controlled variable exceed the upper control limit, and the third successive predicted data point exceeds the upper control limit, corresponding to the unacceptable risk limit 5, this event is defined as a fault. When a fault happens in any individual controlled variable, safety system SIS1 pops up a warning message. When any risk of the three controlled variable is greater than 20, the SIS1 raises an alarm of shutting down the system with severity 4. When the overall risk for the three controlled variables is in range 5-10, safety system SIS2 pops up a warning message; when the overall risk is in range 10-20, the SIS2 pops up a severe warning message; when the overall risk is greater than 20, the SIS2 raises an alarm of shutting down the system with severity 4. In this process, as can be seen, the correlations among the three controlled variables are the summation of risks of three controlled variables is in range 5-10, 10-20 or greater than 20.

2. The Results of the Fault Diagnosis

The results of the fault diagnosis for the steam flow rate, the steam pressure and the steam temperature of the boiler are shown in the Fig. 51.

In Fig. 51, we can see that the three controlled variables, i.e., the steam flow rate, the steam pressure and the steam temperature of the boiler, are being monitored and analyzed simultaneously, so this process is a multivariate monitoring.

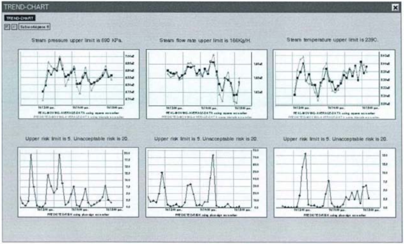

Fig. 51 Trend Charts for Steam Pressure, Steam Flow Rate and Steam Temperature &

Risk Carts for Steam Pressure, Steam Flow Rate and Steam Temperature

Some fault snapshots are shown in Fig. 52, Fig. 53 and Fig. 54.

Note:

1. In all the following figures, the predicted point is aligned with real point by time, i.e., at the same time, the black point is the current value, and the green point is the predicted value.
2. When there are two successive real values exceed the upper control limit, and one predicted value, i.e., the third successive point, exceeds the upper control limit, this situation is defined as a fault.

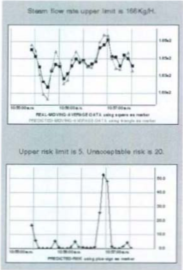

Fig. 52 Steam Flow Rate Trend Chart and Risk Chart

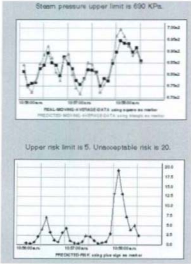

Fig. 53 Steam Pressure Trend Chart and Risk Chart

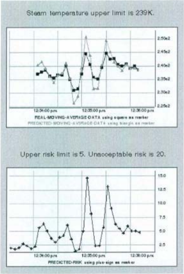

Fig. 54 Steam Temperature Trend Chart and Risk Chart

3. The Realized Functions in SIS1 & SIS2

The realized functions in SIS1 are as follows:

- When there is a fault in any individual variable, the system pops up a warning message.

- When any of the risk (risk of steam pressure, risk of steam flow rate, or risk of steam temperature) is greater than 20, the system raises the alarm of shutting down the system with severity of 4.

The realized functions in SIS2 are as follows:

- When the overall risk (risk of steam pressure + risk of steam flow rate + risk of steam temperature) is in range 5-10, the system pops up warning message.
- When the overall risk is in range 10-20, the system pops up severe warning message.
- When the overall risk is greater than 20, the system raises the alarm of shutting down the system with severity of 4.

In order to indicate the values of individual variable and its predicted value when they reach the extreme value, the following alarms are added:

- When the predicted value for any variable reaches the extreme value, the system raises an alarm with severity of 2.
- When the real value for any variable reaches the extreme value, the system raises an alarm with severity of 3.

4.4.2.3 Comparison with Traditional Approach

To demonstrate the advantages of the proposed methodology over other traditional fault diagnosis and safety management approaches, a comparison between the proposed risk-based SPC method and the knowledge-based real time (KBRT) approach developed by Cen Nan for the same steam power plant system is held as follows.

In the KBRT system, there is only one controlled variable, the steam pressure of the boiler, so it is univariate control. While in the risk-based SPC system, there are three controlled variables, i.e., the steam flow rate, the steam pressure and the steam temperature of the boiler, so it is multivariate control.

In the KBRT system, to produce fault in the steam pressure of the boiler, Unsafe Boiler Pressure button is specially set in the console to obtain high value unsafe steam pressure, as shown in Fig. 55. Using the Unsafe Boiler Pressure button, the obtained steam pressures are around 800 kPa. This indicates that the KBRT fault diagnosis system is not sensitive to fault event, and only with high values that the KBRT system can identify the fault and then take action(s). On the other hand, the maximum pressure for the boiler is 690 kPa, so these high values would destroy the boiler and/or other components in the steam power plant system. Whereas, the risk-based SPC fault diagnosis system is an accurate and sensitive diagnosis approach. It can capture any fault event according to the fault definition. Furthermore, the risk-besed SPC fault diagnosis system can forecast the fault and take action(s) in advance.

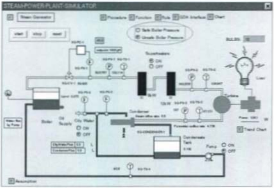

Fig. 55 Unsafe Boiler Pressure Button in Cen Nan's KBRT system

In the KBRT system, the outputs of FDD and SDD depend on the most recent five discrete input data, so the quality of those data could affect the accuracy of identification. This primitive identification approach creates an instantaneous recognition and the result cannot be changed later. Besides, in order to obtain accurate and reasonable results, the membership functions used in the analysis to the system output have to be adjusted for different fault events every time. In risk-based SPC system, the original real time data are directly used as the input to the fault diagnosis system, and the output of the fault diagnosis system are the exact data. In this way, we can avoid input dependency, and assure the accuracy in system output. Besides, since both input and output are exact data, the corresponding risk assessment to the system are also exact results.

In the KBRT system, noise is a major problem in primitive identification. There is no noise canceling technique used in this primitive identification approach. The input sensor data need to be filtered before performing any analysis. While in risk-based SPC system, moving average technique is used to eliminate the noise disturbance.

In the KBRT system, due to the uncertain characteristic of primitive identification and the similar shape between some primitives, it is impossible to perform an exact comparison, so Cen Nan introduced SI to decide the degree of approximation to do the trend analysis. While in risk-based SPC system, all the input, output and risk assessment are exact data or results.

In the KBRT system, to quantify the temporal pattern of sensor data, Cen Nan introduced another variable ROC to act as an input to the fault diagnosis system. Besides, in G2 environment, one fuzzy evidence gate only allows three combined if-then rules, therefore, if more rules are used, like in the KBRT fault diagnosis system, repeated or redundant components are used. In risk-based SPC system, redundancy avoiding design makes the system more compact.

In the KBRT system, the developed application can only be effective to the studied system (Cen etc., 2008). This means the methodology developed by Cen Nan is not good in extensibility. While the risk-based SPC system has excellent extensibility, not only it can be applied in the studied systems, the tank filling system and the steam power system, but also can be popularized to other industrial processes. Furthermore, after modification, it can be extended to be applied in the real time monitoring and prediction to natural catastrophes, such as tsunami, earthquake, etc. and even in economic analysis.

The comparison between the KBRT approach and the risk-based SPC approach for the steam power plant system is shown in Table 10.

Table 10: Comparison between the KBRT Approach and the Risk-based SPC Approach

Characteristics	KBRT approach	Risk-based SPC approach
Controlled Variable	Univariate	Multivariate
BPCS	Yes	Yes
SIS1	No	Yes
SIS2	No	Yes
Real Time Monitoring	Yes	Yes
Forecast Capability	No	Yes
Risk-based Development	No	Yes
Noise Filtering	Yes	Yes
Additional Hardware for Noise Filtering	Yes	No
SIL	2	3
Independency	No	Yes
Redundancy	Yes	No
Adaptability	Not Good	Excellent
Sensitivity to Fault	Not Good	Excellent
Extensibility	Not Good	Excellent

Chapter 5 Characteristics of the Proposed Methodology

From the verifications and descriptions of the tank filling system in Chapter 3 and the steam power plant system in Chapter 4, we can see that the proposed methodology of risk-based SPC fault diagnosis and its integration with safety instrumented systems has the following characteristics:

1. Adaptability

In the fault diagnosis and safety management to process systems, data analysis to the industrial processes data is indispensable. Statistics is a mathematical science pertaining to the collection, analysis, interpretation or explanation, and presentation of data (Moses etc., 1986). From the previous sentence, we can see that Statistics exists for data analysis. In the proposed methodology, statistical techniques like control chart, moving averages and time series are used to do data analysis to the real time monitored process data. Since Statistics is applicable to a wide variety of academic disciplines, including natural and social sciences, government, and business, the proposed methodology will have excellent adaptability to all kinds of industrial processes, and also to other various scientific technology fields.

2. Real-time Monitoring Capability

In the developed systems using the proposed methodology, real time monitoring to the controlled variable(s) is conducted, and both the inputs to the system and the outputs of the system are exact real time data. Using control chart and trend chart techniques, the outcome can be visually observed and monitored in real time, any fault or abnormal situation can not escape to be captured promptly.

3. Forecast Capability

Forecast capability is essential to a fault diagnosis and safety management system. Due to the use of time series and linear trend analysis techniques, the proposed methodology has excellent fault forecast capability to the real time data, and it can perform the best linear trend forecast to the process controlled variables with G2 software. This is very helpful for us to take corresponding actions in advance.

4. Effectiveness and Strong Safety Management Capability

The risk-based fault diagnosis and safety management system is effective both in fault diagnosis and in safety management to the process system. It can capture any fault event according to the fault definition. Furthermore, the risk-based SPC fault diagnosis and safety management system can forecast the fault and take action(s) in advance. This capability helps us to make precaution before faults happen and also offset the effect after faults have happened. After implementing SIS1 and SIS2 to the developed systems, the SIL of the developed systems has upgraded from SIL2 to SIL3.

5. Independency

Unlike in the KBRT system, the outputs of FDD and SDD depend on the most recent five discrete input data, and in order to obtain reasonable results, the membership functions used to analyze the system output have to be adjusted for different fault events every time. In risk-based SPC system, the original real time data are directly used as the input to the fault diagnosis system, and the output of the fault diagnosis system are the exact data. In this way, we can avoid input dependency, and assure the accuracy in system output.

6. Robust Capability

Moving average technique is commonly used with time series data to smooth out short-term fluctuations and highlight long-term trends. Mathematically, a moving average is also similar to the low-pass filter used in signal processing. In the developed risk-based SPC fault diagnosis and safety management systems, moving average technique is used to filter out noise from the real time data. This increases the system robust capability.

7. Transplantable Capability

Considering the transplantable capability for the developed system, standardization and modularization designs are used in the development. Thereby, program can be transplanted from one system to another easily. This increased the flexibility of system development.

8. Reasonability in System Design

Considering the possible future application in practice, some functions are implemented in the software, i.e., in the programs. This capability decreased the number of hardware components in system, and correspondingly reduced the size of system and the cost for development and implementation in practice.

9. Extensibility

The risk-based SPC system has excellent extensibility, not only it can be applied in the studied systems, the tank filling system and the steam power system, but also it can be popularized to other industrial processes. Furthermore, after modification, it can be extended to be applied in the real time monitoring and prediction to natural catastrophes, such as tsunami, earthquake, etc. and even in economic analysis.

10. Multiple Fault Identifiable Capability

The ability to identify multiple faults is an important but a difficult requirement

(Venkatasubramanian et al., 2003). In the risked-based SPC fault diagnosis and safety management system, multiple faults identification has been completed successfully. The breakthrough from univariate monitoring to multivariate monitoring for SPC fault diagnosis has been made in this research, and also the correlation problem among the multiple controlled variables has been solved.

Chapter 6 Conclusion and Future Work

6.1 Conclusion

There are abundant literatures on process fault diagnosis approaches which range from analytical redundancy to knowledge-based systems and neural networks. Broadly, the existing process fault diagnosis approaches can be classified into three general categories. They are quantitative model-based methods, qualitative model-based methods, and process history based methods. Quantitative model-based method is impractical to be utilized in real industrial processes because of system complexity, high dimensionality and process nonlinearity. Qualitative model-based method will generate spurious solutions when reasoning with qualitative models. While the conventional process history-based method needs large amount of historical process data. For these above reasons, Venkatasubramanian et al. (2003) even propose to develop hybrid systems to overcome the limitations of individual approach. In this situation for fault diagnosis in process engineering and the safety incidents that lead to the serious consequences for people, the environment and property, an innovative methodology of risk-based SPC fault diagnosis and its integration with Safety Instrumented System (SIS) for process systems is proposed in this research.

The proposed methodology of risk-based SPC fault diagnosis and safety management neither depends on the process models as model-based methods, nor depends on large amount of historical process data as conventional process history based method. Earlier developed control charts are used to distinguish abnormal situation from normal operation based on three-sigma rule and linear trend forecast. To minimize the number of false alarms, risk indicators are used to identify and determine potential fault(s).

In order to testify the proposed methodology, two process systems are built in G2 development environment. The first process system is a tank filling system in process industry, and the second process system is a steam power plant system located in Thermodynamics and Fluids Lab in Faculty of Engineering and Applied Science building at Memorial University of Newfoundland.

Through the verification of the proposed methodology in the tank filling system in Chapter 3, we can see that all the thresholds, including the maximum volume for the tank, were designated by the designer, and no model is needed in the fault diagnosis and safety management process. Therefore, the fact that the proposed methodology neither depends on any model, nor depends on large historical data has been verified. Further, through the comparison between the tank filling system developed with the proposed methodology and a traditional design for the same system from the previous developer Cen Nan, we can conclude the advantages of the former system over the latter system as shown in Table 9.

Through the verification of the proposed risk-based SPC fault diagnosis and safety management methodology in the steam power plant system in Chapter 4, we can see that the proposed methodology neither depends on any model, nor depends on large historical data, because in the steam power plant system, we just need to know the normal operation values and the extreme limits for the component parameters, while these normal operation values and the extreme limits are just like the nominal values and specification limits for a component, such as a capacitor or a breaker in a circuit. Above all, in this verification, a breakthrough has been made, that is, the breakthrough from univariate monitoring to multivariate monitoring for SPC fault diagnosis, and also the correlation problem among the multiple controlled variables has been solved. Further, through the comparison between the steam power plant system developed with the proposed methodology and the traditional expert systems method for the same system, we can conclude the advantages of the former system over the latter system as shown in Table 10.

From the verifications and descriptions of the tank filling system in Chapter 3 and the steam power plant system in Chapter 4, it can be concluded that the proposed methodology of risk-based SPC fault diagnosis and its integration with safety instrumented systems has 10 outstanding characteristics, such as Accuracy, Real-time Monitoring Capability, Forecast Capability, etc. as described in Chapter 5. With these 10 outstanding characteristics, this proposed methodology is desired to be the ideal solution for the fault diagnosis and safety management in the process engineering.

In summary, the main conclusions for this research are as follows:

- An innovative methodology of risk-based SPC fault diagnosis and its integration with SIS for process systems has been proposed.
- The proposed methodology has been verified through two process systems that it neither depends on any model as model-based approaches, nor depends on large amount of historical data as conventional process history based methods.
- A technique breakthrough, from univariate monitoring to multivariate monitoring for SPC fault diagnosis, has been achieved in this research.
- The advantages of the proposed methodology over Cen Nan's work for Tank Filling System are summarized in Table 9.
- The advantages of the proposed methodology over traditional expert system for Steam Power Plant System are summarized in Table 10.
- 10 outstanding characteristics of the proposed methodology are listed in Chapter 5.

6.2 Future Work

Introduced into the process fault diagnosis in 1931 as the Shewhart control chart, the conventional SPC charts have been extensively used in industrial processes. However, the conventional SPC fault diagnosis method is not written into any branch in Fig. 13, because there are two vital limitations for the conventional SPC fault diagnosis method. One is that the conventional SPC chart is a univariate control chart, and it can not handle multivariate processes and the correlation among controlled variables. The other vital limitation for the conventional SPC method is in the data acquisition technology.

In this research, the first limitation has been solved, that is, the breakthrough from univariate monitoring to multivariate monitoring for SPC fault diagnosis has been made, and also the correlation problem among the multiple controlled variables has been solved. So, the future works for this research are as follows:

1. Further develop the multivariate monitoring for the proposed methodology of risk-based SPC fault diagnosis and its integration with safety instrumented system (SIS).
2. Try to realize another breakthrough for the other limitation of the SPC fault diagnosis in the data acquisition technology.
3. Apply the proposed methodology which has broken through the two limitations into real process systems.

References:

Albazzaz, H. and Wang, Z. X. (2004). Statistical process control charts for batch operations based on independent component analysis. Ind. Eng. Chem. Res., 43, 6731-6741

Bowling, R. S., Khasawneh, T. M., Kaewkuekool, S. and Cho, B. R. (2009). A logistic approximation to the cumulative normal distribution. *Journal of Industrial Engineering and Management*, 2(1), 2013-0953.

Chang, S. Y. and Chang, C. T. (2003). A fuzzy-logic based fault diagnosis strategy for process control loops. *Chemical Engineering Science*, 58, 3395-3411.

Chen, A. and Elsayed, E. A. (2000). An alternative mean estimator for processes monitored by SPC charts, *International Journal of Production Research*, 38(13), 3093-3109.

Crowl, D. A. and Louvar, J. F. (2002). *Chemical Process Safety Fundamentals with Applications*(2nd ed.). New Jersey: Prentice Hall PTR.

Fawcett, H. H. and Wood, W. S.(1982). *Safety and Accident Prevention in Chemical Operations* (2nd ed.). New York: Wiley.

Flott, W. L. (2002), What is SPC? *Metal Finishing*, 100(2), 112-114.

Ghetie, M., Noura, H. and Saif, M. (1998). Fault diagnosis using balance equations methods and the algorithmic redundancy approach. Proceedings of the 37th IEEE Conference on Decision & Control. Tampa, Florida USA.

Ghodrati, B., Akersten, P. and Kumar, U. (2007). Spare parts estimation and risk assessment conducted at Choghart Iron Ore Mine: A case study. *Journal of Quality in Maintenance Engineering*, 13(4), 353-363.

Gruhn, P (1999), Safety Instrumented System Design: Lessons Learned, *Process Safety Progress*, 18 (2), 156-160.

Harms-Ringdahl, L. (2001). *Safety Analysis - Principles and Practice in Occupational Safety* (2nd ed.) Taylor & Francis, London.

Harms-Ringdahl L. (2009). Analysis of safety functions and barriers in accidents. *Safety Science*, 47, 353 - 363.

He, T., Xie, W., Wu, Q. and Shi, T. (2006). Process fault detection and diagnosis based on principal component analysis. Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, China.

Himmelblau, D. M. (1978). *Fault detection and diagnosis in chemical and petrochemical processes*. Amsterdam: Elsevier press.

IEC (International Electrotechnical Commission), (2001). Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (Standard IEC 61508). *IEC*, Geneva.

Jin, N. and Zhou, S. (2006). Signature construction and matching for fault diagnosis in manufacturing processes through fault space analysis. *IIE Transactions*, 38, 341 - 354.

Khan, I. F., Sadiq, R., and Husain, T. (2002). Risk-based process safety assessment and control measures design for offshore process facilities. *Journal of Hazardous Materials*, A94, 1–36

Kirkwood, D. and Tibbs, B. (2005). Developments in SIL determination. *Computing and Control Engineering*, 16(3), pp 21-27.

Knegtering, B. and Pasman, H.J. (2009). Safety of the process industries in the 21st century: A changing need of process safety management for a changing industry. *Journal of Loss Prevention in the Process Industries*, 19, 298-305.

Leonard, A. D. (1996). *Statistical Process Control* (2nd Ed.). New York, NY: Industrial Press Inc.

Lo, C. H., Wong, Y. K. and Rad, A. B. (2004). Model-based fault diagnosis in continuous dynamic systems. *ISA Transactions*, 43, 459-475.

Lo, C. H., Wong, Y. K. and Rad, A. B. (2006). Intelligent System for Process Supervision and Fault Diagnosis in Dynamic Physical Systems. IEEE transactions on industrial electronics, 53(2), 581-592.

Lundteigen, A. M. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, 20, 218 - 229.

Ma, C., Gu, X. and Wang,Y (2009). Fault diagnosis of power electronic system based on fault gradation and neural network group. *Neurocomputing*, 72, 2909–2914.

MacDonald, D. (2004). Practical Industrial Safety, Risk Assessment and Shutdown Systems for Industry. New York: Newnes.

Marszal, Edward M., & Mitchell, Kevin J. (2003). Defining Safety Instrumented Functions. *Safety Instrumented Systems for the Process Industry Conference*, 1-16.

Maurya, R. M., Rengaswamy, R. and Venkatasubramanian, V. (2004). Application of signed digraphs-based analysis for fault diagnosis of chemical process flowsheets. *Engineering Applications of Artificial Intelligence*, 17, 501 - 518.

Mohamed, L. and Ibrahim, A. S. (2002). Model-Based Fault Diagnosis via Parameter Estimation Using Knowledge Base and Fuzzy logic Approach. IEEE melecon, Cairo, EGYPT.

Moses, L. E. (1986), *Think and Explain with statistics*, Addison-Wesley.

Nan, C., Khan, F. and Iqbal, M. T. (2008). Real-time fault diagnosis using knowledge-based expert system, *Process Safety and Environmental Protection*, 86(1 B), 55-71.

Nemeth, E., Lakner, R. Hangos, K.M. and Cameron, I.T. (2007). Prediction-based diagnosis and loss prevention using qualitative multi-scale models. *Information Sciences*, 177, 1916 - 1930.

Ogata ,K. (2004). Modern Control Engineering. Upper Saddle River, N.J.: Prentice Hall.

Ong, H. K., Harvey, M. C., Shehab, L. R., Dechert, D. J. and Darisipudi, A. (2004). The effects of three statistical control charts on task performance. *Production Planning & Control*, 15(3), 313 - 323.

Orantes, A., Kempowsky, Lann, L. T. M.-V., and Aguilar-Martin, J. (2008). A new support methodology for the placement of sensors used for fault detection and diagnosis, *Chemical Engineering and Processing*, 47, 330 - 348.

Pham H. (2006), *Springer Handbook of Engineering Statistics*. New York: Springer.

Simani, S. and Fantuzzi, C. (2000). Fault diagnosis in power plant using neural networks. *Information Sciences*, 127, 125-136.

Singer, G. and Ben-Gal, I. (2007). The Funnel Experiment: The Markov-based SPC Approach. *Wiley InterScience*, 899 - 913.

Stavrianidis, P. and Bhimavarapu, K. (1998). Safety instrumented functions and safety integrity levels (SIL). *ISA Transactions*, 37, 337-351.

Summers, E. A. (2007). Safety Instrumented Systems, *Perry's Handbook of Chemical Engineering* (Fall ed.).

Venkatasubramanian, V., Rengaswamy, R. and Kavuri N. S. (2003). A review of process fault detection and diagnosis Part II: Quanlitative models and search strategies. *Computers and Chemical Engineering*, 27, 313-326.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, N. S. and Yin, K. (2003). A review of process fault detection and diagnosis Part III: Process history based methods. *Computers and Chemical Engineering*, 27, 327-346

Venkatasubramanian, V., Rengaswamy, R., Yin, K. and Kavuri, N. S. (2003). A review of process fault detection and diagnosis Part I: Quantitative model-based methods. *Computers and Chemical Engineering*, 27, 293-311.

Wheeler, D.J., & Chambers, D.S. (1992). *Understanding Statistical Process Control* (2nd Ed.). Knoxville, TN: SPC Press.

Wiegerinck, Jan A. M. (2002). Introduction to the Risk based design of Safety

Instrumented Systems for the process industry. *Seventh International Conference on Control, Automation, Robotics And Vision*, 1383-1391.

Zhang, J. (2006). Improved on-line process fault diagnosis through information fusion in multiple neural networks. *Computers and Chemical Engineering*, 30, 558–571.

APPENDIX I

Table 11: Risk Calculation for Tank Filling System

RanD	Standard	FaultPro	Sev-100	Sev-e	FP*S-100	FP*S-e	Sort-100	Sort-e
5.054846	-2.83546	0.002288	1.010592	1.002291	0.002312	0.002293	0.002312	0.002293
5.152497	-2.54251	0.005503	1.025666	1.005518	0.005644	0.005533	0.005644	0.005533
5.252601	-2.2422	0.012474	1.059128	1.012552	0.013212	0.012631	0.013212	0.012631
5.350631	-1.94811	0.025701	1.125647	1.026034	0.02893	0.02637	0.02893	0.02637
5.448623	-1.65413	0.04905	1.253432	1.050273	0.061481	0.051516	0.061481	0.051516
5.530392	-1.40882	0.079444	1.44174	1.082684	0.114537	0.086012	0.114537	0.086012
5.646788	-1.05964	0.144655	1.946751	1.155641	0.281608	0.167169	0.281608	0.167169
5.73465	-0.79605	0.213001	2.666876	1.237386	0.568048	0.263565	0.568048	0.263565
5.850024	-0.44993	0.326381	4.495331	1.385943	1.46719	0.452345	1.46719	0.452345
5.949793	-0.15062	0.440138	7.590591	1.552921	3.340906	0.683499	3.340906	0.683499
6.132433	0.397298	0.654426	20.3635	1.924038	13.32641	1.259141	5.004979	0.824733
6.211991	0.635974	0.737603	29.86804	2.090918	22.03077	1.542269	13.32641	1.259141
6.407414	1.222242	0.889192	60.03214	2.433163	53.38009	2.163549	22.03077	1.542269
6.56863	1.70589	0.955986	81.65287	2.601233	78.05898	2.486742	53.38009	2.163549
6.647102	1.941305	0.973889	88.67041	2.648224	86.35517	2.579078	78.05898	2.486742
6.715781	2.147344	0.984117	92.94673	2.675449	91.47046	2.632955	86.35517	2.579078
6.85196	2.555881	0.994704	97.59062	2.703924	97.07378	2.689604	91.47046	2.632955
6.000126	0.000378	0.500151	10.00694	1.64897	5.004979	0.824733	97.07378	2.689604

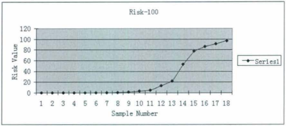

Fig. 56 Risk Value vs Sample Number Graph with Base 100

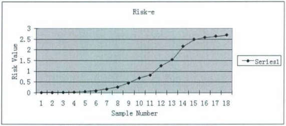

Fig. 57 Risk Value vs Sample Number Graph with Base e

APPENDIX II

Table 12: Risk Calculation for Steam Power Plant System

RanD	Standard	FaultPro	Sev-100	Sev-e	FP*S-100	FP*S-e	Sort-100	Sort-e
711. 2237	1. 273421	0. 898566	62. 68031	2. 456078	56. 32237	2. 206947	0. 003589	0. 003543
719. 3822	1. 762931	0. 961044	83. 57722	2. 614424	80. 32138	2. 512577	0. 016664	0. 015757
702. 1076	0. 726455	0. 76622	34. 07531	2. 151618	26. 10918	1. 648612	0. 05255	0. 044989
690. 0996	0. 005977	0. 502384	10. 11041	1. 652657	5. 079314	0. 830269	0. 243399	0. 151053
688. 0653	-0. 11608	0. 453794	8. 08328	1. 574273	3. 668142	0. 714395	1. 00708	0. 368528
680. 2289	-0. 58627	0. 278848	3. 611573	1. 321607	1. 00708	0. 368528	3. 668142	0. 714395
671. 4093	-1. 11544	0. 13233	1. 839331	1. 141485	0. 243399	0. 151053	5. 079314	0. 830269
661. 4019	-1. 71589	0. 043092	1. 219503	1. 044033	0. 05255	0. 044989	26. 10918	1. 648612
654. 0551	-2. 1567	0. 015515	1. 074062	1. 015636	0. 016664	0. 015757	56. 32237	2. 206947
645. 1015	-2. 69391	0. 003531	1. 016394	1. 003537	0. 003589	0. 003543	80. 32138	2. 512577
726. 8289	2. 209736	0. 986438	93. 94562	2. 681666	92. 67155	2. 645298	92. 67155	2. 645298
740. 1634	3. 009803	0. 998693	99. 39987	2. 714731	99. 26995	2. 711183	97. 58753	2. 694682
762. 723	4. 363378	0. 999994	99. 99705	2. 718264	99. 99641	2. 718247	99. 26995	2. 711183
733. 7204	2. 623225	0. 995645	98. 01439	2. 706469	97. 58753	2. 694682	99. 99641	2. 718247

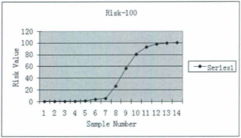

Fig. 58 Risk Value vs Sample Number Graph with Base 100

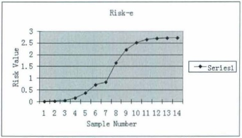

Fig. 59 Risk Value vs Sample Number Graph with Base e