

CENTER FOR INFORMATION INTEGRITY RESEARCH

B-64 (FF), Gulmohar Park, New Delhi – 110 049, INDIA

ELEMENTS OF INFORMATION INTEGRITY

(A Research and Knowledge Development Direction)

INDEX	Page No.
• THE QUESTION	
1. Information Integrity – An Introduction	2
2. Currently Practiced Business Model	2
3. System Failure Concerns Limited to Observable Incorrect Operations	3
4. The Question? – Indirect Consequences Of Incorrect production Of Information	4
• WHY?	
5. Business Realities Not Accounted	5
6. More On What Is Meant By Information As function Of <i>Recipient</i>	6
7. What are implications of not accounting business realities?	7
8. What change is needed?	8
• WHAT?	
9. A Structure for a Good Business Process Model	8
10. Critical Modeling Insights	10
11. Resulting shift in modeling assumptions of business process <i>IS</i> view	14
12. Inadequacy of existing integrity mechanisms	17
13. Information and its Usefulness and Usability Requirements	18
14. Criticality of Information Integrity for competitive advantage – Recognizing Origination of Information A Costly Activity	18
• HOW?	
15. Emerging Information Integrity Requirements	19
16. Guide words based approach to I*I Assessment for Deviation	21
17. A flowchart of I*I Analysis Process	23
18. The Content, Process and System Integrity Processes	24
19. Organization of information origination under uncertainty – Design basis for I*I Analyzer and Controller	26
Appendix 1: Defining Information Integrity Attributes	28
Appendix 2: More on Inadequacy of existing integrity mechanisms	30

ELEMENTS OF INFORMATION INTEGRITY

(A Research and Knowledge Development Direction)

Seeing what's in front of one's nose is a constant struggle.

George Orwell, 1946

Achieving Information Integrity is a constant struggle.

CIIR, 2003

ONWARD MARCH OF CONTROL REVOLUTION

“With advent of steam power, successes in production automation sharply increased the volume and speed of energy conversion and material processing. This precipitated various structured and periodic control responses for ‘standard’ product in high volume business model. With innovations in information technology, the volume and speed of information processing and decision-making has undergone sharp increases. Accordingly, business enterprises for their competitive survival are looking for bigger business opportunities through customized products” say Center for Information Integrity Research Workers. “For competitive advantage, this is requiring businesses to pass on the control baton to controlling Information Integrity of unstructured and aperiodic, i.e., continuous individual information origination and processing situation in the presence of uncertainty.”

1. INFORMATION INTEGRITY – AN INTRODUCTION

Information Integrity is dependability and trustworthiness of information and is a key factor determining strategic business advantage. Its determinants are accuracy, consistency, and reliability of information.

For more details, see Appendix 1.

2. CURRENTLY PRACTICED BUSINESS MODEL

- **Business Drivers are:**
 - Globalization, International competition and Changing Customer Expectations.
- **“Standard” product in high volume business model**
 - Its origin is in the high-volume mechanical manufacture,
 - Comprises physical work systems,
 - Which emphasize material and energy processing,
 - Treats business enterprise system as a closed system,
- **Nature of decision-making in the model**
 - A “collective” decision model,
 - Which is insensitive to customer requirements of local market factor based “individual” situations, and

- Wherein there is no room for local market factor based product beneficiation for strategic advantage,
- **Nature of information processing in the model**
 - Model has information systems,
 - Whose main concern is *only* that information technology accesses, communicates, processes and distributes the already generated information,
 - Which attend *only* to the “exactness” aspect of information requirement,
 - *The universal assumption is that data is perfect, once validated, and most information processing systems do not anticipate defective data.*
 - Accordingly, there is no requirement to originate local market factor based information on decision alternatives and on selection of information decision *endogenous* to decision situation.
- **Nature of allocation of internal organizational resources for information processing**
 - Strategy for competitive survival does not demand committing of organizational resources for information “origination”.
- **Cost of information processing and decision-making**
 - With information technology costs ever decreasing, information processing for decision-making is taken as a *costless* activity.
- **Control systems**
 - Model has input, process and output control systems,
 - Which are tuned to “fixed” i.e., “structured and periodic” data/information decisions determined exogenous to the decision situation.
- **Business objectives**
 - This makes for business objectives of: operational optimization and cost efficiency.
- **Model Assumptions**
 - Complete knowledge of initial condition (i.e., fixed information decision for control implementation),
 - Linearity of process, and
 - Availability on the part of the business enterprise system, its sub-systems and their components of unlimited (i.e., adequate) information processing resources.

3. SYSTEM FAILURE CONCERNS LIMITED TO OBSERVABLE INCORRECT OPERATIONS

Subject of investigational interest here is “integrity”. Integrity deviation is as result of errors, which stem from incorrect operation of a component, sub-system or system.

3.1 Consequences of mechanistic and system equipment failures

The discipline of reliability engineering extensively deals with the study of the consequences of incorrect operation **at two levels**, namely, **(i)** mechanistic failures, service disruptions, failure of computer hardware, etc., which are of stochastic type, and **(ii)** failure of system equipment that is controlled directly by the computer, i.e., by the requirement of correct functioning of the

computer hardware and its software. These studies are based on failure mode analysis methods, which use concepts of ‘fault’, ‘error’, ‘accident’ or ‘adverse event’ and “failure”.

3.1.1 Resulting in Observable Error and loss of Direct Integrity

Briefly, incorrect operation can be a cause or consequence of a fault, which is defined as a defect within a component, sub-system or system. Against this an error is a deviation from the required (standard) function/operation of the component, sub-system, or the system. Accordingly, an error is the mechanism by which the fault becomes apparent, i.e., observable.

An error may lead to a failure or an accident. A component, sub-system or system failure occurs when it fails to perform its required or desired function. And, an accident or adverse event (AE) is the danger (harm) to the *recipient*, i.e., customer, or to the environment, which is also treated as *recipient*. It may be mentioned that notion of “harm” includes ineffective and inefficient delivery of service to the customer. Obviously, like error, failure and adverse event are also observable. From this angle, resulting integrity, indicating the extent of loss of degree of adherence to desired function or desired purpose, can be termed as Direct Integrity.

3.2 Currently Practiced Direct Integrity Mechanisms

Under the “standard” product in high volume business model, where there is no requirement for local market factor based product beneficitation and wherein control systems are tuned to “fixed” information decision, error occurs in the “fixed” information decision, which is assumed known. Understandably, entire direct integrity effort through error reduction is based on the assumption that same error occurs and that, too, at the same location. Error, even if stochastic, is predictable, its moments being known. This leaves integrity concern limited to only “exactness” requirement of information and integrity mechanism attending only to consistency of internal objects of the component, sub-system or system, whose integrity is the concern.

Examples of such integrity mechanisms currently in vogue are Data Integrity, Auditing Solutions, Quality paradigm, Noise reduction technologies from communication systems, Subjective Utility Theory from Decision Theory, etc.

4. THE QUESTION? – INDIRECT CONSEQUENCES OF INCORRECT PRODUCTION OF INFORMATION

Recognition of incorrect operations at two functional levels as above brings in the question of consequences of incorrect operations **at the third level**, i.e., due to the incorrect production of information. This is a very real question. Literature reports one study across various types of systems, which attributes 40% of errors to material, electrical, and mechanical failures. The remaining 60% are attributed to information errors (see Section (10)).

Further, there is another - informational that is - angle to look at the mechanistic failure; that is to model it as a design failure. Specifically, what is construed to be otherwise observable failure can be seen as an indirect consequence of incorrect production of design. Process of design being an exercise in processing design information, this makes a case for viewing a mechanistic failure

(other than wear and tire), also, as an indirect consequence of information processing in a mechanistic situation.

Entirety of above visualization is a quantitative pointer to the recognition of need for reduction of information errors in a system development and implementation life cycle (*SDILC*) model, thereby leading to improvement in its Indirect Integrity, which understandably also accounts for Direct Integrity.

The present Information Integrity investigation precisely addresses this issue.

5. BUSINESS REALITIES NOT ACCOUNTED

CEOs and business managers operating modern complex enterprises are known to acknowledge value of information, but are observed to treat information rather as by-product and not as product. They are known to agree that data integrity and quality information are critical to business success, but are not always observed to commit internal resources of businesses to access and deliver quality information by their internal and external users. This is because information system (*IS*) model employed by the currently practiced business does not account for following business realities:

5.1 Business information as function of recipient

- **Required perception of reality:** With trend towards system integration and with internal and external user aspirations becoming increasingly local and instant, each of business enterprise many systems, their sub-systems and components represents a distinct environment (local market factor) with its own goals, norms, and practices. This makes business information processed a function of “source”, “process” and “recipient.”
 - **Existing incorrect perception of reality:** Prevailing business information systems, however, model information mainly as function of “source” only (information in this case is termed as “data”) and at the most of the “source” and the “process.”

5.2 Need for informational view of business enterprise system

- **Required perception of reality:** In a paradigm shift, above suggests an informational view of the business enterprise system as a potential source of data and information, and describes it as a network of interdependent business informational variables. Every material object contains no less than infinity of variables, i.e., facts, which are data and, when processed, information, and, therefore, possible systems. In the event of the reality of localized market factors, what is required is to *cull out* information variables that are relevant to the identified system or component goal (Usefulness factor).
 - **Existing incorrect perception of reality:** This system definition is at structural variance from that for “standard” product in high volume seeking currently prevailing business enterprise systems, which are described as “collection of objects united by some form of interaction or interdependence.”

5.3 Open system view of business

- **Required perception of reality:** This sets the basis for recognizing business enterprise system, its sub-systems and their components as open systems. Open systems are distinguished from closed systems in that they (open systems) have purpose (objective), possess porous boundaries with their environment, and, whatever else they do, they necessarily originate and process (import and export) information with their environment.
 - **Existing perception of reality:** These features are not present in closed systems. Specifically, “standard” product in high volume business model is a closed system as it is based on “fixed” information decision for control implementation and has no requirement to “manipulate” information decision smartly for maximizing information use for strategic advantage.

6. MORE ON WHAT IS MEANT BY INFORMATION AS FUNCTION OF *RECIPIENT*?

Information is at different levels.

6.1 Information as function of source

At one level, information refers to the potential message in an entity or event, or in reports about it. Information is viewed, in this context, as ‘data’, i.e., as a function of the source only.

6.2 Information as function of source and process

At another level, it refers to transmission of message; as a function of both source and means of conveyance as in communication theory, which uses probability to quantify the properties of symbols to convey message. Its primary value in studying management information systems lies in the key ideas of probability and reduction of uncertainty and notions of noise, lag and error in transmission.

6.3 Information as function of source, process and recipient

And at a higher level, information refers to the meaning gained by the recipient; the extent to which uncertainty is reduced and recipient knowledge increased. Information, in this context, is a function of source, process (includes communication medium and/or people) and the specific recipient.

6.3.1 Information as function of local market factors, i.e., condition of recipient

It is open system, which processes information as function of source, process and recipient. Here by “recipient” is meant condition of the recipient or rather of the recipient’s environment. These conditions constitute local market factors for the system under consideration.

For example, consider a circuit with a resistor, which is capable of dissipating one watt. It is expected the circuit will deliver required current. But incident takes place wherein this resistor is made to dissipate two watts and as a result the resistor fails, leaving system processing function of the condition of the recipient (instead of delivering required current, by failing to do so). Emerging issue is why is the supply value not validated? The **information-processing flaw** *here* is that, in ballistic behavior, taking (information) decision on value of the supply correct as already validated and not to anticipate error; that is **loss of Operational Integrity**.

Similarly, a mistake in a logic circuit design may result in a system giving an incorrect output for a local situation of given combination of inputs. The question then becomes that of **loss of Design Integrity**. And, in yet another situation, electromagnetic compatibility of a system may be compromised due to local changes of components during maintenance. The issue here is of **loss of Maintenance Integrity**.

6.3.2 Recipient covers a wide spectrum that includes software, machine, etc.

The question of loss of integrity critical though, what these examples tell is when one says information as function of recipient; it is not natural *here* to think of humans as recipient. *Recipient* covers concrete objects (machines, hardware), abstract objects (accounts, sales forecasts, policies), humans (external and internal customers, society), rules (established procedures), norms (codes of practice), commands (software, standing orders), etc. These recipients, along with source and process, comprise systems and components that are open systems. Accordingly, a distinct environment representing local market factors with unique goals, norms and practices, characterizes each of these. This makes the system processing, which in this case is information-processing, function of *these* recipients, which in fact is the main concern of the present investigation.

7. WHAT ARE IMPLICATIONS OF NOT ACCOUNTING BUSINESS REALITIES?

7.1 In ballistic behavior adherence by businesses to past practices of ensuring

Direct Integrity

CEOs and business managers persist with information processing methods in practice as of day, such as data integrity techniques, auditing solutions, mainly process-centered quality paradigm, etc., but invariably the exercise becomes end in itself, slowing down the process, and increasing failure risk.

7.2 Problems from poor data quality

- 75% businesses experience significant problems due to faulty data.
- 67% of businesses do not feel confident in the quality of their company's data.
- Many executives and industry experts suggest total cost of integrity related activities within an enterprise could be in the range of 1- 5% of revenue.
- Another study estimates poor data quality costs business \$611 billion per year in the United States alone.

7.3 Need to change business processes

These informational failures and resulting loss of integrity can now be seen as increasing problem as businesses move from crisis to crisis. Accordingly, businesses are experiencing need to change, the need being most severe when it comes to processes by which they are built and operated.

8. WHAT CHANGE IS NEEDED?

What is called for is simplification and speed through paradigm shift.

8.1 A Good Business Model

A competitive business strategy calls for a good understanding of business process, which in turn requires choice of a good business process model.

8.2 What are its characteristics?

- *Emphasizing* information,
- Comprising informational work system and physical work system, and
- Treating information as product.

8.3 What must it do?

For competitive advantage, informational work (IW) must be maximized. Specifically, informational work comprises activities of:

- (i) Originating from business process activities raw data/information, which is characterized by local market factors and by accompanying uncertainty and errors, and
- (ii) Processing this information on current basis for undertaking customized planning and evaluation of alternatives and delivering flexible information decision.

This points to modeling a generic business process covering enterprise wide supply chain (from design to delivery and follow-up), which accounts for physical work system, as integral to a closed loop information and control system model. We designate this as “business process *IS* view.” This is an open system view of an *IS*.

9. A STRUCTURE FOR A GOOD BUSINESS PROCESS MODEL

9.1 IS A Decision Process Model

Most information processing involves some type of data conversion to information in *use* and, therefore, is closely related to a decision process with an objective. Even when the information is transmitted without changing form, as in a communication system, the issue is to decide the purpose or objective of the transmission.

Traditionally, decision process is viewed to comprise stages of forecasting, evaluation of alternatives and selection; information being considered basically as function of “source” (i.e. as “data”) and at the most of “source” and “process”

9.2 Business Process IS View A Multistage Decision Process – A More Workable Decision Process Model

However, research in I*I show that for open system based business process *IS* view more workable model of a decision process spans multiple decision stages. These may be categorized

as (a) flexible information origination processes under informational work system and (b) information processing with reference to requirements of physical work system.

9.2.1 Comprises Information Origination Processes under Informational Work System

These decision process stages are:

- (A) Laundry List Preparation
- (B) Influence or Structure Diagram Preparation
- (C) Structure Characterization leading to *IS* View
- (D) Unstructured and Aperiodic Information Processing for Flexible Information Decision for Control Implementation

9.2.2 Comprises Information Processing for requirements of Physical Work System

Here decision process stages are:

- (E) Control Implementation
- (F) Plant Operation for product/system/service delivery to customer satisfaction

9.3 Information origination at each of decision process stages characterized by:

9.3.1 Dynamic Decision Making Requirements of:

- **IDILC Model:** Covering the process spectrum of information recognition and observation (origination), validation, storage, retrieval, manipulation, communication and distribution, *use*, and discard or storage for further use,
- **Endogenous Information Requirements:** Having a need to *originate* information requirements “*endogenous*” to *the* decision situation (local market factor). This is applicable particularly to Stages A-D and,
- **Implications of Delay:** Having a need to *originate* information requirements that start small and come with delay.

9.3.2 Uncertainty Implications of:

- **System Environmental factors:** What is of further consequence is all these decision process stages are impacted by system environmental factors of complexity, change, communication, conversion, and corruption (5”C”s). This gives rise to uncertainties and, hence, information errors leading to loss of Information Integrity in each of decision stages and in entire business process *IS* view and in information there from. This draws attention to an important question as follows.
- **Goal Change:** What if, in above *IS*, the “goal” leading to usefulness factor with reference to information originated, though given, continuously needs adjustment due to constantly changing environment or is not known or is out of date or is by itself complex? These are the conditions to be observed in the real world problem solving. Specifically this leads to following problem.
- **Dynamic nature of structure diagram preparation task:** Tasks of culling out relevant facts (usefulness factor with reference to data and information variables) and of defining their interrelationships under the subsequent decision stages of the business process *IS* view cannot be treated as static ones determined uniquely and exogenously as in case of closed systems, but would acquire dynamic - open and *endogenous* to the decision

making situation in that – character in the presence of 5“C”s, and they (data and information variables) would need to be *continuously* originated and processed.

9.4 Emerging Business Process IS View: Information Origination in presence of Uncertainty

This reality leads to model information processing under the business process *IS* view as a ***continuous individual information originating and processing situation in the presence of uncertainty***, so as to account for demands of continuously determined specific goal based individual situation in a complex and changing environment.

We designate this model as “**information origination in presence of uncertainty.**”

10. CRITICAL MODELING INSIGHTS

Having identified the structure of Business Process *IS* View, it should be useful to analyze it further particularly from the point of modeling factors that are critical but are not considered under “standard” product in high volume business model currently practiced.

10.1 Difference between treating information as product versus as by-product

Example in Sub-section (6.3.1) of a circuit with a resistor capable of dissipating one watt being made to dissipate two watts, considered a situation of circuit failing in its function due to failure of resistor. If successful functioning of the resistor and the circuit are seen as the system objective or operable goal, then many clarifications follow.

- (a) **Open system view and interconnection as entity:** Resistor is a component of the circuit. Let us assume the resistor component integrity is correct. In the circuit the resistor receives supply through voltage supply line, which represents the *interconnection* between the supply and the component. For the investigation at hand, this interconnection, which the “supply line” is, then constitutes an entity for the open system that the circuit system under consideration is.
- (b) **Attribute, value and standard:** Entity is defined by its attribute and, for the “supply line” entity, supply voltage represents attribute. The supply voltage value as validated when the resistor was tested with the circuit, is the “standard” value for the attribute.
- (c) **Incorrect production of information and loss of I*I:** Any deviation of actual supply value from the above standard is a case of incorrect production of information resulting in information error in respect of value of “supply” and, hence, loss of Information Integrity in the “circuit operation” setting, which may be termed as Operational Integrity.
- (d) **Loss of Goal Integrity:** It is expected the circuit will deliver required current. But if due to loss of Operational Integrity an incident takes place wherein this resistor is made to dissipate two watts and as result the resistor fails, the circuit fails in its function. This is the case of loss of Goal Integrity and it occurs as soon as incorrect information on the supply value is produced.

- (e) **Loss of competitive advantage:** When there is loss of Goal Integrity, there is loss of competitive advantage, which in view of above analysis can now be seen to be because of loss of Operational Integrity.
- (f) **Need to improve I*I for competitive advantage:** The only way to ensure the competitive advantage then is by improving the Operational Integrity, i.e., Information Integrity in the ‘circuit operation’ setting.
- (g) **Information as product:** Above shows that when modeled as open system, integrity analysis offers information on value of supply voltage as a “product”, which when delivered with requisite integrity, facilitates satisfactory resistor and circuit functioning and, thereby, the achieving of goal and hence competitive advantage.
- (h) **Inadequacy of Direct Integrity mechanism:** If this open system modeling view is not taken, then there is no choice of modeling “interconnection” as entity and there is no opportunity to improve Operational Integrity; the information about “value” of supply voltage being taken assumed as already validated, thereby treating it as by-product. Acting in a ballistic and in ad hoc manner, at the most, efforts may be made post event to hold circuit operators or resistor procurement staff accountable or to improve quality of resistor component, which may seem to suggest that a quick action is being taken and at less cost. But in future, when supply voltage value again varies (and it would certainly do), the component and system failures leading to loss of competitive advantage would occur again and in the long run the entire operation would work out costly.
- (i) **I*I control must for achieving system benefits and reducing costs:** Against this Operational Integrity Analysis as above and subsequent implementation of Operational Integrity Controller for I*I Improvement would take time and cost the user on immediate basis, but it would be a scientific and analytical approach. In the long run it would reduce costs and certainly reduce failures (informational as well as functional) resulting in competitive advantage.

10.2 Observed error versus Informational error

As discussed in Sub-section (3.1), business process models controlled by structured and periodic control responses emphasizing “fixed” information decisions account for incorrect operations, which are functional and hence observable. Accordingly, they treat an error as a deviation from the required (standard) function/operation of the component, the sub-system, or the system. The error is the mechanism by which the fault becomes apparent, i.e., observable. A sub-system or system failure occurs when the sub-system or system fails to perform its required or desired function.

However, as mentioned earlier, the issue of errors is at the third level, too, and it pertains to errors from production of incorrect information. Incorrect information leads to decision failure, which in turn may lead to observable error and observable system failure. In the above-described example of resistor and circuit failure, loss of Goal Integrity occurred the moment the value of supply voltage was assumed correct as validated earlier. This is an informational error, which is not observable. It has an indirect consequence in that it resulted in decision failure by so assuming the supply value, which led to so operating circuit and at that particular instant, when the supply varied by that much, *that* resistor failed.

In other words, when one considers information error, it is useful to decide on “error” model. What can be construed as an error? From the viewpoint of an external observer, an error then can be seen as a failure to ensure an optimum, desired, or intended value (for a view, format, variable, or process, etc. as the case may be) that is correct given the circumstances (situation), the cause and form of error notwithstanding. An error can occur only if there is an appropriate identified source of value (standard) to ensure on the basis of a documented state of events.

The above error model offers a workable framework for studying informational errors and their integrity implications, which are the concern of present investigation. If failure is defined as observed collapse, there would be few failures. But informational failures in the manner of information *use* (i.e. decision) failures, where the implication of observed failure (i.e., observed collapse, accident or adverse event) is captured even when it has yet not occurred, is defined within the framework of above error model by nonconformity with specifications or expectations or defined standards. This is more scientific approach, and if one takes the trouble to measure the shape, position, and condition of products (intermediate products inclusive) at the delivery of each of informational products and services delivered during *SDILC* stages, there are many failures – far more than the list of incidents that are covered by the media, both technical and public and far more than the percentages reported in the literature.

10.3 Direct Integrity versus Indirect Integrity

As discussed in Sub-section (3.1), when error is observable, it results in loss of degree of adherence to desired function or desired purpose, which is termed as Direct Integrity.

However, when informational error occurs, it being not observable, it leads to indirect loss of integrity. For example, in the above-described example of resistor and circuit failure, loss of Goal Integrity occurred the moment the value of supply voltage is assumed correct as validated earlier and when no error is anticipated. Thus even when observable error of resistor failure has not occurred, the information error and hence loss of Information Integrity has occurred in the circuit operational setting. And this led to a decision failure of creating condition for the resistor to dissipate higher watts than it can, which is due to loss of Operational Integrity and Goal Integrity resulting in loss of competitive advantage.

From above it can be seen that indirect integrity in fact is Information Integrity. Further, I*I is a holistic presentation of integrity as it accounts for all errors – non observable as well as observable – and includes implications of Direct Integrity.

10.4 Understanding environmental factors

Sub-section (9.3.2) mentions uncertainty implications of system environmental factors. This is a rigorous research query and it is not intended to address it here. Instead, what is desired is to emphasize some critical environment factor modeling issues as applicable to an open system.

- i) Let us consider the ‘resistor failure’ example in Sub-section (10.1). In fact if this system representing the circuit is seen as a closed system, as indicated at Item (10.1 [h]), the problem is an easiest one to address. For all that matter, on immediate basis, the resistor

- costs so very less that best answer is just to replace it by a new one and forget about the problem. At the back of this solution are the model assumptions as stated in Section (2).
- ii) But the instant an open system view of the circuit is taken, entities in the form of “interconnections” came into play. It now becomes necessary to look at the supply voltage value, current value (not mentioned earlier), etc. That is as mentioned in Section (5.1), it becomes necessary to account for the local market factors representing condition of the resistor. In reality what this introduces are more information variables in the integrity analysis, thereby requiring informational view of the resistor and circuit operation. This increases informational complexity in the system description, which otherwise (as mentioned above) when viewed from a closed system angle is perhaps the simplest one (system description) to come across. At this stage it may be pointed out that Sub-section (9.3.2), while discussing the uncertainty implications of system environmental factors, identifies complexity as an environmental factor.
 - iii) From here onwards, we may generalize the analysis framework. Systems would have material objects such as say electrical and mechanical systems. For them environmental factors contributing to interdependency as experienced by resistor component in the exemplary incident could be: quality of materials and particularly for electrical components quality level; temperature; humidity, salt, dust in atmosphere; exposure to frost; nature of process material: corrosive, erosive, dirty, multiphase; vibration; mechanical shock; electromagnetic radiation; etc. Behavior of electrical and mechanical components is dependent on environmental stress factor also. Specifically these are: stresses emanating from mechanical stress, from pressure, from voltage, from torque, from effect of complexity and of maturity of manufacturing process; etc. (in fact this is the situation in the exemplary incident).
 - iv) Coming to environmental dependency of computer controlled hardware and of embedded microcomputers on software, it could be because of undetected errors in the program; errors due to complexity; etc. Further, in this context there is the issue of failures due to incorrect production of information. For example there is the question of delay in processing information. The hardware of the computers used to run these packages must also be considered, as a system fault could also lead to incorrect information.
 - v) Similarly, one can see humans, norms, rules, policies, etc., all, have environmental dependency. In fact as one takes the open system view of *IS*, there is a question of implications of internal and external system environmental factors of complexity, change, communication, conversion and corruption that impact each of these entities and interconnections their between. This entire study is a part of extensive research. For the purpose of present investigation it suffices to recognize how, therefore, modeling information as function of recipient, where recipient covers a wide spectrum covering objects, people, rules, norms, policies and commands, and how recognizing that recipient has its own environment and, accordingly, accompanying interconnections with it, is critical to develop an open system view of business process *IS* view.

10.5 Criticality of Usefulness factor

By considering information as function of recipient, yet another critical factor emerging is that information is for *use* (of *recipient*). This makes the relevance, i.e., Usefulness factor of

information requirements critical to *IS* view development; thereby providing a basis to work towards development of Usefulness-Usability-Integrity paradigm

10.6 Criticality of maximal (and not minimal) information requirements

Consistent with process requirements of business process *IS* given as under Sub-section (9.2), above makes it necessary to develop information requirements covering following spectrum:

- 10.6.1 Information requirements describing Business Process Goal;
- 10.6.2 Information requirements of ‘many factors’ & ‘multiple criteria’ characterizing business task (problem) complexity;
- 10.6.3 Information requirements of operable goal;
- 10.6.4 Information requirements of planning & design constraints and opportunity spaces;
- 10.6.5 Information requirements giving *culled out*, i.e., useful (relevant) information variables;
- 10.6.6 Information requirements of critical, i.e., independent information variables; and
- 10.6.7 Information requirements describing interconnections, i.e., relationships (interdependencies) between culled out information variables.

As can be seen the “standard” product in high volume business model, which has closed system interpretation, has requirement *only* for minimal, i.e., critical/irreducible/independent information variables. Against this the business process *IS* view, which has open system interpretation, has requirement for maximal information as identified above.

11. RESULTING SHIFT IN MODELING ASSUMPTIONS OF BUSINESS PROCESS *IS* VIEW

This suggests a shift in business model building assumptions from that in Section (2); and the same is summarized in Table (11.1).

Table 11.1: Shift in business model building assumptions from those currently practiced

Business Model Currently Practiced [Ref. Section (2)]	Business <i>IS</i> View A Multistage Decision Process [Ref. Sections (9,10)]
Business drivers are globalization, international competition and changing customer expectations.	Business drivers are globalization, international competition and internal and external customer expectations that are increasingly becoming local and instant.
A closed system view of business process <i>emphasizing</i> material and energy flow	An open system view of business process <i>emphasizing</i> information flow.
Input-Output Business Process Model, integral to which are information systems.	A closed loop information and control system, integral to which is a generic business process.
A “collective” decision model, wherein there is no room for local market factor based product beneficitation for strategic advantage,	An “individual” decision model based on local market factor based product beneficitation for strategic advantage.
Its origin is in the high-volume mechanical	It aims at “flexible” automation to achieve

manufacture characterized by inflexible automation for business objectives of operational optimization and cost efficiency.	business objectives of effectiveness and efficiency through requirements of: mass customization, agility – focused on customer responsiveness, IT driven market differentiation, supply chain synchronization by integration maximization, and financial optimization.
Model comprises physical work systems, which emphasize material and energy processing.	Model comprises: (a) informational work system, which emphasizes information ‘transformation’ (as against transfer), and (b) physical work system.
Model has input, process and output control systems, which are tuned to “fixed” i.e., “structured and periodic” data/information decisions.	Model is based on “flexible” information decision for control implementation for physical work system.
Main IS concern is <i>only</i> that information technology accesses, communicates, processes and distributes the already generated information,	IS concern is information origination and processing “ <i>endogenous</i> ” to the decision situation.
Information processing attends <i>only</i> to the “exactness” aspect of information requirement and accordingly accounts for implications of noise present in the information.	Information origination and processing has a need to attend to “correctness” aspect of information requirements, which includes “exactness” aspect. Accordingly, IS has a need to account for incorrect production of information due to “distortion” and “noise.”
<i>Assumption is that data is perfect, once validated, and most information processing systems do not anticipate defective data.</i>	<i>In the presence of uncertainties due to system environmental factors, it is not acceptable that data is assumed perfect, once validated, and that most information processing systems do not anticipate defective data.</i>
There is <u>no</u> requirement to originate local market factor based information on decision alternatives and on selection of information decision <i>endogenous</i> to decision situation.	There is a continuous requirement to originate local market factor based information on decision alternatives and on selection of information decision <i>endogenous</i> to decision situation.
IS processes “minimal” information. This ends up treating information as by-product.	IS has a requirement to originate and to process “maximal” information. This enables treating information as product.
Strategy for competitive survival does not demand committing of organizational	Strategy for competitive survival requires committing of organizational resources for

resources for information “origination”.	information “origination”.
With information technology costs ever decreasing, information processing for decision-making is taken as a <i>costless</i> activity.	Information origination is a costly activity. (See section [14]).
Model assumes complete knowledge of initial condition (i.e., fixed information decision for control implementation).	Model has incomplete knowledge of initial condition (Flexible information decision with uncertainty for control implementation).
Model assumes linearity of process.	Model has non-linear processes.
Model assumes availability on the part of the business enterprise system, its sub-systems and their components of unlimited (i.e., adequate) information processing resources.	Model considers inadequacy on the part of business enterprise system, its sub-systems and components of information processing resources. This is because information origination is a costly activity. This makes all decision processes (Ref. Sub-section [9.2] and Section [15]) identified under business process IS costly activities.
<ul style="list-style-type: none"> • Model recognizes errors in respect of “exactness” aspect of information processed. • This error accounts for implications of “noise.” • An error is defined as a deviation from the required (standard) function/operation of the component, sub-system, or the system. • Accordingly, an error is the mechanism by which the fault becomes apparent, i.e., observable. • The system failure concern is only in terms of functional, i.e., observable failures. 	<ul style="list-style-type: none"> • Model has a requirement to recognize errors in respect of “correctness” aspect of information processed. • This accounts for implications of “distortion” and “noise”. • An error is defined as a failure to ensure an optimum, desired, or intended value (for a view, format, variable, or process, etc. as the case may be) that is correct given the circumstances (situation), the cause and form of error notwithstanding. An error can occur only if there is an appropriate identified source of value (standard) to ensure on the basis of a documented state of events. • The system failure concern goes beyond functional, i.e., observable failures and includes Decision Failures from: <ul style="list-style-type: none"> a. Design errors, Development errors, Deployment errors, Data errors and Detection errors, b. Errors in originating maximal information requirements, etc. <p>Note: These errors, which in fact are</p>

	<p>information errors, and decision failures there from, both, are unobservable. It is risks from these decision failures that are crucial to strategic advantage.</p>
--	--

12. INADEQUACY OF EXISTING INTEGRITY MECHANISMS

Literature reports integrity studies from different angles: security based definitional approach to integrity, auditing research, process centered quality approach, noise reduction based technology under communication theory, and the Savage (Subjective) Expected Utility (SEU) theory under decision-making (see Sub-section (3.2)).

12.1 Integrity concern limited to Direct Integrity only

IS models under these integrity mechanisms do not account for the requirement of continuous origination of information endogenous to the specific decision situation. Their main concern is *only* that information technology accesses, communicates, processes and distributes the *already* generated ‘minimal’ information. This is a requirement of “exactness” aspect of information. Accordingly, these mechanisms end up considering implications of only observable incorrect operations due to mechanistic failures and, with additional efforts, due to failures of system equipment that is controlled by computer (See Sub-sections (3.1) and (3.2)).

12.2 Integrity concerns of incorrect production of information not attended

However, as mentioned in Section (4), there are consequences of incorrect system operations at third level, too. These consequences relate to indirect consequences or production of incorrect information. These considerations are of relevance in a wide range of systems, such as medical imaging and patient records systems. Here, amongst other things, one faces the consequences of undesirable delays. Other examples from this category relate to automated tools that are used in the design of safety-related equipment. Faults within such tools could lead to incorrect designs and accordingly to loss of Design Integrity, which could result in delivery of ineffective and unsatisfactory product to the customer. From this example it is clear that the use of computer packages such as databases, finite element analysis utilities and even word processors could be considered to have integrity implications across the system development and implementation life cycle (*SDILC*) phases. The hardware of computers used to run these packages must also be considered, as a system fault could also lead to incorrect data and information.

12.3 Incorrect production of information due to “Distortion” and “Noise”

While the consequences of incorrect operations at first two levels, basically take stochastic interpretations and are addressed by modeling uncertainty in information processing as “noise”, the consequences of incorrect production of information relate to consequences of incorrect information origination and processing and require that uncertainty be modeled as comprising “distortion” and “noise”. And more importantly, it transfers the issue of cause and consequence of incorrect operations from that of “exactness” requirement of information to that of “correctness” requirement of information.

For more explanation, see Appendix 2.

13. INFORMATION AND ITS USEFULNESS & USABILITY REQUIREMENTS

For competitive business advantage, the business process *IS* view, ridden with uncertainty (by the way of distortion and noise) and errors, must manipulate information “analytically” so as to achieve improved decision; that is, it must process information efficiently and economically. What is this information are we talking about here?

I*I research shows this information {I}, so to be *originated* and processed, in fact, has three components. These are:

- (j) Information (I₁), which is in a form of an aggregate or a measure so as to compare two or more alternatives and to select one flexible (customized) information decision for control implementation,
- (ii) Information “I₂” on market imbalances indicating business opportunities, and
- (iii) Information “I₃” constituting knowledge of working mechanisms for resource allocation.

Further, *recipient* (local market factors) requires that business *IS*, as above, *originates* and processes that {I=I₁+I₂+I₃}, which is *useful* (relevant) and makes it easy to function in the market, i.e. which is *usable* to rank the *originated* alternatives for comparison and to make a customized information decision selection. This is an analytical pointer to the product nature of the information “I₁”.

14. CRITICALITY OF INFORMATION INTEGRITY FOR BUSINESS COMPETITIVE ADVANTAGE – RECOGNIZING ORIGINATION OF INFORMATION A COSTLY ACTIVITY

For efficient processing of information {I}, there *has* to be economic trade off between:

- Costs of originating & processing information “I”, and
- Loss due to incorrect information, i.e., due to I*I Risk.

That is *that IS* which, for a certain kind of information *origination*, processing, storage, distribution and discard, is able to arrange them (costs) at the lower level *will* tend to prevail. In view of this it follows that, *to compete successfully*, information “I₁” – the aggregate information; (b) information “I₂” on market opportunities, and (c) information “I₃” constituting knowledge of working mechanisms for resource allocation must have *integrity*. In other words, each detail in each of these information statements (the aggregate or the measure, the opportunities, and the knowledge capital), and *not only* the bottom line statements, must have

integrity; as it is only through ensuing of optimal integrity that it is possible to achieve efficient and economic processing of aggregate information in the business *IS* view described above.

15. EMERGING INFORMATION INTEGRITY REQUIREMENTS

15.1 For Information Origination Processes under Informational Work System

Information Integrity then must be ensured for following decision process stages:

(A) I*I of Laundry List Preparation stages comprising processes of:

- (a) *Setting* Business Process Goal;
- (b) *Originating* ‘many factors’ & ‘multiple criteria’ characterizing business task (problem) complexity;
- (c) *Recognizing* (deciding) operable goal;
- (d) *Defining* planning & design constraints and opportunity spaces;
- (e) *Culling out* useful (relevant) information variables;

(B) I*I of Influence or Structure Diagram Preparation stages comprising processes of:

- (f) *Recognizing* relationships (interdependencies) between culled out information variables.
 - 1) Application of Cross-correlation technique;
- (g) *Developing* state transition (forecasting) equations for culled out state (information) variables;

(C) I*I of Structure Characterization stages comprising processes of:

- (h) *Determining* dynamic structure characterization model, i.e., *IS* view based on structure diagram;

(D) I*I of Unstructured and Aperiodic Information Processing stages comprising processes for Flexible Information Decision for Control Implementation

- (i) *Collecting* (i.e., *originating*) on current basis input data in the form of requirements of:
 - a. *Recipient* (customer) under consideration;
 - i. *Recipient* covers concrete objects (machines, hardware), abstract objects (accounts, sales forecasts, policies), humans (external and internal customers, society), rules (established procedures), norms (codes of practice), commands (software, standing orders), etc.
 - b. Business process capabilities and costs;
 - c. Questions, etc;
- (j) Processing of current basis input data *originated* at Stage (i) through information system model originated at Stage (h) above and *obtaining* flexible (customized) *recipient* based information decision.

Note: Stages through (a-j) correspond to, what may be termed as 6th level “information control” requirement for maximizing information *use*. Accordingly, information control delivers customized planning & design and *originates* alternatives for evaluation and selects flexible information decision for control implementation;

15.2 For Information Processing with reference to Requirements of Physical Work System

Here decision process stages are mainly with reference to “exogenously” generated alternatives and information. Specifically, this information processing is with reference to requirements of:

(E) I*I of Control Implementation stages comprising processes of:

- (k) Processing of information decision obtained from Stage (j) by various lower level process controls under the physical work system. These lower level process controls are:
- 1) 5th Level Process Control: Scheduling Control (PERT, CPM, techniques),
 - 2) 4th Level Process Controls: Forecasting Applications, R&D Activities, Financial Management Applications, Risk Analysis Methods, Manpower databases, CRM,
 - 3) 3rd Level Process Control: Allocation of Machine (Assignment problem), Allocation of HR, Inventory Control System,
 - 4) 2nd Level Process Control: Accounting Applications, Monitoring Work Progress (Time & Motion Study), Quality control System,
 - 5) 1st Level Physical Variables’ Control: Pressure Controller, Flow Controller, Position controller, Voltage Controller, Critical Performance Variable Controllers

Note: Stage (k) delivers input, process and output controllers for the business plant/process/activity.

(F) I*I of Plant Operation Stages comprising processes of:

- (l) As per control inputs from Stage (k), processing of business inputs through business process to deliver product/system/service (information product inclusive) to the *recipient* (customer) as per requirements.

15.3 For Individual elements of each of decision process stages

Requirement is to ensure I*I for each of above decision process stages from A-F, which by themselves are information origination activities. Towards this workable mechanism would be to ensure I*I of individual elements of each of these decision processes. This entirety is a rigorous research query not to be attempted here. However, in an effort to complete the exercise undertaken this sub-section identifies the individual elements as applicable to the decision process at stages from (D-F). Specifically, requirement is to ensure I*I for each of following elements.

15.3.1 I*I of individual elements of decision processing stages in respect of Selection of Flexible Information Decision and Control Implementation:

Element 1: Observation of the Real World Events

Element 2: Verification of Problem Area Data Observed

Element 3: Problem Recognition or Operable Goal Setting

Element 4: Prediction of Future States

Element 5: Coordination of information origination activities with reference to:

- Attending to data
- Prioritization of problems and activities
- Selection of flexible information decision
- Control implementation

- Reevaluation
- Element 6: Selection of Flexible Information Decision and Control Scheduling
- Element 7: Input-process-Output Implementation
- Element 8: Reevaluation
- Element 9: Information origination resource management

16. GUIDE WORDS BASED APPROACH TO I*I ASSESSMENT FOR DEVIATION IN INDIVIDUAL ELEMENTS

Strategic advantage calls for controlling I*I. This calls for assessment of I*I for deviation.

The system of investigational concern here is the business process *IS* view, which is an open system as defined by information origination in presence of uncertainty. A system as this comprises of: objects (some concrete such as hardware and some abstract such as applications), internal and external users (humans, software and machines inclusive), rules, norms, policies and financial mechanisms of cost and benefits. Each of these systems, sub-systems and their components by themselves are also open systems. These open systems between and within them process information. This gives rise to the business process *IS* view, which is uncertainty and error ridden. For competitive survival this *IS* must process information with integrity.

Within above framework, information processed by open systems can be seen as *interconnections* between the systems, sub-systems and components as above (see Sub-section [10.1]). For I*I deviation study, the effort then needs to concentrate on these *interconnections*, which in fact represent information originated and processed at different decision stages of the business *IS* view. When dealing with informational work system (*IWS*), these *interconnections* are modeled as information systems and are defined by information content, process and system. When dealing with physical work system (*PWS*), these *interconnections* are modeled as “plant” described by (a) content made up of material or signal or data, (b) process of material flow or of electricity, signal or data flow, (c) and system.

It is these *interconnections* described by content, process and system that then constitute ‘**entities**’. Each entity has certain properties or ‘attributes’, which determine the “correctness”, i.e., integrity, of information and information system for the *IWS* and of the system’s operation in case of *PWS*. More specifically, deviations from the design values for these attributes have implications for the correctness of information and of information system and of physical system operation in the manner of loss of Information Integrity.

If modeled as above, the problem of assessment of I*I deviation is analytically tractable using the methodology of Hazard and Operability studies (HAZOP) developed in chemical engineering. Specifically, the study is based on a rigorous and systematic investigation of possible deviations from each of the identified attributes. In order to structure the assessment process a series of ‘guide words’ is used to define particular types of deviation from the standard value. Examples can be: no, more, less, as well as, part of, reverse, other than, early, late, before, after, relevant, goal explicit, goal positive, goal negative, goal unclear, goal specific, goal

implicit, constrain (i.e., limit) violated, opportunity lost, environmentally dependent, interdependency relationship, nature of system dynamics, nature of structural characterization, etc.

The various guidewords are given varied interpretations depending on the industry concerned and where they are applied. For this reason the meaning, or meanings, of each guideword must be defined as part of the study. Once the study identifies the applicable guideword, next step is to investigate the cause of deviation and its consequence on the information system and on information therefrom. This would facilitate the decision on the recommendation for further investigation for I*I risk reduction and for integrity improvement. Table (13.1) indicates this study structure. .

Table (13.3.2) : Integrity Analysis Methodology

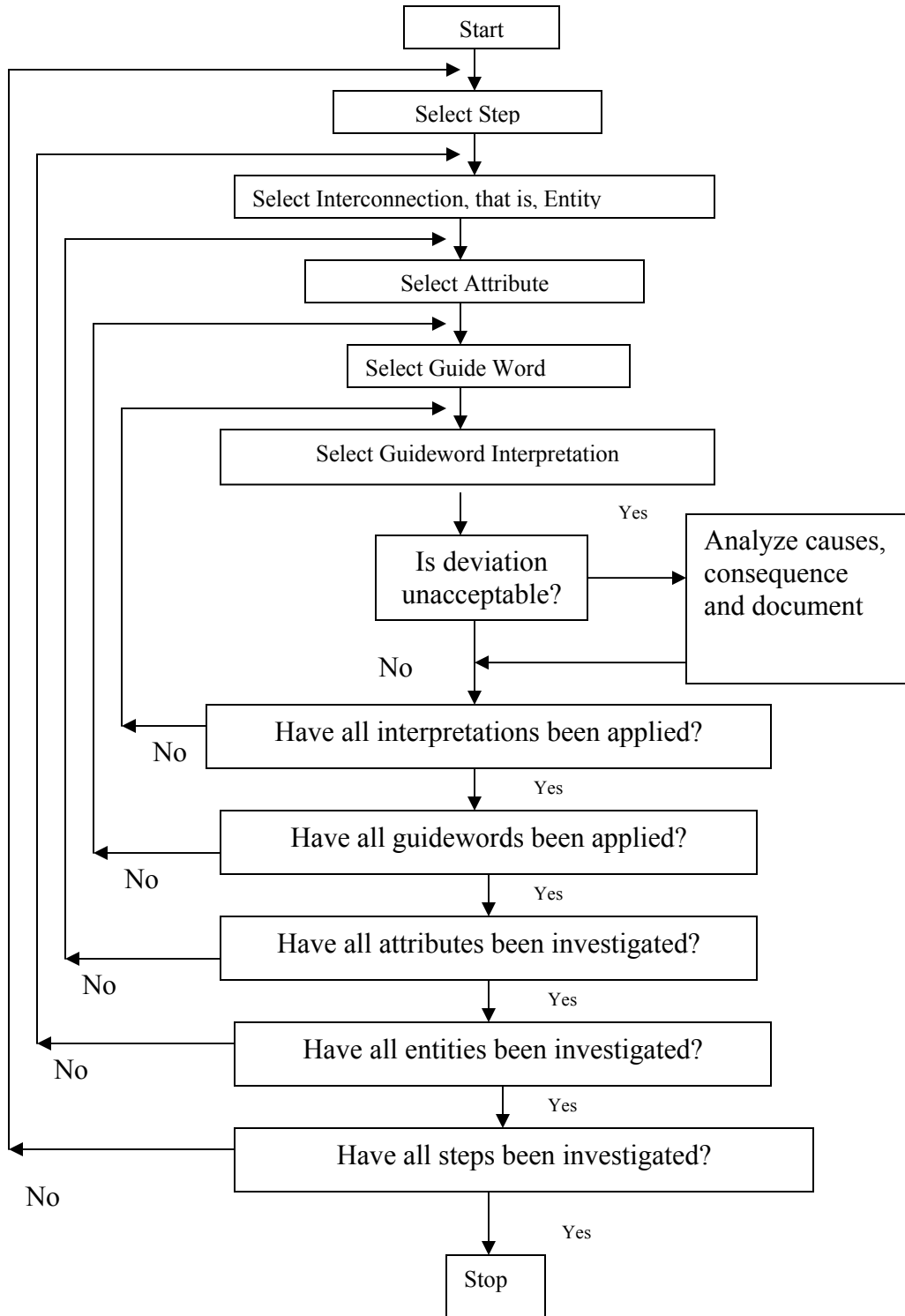
Item	Entity, i.e., Inter-connection	Attribute	Guideword	Cause	Consequence	Recommendation

The final stage of the Integrity analysis is to prioritize the results to identify areas that justify further investigation. Once integrity risks are identified it may be useful to present data using fault trees.

It follows integrity analysis plays a vital part in the development of any computer embedded system. Its findings affect not only the system design but also the development methods used. It is therefore clear that integrity analysis must be carried out at an early stage, as its results have great integrity implications on all aspects of information processing (project). However, it would be incorrect to assume that the analysis of I*I is a ‘one-off’ process performed in the beginning of the project. In fact, I*I analysis is concerned not only with the characteristics of the system but also with the details of the design. Therefore, when the preliminary analysis shows that a system is integrity-related (i.e., integrity is critical; and with open system view in fact all systems are integrity-related), integrity analysis will normally continue throughout the development (and shall we say also through the implementation) process. The nature of this work, and the effort involved, will be determined by several factors, including the level of integrity risk associated with the system, as identified by the early stages of I*I analysis.

17. A FLOWCHART OF THE I*I ANALYSIS PROCESS

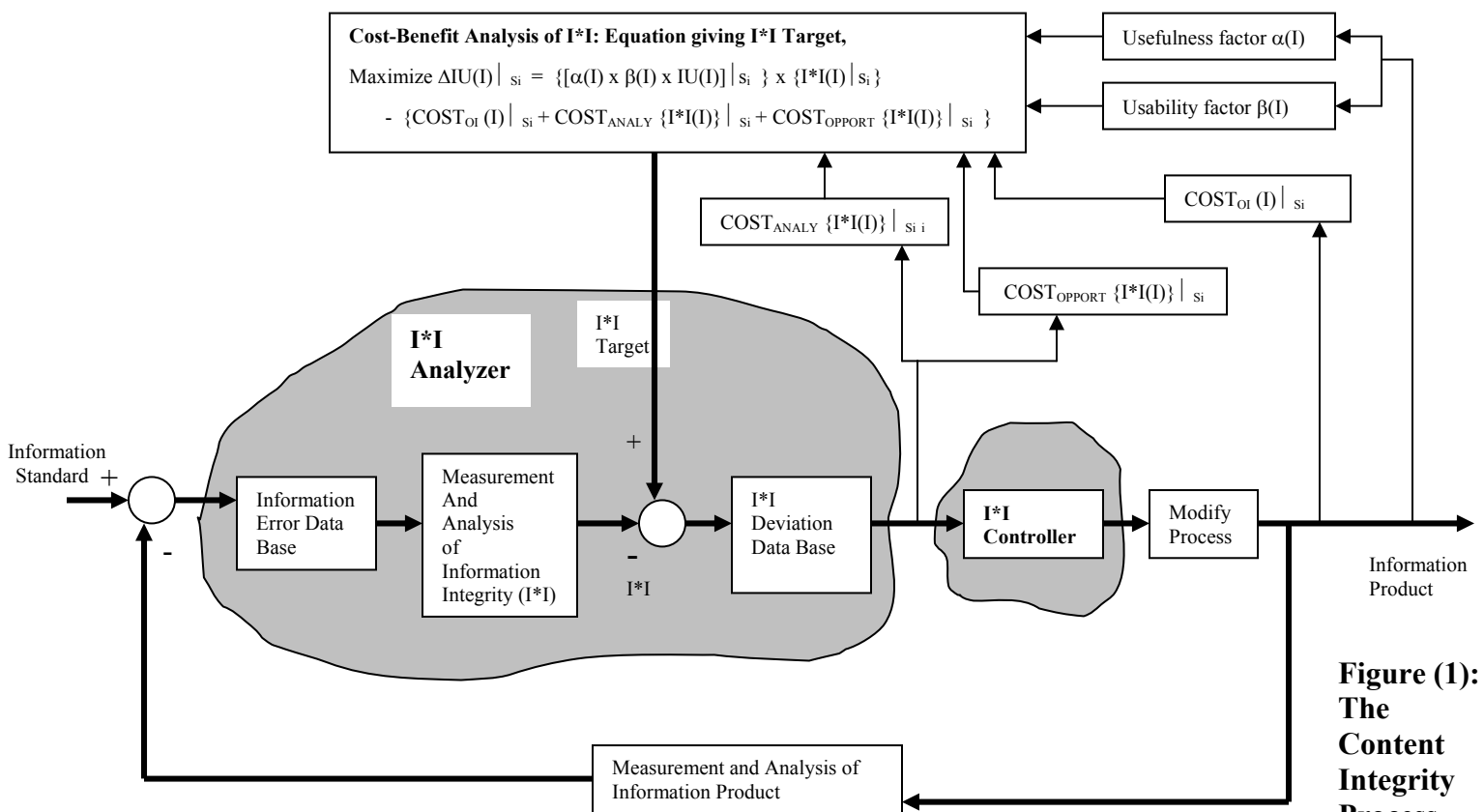
Within the framework of integrity assessment for deviation and within the framework of risk analysis in the context as above that then the following I*I Analysis Flowchart emerges



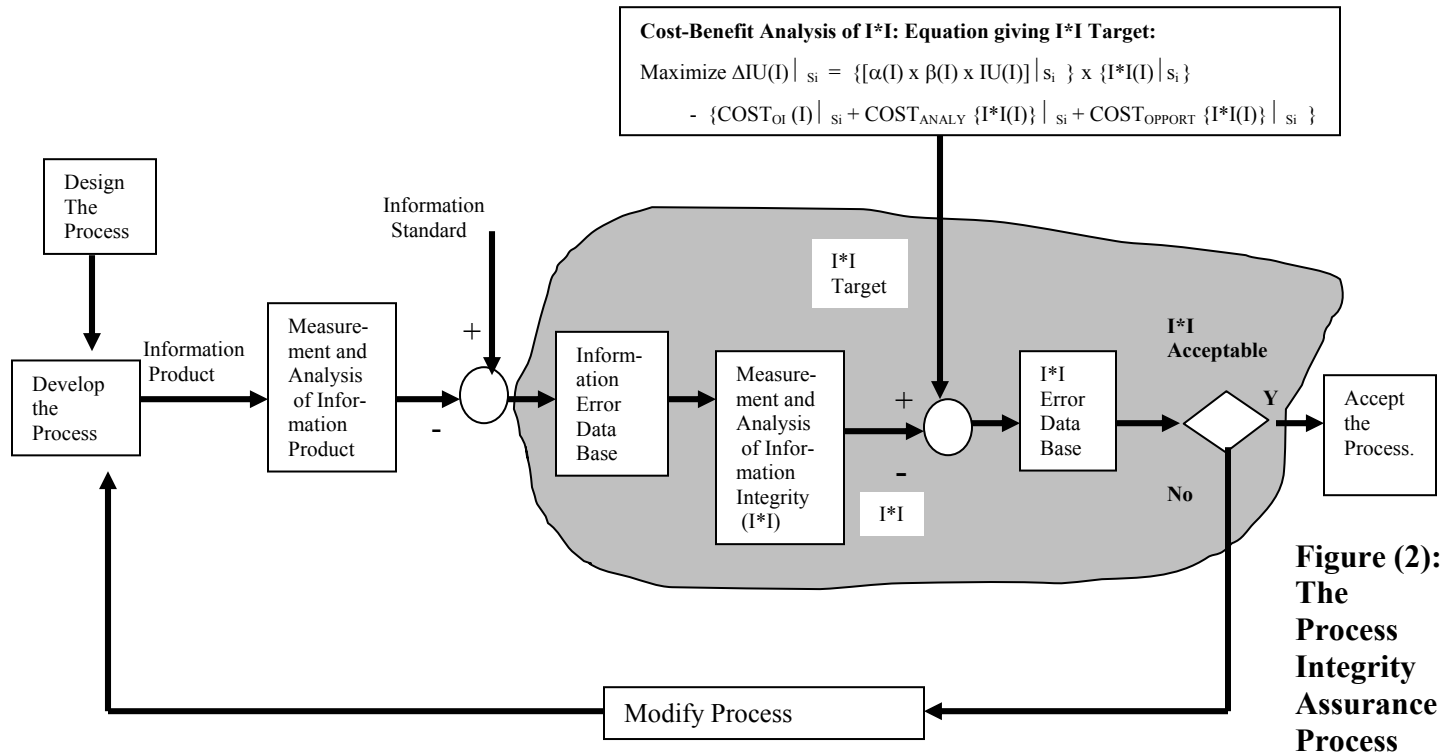
18. THE CONTENT, PROCESS AND SYSTEM INTEGRITY PROCESS

What one is talking here is development of Integrity Analyzers and Integrity Controllers. As mentioned in Sub-section (16), this calls for *Content Integrity*, *Process Integrity Assurance* and *System Integrity Assurance* processes. Specifically, Content Integrity should be ensured for each of categories of information requirements as under maximal information requirements identified in Sub-section (10.6).

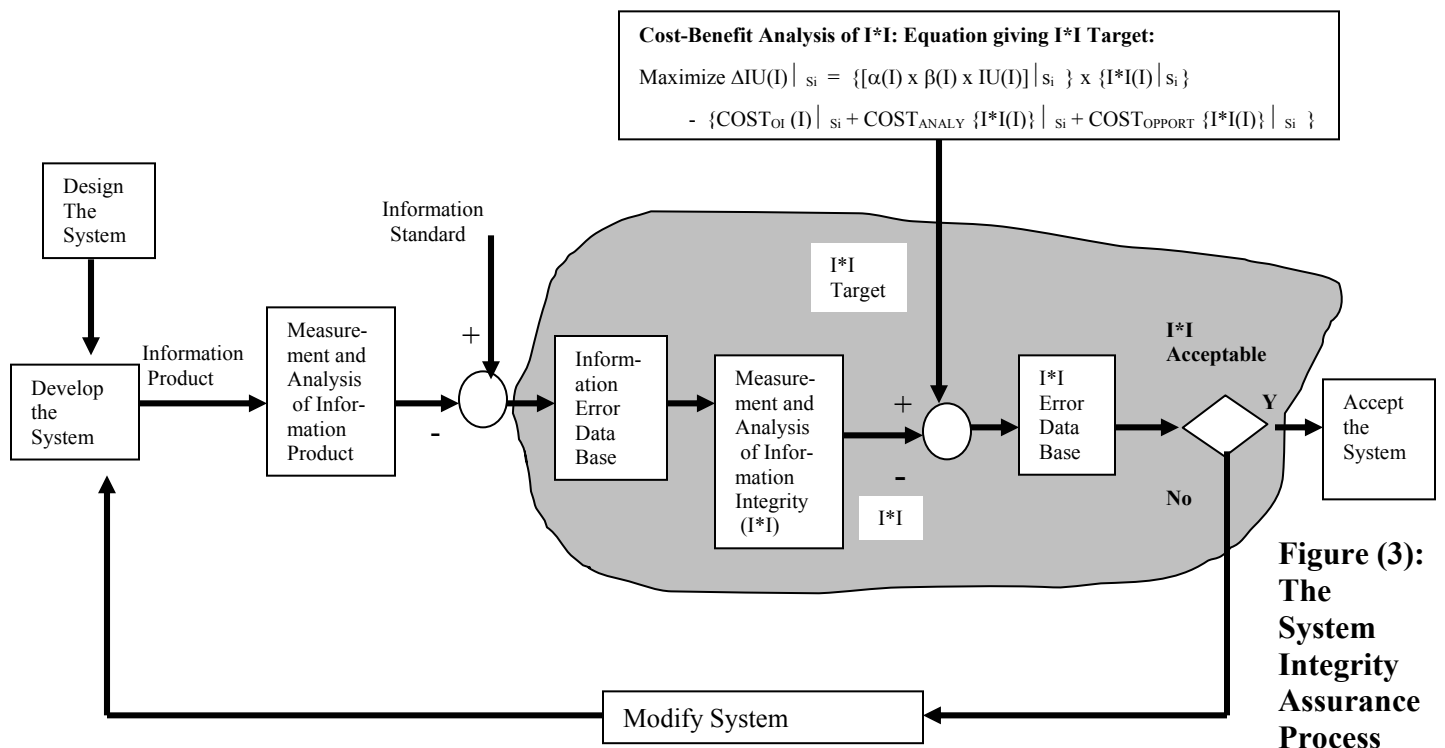
Accordingly, for each of categories, it is first necessary to establish Information Standard and I*I Standard, i.e., I*I Target. Having established these, the need is to generate “Information Error Data Base” and “I*I Error Data Base”. With this achieved, then I*I Error Data can provide a control signal so as to modify corresponding process so as to achieve needed I*I for the particular information requirement from the category under consideration. Figure (1) gives this generic description of the Content Integrity Process.



Further, figures (2) and (3) give generic descriptions of the Process Integrity Assurance and the System Integrity Assurance processes, respectively.



**Figure (2):
The
Process
Integrity
Assurance
Process**



**Figure (3):
The
System
Integrity
Assurance
Process**

19. ORGANIZATION OF INDIVIDUAL INFORMATION ORIGINATION UNDER UNCERTAINTY – DESIGN BASIS FOR I*I ANALYZER AND CONTROLLER

For the successful implementation of the organization of above informational capability of efficient and economic processing of business process *IS* characterized by uncertainty, the *IS* specifically needs to incorporate integrity analyzers with the capability of generating and analyzing any deviation from standards in information origination, storage, retrieval, validation, processing, communication, *use* and subsequent discard or storage for future *use* (as the case may be) under the *IS* and identifying its cause, and of reporting it (deviation) and its cause to Integrity controller. In other words control of the business process should become centralized not in the information processing system (structured and periodic in that), as is the case currently, but in its Information Integrity analyzer and controller, which will have detailed programs for:

- (a) Standardized statement of the *IS* Task (problem), which is obtained from the functional work activity of interest and which in all probability will be a complex goal statement having multiple criteria with many embedded information variables,
- (b) Standardized operable *IS* goal statements (performance standards that go to make complex goal statement as in (a)),
- (c) For each performance standard as in (b), standardized performance criteria describing performance standard (Criterion would normally describe “process” standards for *factors & measures, actions, optimality conditions*, and for *information reports* offering a mechanism to evaluate and measure if the product/service output (informational work included) delivered meets the performance standard, i. e., the expected operable goal),
- (d) For each performance standard as in (b), standardized performance evidences in the form of:
 - (i) Quantity and quality of product/service delivered over defined time period,
 - (ii) Demonstration of achievement of defined level of specialization in *IS* design and technology content,
 - (iii) Documented record of relevant, proven prior performance achievements defined with reference to the *IS* task corresponding to the operable goal,
- (e) Standardized information origination and processing methods,
- (f) Standardized information system environmental parameters covering relevant contexts, specificities or individual situations with respect to:
 - (i) Different decision process stages of *IS* as at (e), and
 - (ii) Standards as defined under (c), (d) above,
- (g) Standardized methods for reporting deviations from the standards at (c), (d) and (e). These deviations will be measured and reported as loss of Information Integrity (i.e., in the form of loss of Accuracy, Consistency and Reliability).

Thus Information Integrity Analyzers and Controllers constitute the technology to be used as programmable, distributed decision makers in the control of fast-moving changes (in local market objectives, their information requirements, interdependencies between the information variables, and their non-linear dynamics) through the business process *IS* view system of the information flow whose scale and speeds otherwise preclude control by more centralized structures. The Information Integrity Technology in the form of integrity analyzer and integrity controller would thus extend the capability of *IS* from that of information storing and processing

(characterizing structured and periodic information processing) to that of information *origination*, storage, retrieval, evaluation, processing, communication, *use* and subsequent discard or storage for further *use* (characterizing unstructured and a periodic information processing). In other words the Information Integrity Technology would develop processing of unstructured and a periodic information processing under uncertainty as a powerful tool for optimization of informational work for global business processes delivering products under local factors' based market place, which in 21st century would occupy a dominant space.

-Center for Information Integrity Research workers: Vijay V. Mandke, Madhavan K. Nayar and others.

0-0-0-0-0

Appendix 1

Defining Information Integrity attributes

Literature identifies a universe of information attributes; namely, accuracy, usability, reliability, independence, timeliness, precision, completeness, relevance, sufficiency, ease of understanding, freedom from bias, consistency, trustworthy, brief, etc. Appropriate attributes from these concerning context, goal, and nature of information use, i.e. relevance and feasibility of use, then can be categorized under the usefulness and the usability objectives. This facilitates a workable framework for defining intrinsic integrity objective in the form of accuracy, consistency and reliability attributes of information covering correctness aspect. Information requirements of usefulness, usability, and integrity are, then, the determinants of information value. Seen more critically, usefulness and usability factors are also defined by their respective information requirements. It goes without saying these information requirements must also have integrity. In other words, integrity attributes of accuracy, consistency and reliability are fundamental or basic to the information requirements of usefulness and usability and, therefore, to the value of information; and as a result a critical requirement of an *IS*. Further, as information value can be seen to define information use (IU) quantum, within above framework the integrity objective then can be seen as to optimize "IU" quantum for a given information processing situation, so as to offer competitive advantage.

At this stage, it should be of help to get a clearer view of integrity attributes of accuracy, consistency and reliability so as to be in a position to develop the equation for cost-benefit analysis of Information Integrity.

4.3.1.1 Accuracy Attribute

Within above framework then Accuracy attribute (A) is defined as the degree of agreement between a particular value and an identified source. It can be assessed by identifying the relevant established source (standard) and by determining an acceptable tolerance. Specifically, the identified source provides the correct value – preferably the value corresponding to the optimum Integrity.

4.3.1.2 Consistency Attribute

Against this, Consistency (C) is defined as the degree to which multiple instances of a value satisfy a set of constraints. The multiple instances may exist across space (such as databases or systems) or over time. Consistency is then with respect to a set of constraints and data/information is said to be consistent with respect to a set of constraints if it satisfies all constraints of the data/information model.

4.3.1.3 Reliability Attribute

Reliability attribute (R) is a little complex attribute to define. Traditionally, it is a large concern in system development lifecycle model and refers to a wide range of issues relating to the design of large systems (complex computerized information system (*CIS*) included), which are required to work well for specified periods of time. From this point of view for an *IS* the definition of reliability given as “accuracy with which information obtained represents data item in whatever respect the information system processed it” can be seen to define the reliability requirement for the *IS* as a whole. Then, reliability is also seen as ‘completeness’ issue. Of course, the completeness requirement itself has two different aspects. One is that of “exactness”

requirement. This requirement occurring due to the ever-present system “noise” is the main concern in communication theory and in security research as also in the “standard” product in high volume seeking business models under quality paradigm emphasizing “reduced defects” in system processing.

There is another aspect of “completeness” requirement, though. In the form of “observability”, it is to be found in system theory. Specifically, the problem considered is that of state variables derived based on measured system outputs at several times and the knowledge of the system-forcing function (control) effort. It is conceivable that the structure of the system and/or measurements taken is such that the measurements do not contain *all* the information about the system states. The usual technique in systems engineering is to generate control efforts (strategies) based on measurements of system outputs. If the measurements are *missing* basic information on actual system response (that is, if there is information distortion), erroneous control efforts could be generated, which is not desirable; just as, if, in the *IS*, value of information element is missing from the information record, the desired information use (IU) value is not achievable, however high may be the information usability factor.

In other words, when concerned with reliability factor under *correctness* requirement of information, there are incompleteness issues due to “noise” and “distortion”. For the purpose of the investigation at hand, whether “inexactness” due to the ‘noise’ factor or “incorrectness” due to ‘distortion’ factor, both result in information item exhibiting error and therefore loss of integrity. As a result, reliability attribute of “*correctness*” aspect of information requirement in considering ‘completeness’ must account for both these possibilities. It is within this framework then the reliability (R) can be heuristically defined as follows: Reliability (R) refers to completeness, currency and auditability of data/information. Specifically, data/information is complete when all component elements are present (effects both of distortion and noise are counted). Information is current when it represents the most recent value. And, information is auditable if there is a record of how it was derived and that record allows one to trace information back to its source.

4.3.2 Analytical Definition of I*I

For the analytical convenience, let us denote the reliability attribute defined based on “completeness” perception, which accounts for ‘distortion’ as mentioned above, by “R1”. Further, let us denote the reliability attribute, which is with reference to “noise” factor and is based on “exactness” perception, by “R2”. Then, the reliability attribute “R” should cover both “R1” and “R2” and is given by Equation (1).

$$\text{Reliability attribute index} = R = R1 \times R2 \quad \dots \text{Equation (1)}$$

What are defined are attributes of Information Integrity (I*I) for information value, i.e., for the content of information processed by *IS*. Content of information would, therefore, have I*I value as in Equation (2).

$$\text{Information Integrity} = I*I = A \times C \times R1 \times R2 \quad \dots \dots \dots \text{Equation (2)}$$

With determination of I*I attributes and I*I, one can now proceed with cost-benefit analysis of

0-0-0-0-0

Appendix 2

More on inadequacy of existing integrity mechanisms

Literature reports integrity studies from different angles: security based definitional approach to integrity, auditing research, process centered quality approach, noise reduction based technology under communication theory, and the Savage (Subjective) Expected Utility (SEU) theory under decision-making. Briefly, in computer science security is taken to mean confidentiality, integrity and availability with the word “integrity” describing a range of requirements. Further, database integrity models and methods, while context specific, do not lend themselves to any comparative, analytical studies. In accounting/auditing research, with respect to accounting information, relevant part of the internal control structure is made up of three basically ad hoc categorizations: the control environment, the accounting system, and the control procedures. This offers a way of structuring the analysis of different possible control mechanisms but with no explicit coupling to cost and benefits in the sense items in different categories can be compared. Same limitation is with the qualitative COSO report that sees internal control, from the management angle, as consisting of five interlocking factors: monitoring, information and communication, control activities, risk assessment, and control environment.

Quality paradigm has two aspects; namely, (a) quality assurance concentrating on the process and attempts to ensure that it is done correctly, and (b) quality control to ensure that the product delivered to customer (recipient) is correct, where the term ‘product’ represents a system or component or service. In practice, however, the quality paradigm operates in the ‘standard’ product mould, emphasizing incremental changes, and sees its operable goal as ‘reduced defects’; thereby emphasizing cost reduction aspect but not the cost-benefit angle. This leaves the quality emphasis weighing more on the side of ‘process’-centered issues rather than ‘product’-centered issues. In the wake of ever-present channel noise, *IS* model in communication theory is concerned with the problem of reproducing at one point (destination) either *exactly* or approximately a message selected at another point (source). The noise reduction technology envisaged is optimization of variable parts of *IS* (encoders and decoders) so as to improve reliability, increase the data rate, or decrease the cost. This *IS* model does not take a decision process based view of the message through the channel. In fact, although the measurements in information theory are significant to communications engineer, they are not related to decision issues, except by chance. Accordingly, then there is no reference to the cost-benefit framework for the degree of “exactness” of message achieved.

The SEU Theory analytically studies a decision process model under uncertainty based on the concept of information value and hence in the first instance seems to be an attractive proposition to study integrity issues. However, SEU maximization is descriptively *invalid* – falsified – as a model of how individual decision makers behave. Nevertheless it is descriptively *valid*, or at least constitutes the best alternative currently available, as a model of individual decision making when building theories of collective decision making at the market level. When dealing with a problem as at hand, this apparent paradox causes confusion. Further, SEU Theory defines the

monetary value of perfect information as amount of money which renders the decision maker indifferent between using and not using information; and thus does not consider in its treatment any explicit coupling to cost-benefit analysis for the information value it measures.

In summary, the *IS* models presently in vogue in integrity research literature do not account for the requirement of continuous origination of information endogenous to the specific decision situation. Their main concern is *only* that information technology accesses, communicates, processes and distributes the *already* generated information. With information technology costs ever decreasing, the information processing for decision-making is, therefore, taken as a *costless* activity; resulting in *IS* models having no explicit reference to cost-benefit of information processed. The reality and its requirements though are different. The *IS* under consideration comprises individual decision process stages that are characterized by activities of information “origination”, which is a *costly* activity. This calls for cost-benefit analysis framework for information originated and processed, so as to work towards ensuring economic processing of information. It is through control of Information Integrity that this economy is ensured; thereby the cost-benefit analysis framework required in fact being that of Information Integrity. Towards this objective then can be considered development of information Usefulness-Usability-Integrity paradigm with the objective of describing the attributes of Information Integrity.

0-0-0-0-0