Systems of system failures: Meta system methodology to prevent system failures

Takafumi Nakamura1*, Kyoich Kijima2
1Tokyo Institute of Technology, Graduate School of Decision Science and Technology,
2-12-1 Ookayama, Meguro-ku, JAPAN, nakamura.takafu@jp.fujitsu.com
2Tokyo Institute of Technology, Graduate School of Decision Science and Technology,
2-12-1 Ookayama, Meguro-ku, JAPAN, kijima@valdes.titech.ac.jp
*Correspondence can be directed to this author, as the primary contact.

ABSTRACT

We first propose a new meta methodology, called SOSF (Systems of system failures), to prevent system failures. The basic idea of SOSF is inspired by collaborating SOSM (Jackson,M. (2003)) with Taxonomy of failures (Gigch,J.P.Van.(1986)). SOSF tries to map the elements of mata system failure model into SOSM frames. Since SOSF enables us to identify a paradigm of where system failures resides, with its help we can adopt an appropriate methodology to a target problem. Then, we apply the proposed meta methodology to IT systems so as to confirm the results obtained are quite useful for promoting preventative measures that are not learned otherwise.

Every organization has hierarchical structure of their processes. It is very important to identify what function of the organization has to be rectified learning from system failures. In order to achieve this, we must have some common language to understand fully what have happened, what should be a root cause and what should be a counter measure. Various trouble shooting techniques proposed for dealing with systems failures so far mainly have focused on so called hard approaches where reductionism plays a dominant role. This paper, instead, provides one of actual application examples of so called “soft system thinking” (Checkland,P (1999)) in engineering arena.

SOSF is, among others, practically useful to achieve the following tasks. i) To Promote common understanding between various stakeholders by uplifting specific system failure and a specific organizational malfunction into conceptual world through modeling using common (meta) language. ii) To understand system failure holistically through modeling a system failure and its root cause. iii) To identify what function of an organization should be rectified in hierarchy of the organization. iv) To confirm MECE (Mutually exclusive collectively exhaustive) of counter measures.

SOSF is unique in the sense that it could provide various practical application tools, such as SO-space Map, OP Matrix and Failure diagnostic flow. We structuralize the two extremes positions (i.e. ideal status and system failures) into several relations between ideal status, goal (objective), responsibility, causes and system failures. If we can detect disjunctions between elements proactively, there should be a good chance to prevent

further occurrence of system failures by minimizing recognized disjunction between stakeholders.

Keywords: Systems thinking, Meta system approach, VSM, SSM, Double loop learning

1. Introduction

1.1 Meta system methodology and model of system failure

Modeling is a decision-making process in which the problem is defined, the model is applied, and the problem is solved. And metamodeling consists of specifying the requirement that must be met by the modeling process. To metamodel is to design the system that designs. Therefore failure of higher hierarchical level (i.e. metamodeling level) of design will lead to system malfunctions and system failures.

Gigch,J.P.Van.(1986) identifies three phases in the meta system design process. That is (i) reality appreciation (appraising its nature and choice of paradigm), (ii) modeling (problem definition, choice and application of model and appling solution), and (iii) meta-modeling (design the system to design; i.e. double loop learning) In the process it is essential to uplift reality into model to understand reality fully followed by uplifting model into meta-model which is also essential to enhance organizational learning into double loop learning in order to rectify design of the system design.

If the error cause could be identified at higher abstraction level (i.e. modeling or meta modeling), then the coverage of prevention level would be broader than lower abstraction level. (Fig 1.1)

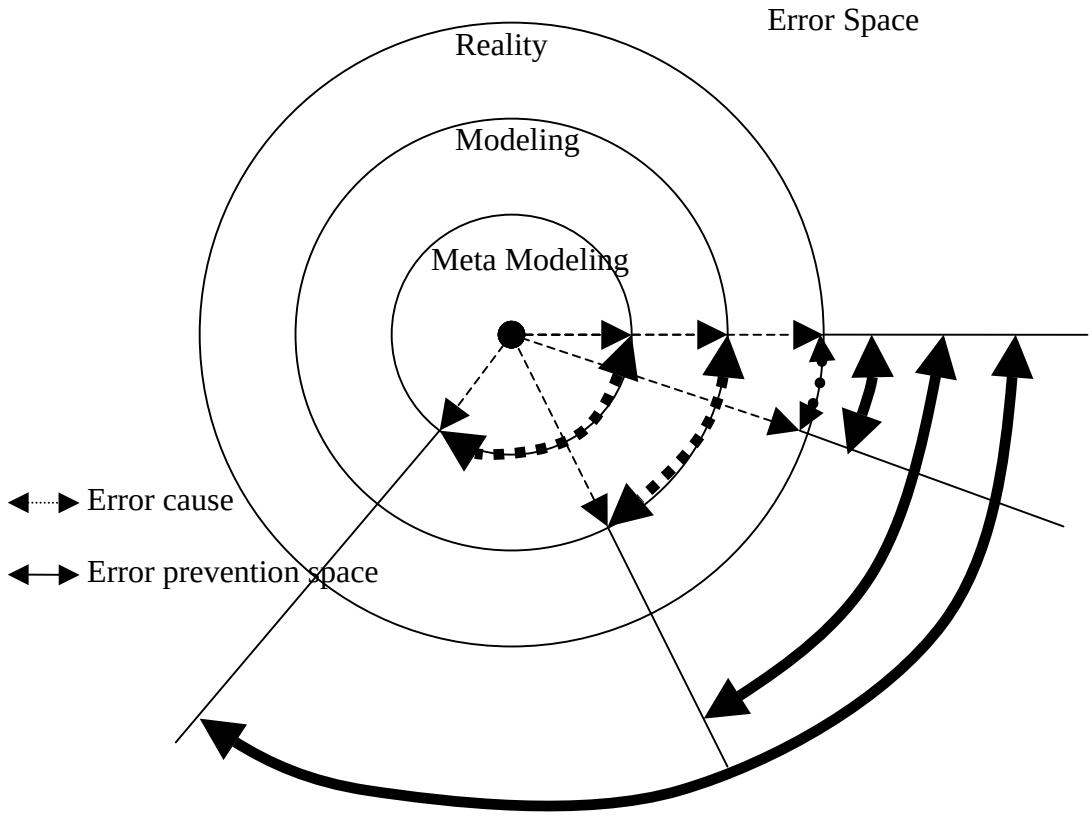


Fig 1.1 Error space and prevention level

In order to redress system malfunction or system failure, among others it is necessary to uplift specific failure event into modeling world (see Appendix 1). Through the process we appraise the nature of reality holistically, and then discuss system failure's model of model phase (i.e. metamodeling) why happened, what is a countermeasure and what should be learned in organization process to avoid further occurrence of system failures.

In this context Beer's VSM model serves very well to rectify organizational process. In the model Systems 1 to 3 correspond to operational level while systems 4 and 5 do to meta level which decide operating norm by communicating with environment outside of the system.

More precisely, at Systems 1 to 3 the system ensures that internal harmony is maintained at level 3 (internal homeostasis). At System 4 it integrates internal and external inputs in order to chart the firm's strategies at level 4 (external homeostasis), while at System 5 the system formulates long-term policies at level 5 (planning, foresight).

It is crucial to reflect deeply upon system4 (external homeostasis) as well as System5 (planning, foresight) for preventing further occurrence of system failures.

1.2 SOSM and SOSF

To propose SOSF, we adopt SOSM as a basic framework. SOSM is the methodology created by Jackson,M (2003) and its main features are as follows: i) Meta systemic approach (soft system thinking to foster double loop learning), and ii) Complementarism by encompassing multi paradigms (contingent approach by combination of various methodologies from various paradigm depending upon problem situations) . Fig.1.2 shows the frame of SOSM. Various systems thinking are located on the space spanned by two dimensions (i.e. Participants and Systems).

SOSF can be designed by allocating each type of failures from Appendix 1 into SOSM space (Fig 1.3). There is no coercive domain in SOSF because the main focus of this paper is on technological systems arena rather than on social systems one. The allocation of each type of failure is quite straightforward from SOSM.

The structure between SOSM and SOSF is sown in Fig 1.4. It is worthwhile to mention recursive feature of SOSF depending upon the view point of the system. If target system breaks down into subsystems, each subsystem has its own SOSF. So the failure of technology might be a failure of evolution form one level down of the view point of subsystem. Also the failure of evolution might be a failure of regulation one level upper of the view point of system of systems.

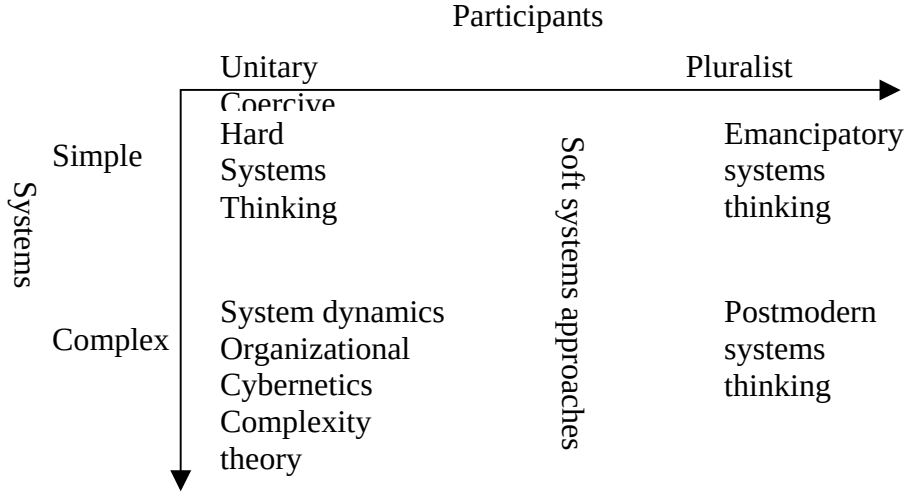


Fig 1.2 systems approaches related to problem context in the System of System Methodologies (SOSM).

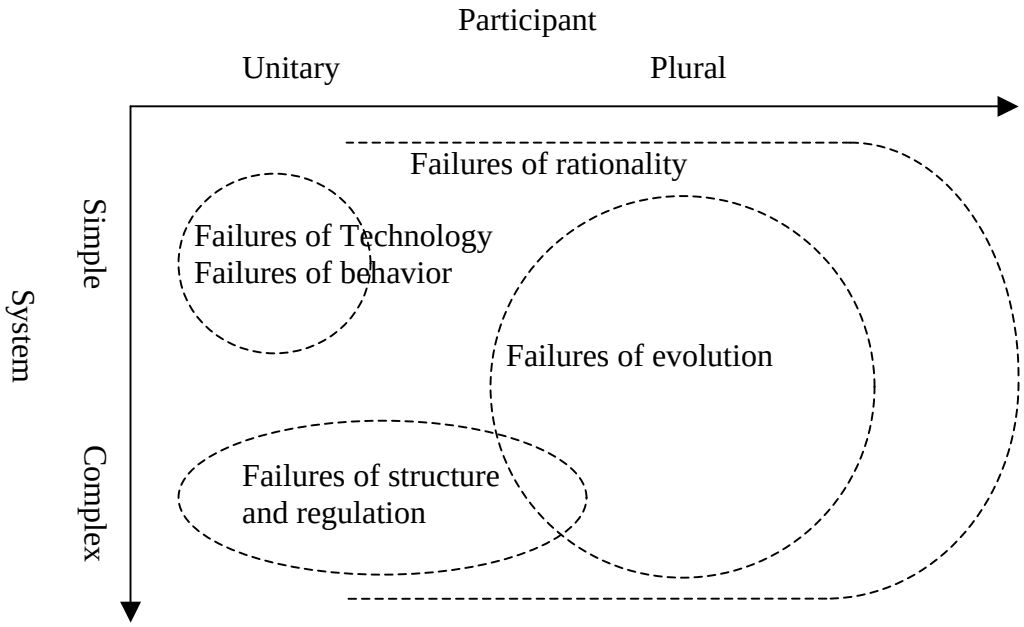


Fig 1.3 SOSF (System of System Failures)

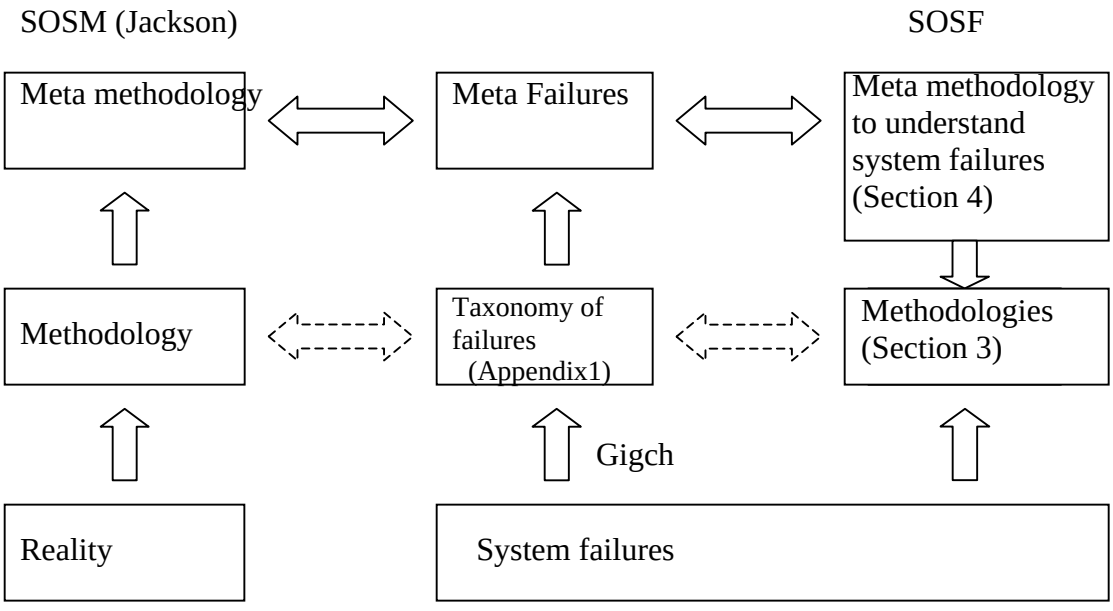


Fig1.4 Meta modeling of system failure and SOSF using SOSM

1.3 The structure of this paper

The structure of this paper is that we first introduce meta methodology named SOSF, then overview the system improvements and its pitfalls in section 2. Section 2 will depict the importance to focus on the various disjunctions between ideal status and problem. This approach is beyond the focus of so called system improvement and indispensable to prevent system failures. It is crucial to ask 'what' rather than 'how' even engineering arena where system improvement playing dominant roles. This is the basic reason to introduce meta methodological approach. Then we introduce various practical tools to surface disjunctions in section 3 followed by synthesising SOSF and tools into Diagnostic failure flow in section 4. And concluding remark is to denote further elaboration of the methodology to manage organizational decision making failures as the next task.

2. System improvement pitfalls; Clarification of the structure between ideal status and problems

In every organization it is vital to improve their system to prevent system failures proactively. The ability to learn in order to rectify current operating norms from meta modelling perspective is one of the indispensable critical success factors for todays' firm. From the view point of system improvement, the main problems to be solved are the followings:

- The system does not meet its established goals.
- The system does not yield predicted results.
- The system does not operate as initially intended.

However the treatment of system problems by improving operation of existing systems bounds to fail. System improvement can work only in the limited context of small systems with negligible interdependence with other systems. Gigch.J.P.Van (1991) points out the main shortcomings of system improvement as follows.

1) Looking for causes of malfunctions within system boundary.

This is the pitfall for local optimization. The rational of system improvement tends to justify systems as ends in themselves without considering that a system exist only to satisfy the requirements of larger systems in which it is included.

2) Restoring the system to normal

This is the pitfall to keep status quo. A lasting solution cannot result from an improvement in the operation of presently existing systems. An improvement of operations is not a lasting improvement.

3) Incorrect and obsolete assumption and goals

This is the pitfall of failure to evolve. It is not difficult to find organizations in which the formulation of assumptions and goals has not been explicit. Therefore there are potential to introduce stakeholders' responsibility disjunctions. To foster system improvement in this context is senseless.

4) Planner Leader or Planner follower

This is the pitfall for pursuing wrong goal (i.e. effectiveness vs. efficiency). Another manifestation of the problem of holding the incorrect assumptions and pursuing the wrong goals can be traced to different concepts of planning and of the planner's role. In the context of system design, the planner must be a "planner leader: planning to influence the trends" instead of a "planner follower: planning to satisfy the trends".

Bignell,V. and Fortune, J.(1984) denote that the assessment of an outcome as failure is dependent upon the values held by the person making the judgement. We can never be completely sure because an understanding is subjective and disputable: different people may identify different sets of failure contributory factors. Therefore it is important to aware intentionally the disjunction arising from i) out of system boundary and other environmental change and ii) other stakeholders' world view. The awareness of disjunctions is indispensable to overcome above mentioned system improvement shortcomings. These disjunctions are fatal blind spot for system improvement perspective that is bound to become system failures. Therefore detecting various disjunctions proactively is vital to achieve organizational idealistic goals. Every organization peruses its goal, various problems emerges during its activity. It is necessary to clarify the structure between ideal status and problems.

It is natural to assume the following five elements between ideal status and problems and its features.

1) Ideal status: Ideal status should be covered by goals.
2) Goals (objective): Goals should relate responsible agents.
3) Responsibility: Responsible agent relates problems' causes.
4) Causes: Causes incurs problems.
5) Problems: Problems have its causes. It may not always obvious.

All elements are value dependent of stakeholders subjectivity. Therefore they may have disjunction between what is designed and what should be designed depending upon stakeholders' view. Fig 2.1 shows the above mentioned relationship. It is necessary to have cognitive filter to see above mentioned disjunctions. We propose SOSF and some tools to functionalize as cognitive filter through which we can see various disjunctions. Every disjunction between the elements should be fulfilled to prevent further occurrence of system failures. Based on the shortcoming of system improvement as Gigch.J.P.Van

(1991) pointed out and disjunctions between the above five elements, Cognitive filter should have following features.

1) It should navigate whole SOSF space and identify appropriate causes thoroughly.
2) It should surface disjunction between ideal status and problem.
3) It should manage recursive feature of SOSF

We will provide a diagnostic flow consisting of various tools to satisfy above features. The diagnostic flow will identify all of five error types then confirm disjunction between stakeholders. The detail will be discussed in section 4.

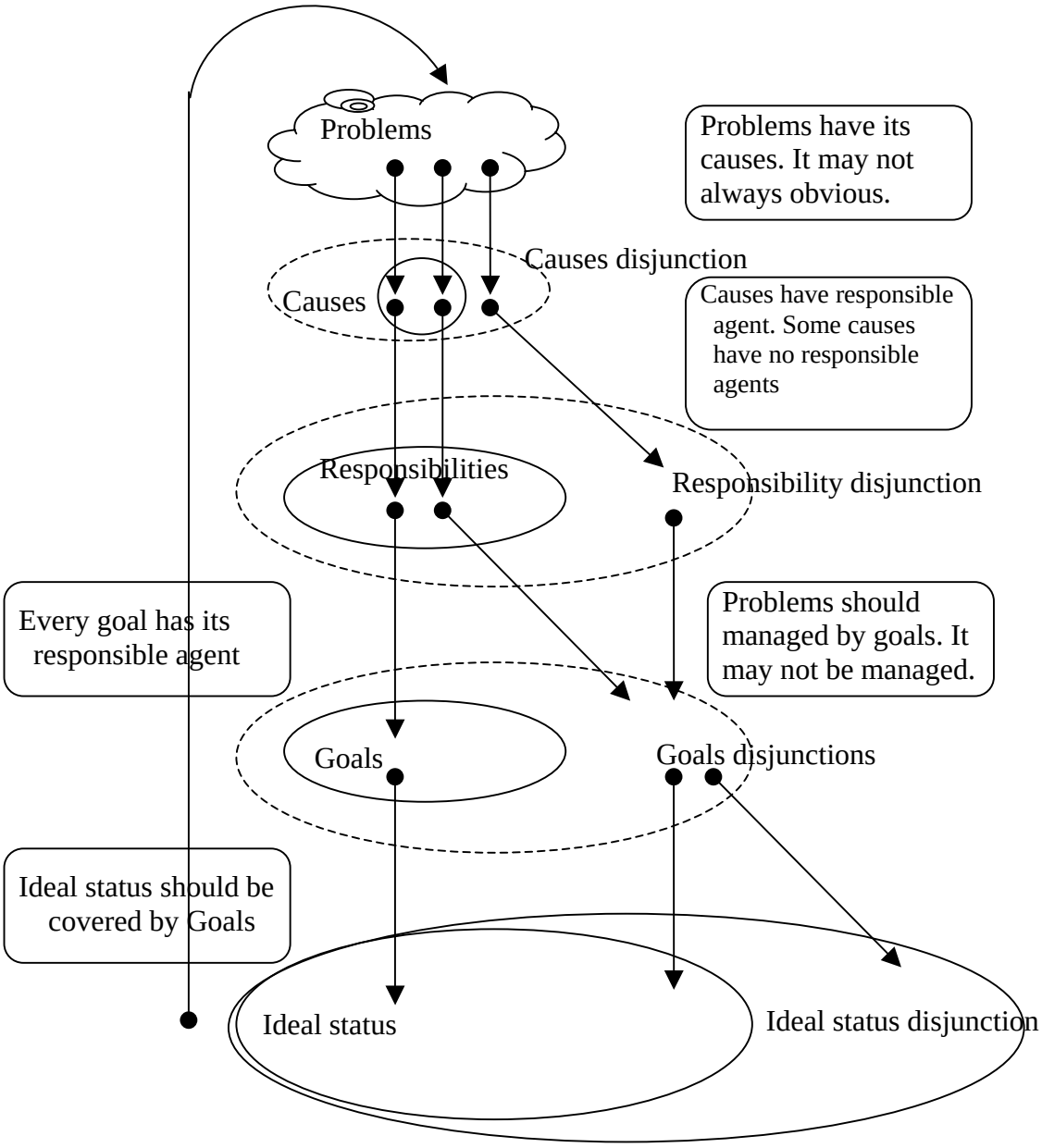


Fig 2.1 Ideal status—Goal—Responsibility—Cause—Problem Relationship

3. Introduction of various Tools and cognitive filter to identify problem paradigm

There are several paradigms as Jackson introduced in the SOSM. They are hard system thinking, Soft system thinking and others. First we introduce several tools to identify problem paradigm to solve problem effectively through understanding problem nature holistically. Then in the next section we construct diagnostic failure flow. Fig 3.1 shows

relation between cognitive filter and problem paradigm. Cognitive filter should play a role of diagnosing system failures. Diagnosing flow navigates all of SOSF space; this is essential to assure that all of possible causes are thoroughly checked and identifies its paradigm.

SO-Space Map

SO stand for Subjective view and Objective view. SO-space is spanned by two dimensions. If goals or causes are target of examination, they are relating with responsible agents as explained at section 2. It is essential to minimize disjunction between stakeholders, and SO-space Map is useful to surface hidden presumption or illusion tacitly holding by each stakeholder.

The practical utilization of SO-Space Map is to clarify failure causes during diagnosing system failures (Fig 3.2 and Fig 3.3). If there is no responsibility disjunction between stakeholders, there is most likely the case that the problem is within system boundary (i.e. Failure of technology, structure and control). Otherwise, it may be the failure of evolution or rationality and the counter measure should be studied whether to change the current operation norm after debating between stakeholders. After accommodating disjunction surfaced by SO-Space Map, ultimate idealistic status of SO-Space Map would be i) no responsibility disjunction between stakeholders and ii) confirm MECE under single subjective stakeholder (Fig 3.4).

OP Matrix

OP stands for Objective and Problem. This matrix is used to surface disjunction between Objective and Problem to verify current objectives are well encompassing past system failures (Fig 3.5). This is useful to check the plural system failures experienced during certain period of time rather than to use when each single system failure happens. This is to verify current directions of system following on the right track to idealistic goal.

For example, similar type of problem continues happening although current organizational goal (objectives) are achieved. This is most likely the case of disjunction of goal setting between stakeholders, further attention of higher level (system 3, 4 or 5) should be required to check if the real cause of goal setting disjunction. If necessary identify appropriate stakeholder who cover new goal through debating between stakeholders and alter current system which is either to change operation norm or outer environment. The other scenario is that similar problems have not been appeared yet some of the organization goals have not achieved. This could be a sign of system failures, so that the past failure analysis and counter measure should thoroughly checked as a preventative measure.

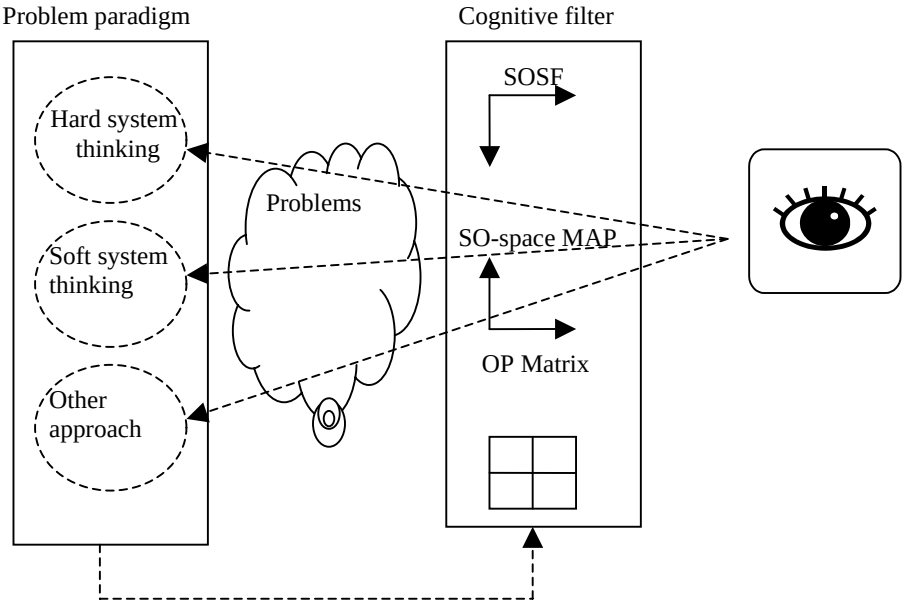
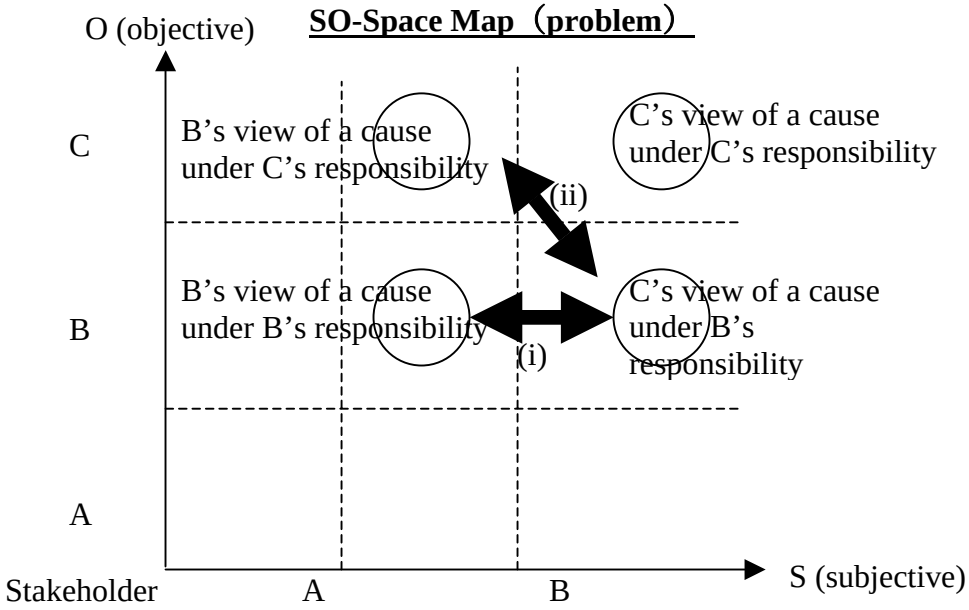


Fig3.1 Cognitive filter and problem paradigm



(i) In case of identical, system failure reside in hard system paradigm
(ii) In case of disjunction, system failure reside in soft system paradigm

Fig 3.2 SO-Space Map (problem)

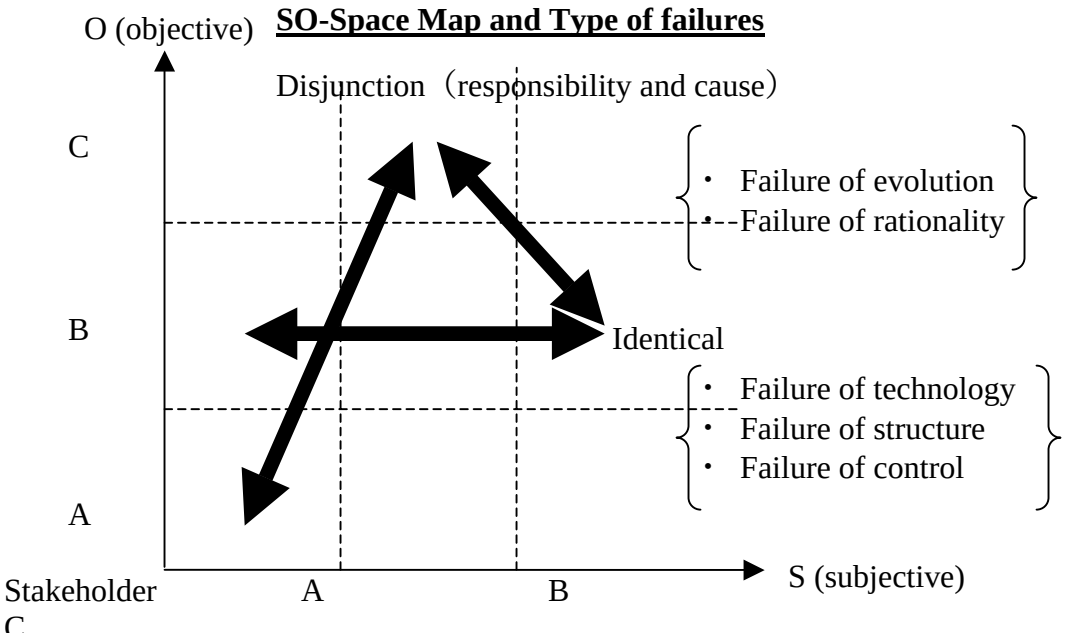


Fig 3.3 SO-Space Map and type of failures

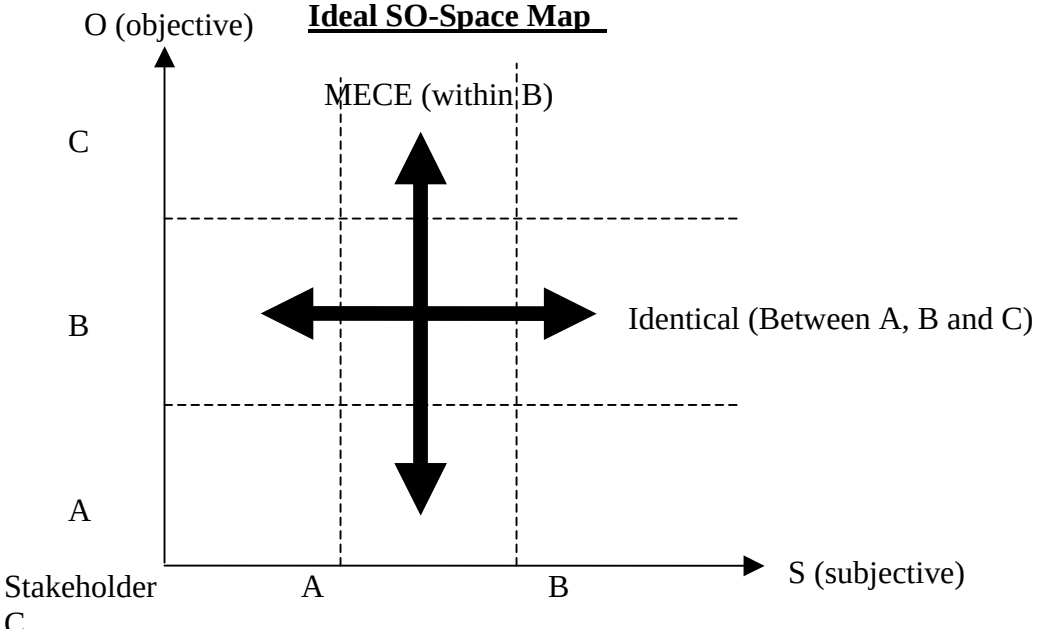


Fig 3.4 Ideal SO-Space Map

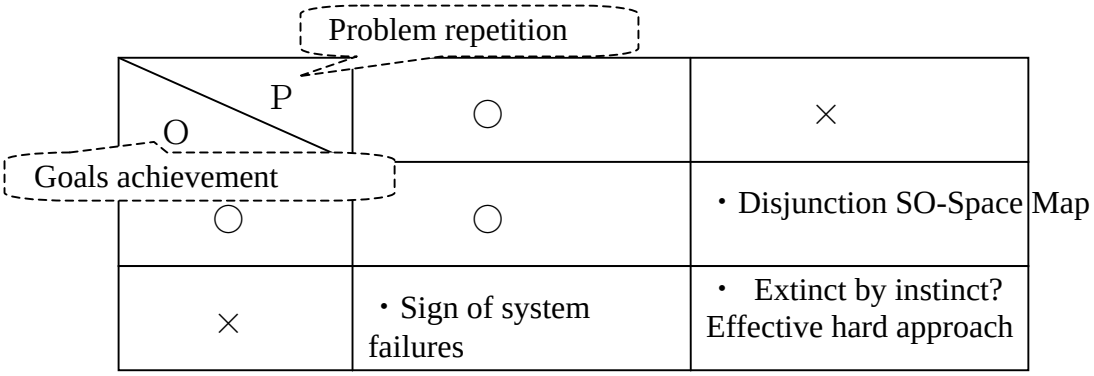


Fig 3.5 OP Matrix (Objective-Problem)

4. Diagnostic system failures flow

Now we propose cognitive filter to identify problem paradigm. Based upon the previous discussion, the proposed cognitive filter should satisfy two requirements. The first requirement is it could manage recursive feature of SOSM and the second requirement is it could promote double loop learning.

The first requirement (i.e. managing recursive feature of SOSF) should be satisfied through checking all of the five error types in SOSF (i.e. Failure of i) technology, ii) behaviour, iii) structural and regulation, iv) evolution and v) rationality). The failure of technology resides in unitary-simple domain of SOSF space. However, if we drill down the target system into subsystems, the failure of technology of higher-level might have plural-complex features in lower subsystem level. Therefore diagnostic system failure flow should have disjunction check even for the type of unitary failure type as failure of technology. Fig 4.1 is the cognitive filter to diagnose system failure. Left hand side ensures to verify entire SOSF space has to be navigated corresponding above mentioned five failure types. This ensures to manage recursive feature of SOSF. And due to the recursive feature of diagnostic failure flow, every level of organization in Beers' notation can be applicable to diagnose malfunctions.

The second requirement (i.e. promoting double loop learning) should be satisfied through detecting disjunction between stakeholders. Right hand side of Fig 4.1 utilizes OP Matrix and SO-Space Map to identify problem paradigm to invoke debate between stakeholders by surfacing various disjunctions. In case of any disjunctions, debate should be required between stakeholders to confirm cause and responsibility. In case to rectify process, system level in Beer's notation should be intentionally aware depending upon the problem paradigms (i.e. hard or soft). This promotes double loop learning by adapting outer environmental change to evolve and breaking status quo. Fig 4.2 is the summary of cognitive filter system which generates two outputs, one is new goal and the other is new process. This system promotes double loop learning as well as managing recursive feature of SOSF as explained above.

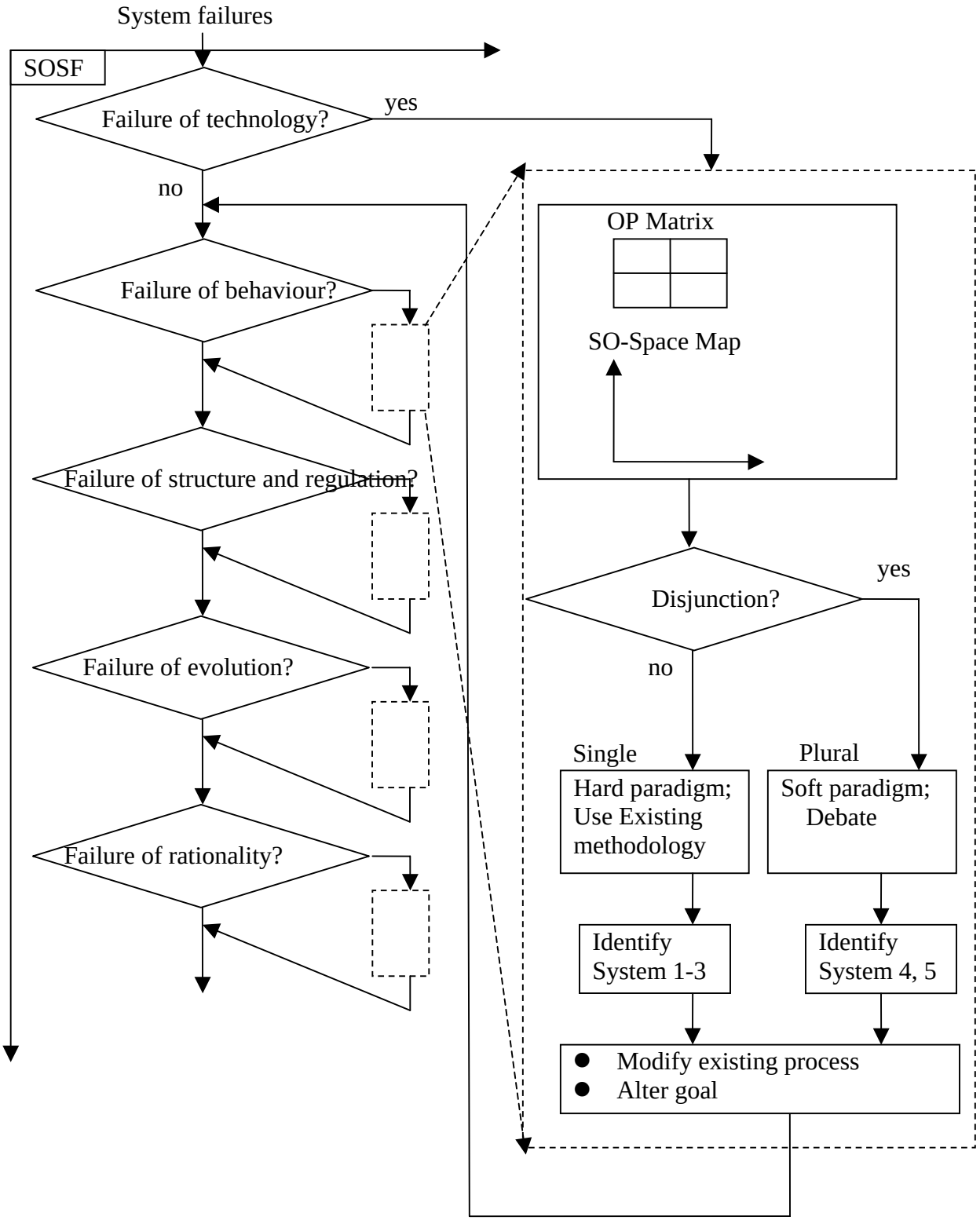


Fig 4.1 Diagnostic failures flow as cognitive filter

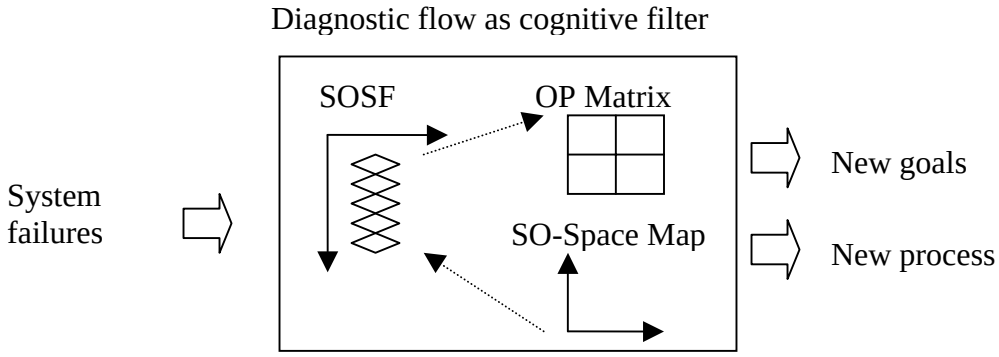


Fig 4.2 Cognitive filter system

5. Concluding remark

The methodologies to enhance IT system's safety and security have well established and they have become international standards as ISO or IEC. However current existing methodologies or norms are based mainly upon hard systems thinking or goal seeking model. This is the realm of system improvement as mentioned in section 2. There are few strands or methodologies which pursue "what" rather than "how". The problem is not the ISO or IEC standard but the ability to question reality and to change status quo. This ability will promote double loop learning process in organizations therefore will prevent system failures. We have proposed a meta methodology to focus on disjunction between various stakeholders to prevent system failures.

For further research we need to verify real application example to improve proposed methodology in terms of organization decision making better. Also in this paper we mainly applied system thinking in diagnosing system failures and little focus on organizational decision making. Next task is to elaborate organizational decision failure based upon organizational decision making model to study root cause of system failures from different perspective.

References

Beer,S.(1979). The Heart of Enterprise. John Wiely & Sons.
Beer,S.(1981). BRAIN OF THE FIRM, second edition. John Wiely & Sons.
Bignell,V. and Fortune, J.(1984). Understanding System Failures. Manchester University Press.
Checkland,P.(1981). System thinking, system practice. John Wiely & Sons.
Gear,M.C., Hill,M.A. and Liendo,E.C.(1981).Working Through Narcissism. J.Aronson
Gigch,J.P.Van.(1986). Modeling, Metamodeling, and Taxonomy of System Failures. IEEE trans. on reliability, vol. R-35, No.2, 1986 June pp131-136

Gigch,J.P.Van.(1991). System design Modeling and Metamodeling. Plenum
Jackson,M.(2003).System Thinking-Creative holism for Managers. John Wiely &Sons.
Kickert,W.J.M.(1980).Organization of decision-making. North Holland
Kontaratos,A.N.(1974). "A system analysis of the problem of road casualties in the United States". Accident analysis and prevention, vol6, 1974, pp223-41
Prigogine,I.(1976). "Order through fluctuation: Self-organization and social systems," in Evolution and Consciousness, edited by Jantsch,E.,Waddington,C.H. Addison-Wesley.

Appendix1. Taxonomy of System Failures

Type of failure	Symptom or component	Problem or malfunction
FAILURE OF STRUCTURE	Levels of recursion & Domain Structure	Not specified or not clearly defined Subsystem, Aspects systems, and Phase systems not performing assigned functions (Kickert, W.J.M., 1980).
FAILURE OF TECHNOLOGY	Hardware Software	Problem of design Human error Problem of design Human error
FAILURE OF REGULATION	*Regulation & control* (Beer,S., 1979,1980) Viability Anti-Oscillatory Cohesiveness and variety matching Viable regulation	 System One not viable System Two not formalized Systems Three, Four, and Five not Providing Requisite Variety Model of Regulated System not Available or Formalized
FAILURE OF RATIONALITY	*Evidence* Data Information Intelligence *Rationalities* Structural Evaluative Substantive Procedural	*Dysfunctions* Structural Teleological Closure Disjunction Compatibility

FAILURE OF BEHAVIOR	Receptor (SYNTACTICS & SEMANTICS)	*Perceptual malfunction* No Message from Sender to Receiver Wrong Message is Sent Message is not Received or Sender/Receiver Does not Hear Message Use of Improper Codes
	Central mechanism (PSYCHOLOGY)	*Decisional malfunctions* (Gear,M.C., Hill,M.A. and Liendo,E.C.,1981) Mutilation Repression Projection Transduction Renegation Evacuation Introjection Suppression Rationalization
	Effector (ERGONOMICS)	*Executional malfunctions* (Kontaratos,A.N. 1974) Intentional Responses Unintentional Responses Neuromuscular Disabilities Inadequate Ergonomic Design Inadequate Knowledge and Training Unfamiliarity with Systems Limitations and Handling Capabilities
	User (PRAGMATICS)	*Influence* Meaning of Message or Its Consequences not Understood Influence of Message Placed into Question Awareness of Respondent Questioned World-Views or Mindscapes Mismatched
FAILURE OF EVOLUTION (Prigogine,I.1976)	Disjunction of Values Disjunction of Structure	Mismatch Between Values and World Views of Decision Makers and Environment Mismatch Between Structure of Organization and Environment Demands

	Order Through Fluctuation	System Goes Over Threshold of Stability Mismatch in Variety Between System and Controller