Hierarchy of Information Security Issues in Indian Context

MM CHATURVEDI, MP GUPTA AND JAIJIT BHATTACHARYA

Introduction

Ongoing research at IIT Delhi has identified most important issues connected with Information Security using Delphi methodology. The Delphi methodology (Dalkey, 1963; Gordon, 1964; Linstone, 1975; Turoff, 1970 ; Rowe, 1999) , is a social research technique which seeks to obtain a reliable group opinion from a set of experts. This is a method of structuring communication between experts who can provide valuable aid for solving a complex problem. It has been used since the sixties in academic and business spheres and has been employed principally as a technique for planning and consensus in uncertainty situations in which it is not possible to use other techniques based on objective information. In this paper we attempt to generate a view of the interplay and dependency of these already identified issues using Interpretive Structural Model (ISM).

Analysis of interplay of dependency among issues

The ISM is helpful tool to capture the consensus views of the experts about causal relationships of various issues connected with a complex problem (Warfield, 1974). The experts work in group setting to indicate dependency of related issues. In any

complex problem solving context certain issues are more important than others and the prioritization of issues is essential. When the number of involved issues are less we can intuitively reach this prioritization. However in complex context like the one under study having large number of diverse issues, our ability to reach pragmatic conclusions and communicate to others our rationale for prioritization of issues intuitively is not dependable and more structured methodologies like ISM have to be used. The rigor of ISM methodology provides us ability to separate various issues in well defined levels much like the process of fractional distillation of petroleum and its products. The details of ISM methodology are provided at **Appendix "A"** to this paper. The identified key Information Security issues using Delphi methodology are listed in Table 1 of **Appendix "A"** .The issues are allocated code numbers to facilitate their convenient representation in various matrices used in ISM technique and subsequent analyses.

Dependency Structure of identified key Information Security issues

The ISM analysis provides us a hierarchy of key in the form of a diagraph depicting dependency relationships as shown in Figure 1.

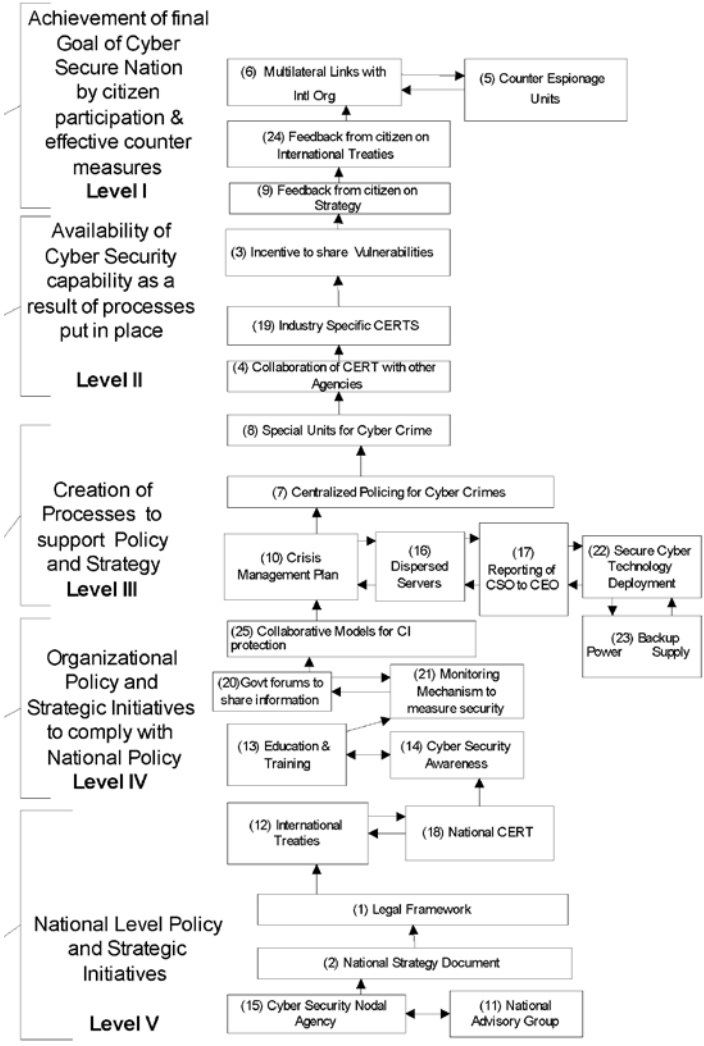
Analysis of hierarchical relationships of key issues

As can be seen the national level policy and initiatives (shown as level V issues in Figure 1) viz. Cyber Security Nodal Agency at national level (15) and National Advisory group (11) combine to design a suitable National Strategy to secure cyber space (2). The strategy drives the national effort for creation of effective legal framework. The legal framework facilitates engagement with International entities (12) both nation states and institutions by way of formal treaties. The creation and empowerment of national level Computer Emergency and Response Team (CERT) (18) to engage with other countries' CERTs and internal coordination is possible under suitable legal provisions.

The organisational initiatives (shown as level IV issues in Figure 1) by way of Cyber Security Awareness (14), Education and Training (13), Monitoring mechanism to measure security (21), Government forums to share information (20) and finally creation of collaborative models for protection of Critical Infrastructure (CI) (25) become basis for sustainable processes.

The creation of processes (shown as level III issues in Figure 1) like ensuring back up power supply (23), geographically dispersed servers (16), Cyber Security Officer reporting directly to CEO thus enhancing security perception of the top

Figure 1: Hierarchical Diagraph of Key Issues of Information Security



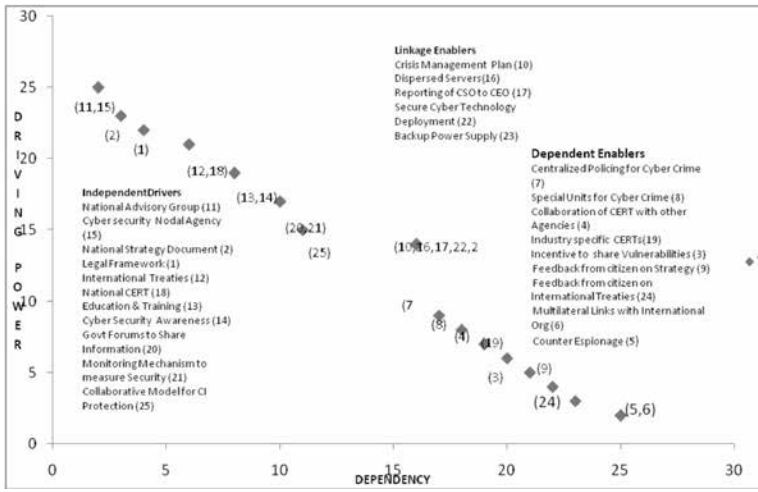
management (17), secure cyber technology deployment (22) and availability of detailed crisis management plan (10) are essential pre conditions to acquire capabilities for cyber security.

These achieved capabilities (shown as level II issues in Figure 1) as a result of processes put in place are centralised policing of cyber crime (7), creation

of special units for cyber crime (8), collaboration of Indian CERT with other agencies (4), and finally incentive to share vulnerabilities (3).

The above indicated capabilities would help India in achieving her final goals of a cyber secure nation by (shown as level I issues in Figure 1) proactive involvement of citizen in reviewing national strategy / international treaties (9) (24), establishment of multilateral international links and counter espionage units (6) (5).

Figure 2: Plot of Issues using Dependency and Driving Power in Reachability Matrix



Driving power and dependency of Indicators

The reachability matrix (refer table 3 in Appendix "A") indicates driving power and dependency of elements. In reachability matrix the driving power and the dependency of each of the 25 elements are calculated by totaling entries with 1's in the row and column emanating from the elements. Based on the driving power and dependency of elements they have been plotted in Figure 2.The indicators having strong driving power and weak dependence are called "Independent enablers". The indicators having strong driving power and also strong dependence are called "Linkage enablers". These enablers are unstable in the sense that any action on these enablers will have an effect on others and also a feedback on themselves. The third group consists of "Dependent enablers" that have weak driving power but strong dependency. Variables with very strong driving power are called key variables and fall in the category of independent and linkage enablers.

This analysis reinforces the importance of independent drivers listed below. Adjacent to the listed indicators, driving power and dependency are indicated within

bracket. The independent drivers are analogous to roots of a tree. The foundational deep drivers with highest driving power viz. National Advisory Group, Cyber security Nodal Agency, National Strategy Document, Legal Framework facilitate engagement with International entities creation and empowerment of national level Computer Emergency and Response Team (CERT).

Cyber Security Awareness reinforces Education and Training on Cyber Security issues. Establishment of government forums to share information with private sector provides nurturing environment for organisations to setup monitoring mechanism to measure Security and thus pave the way for collaborative model for Critical Infrastructure (CI) protection.

- National Advisory Group (25,2)
- Cyber security Nodal Agency (25, 2)
- National Strategy Document (23,3)
- Legal Framework (23,3)
- International Treaties (22,4)
- National CERT (22,4)
- Cyber Security Awareness (21,6)
- Education and Training (21,6)
- Government Forums to Share Information (19,8)
- Monitoring Mechanism to measure Security (19,8)
- Collaborative Model for CI Protection (15,11)

The linkage enablers given below are the processes that help us achieve capabilities for cyber security. These processes are also termed key variables along with Independent Drivers. They are characterized by high driving power and high dependency. The high dependency renders them particularly sensitive to indirect links and their importance gets amplified when effect of indirect links is factored in. The linkage enablers are analogous to trunk and branches of a tree.

- Crisis Management Plan (16,14)
- Geographically Dispersed Servers to enhance disaster recovery (16,14)
- Reporting of Cyber Security Officer to CEO to enhance top management awareness of Cyber Security (16,14)
- Secure Cyber Technology Deployment (16,14)
- Sustainable Backup Power Supply for enhancing availability (16,14)

The dependent enablers given below are the capabilities and the final goals of a cyber secure organisation. They are characterised by weak driving power

and high dependency. These are the fruits of the cyber security tree. Fruits are dependent on roots (independent enablers) and trunk/branches (linkage enablers) for their sustenance.

- Centralised Policing for Cyber Crime (9,16)
- Special Units for Cyber Crime (8,18)
- Collaboration of CERT with other Agencies (7,19)
- Industry specific CERTs (6,20)
- Incentive to share Vulnerabilities (5,21)
- Feedback from citizen on Strategy (4,22)
- Feedback from citizen on International Treaties (3,23)
- Multilateral Links with International Organizations for effective mitigation of the cyber threats (2,25)
- Creation of Counter Espionage units for proactive protection of nation's Cyber domain (2,25)

Managerial Insights

The findings of this research are indicative of our current concerns. The national level strategy, nodal agencies, evolved and functional legal framework are need of the hour. For developed countries with evolved legal frameworks and national level strategy in place, these aspects are taken for granted, as they are at higher point in the maturity continuum. In this context, it is helpful to recount the works of Chew et al (2008) who suggested viewing the cyber security in terms of leading, coincident, and lagging indicators. A coincident indicator reflects security conditions happening concurrently, while leading and lagging indicators reflect security conditions that exist respectively before or after a shift in security. The hierarchical structure (refer figure 1) created using ISM brings distinction between leading and lagging indicators. The level V variables are leading indicators compared with level I and II variables. It implies that presence of lagging variable depends on leading variable and even if the leading variables are withdrawn the level I and II variables may continue to be manifested for sometime as they are lagging variables. Stoppage of watering the roots would show effect on the condition of branches after some elapsed time. There can be no sustainable cyber security at national level without these leading indicators.

India as a developing country appears to be at level V and IV where national strategy of cyber security and legal framework are articulated. ISO 17799 has been adopted as security standard, and alignment of IT act 2000 to the emerging cyber security challenges has been attempted by recent amendments in February

2009 and formulation of rules under the act (DSCI, 2010). Creation of processes has stabilised in some premier IT companies and financial sector to ensure mandatory compliance with relevant cyber security standards (DSCI, 2010). Proactive regulatory framework and matching capability in law enforcement agencies would provide the nurturing environment to mitigate cyber threat.

Concluding Remarks

This paper has evolved the hierarchical relationship of identified key Information Security issues. The stages in achieving a cyber secure nation status are delineated using rigorous ISM methodology. Information Security maturity of all organizations and nations evolves through a continuum. We cannot skip the intermediate stages and jump to final state of Cyber Security. The fruits of Cyber Security are not possible without root, trunk and branches of the Cyber Security infrastructure "tree". As India evolves on her journey to secure cyber space the insights generated by this analysis may be useful to policy makers.

Air Cmde **MM Chaturvedi** (Retd) is a retired Indian Air Force officer pursuing PhD at IIT Delhi, Prof. **M.P.Gupta** is Chair-Information Systems Group and Coordinator-Center for Excellence in E-gov at the Department of Management Studies, Indian Institute of Technology (IIT Delhi).
Dr. Jaijit Bhattacharya is an e-Governance expert and is Adjunct Professor at IIT Delhi and President of Centre for Digital Economy Policy Research (C-DEP).

References

Chew Elizabeth et al. (2008). Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Revision 1, July 2008, http://csrc.nist.gov/publications/nistpubs/800-55 rev1/sp800-55.pdf

Dalkey, N. and Helmer, O. (1963). An experimental application of the Delphi Method to the use of experts. *Management Science. 9 (1963) 458–467.*

DSCI(2010). Data Security Council of India, http://www.dsci.com.in. Accessed on 25
February 2010.

Gordon, T.J., Helmer, O. (1964). *Report on a Long-range Forecasting Study*, The Rand Corporation P-2982, Santa Monica, CA.

Linstone H.A., Turoff M.(1975).(Eds.), *The Delphi Method, Techniques and Applications*, Addison–Wesley, Reading, MA, 1975.

Rowe, G. and Wright G. (1999), The Delphi technique as a forecasting tool: issues and analysis, *Int. J. Forecast. 15 (1999) 353–375.*

Turoff, M.(1970).The design of a Policy Delphi, *Technol. Forecast. Soc. Change 2(1970) 149–171.*

Warfield, J.W. (1974). Developing interconnected matrices in structural modeling. *IEEE Transactions on Systems Men and Cybernatics, Vol. 4 No.2, pp.51-81*

Appendix "A"

Details of ISM Methodology

ISM as propounded by Warfield (1974) is an interactive learning process whereby a set of different directly and indirectly related elements are structured into a comprehensive systemic model. The model so formed portrays the structure of a complex issue in a carefully designed pattern employing graphics as well as words. For complex problem like Cyber Security, a number of enablers may be influencing the final goal of effective Cyber security. However, the direct and indirect relationships between the enablers describe the situation far more accurately than individual factors taken in isolation. Therefore, ISM develops insight into collective understanding of these relationships.

The ISM methodology is interpretive, from the fact that the judgment of the group decides whether and how the variables are related. It is structured too, as on the basis of relationships an overall structure is extracted from the complex set of variables. It is a modeling technique in which the specific relationships of the variables and the overall structure of the system under consideration are portrayed in a diagraph model. ISM is primarily intended as a group learning process.

ISM methodology suggests the use of the expert opinion based on various management techniques such as brain storming, nominal group technique, etc in developing the contextual relationship among the variables. This paper is using as an input to ISM the critical cyber security issues identified by the members of an Indian cyber security group. The dependency relationships between these issues are depicted in the form of Structured Self Interaction Matrix (SSIM), as per the following convention:

V : enabler *i* will ameliorate enabler *j*;
A : enabler *j* will be ameliorated by enabler *i*;
X : enablers *i* and *j* will ameliorate each other;
O : enablers *i* and *j* are unrelated.

The variable code numbers in SSIM are as described in Table 1. SSIM derived for our context using above convention is shown in Table 2.

The dependency relationship used to construct SSIM is based on consensus view of available cyber security experts in a security forum in India. The SSIM is transformed into a binary matrix, called reachability matrix as shown in table 3 by substituting V,A, X,O by 1and 0 as per the following rule:

- If the (*i* , *j*) entry in the SSIM is V, then the (*i* , *j*) entry in the reachability matrix becomes 1 and the (*j*,*i*) entry becomes 0;
- If the (*i* , *j*) entry in the SSIM is A, then the (*i* , *j*) entry in the reachability matrix becomes 0 and the (*j*,*i*) becomes 1;
- If the (*i* , *j*) entry in the SSIM is X, then the (*i* , *j*) entry in the reachability matrix becomes 1 and the (*j*,*i*) entry also becomes 1; and
- If the (*i* , *j*) entry in the SSIM is O then the (*i* , *j*) entry in the reachability matrix becomes 0 and the (*j*,*i*) entry also becomes 0.

Following these rules and after checking transitivity rule the final reachability matrix is created. According to transitivity rule for any elements *A, B* and *C* and set *S,* given that *A* ***R*** *B* and *B* ***R*** *C*, it necessarily follows that *A* ***R*** *C*. If the transitivity rule is found not to be satisfied, the SSIM is reviewed and modified. In reachability matrix the driving power and the dependency of each of the 25 elements are calculated by totaling entries with 1's in the row and column emanating from the elements. The driving power and dependency of elements are used for grouping them in terms of independent, linkage and dependent elements.

Identifying Hierarchy of Indicators

From the final reachability matrix, the reachability (R(P)) and antecedent (A(P)) set (Warfield, 1974) for each element are found. The reachability set consists of the element itself and the other elements which it may impact where as the antecedent set consist of the element itself and the other elements which may impact it. There after the intersection of these sets is derived for all the elements. The elements for whom reachability and the intersection sets are same occupy the top level in the ISM hierarchy. Once the top- level element is identified, it is separated out from the other elements in the next level. The top-level element is the final objective of the complex problem under study and is having least driving power and maximum dependency. Elements identified for next levels are contributing to achievement of the top-level elements. Their ability to contribute (driving power) is dependent on their level in the hierarchy. The bottom most level which is revealed last has maximum driving power. This process is continued until level of each element is found.

In table 4 first iteration of level partitioning of reachability matrix is depicted. Elements 5, 6 are at level 1 because R (P) and intersection of R (P) and A (P) are identical for both 5 and 6. After separating out 5, 6 from the above table, next level (2) is found to be 24 as R (P) and intersection of R (P) and A (P) are identical.

Continuing these process lower levels is identified. Level 3 to 16 are indicated below with the elements placed next to them in bracket.

Level 3 (9) ; Level 4 (3); Level 5 (19); Level 6 (4);Level 7 (8); Level 8 (7);Level 9 (10 ,16,17,22,23) ;Level 10 (25) ;Level 11 (20,21) ;Level 12 (13,14) ;Level 13 (12,18) ;Level 14 (1) ; Level15 (2) ; Level 16 (11,15).

These levels are used to draw digraph shown at Figure 6.1.The term diagraph denotes the graphical relationship of elements connected by arrows from the bottom most level to succeeding levels. The bottom most level (level 16) elements are placed at the base of diagraph and connected to next level (level 15) elements. As we move up from the bottom most level the driving power decreases and dependency increases. The level 16 elements have maximum driving power and least dependency while level 1 elements have least driving power and maximum dependency.

The details of SSIM and reachabiliy matrices and level partitioning are placed at table 2, table 3 and table 4 respectively.

Table 1: Important Issues identified by Delphi Panel

Code no in ISM Analysis	Description of Issues
1	Legal Framework
2	National Strategy Document
3	Incentive to share Vulnerabilities
4	Collaboration of CERT with other Agencies
5	Counter Espionage Units
6	Multilateral Links with International Organizations
7	Centralized Policing for Cyber Crimes
8	Special Units for Cyber Crime
9	Feedback from citizen on Strategy
10	Crisis Management Plan
11	National Advisory Group
12	International Treaties
13	Education and Training
14	Cyber Security Awareness
15	Cyber Security Nodal Agency
16	Dispersed Servers
17	Reporting of CSO to CEO
18	National CERT
19	Industry Specific CERTs
20	Govt forums to share information
21	Monitoring Mechanism to measure security

22	Secure Cyber Technology Deployment
23	Backup Power Supply
24	Feedback from citizen on International Treaties
25	Collaborative Models for CI protection

Table 2: Structured Self Instruction Matrix (SSIM)

	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2
1	V	V	V	V	V	V	V	V	V	V	A	V	V	V	A	V	V	V	V	V	V	V	V	A
2	V	V	V	V	V	V	V	V	V	V	A	V	V	V	A	V	V	V	V	V	V	V	V	
3	A	V	A	A	A	A	A	A	A	A	A	A	A	A	A	A	V	A	A	V	V	A		
4	V	V	V	A	V	A	V	A	A	V	A	A	A	A	A	A	V	A	A	V	V			
5	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	X				
6	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A					
7	A	V	A	A	A	A	A	A	A	A	A	A	A	A	A	A	V	V						
8	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	V							
9	A	V	A	A	A	A	A	A	A	A	A	A	A	A	A	A								
10	A	V	X	X	A	A	V	A	X	X	A	A	A	A	A									
11	V	V	V	V	V	V	V	V	V	V	X	V	V	V										
12	V	V	V	V	V	V	V	V	V	V	V	V	V											
13	V	V	V	V	V	V	V	A	V	V	A	X												
14	V	V	V	V	V	V	V	A	V	V	A													
15	V	V	V	V	V	V	V	V	V	V														
16	A	V	X	X	A	A	V	A	X															
17	A	V	X	X	A	A	V	A																
18	V	A	V	V	V	V	V																	
19	A	V	A	A	A	A																		
20	V	V	V	V	X																			
21	V	V	V	V																				
22	A	V	X																					
23	A	V																						
24	A																							

Table 3: Reachability Matrix

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	Driving Power
1	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	22
2	1	1	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	23
3	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	5
4	0	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	7
5	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
6	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
7	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	9
8	0	0	1	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	8
9	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4

10	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	14
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	25
12	0	0	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	21
13	0	0	1	1	1	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	1	1	1	19
14	0	0	1	1	1	1	1	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	1	1	1	19
15	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	25
16	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	14
17	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	14
18	0	0	1	1	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1	21
19	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	6
20	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	1	1	1	17
21	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	1	1	1	17
22	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	14
23	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	0	14
24	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3
25	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	1	1	0	1	0	0	1	1	1	1	15
Dependency	4	3	21	19	25	25	17	18	22	16	2	6	8	8	2	16	16	6	20	10	10	16	16	23	11	

Table 4: Level Partitioning of Reachability Matrix (First Iteration)

Variable (P)	Reachability Set : R(P)	Antecedent Set :A(P)	Intersection R(P) and A(P)
1	1,3,4,5,6,7,8,9,10,12,13,14,16,17,18,19,20,21,22,23,24,25	1,2,11,15	1
2	1,2,3,4,5,6,7,8,9,10,12,13,14,16,17,18,19,20,21,22,23,24,25	2,11,15	2
3	3,5,6,9,24	1,2,3,4,7,8,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25	3
4	3,4,5,6,9,19,24	1,2,4,7,8,10,11,12,13,14,15,16,17,18,20,21,22,23,,25	4
5	5,6	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25	5,6
6	5,6	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25	5,6
7	3,4,5,6,7,8,9,19,24	1,2,7,10,11,12,13,14,15,16,17,18,20,21,22,23,25	7
8	3,4,5,6,8,9,19,24	1,2,7,8,9,10,11,12,13,14,15,16,17,18,20,21,22,23,25	8
9	5,6,9,24	1,2,3,4,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25	9
10	3,4,5,6,7,8,9,10,16,17,19,22,23,24	1,2,,10,11,12,13,14,15,16,17,18,20,21,22,23,25	10,16,17,22,23
11	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25	11,15	11,15
12	3,4,5,6,7,8,9,10,12,13,14,16,17,18,19,20,21,22,23,24,25	1,2,11,12,15,18	12,18
13	3,4,5,6,7,8,9,10,13,14,16,17,19,20,21,22,23,24,25	1,2,11,12,13,14,15,18	13,14

14	3,4,5,6,7,8,9,10,13,14,16,17,19,20,21,22,23,24,25	1,2,11,12,13,14,15,18	13,14
15	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25	11,15	11,15
16	3,4,5,6,7,8,9,10,16,17,19,22,23,24	1,2,,10,11,12,13,14,15,16,17,18,20,21,22,23,25	10,16,17,22,23
17	3,4,5,6,7,8,9,10,16,17,19,22,23,24	1,2,,10,11,12,13,14,15,16,17,18,20,21,22,23,25	10,16,17,,22,23
18	3,4,5,6,7,8,9,10,12,13,14,16,17,18,19,20,21,22,23,24,25	1,2,11,12,15,18	12,18
19	3,5,6,9,19,24	1,2,4,7,8,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25	19
20	3,4,5,6,7,8,9,10,16,17,19,20,21,22,23,24,25	1,2,11,12,13,14,15,18,20,21	20,21
21	3,4,5,6,7,8,9,10,16,17,19,20,21,22,23,24,25	1,2,11,12,13,14,15,18,20,21	20,21
22	3,4,5,6,7,8,9,10,16,17,19,22,23,24	1,2,10,11,12,13,14,15,16,17,18,20,21,22,23,25	10,16,17,22,23
23	3,4,5,6,7,8,9,10,16,17,19,22,23,24	1,2,10,11,12,13,14,15,16,17,18,20,21,22,23,25	10,16,17,22,23
24	5,6,24	1,2,3,4, 7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25	24
25	3,4,5,6,7,8,9,10,16,17,19,22,23,24,25	1,2,11,12,13,14,15,18,20,21,25	25

Note:
In table 4 first iteration of level partitioning of reachability matrix is depicted. Elements 5, 6 are at level 1 because R (P) and intersection of R(P) and A(P) are identical for both 5 and 6. After separating out 5, 6 from the above table, next level (2) is found to be 24 as R(P) and intersection of R(P) and A(P) are identical. Continuing this process lower levels are identified. Level 3 to 16 are indicated below with the elements placed next to them in bracket.
Level 3 (9) ; Level 4 (3); Level 5 (19); Level 6 (4);Level 7 (8); Level 8 (7);Level 9 (10 ,16,17,22,23) ;Level 10 (25) ;Level 11 (20,21) ;Level 12 (13,14) ;Level 13 (12,18) ;Level 14 (1) ; Level15 (2 ; Level 16 (11,15). These levels are used to draw digraph shown at figure 6.1