

INFORMATION MECHANISM ADAPTATION TO SOCIAL COMMUNICATION

Yngve Monfelt, Stockholm University, yngvem@fc.dsv.su.se

ABSTRACT

Information technology applications have to be adapted for meaningful dependable social mind to mind communication needs and purposes concerning strength, weakness, opportunity, and threat (SWOT) risks. For successful adaptation it seems to be important to dichotomize the mechanistic equipment participation in communication from analogous social understanding of the conveyed meaning intention. The first step towards this objective is to be aware of the meanings in and interrelations between below chosen keywords. The second step is to note that information is a subjective situation and a context dependent interpretation of meaning in a sensorially interpretable message or signal. The third step —and a function dependability conditioning— is to, among a lot of expressed meanings, effectively select the appropriate ones to be controlled and audited in a life cycle management objective perspective. For that any executive manager has to relay on the very basic and in a policy express —perhaps forgotten or redefined— contents of the six cited keywords. The main aim of this essay is to release thinking from sensational or imaginary meanings of the six keywords, and anchor them as close as possible to the responsible managers' reality. The approach aims for complexity reduction through 'good will' variety integration in order aspects to override 'bad will' or 'do not care' attitudes.

Keywords: Knowledge, Information, Data, Message, Communication, Adaptation

INTRODUCTION

A lot of messages about facts or behaviors are available on or via the Internet. With contextual a priori knowledge these will be accessed and informed for subjective meanings as a base for decisions and aimed effects. The main problem is to find the kernel or origin and hence achieve a sustainable —and manageable— common sense of what is wanted to be controlled and audited for life cycle management:

‘...When competing hypotheses are equal in other respects, the [Occam's (c. 1285–1349) razor] principle recommends selection of the hypothesis that introduces the fewest assumptions and postulates the fewest entities while still

sufficiently answering the question. It is in this sense that Occam's razor is usually understood. To quote [Isaac Newton](#) [1643—1727], "We are to admit no more causes of natural things than such as are both true and sufficient to explain their appearances. Therefore, to the same natural effects we must, so far as possible, assign the same causes." [1]

The Essay Characteristic Intentions

This essay intend to focus on some information system applications of which depend on artificial components and emphasizes factors that may facilitate their implementation as a complexity decreasing enabling system. These implementations causes cultural, ethical and legal changes which have to be accepted and “can be or can have” rules for maintained dependability (DPY) [1] within the system's decided requisite variety width (RQW) and life cycle —including retirement— perspective (LCP). The tasks are about "shall be or shall have" protection (PRT) of the conditional statement dependent system's ability to adapt the RQW requirements per authorized role to be "is or has" in parity with the SWOT-Risk, account (ACT) and audit (AUD) management (MGT) capabilities.

Dependability is Ability Conditioned

The aim of this essay is to point out what meaning syntaxes have in mechanistic system contexts such as how information and data communication technology (DCT) affects the system as such. These systems are composed by human developers and requested by themselves or by other human real —instrumentally quantifiable— or imaginary —subjectively qualitative— satisfaction needs; i.e., quality of service (QoS). For that the DCT has to be adapted for its communication —enterprise communication architecture (ECA)— purpose through exchange of measurement messages (MSG) and hitherto relative or absolute evaluation scale. Absolute scales are compounds of elementary computable physical quantities; e.g., electric charge, time, distance, mass, acceleration and energy (temperature or entropy). These quantities are found through reduction or deduction analysis of holistic views to its parts which may be integrated through induced synthesis to alternative wholes. The physical quantities are —like a thunderstorm sensational lightly and loudly events

or occurrences— energy quanta that propagate through some appropriate physical media and impact the human senses of which sensitivity is situation dependent:

“A group of researchers headed by Benjamin Bloom defined in the early fifties [1956] a cognitive taxonomy, which is based on six hierarchical levels:

1. Knowledge —the ability to memorize and recall relevant information (facts, procedures and concepts [contextual cognitional associations]).
2. Comprehension —the ability to understand the meaning of [signals, messages as] information and to translate the knowledge into a new context.
3. Application —the ability to use the knowledge [information ↔ gained knowledge] (facts, methods, concepts) in different and new situations.
4. Analysis —the ability to identify various components and find hidden information (meaning or logic) embedded in them.
5. Synthesis —the ability to combine several components and to build a new product or idea. Draw conclusions or predict based on different areas.
6. Evaluation —the ability to compare and subjectively assess the value of different approaches.” [2]

Dependability has to Be Authorized and Audited

The current essay is a step towards adaptation (APT) of the Controlled Information Security (COINS) 14 Layered Framework [3] context. See below Figure 1 for the enterprise (EPR) entity (ETY) four state analogy model; EPR {EXE, QoS, ECA, DCT} where EXE| executive decision, QoS| recognized and information security (ISC) classified ability assets (AST) for quality of service (QoS) in the mission performance, ECA| the ability to communicate the QoS and DCT| the mechanistic rules for automated data processing (ADP) including the manual (MDP) ditto and transports.

Supposedly, the APT control objective context is for information security (ISC) in mind. ISC is conditioned by audit (AUD) of confidence (COF), integrity (ITY) and availability (ABY) in abilities; i.e., quality of service (QoS), assets (AST).

Control, Audit, Security and Protection Legend

Available abilities (ABY) are system functional qualities as assets (AST) to, on executive’s (EXE) behalf, be managed (MGT) through authorizing (ATH) any authentic (AUT) identity (IDY) because of the enterprise (EPR) SWOT-Risk evaluation

assurance level (EAL) based policy (PCY) and its communication architecture (ECA) role with respect to need to know requisite variety width (RQW) cognition (COG) and its situational behaviour (BEH) dependability (DPY). Each IDY has to be assigned access (ACS) right, in parity with its ATH role, to the AST. The actions will be accounted (ACT) with respect to incidents (ICI), quality of service (QoS) performance and rule compliance (LAW). The ACTs have to be audited (AUD) for updating of the PCY.

Information of Messages is a Subjective Task

Information: “the communication or reception of knowledge or intelligence [1]” is, for the actual context, enough motivated in Skovira [4]. But, decades of unawareness, in informatics disciplines to, when implementing the mechanistic applications dichotomize these aspects from social ditto, for real social analogous communication. That focus on efficiency means, instead of effectiveness for user’s —what to do— communication objectives, represents a systematic fault; i.e., the ubiquitous inherent cause to accuracy bias error. Also, there is inefficiency because of imprecise or fuzzy ‘information’ or ‘communication’ —how to do— related attributes. Supposedly, slump conditioned precision faults causes confusing friction errors in related accuracy dependent efforts to achieve objective focused mission processes in some RQW defined environment holistic context.

To change the view is to change a worldwide cultural influence. It is a hard task to achieve because of possible; e.g., Kafkaesque rigidity in behavior and unawareness of Machiavellian characteristics when implementing conditional statements. So, it will be better to respect the circumstances in any particular application.

“True” or “False” characterizes mechanistic aspects. “May be” has to be added to the social characteristics resulting in two bit combinations instead of one bit ditto. For reducing the uncertainties, it will be need to relay on meanings in an open, universal and easy to access terminology meanings instead of some particular culture influenced ditto.

HUMAN ART OF COMMUNICATION

Ignorance: ”the state or fact of being ignorant: lack of knowledge, education, or awareness [1]”, belong to a class fault of which may —like other human needs and ergonomic RQW limitations— by some actor

influence cause intentional or unintentional erroneous misunderstanding incidents, of which, if not properly managed, can escalates to failures and risks.

There are Opportunities and Threats

There may be hesitations about what the information science is about [5], but without doubt it includes implementation of conditional statement based artifacts for controlling its environment. Hence it is a question of how to manage and maintain the [6] LCP dependability. A step for that may include qualities as in [7, 8 and 9] about, personnel factors, consensus and human capital.

Table 1 may represent a rule to begin with when estimating risk in conditional statements situations. 'P' in the table may represent a provider and 'Q' may represent a quality of service (QoS) requesting customer.

Table 1. SWOT analyze of the conditional statement.

P	Q	P→Q	SWOT	Comments
T	T	T	Strength	Peer to peer
T	F	F	Threat	Unprotected
F	T	T	Opportunity	Awareness
F	F	T	Weakness	Unawareness

Fundamental Statements

A [Shannon] Theory of Communication:
 "... The fundamental problem of communication is that of

reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design. ... [10]"

Weaver [11]:
 "... Relative to the broad subject of communication, there seem to be problems at three levels. Thus it seems reasonable to ask, serially:
 LEVEL A. How accurately can the symbols of communication be transmitted? (The technical problem.) [Data Communication Technology (DCT)]

LEVEL B. How precisely do the transmitted symbols convey desired meaning? (The semantic problem.) [Enterprise Communication Architecture (ECA; organization)]

LEVEL C. How effectively does the received meaning affect conduct in the desired way? (The effectiveness problem.) [A mission performance Quality of Service (QoS) issue]

... The word information, in this [Shannon] theory, is used in a special sense that most not be confused with its ordinary [mind to mind] use. In particular information must not [in the Shannon theory context] be confused with meaning. ... [10]"

FRISCO [12]:

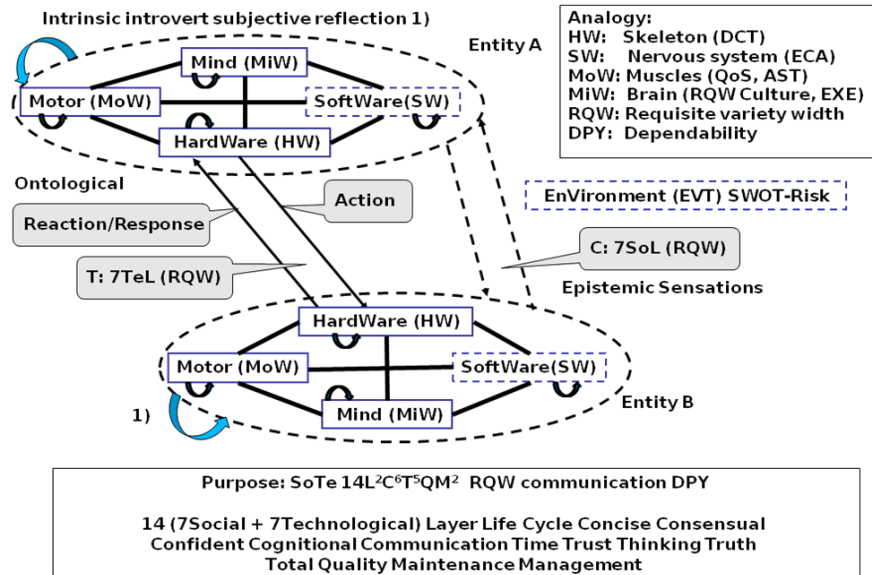


Figure 1: A molecular communication model: EPR {EXE, QoS, ECA, DCT}

"There is a growing concern within IFIP WG 8.1 about the present situation, where too many fuzzy or ill-defined concepts are used in the information system area. Scientific as well as practice-related communication is severely distorted and hampered, due to this fuzziness and due to the frequent situation that different communication partners associate different meanings with one and the same term. There is no commonly accepted conceptual reference and terminology, to be applied for defining or explaining existing or new concepts for information systems" [12].

REDUCTION OF COGNITION RISKS

Meaning in the keywords are interrelated, but almost often not concisely defined how with respect to the contextual situation. 'Information' and 'Communication' are commonly used for both of social meanings and technological applications of these.

That fuzziness or imprecision increases complexity confusions and hence increases uncertainty and contradicts the real meaning of 'information'. To handle increasing complexities is treated as managing availability in classes of a living system's [13] output quality attribute values like resources, assets etc. abilities for controlled authorized and accounted access. But it has to be done with protection (PRT) means to ensure the system's RQW dependability and, on conditional statement based, risk evaluation in mind.

The Evaluation Approach

The approach is to relay on the Shannon [14] example for a communication theory application on basis of discrete Markoff (Markov) processes and hence Bayesian conditional probability principles [15].

The #6 keywords have to be adapted together for a mission enterprise constituting an enterprise system (EPR) entity —A or B in Figure 1— based on an executive's policy of mission intentions. Supposedly, the 'S' has four states: EPR {EXE, QoS, ECA, DCT}, where EXE| executive decision, QoS| recognized and information security (ISC) classified ability assets (AST) for quality of service (QoS) in the mission performance, ECA| the ability to communicate the QoS and DCT| the mechanistic rules for automated data processing (ADP) including the manual (MDP) ditto and transports.

The 'EPR' has #4² = 16 performance possible Table 2 states to change among for RQW- harmony adapted to the dynamic environmental events (EVT).

The sum of column $j \in \{1, 2, 3, 4\}$ probabilities on each row $i \in \{1, 2, 3, 4\}$ is = 1.

If for a moment, the process is in state #i then which is the probability p_{ij} for chancing to state ij |#i ≠ #j or remain in state ij |#j = #i?

Table 2. EPR¹ {EXE, QoS, ECA, DCT} flow

i\j	exe	qos	eca	dct
exe	p_{11}	p_{12}	p_{13}	p_{14}
qos	p_{21}	p_{22}	p_{23}	p_{24}
eca	p_{31}	p_{32}	p_{33}	p_{34}
dct	p_{41}	p_{42}	p_{43}	p_{44}

1) exe ∈EXE, qos ∈QoS, eca ∈ECA, dct ∈DCT

The control (CTR) strategy is to decide (DEC) a policy (PCY) about what 'ought to be' and what 'can be' achieved and audited (AUD) through tactical 'shall be' done and accounted (ACT) what operationally 'is'. With the respect to RQW according to Table 1 SWOT-Risk conditions.

Supposedly in the Figure 1 —of which ideas mainly are found in references [16, 17, 18]— RQW includes fourteen layers as is applied in COINS [3]. These are in top-down order seven social layers; 7SoL {SWOT-Risk, Culture, Ethic, Legality, Management, Organization, Adaptation} adopted from [17]. The seven Open System Interconnection (OSI) technical layers constitute the 'DCT' ↔ 7TeL).

The 'DCT' applications have to be adapted (APT) for the 'EPR's social activities: ACT {IDY, INF, DAT, MSG} ↔ ACT {IDY| Authorized (ATH) identity (IDY), INF| information, DAT| Data, MSG| message with an aimed meaning related with some requested QoS-effect}. Without distinct definition of the 'ACT' elements, there will —with□ tacit knowledge eventualities or skepticism because of no recognizable criteria— be at least □#2⁴ =16 dynamic uncertainties instead of #4 static certainties to handle.

The above conclusion is an example of 'MSG' flow with some meaning(s) for some entity (IDY) having enough ability to recognize the contextual situation; i.e., has accurate peer to peer authority (ATH) or RQW.

One meaning may be that the 'EPR' will be an administrative 'DCT'-problem —the probability for 'EPR' being in 'DCT'-state will be relatively high— for most of the performance time (t) and hence cause dependability risk for 'EPR' to survive in its

environment. That conclusion is an example of gained knowledge [19], relatively to a priori ditto, and hence 'INF' for the authorized interpreter of the meaning.

The above conclusion may be expressed by the —almost ignored— Langefors's [20] formula: $I = i(D, S, t)$ with meaning that I | information is a subjective function conditioned by i | as the interpreters ability to recognize the meaning in D | data from the S | the system context on t | time of the system. In Figure 2 is illustrated a how to 'estimate information value per message' concept.

Subjective information,

$I = i(\text{Message}) \leftrightarrow I = i(\text{MSG}) \leftrightarrow i(D, S, t)$, where

i : cognition (COG) conditioned on individual a priori context knowledge (is base for authorisation, ATH)

D : data in a system point: S at situation time: t

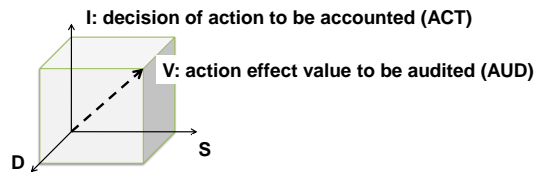


Figure 2: $I = i(D, S, t)$ value estimation.

So the effect of 'INF' is the interpreter's (IDY) action (ACT) behavior (BEH) of which, in its 'EPR' physiological and psychological environmental (EVT) context, has to be accounted (ACT) for feedback and compliance audit (AUD) purpose and policy (PCY) revisions. Furthermore, according to Langefors [20], any 'MSG' expresses the composer's subjective meaning based on what phenomenon is observed. So it is impossible to inform another entity. It is only possible to orient another entity trough 'MSG' including 'DAT' with its contextual relation attributes and then observe the entity's response behavior (BEH) effect.

Responsibility in Parity with Role Authority

In Calvasina and Ramaswamy [21] are the reasons for quality in data and responsibility motivated. Here, in the current context with |DAT as quantified attribute, the principles may suit the classification of 'QoS' assets for confident 'ECA' actions for 'MSG' to be expedited with authorized (ATH) —accredited (ACR)— 'DCT' equipments by authorized (ATH) role performers (IDY).

The actions —creation of 'MSGs'— have to be accounted (ACT) for DPY control purpose. If assuming that the 'DAT' are classified for three decision levels, as well as roles (IDY) are, then there will be three classes (CLS) of roles (ROL) to authorize (ATH) and account (ACT) for access (ACS) right behavior (BEH) per 'DCT' application.

In Figure 3 is illustrated a dependability taxonomy on basis of ITU-E.800 [22] associations.

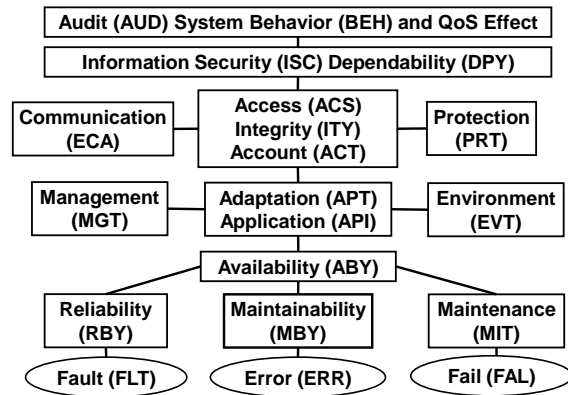


Figure 3: An adapted dependability [6], [22] taxonomy to be controlled per DCT API.

In Figure 3, the 'Fault – Error – Failure' chain, of which causes security risks, is aimed to be treated as: Any entity; e.g., application has some inherent fault. It is revealed when an error event occurs. If maintainability in parity with maintenance resources, then availability incident within risk tolerance. On the contrary, if maintenance ability not in parity with maintainability, then integrity breach and failure risk.

CONCLUSION

Avoidance to define 'INF' for any context has to be audited (AUD) as avoidance of responsibility in parity with authority (ATH). 'INF' can never be in ones hands, but 'MSG' can be for; e.g., in 'DCT' supplies of which implementation has to be accredited (ACR) with respect to the 'EPR's mission risk policy (PCY) based on SWOT {Strength, Weakness, Opportunity, Threat} evaluation for some trustworthy conditional statement dependent future.

The #control categories, on basis of SWOT-Risk policy (PCY), are, with defined 'ACT', at least #EPR * #ACT * #CLS * #DCT \leftrightarrow 16 * 4 * 3 * #DCT \leftrightarrow 192 * #DCT. With undefined ACTs there will be 16 * 16 * 3 * #DCT control categories. Then the complexity, to be RQW-adapted, dependability (DPY) managed (MGT) and assessed, is conditioned

by the appropriateness in the 'EPR's flow probabilities and the #DCT applications.

REFERENCES

1. Merriam-Webster Online Dictionary; <http://www.merriam-webster.com/dictionary/> and *The free Encyclopedia*; <http://en.wikipedia.org/wiki/> are referred too for general facts and general meaning in keywords and acronyms like SWOT or DPY.
2. Yadin, Aharon (2007). Implementation of Bloom's Taxonomy [Bloom, B.S. (1956) Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain, New York: David McKay Co. Inc.] on Systems Analysis Workshops . *Computer Science and Information Systems Department . The Max Stern Academic College of Emek Yezreel . Proceedings of the AIS SIG-ED IAIM 2007 Conference*; p. 5) www.sig-ed.org/ICIER2007/proceedings/implementationimplementation_of.pdf <2010-07-10>
3. Monfelt, Y., Pilemalm, S., Hallberg, J. Yngstrom, L. (2010). The 14 layered framework for including social and organisational aspects in security Management. *Proceedings of the South African information Security Multi-Conference, SAISMC 2010, Port Elizabeth, South Africa 17-18 May 2010 editors Nathan L Clarke, Steven M Furnell, Rossow von Solms Centre for Security, Communication & Network Research, University of Plymouth ISBN 978-1-84102-256-7.* <http://www.cisnr.org/default.asp?page=viewabstr&paperid=606> <2010-07-14>
4. Skovira, Robert Joseph, (2007). Ontological Grounding of a Knowledge Mapping Methodology: Defining Data, Information, And Knowledge. *IACIS, Volume VIII, No. 2, 2007, 258-264.* Available: http://www.iis-online.org/iis/2007_iis/PDFs/Skovira.pdf <2010-05-09>
5. George Beena (2003), *University of St. Thomas*; Taylor, David S. & Kohers, Gerald (2003), *Sam Houston State University.* Management Information Systems: Are We Teaching a Science? *IACIS 2003*: http://iacis.org/iis/2003_iis/PDFfiles/GeorgeTaylorKohers.pdf <2010-05-13>
6. Avizienis, A., Laprie, J-C. and Randell, B. (2001). *Fundamental Concepts of Dependability.* Research Report No 1145, *LAAS-CNRS*, April 2001 <http://www.cert.org/research/isw/isw2000/papers/56.pdf> <2010-05-13>
7. Havelka, Douglas (2002). User Personnel Factors That Influence Information System Development Success. *Miami University IASIS 2002.* http://iacis.org/iis/2002_iis/PDF%20Files/Havelka.pdf <2010-05-13>
8. Wagner, Christian *City University of Hong Kong*, Back, Andrea, *University of St. General meaning of acronym (ANY) (2008).* In Group wisdom support systems: Aggregating the insights of many through information Technology. *IACIS VOL IX, No. 2, 2008.* http://iacis.org/iis/2008_iis/pdf/S2008_992.pdf <2010-05-13>
9. Liebowitz, Jay (2004). Linking Knowledge Management With Human Capital Strategy Development. *John Hopkins University. IACIS Volume V, No 1, 2004.* http://iacis.org/iis/2004_iis/PDFfiles/Liebowitz.pdf <2010-05-13>
10. Shannon, C. E. (1948). A Mathematical Theory of Communication. *The Bell Technical Journal, Vol. 27, pp. 379-423, 623-656, July, October 1948.* Available p. 1: <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf> <2010-05-09>
11. Shannon, C E; Weaver, W (1998). The Mathematical Theory of Communication. *The Board of Trustees of the University of Illinois (1949). Library of Congress Catalog Card No. 49-11922 252 72548 4.* pp. 4, 8.
12. IFIP (1998). A Framework of Information System Concepts. The FRISCO Report (Web edition). *International Federation for Information Processing ISBN 3-901882-01-4.* p. 2. <http://www.mathematik.uni-marburg.de/~hesse/papers/fri-full.pdf> <2010-05-09>
13. *U.S. Department of Defense (1974).* Mil. Std. 499B. Systems Engineering. <http://www.afit.edu/cse/docs/guidance/MS499BDr1.pdf> <2010-05-13>
14. [10] pp. 7-10.
15. 2006 Peter G. Doyle (2006). This work is a version of Grinstead and Snell's '*Introduction to Probability, 2nd edition*', published by the American Mathematical Society, Copyright (C) 2003 Charles M. Grinstead and J. Laurie Snell. This work is freely redistributable under the terms of the GNU Free Documentation License. <http://www.math.dartmouth.edu/~prob/prob/prob.pdf> <2010-05-09>
16. Sjöqvist, Eva (2008). Electronic Mail and its

- Possible Negative Aspects in Organizational Contexts. *Department of Computer and Systems Sciences Stockholm University/Royal Institute of Technology, Forum 100, S-164 40 KISTA. DSV Report series No. 08-005, ISBN 978-91-7155-578-6, ISSN 1101-8526, ISRN SU-KTH/DSV/R--08/5—SE: p. 165, Fig. 8.*
<http://www.hgo.se/~evas/080514-EVA-S-Avhandling.pdf> <2010-05-13>
17. [12], p. 54, Fig. 3-5.2
 18. Hawkins, F.H. (1987). Human factors in flight. *Ashgate, England 2nd ed. 1987. ISBN 1-85742-134-5.*
<http://www.hse.gov.uk/pubns/indg90.pdf> <2010-05-13>
 19. [12], p. 69, Fig. 3-8.2.
 20. Langefors, B. (1973). Theoretical Analysis of Information Systems. *Studentlitteratur Lund, 4th ed. 1973 (1963). ISBN 91-44-08154-5, pp. 248, 319.*
 21. Calvasina, Richard; Calvasina, Eugene; Ramaswamy, Mysore; Gerald Calvasina, (2009). Data Quality Problems in Responsibility Accounting.
http://www.iis-online.org/iis/2009_iis/pdf/P2009_1153.pdf <2010-05-10>
 22. ITU-E.800 (1995), Telephone network and ISDN quality of service, network management and traffic engineering, Terms and definitions related to quality of service and network performance including dependability, *International telecommunication union (ITU-T), Geneva, Switzerland, recommendation E.800 (08/94).*
<http://www.itu.int/net/about/index.aspx> <2008-08-20>
<http://wapiti.telecom-lille1.eu/commun/ens/peda/options/ST/RIO/pub/exposes/exposesrio2008-ttnfa2009/Belhachemi-Arab/files/IUT-T%20E800.pdf> <2010-08-20>