Systematic Achieving Trouble-free Operation

Dr. Leos Tovarek, *Senior Member of IEEE*

***Abstract* — The all effort in research, development, manufacturing and implementation in the field of ICT (Information and Communication Technologies) aims to trouble-free use and operation. International senior professional career of the author in university education, SW and HW R&D, highly available reliable and secure systems, application development, management and consulting led him to cognition of a necessity of the systematic integrated interdisciplinary approach to the trouble-free operation of ICT, believing, that such approach could bring positive inspiring and synergy effects. That's why he proposed a systematic integrated multidisciplinary approach aiming to the trouble-free operation of ICT systems. The article explains in brief that concept.**

***Keywords* — alerting, interdisciplinary, monitoring, operation, prevention, security.**

I. INTRODUCTION

This article explains in brief the concept of the systematic integrated multidisciplinary approach aiming to the trouble-free operation of ICT systems understood as man-machine systems in terms of preventing, disclosing, predicting and removing problems.

II. MODEL OF MAN-MACHINE SYSTEMS

In some abstraction point of view we can see the dynamic operation of a man-machine ICT system as a multidimensional space where each of the *n* parameters or dimensions of the system is represented as an axis of a multidimensional space:

$$\mathbf{O} = (\mathbf{a1}, \mathbf{a2}, \mathbf{a3}, ..., \mathbf{an})$$

Every possible state of the system, or every allowed combination of values of the system's parameters, represents a point in that multidimensional space, which can be interpreted also as an event. Then, behavior of the system can be seen as some sets of those points or "generalized trajectories" in that multidimensional space. Let's note, that some points are normal or welcomed while others are unwanted, forming incidents or problems and their fixing.

For the purposes of the integrated interdisciplinary systematic approach to the trouble-free operation of ICT it is reasonable to define a subspace of **O** as given in the following Fig.1.

Dr. Leos Tovarek, is a holder of Erdos #2 (see Oakland University, USA), inventor, senior member of IEEE, member of ACM, member of SEI Carnegie Mellon University, currently a consultant in Kuwait (phone, +965 66006968, e-mail: drleos@usa.net).

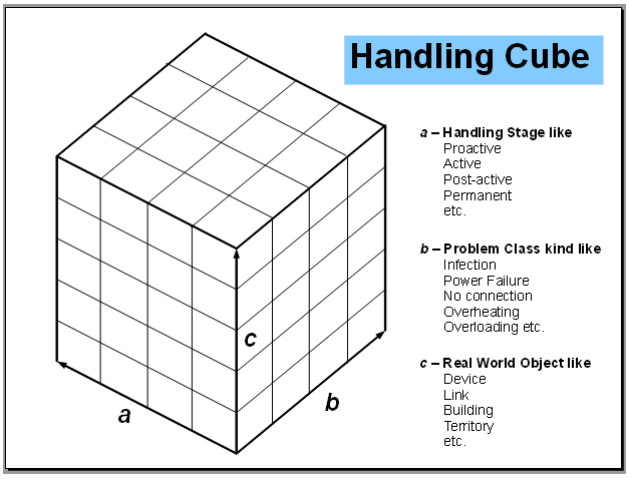

Fig.1: Problem Handling Cube

There are more possible axes of such multidimensional system e.g.:

- Relations to the actual moment
- Character of events
- Scope character of events
- Origin character of events
- Originator character of events
- Severity character of events
- Time and many others.

It implies that also more subspaces can be defined for different purposes, for example, as given in the Fig. 2.

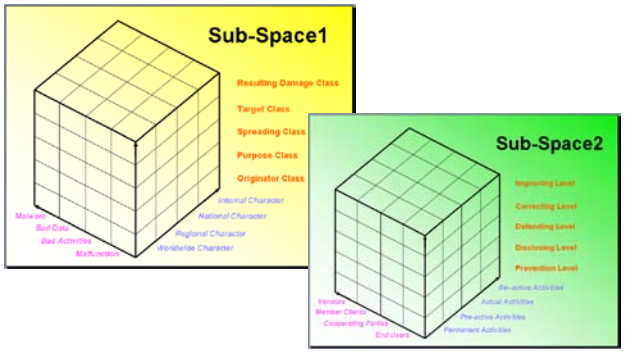

Fig.2: Examples of other **O** sub-spaces.

III. ACHIEVING SMOOTH OPERATION

As it implies from author's long-term experience and implementations of different systems for automation of ICT operation, for trouble-free and fluent operation of large ICT systems the following principles are most important:

1. To prevent problems to happen
2. To disclose problems ASAP (even in advance)
3. To inform about problems the responsible staff
4. To ensure that the staff reacts on alerts received
5. To ensure that the staff can solve problems.
6. Automated problem solving.

While the both points of 4 and 5 depend on human environment, the points of 2, 3 and 6 can and should be done automated way and 1 is of the both nature.

Ad 1: Preventing ICT operation problems can be achieved in addition to human supervision mainly by

- Technical means
- Education field

Here, among the technical means we can count redundancy techniques, dynamic firewalls (like in [9]), selective access, traps, honey pots etc. and in education field educating staff to responsibility, professionalism and skills.

For institution or units with large-area impact [7], [10] also ethical educating the youth is important [2], as many threats are being created intentionally and in the security field there are about 40% of bad-will sabotages.

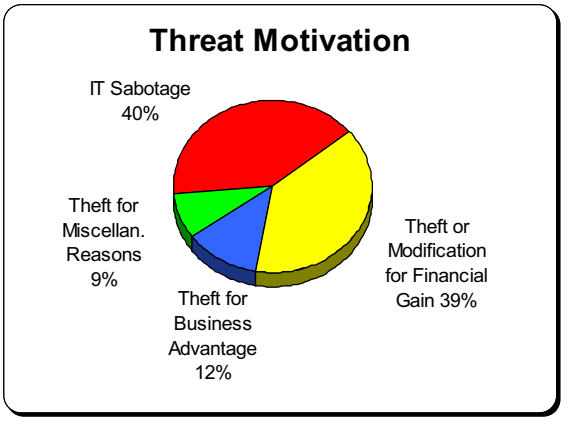

Fig.3: Threat motivations

Ad 2: In the Fig. 4 below the principles of monitoring are given in a graphical way:

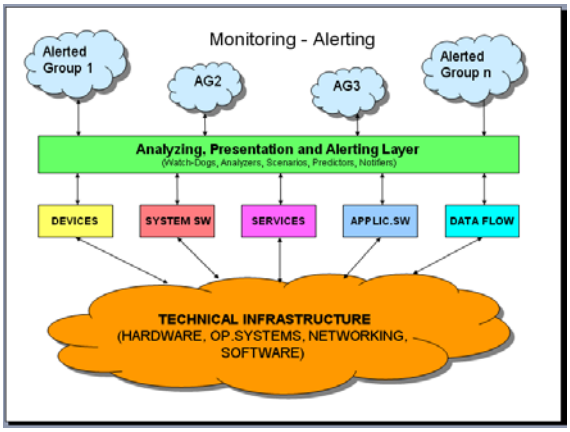

Fig.4: Principles of monitoring

For disclosing problems in ICT operation there have been many monitoring methods developed dealing with

- Devices
- Communication channels
- Data flows
- Activities (of humans and automats)
- SW functionality
- Reserves available.

Wherever it is possible and reasonable, the monitoring system should contain also predictive parts which analyze behavior of ICT continuously and warn about possible problems in advance as e.g. it was implemented in [1] or [9]. It is possible to do so also in the field of security threats, as given in the patent pending solution [8].

Ad 3: Alerting needs to be done in multiple ways like

- Visual way
- Voice or speech way
- By e-mail
- By SMS.

It should be done the way, that alerting messages are delivered also in the cases when the monitored technical infrastructure faces problems or doesn't work at all. For example as it was implemented in [1], [3] or [9] and shown in the example on Fig. 5 below:

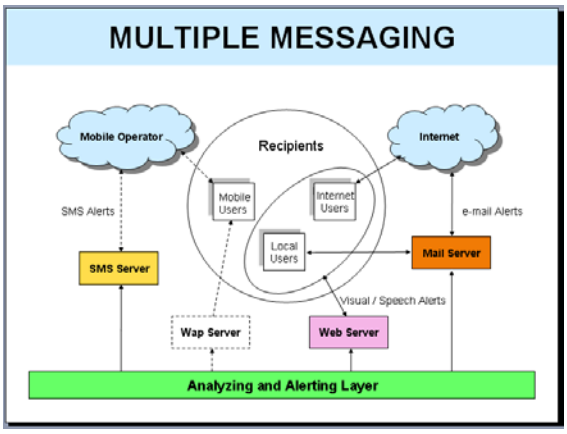

Fig.5: Example of multi-way messaging system

Ad 4: In the problem-predicting able systems it is also necessary to ensure, that the staff knows about such abilities and believes the pro-active warnings.

Note: I remember a documented case several years ago, when the new problem predicting feature of [1] warned about a serious problem coming, but the NOC staff didn't believe it, as everything was working normal way and nobody complained about anything. Several minutes later the network collapsed.

Not everybody is so responsible person as needed in ICT operation. Sometimes alerts are issued but people ignore them and no actions are taken. That's why it is reasonable that the alerting system contains also a BPL (Business

Process Logic) part and, if needed, informs another person or a supervisor, as it was implemented e.g. in [6].

Ad 5: For achieving the goal that people in the operation can solve problems which occure, it is reasonable to use the following methods:

- Provide the staff training
- Define the 1st and 2nd level responsibilities
- Rotate persons over their responsibilities
- Keep records about problems solved out.

Applications of the methods, of course, depend on the technology systems supported by the staff. But in any case it is useful, that a good collaborative atmosphere is achieved in the team.

Ad 6: Automated problem solving is a strong tool for achieving trouble-free operation, as it can fix problems immediately or with a minimal delay and unwanted consequences. On the other hand, it can produce disadvantages, if applied improper way.

In any case, the automated resolving problems should produce alert for informing appropriate persons as they should investigate the incident in deep to know the reasons causing it. If such investigation doesn't follow, the automated solving of the problem can lead in more serious consequences later.

Additional notes: My works in the field of Artificial Intelligence in the Academy of Science in eighties gave me the experience that a human brain works the way, that it suppresses some less important activities whenever its performance is missing for solving more important emergency tasks. Using the same principle in ICT system can bring immense improvement for trouble-free operation as experienced in the system described in [1].

IV. UNIT FOR ACHIEVING PROBLEMLESS ICT

In order to create a shared unit for supporting ICT operation, it should follow principles of the multidisciplinary approach and dynamic aspects. The figure below shows proactive, active, retrospective and permanent character of supporting a trouble-free ICT operation unit:

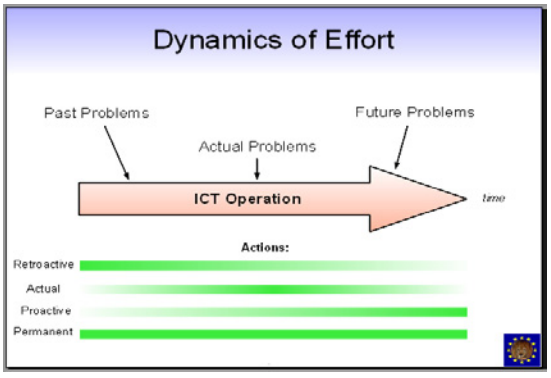

Fig.6: Dynamics of ICT operation effort

The supporting unit should contain the following means for achieving its goals:

A) Human resources for
- **a.** R&D for development the whole solution
- **b.** Operating NOC in 24/7 regime
- **c.** R&D for enhancement of the solution
- **d.** Quality control of the operation
- **e.** Analyzing the operation and proposing improvements
- **f.** Expert support for disaster recovery
- **g.** Competent Management

B) Monitoring for Disclosing Problems:
- **a.** Communications
  1. Availability
  2. Traffic
  3. Errors
  4. Elapsed times
- **b.** Devices
  1. Process performance consumption
  2. Using disk space
  3. Using different kinds of memories
  4. Errors recognized by devices
  5. Temperature
  6. Anything what devices can measure
- **c.** System services (e.g. for protocols)
  1. Availability
  2. Response time
  3. Load
- **d.** Application software
  1. Availability
  2. Response time
  3. Number of users
  4. Anything that can be measured
- **e.** Security
  1. Unwanted activities
  2. Infections
  3. Data flow
  4. Automated investigations

C) Watch Dogs:
- **a.** Anything under monitoring can be watched
- **b.** Watch Dog Packs (e.g. locality-oriented etc.)
- **c.** Personal Watch Dogs

D) Analyses
- **a.** Extreme analyses
  1. On-line minimal values collected
  2. On-line maximal values collected
  3. Time-related analyses (e.g. extremes)
- **b.** Grid analyses
  1. Analyses of 2-dimensional events
  2. Analyses of 3-dimensional events
  3. Analyses of multi-dimensional events
- **c.** Trend Analyses
  1. Trends of values (or occurrences)
- **d.** Security investigations
  1. Sources of wrong-doing
  2. ISP and authorities responsible
- **e.** Predicting Problems
  1. Signal information

2. Coincidence
3. Changing distribution

E) Presentations and Alerting:

a. Textual
1. Dynamic web sites
2. E-mails
3. SMS

b. Voice:
1. Dynamic web sites
2. Voice messages

c. Graphical
1. Live 2D graphs (y = f(x))
2. Live 3D graphs (y = f(x1, x2))
3. Live charts (like bars, pies etc.)
4. Live diagrams (e.g. networking)
5. Live maps (the real or symbolic)
6. Problem-oriented presentations

F) Remote control:

a. Wireless-oriented
1. By means of SMS
2. By means of hand-held devices

b. Web-oriented

G) Automated Problem Solving

a. Reconfigurations
b. Rebooting
c. Moving Virtual FW
d. Device-dependent
e. etc.

H) Supervising

a. Web-oriented system
b. SMS-oriented system

I) Services

a. Consulting and assistance
b. Auditing
c. External Collaboration

J) Publicity and Information Exchange

The arrangement of such Unit for supporting ICT trouble-free operation could look like given below:

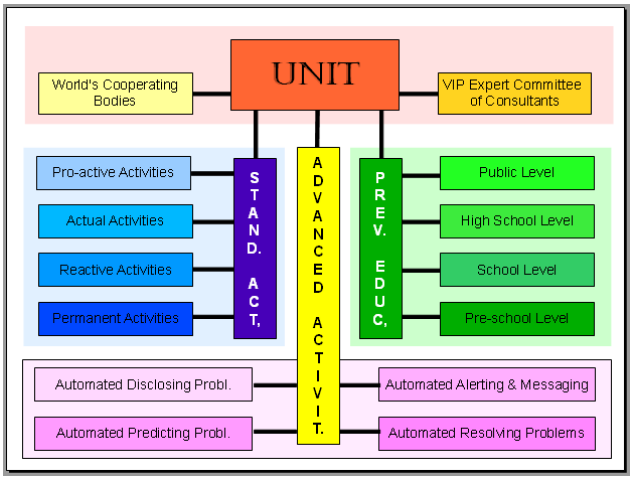

Fig. 7: Unit for trouble-free ICT operation

It is necessary to say explicitly, that behind the blocks above there are many means implemented and verified in the 24/7 operation (some of them patent pending), or education projects developed.

It should be also added, that for ICT systems which serve subscribers, customers or any other public users, it is extremely important having also a well operating Customer Support. Instead of that incompetent support can be found very often. The agents need to be well trained and supported by tools e.g. like given in [5], to be able salvage the image when there are problems.

As it can be seen, comparing to CERT-like units dealing with security fields, the coverage of the needs of ITC operation and the proposed Units is much larger.

V. CONCLUSIONS

In the past there were many advanced systems and features implemented by the author for automated operation, as monitoring, multi-way alerting and messaging, problem prediction, 2D and 3D visualization, live maps and charts, speech and sound alarms, remote detecting infections, predicting problems of different natures, mass dynamic multi-view watch dogs, problem-solving experts, high-performance clusters, highly-redundant fast databases, HD support systems and others. Some of them are given in the references of [1] – [9].

Those means and the others not listed here can create good basements for the works aiming to supporting systematic effort for trouble-free ICT operation as a new IEEE Unit on the ground of IEEE [10] as local, national, international or worldwide infrastructure serving for different ITC service providers and other institutions (as Banks, Enterprises, Government sector institutions etc.).

VI. REFERENCES

[1] L. Tovarek, "Fault-tolerant Multi-ISP Kernel," in *Proc. World Multiconference on Systemics, Cybernetics and Informatics,* Orlando, FL, USA, 2001, vol. 1, pp 114-120.

[2] L. Tovarek, "Contribution to Building Computerized Society", Research memorandum, Kuwait, 2002

[3] L. Tovarek, "Fault-tolerant Error Alerting System", Patent Pending, Kuwait, 2004.

[4] L. Tovarek, "X.25 Monitoring and Supervising System for ATM Network", Qualitynet, Kuwait, 2003

[5] L. Tovarek, "LTTOOLS – Complex Support System for ISP Operation", Qualitynet, Kuwait, 2005

[6] L. Tovarek, "Wireless Support for In-site Solving Problems", Research Memorandum, Kuwait, 2006.

[7] L. Tovarek, "Building CERT-like Unit", Presentation for CAIT by Net Telecom Consultants, Kuwait 2008.

[8] L. Tovarek, "System for Predicting Threats", Patent Pending, Kuwait, 2009

[9] L. Tovarek, "MOCCA – Monitoring, Alerting, Predicting, Provisioning and Expert Support", MOC, Kuwait, 2010.

[10] L. Tovarek, "New Chapter in IEEE Kuwaiti Section", Research Memorandum, Kuwait, June 2010.