Towards families of resilient systems

An article presented at the Yossi Levin conference, January 9th, 2013

Dr. Avigdor Zonnenshain — Rafael

Avi Harel — Ergolight

Component reuse

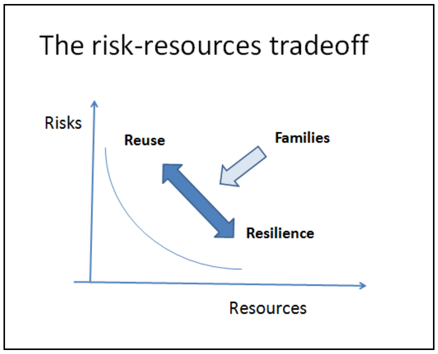
A common practice aimed at reducing the costs of the development of new systems is by reusing components and sub-systems of previous versions. By defining families of systems we can plan common modules ahead, which may be used by all systems belonging to a family, even before the designing of the first prototype. This enables reducing the costs of designing replicas of these modules for the individual systems.

Limitation of component reuse

Although reducing the development costs by reengineering is tempting, this strategy should be examined carefully when the results of possible failures are costly, as is the case of safety-critical systems. An example of the operational risks due to reengineering is the series of accidents of the Therac-25 radiotherapy system. Due to changes in the operational procedures, which were not reflected in the component design, between the years 1985-87 these systems caused the death of three patients, and severe injuries to three others. (link to wiki). There is therefore a need to find a way to define and develop low-cost resilient systems.

The risk-resource tradeoff

The following chart illustrates the risk-resource tradeoff:



The chart shows that we need to invest in development resources in order to assure that the system is resilient, by sharing and reusing solutions, we should expect that the system is more vulnerable and fault-prone. Our challenge is to reduce the operational risks within the budget constraints. The method proposed here is by families of resilient systems.

Developing resilient systems

Recently, The Gordon Center at the Technion, in collaboration with Iltam and INCOSE-IL, supports studies aimed at assuring the system resilience to operational faults. The studies are about:

- Classification of operational faults and suggestions for dealing with them, (Hebrew)
- Guidelines about handling unexpected events (article)
- Application of the guidelines to ITS driver warning systems (article)
- A model of resilient systems and guidelines for designing resilient systems.

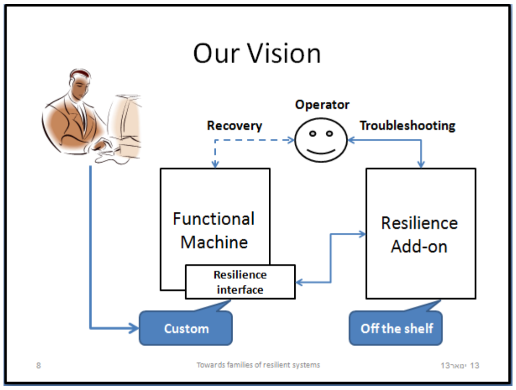
Applications

The model and guide for assuring the system resilience are applicable to:

- Safety-critical systems: transportation, military, process industry
- User productivity: information systems, production control, walk-up and use systems
- Consumer products: home appliances, communication devices, entertainment.

Architecture

In the context of families of systems, our challenge is to define standard modules that may handle typical failure modes.



Our Vision

8 Towards families of resilient systems 13 מאי 13

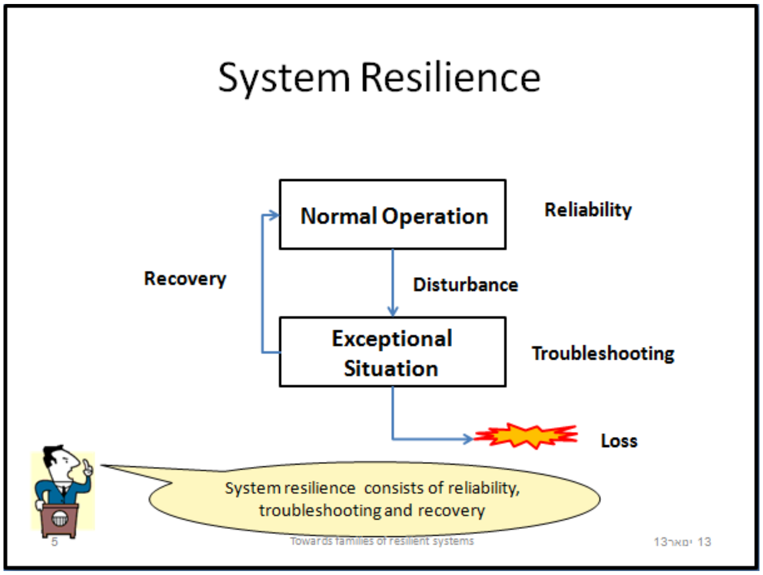
An example of a standard module is of a power control module, intended to turn a facility (such as a simple engine) On or Off. Such module should deal with the malfunctions such as:

- Stuck switch: the power switch might be stuck in the On or Off position
- Engine failure: performance parameters such as yield or load might deviate from a norm
- Loose contacts: loose contacts in the engine or in the power control might result in random changes in the operating mode.

In addition to hardware failures, the control module may deal with operator's faults, such as disregarding or forgetting the engine state, and unintentional or inadvertent changing of the engine state. To facilitate detection of such faults, the module may indicate the engine operating state, for example, by LEDs. Also, the module should incorporate means to identify secondary malfunctions, namely, faults in the safety add-ons, such as the LEDs used to indicate the engine state.

The resilience model

The system resilience is defined as an emergent property, associated with three system properties: reliability, troubleshooting and recovery. The following chart depicts this definition:



System Resilience

Normal Operation

Reliability

Recovery

Disturbance

Exceptional Situation

Troubleshooting

Loss

System resilience consists of reliability, troubleshooting and recovery
5
Towards families of resilient systems
13 ינואר 13

The resilience sub-unit

The features of the resilience sub-unit should depend on the operational requirements. For example, the module used for resilient control of a remote facility should incorporate special means to help the operator to always be aware of the engine state. A module used to control several facilities should have special means to prevent controlling the wrong facility. Special means should also be used to enable resilient control from several locations. A module that enables detecting deviations of performance parameters (such as yield or load) from a norm should comprise means to measure and present these parameters, for example, by methods of statistical process control (SPC).

Human factors

The ideal way to handle disturbances such as unintentional actions is by automation. However, a main concern of the resilience model is about situations such as hardware failures, in which a human intervention is required to identify and recover from the disturbances in time. Accordingly, the resilience model is based on a paradigm about the system vulnerability to use errors, namely, the Human Factors version of Murphy's law:

> **If the system enables the users to fail, eventually they will!**

This paradigm implies that it should be the developer's responsibility to design the system such that use errors are impossible. Specifically, in order to facilitate the operators' intervention, the machine should provide them with information about its state, and the information should be presented in forms considering the limitations of the human perception. Accordingly, our resilience model focuses on requirements and methods for alarming the operators about changes in the machine state, of which the operator must be aware, and about exceptional situations, for which the operator's intervention may be required.

Alarm systems

The design of alarm system should focus on the effect on the operator's behavior. Special facilities are required to ensure that operators can perceive the alarms properly, so that they know how to respond when they face a real problem (link to article). Special modules may implement the requirements and methods for enforcing proper operator's responses to the alarms. Candidates for families of alarm systems include:

- Medical alarms, such as those used in monitors
- Control room alarms, such as those used in the Process Industry
- Vehicle driving ITS safety alarms
- Modules used for alerting the public about emergency situations, such as natural disasters, environmental hazards or enemy attacks.

Each of these modules needs to employ special features, which sets it apart from the others. For example, the module used for medical alarms should implement a feature of safe muting, to facilitate occasional consultation of the medical team, while maintaining a reminder about the state of alert. The module used for driving alarms should employ a combination of physical sensing modalities and special audio alarms, to allow very fast hazard perception. The module used to warn the public about emergency situations should provide the people with information about what they should do in order to save their lives.

Implementation example

The design of the module used to warn the public about emergency situations is based on lessons learned from using war alarms during the war with Hezbollah (postscript). Until this war, the alarms were based on equipment used for memorial days and for war times. In memorial days, these equipments produced a monotonous tone, and in war they produced alarms with sinusoidal pitch. Many people did not obey the alarms, and those who did, often took the wrong actions. Sometimes, the results were fatal.

Developing a resilience module

The development process has five stages:

1. Recognize that we have a problem
2. Analyze the problem
3. Requirement specification
4. Propose solutions and show feasibility
5. Design and implement.

An example of the development process of alarm systems follows:

Recognize that we have a problem

A main conclusion from the fighting with the Hamas was that the organization should maintain a safety climate. Rather than blaming the victims, the organization should focus on developing means to prevent mishaps.

Analyze the problem

One conclusion from this war was that people ignored the alarms, because most of them were irrelevant, therefore, were perceived as false alarms. Another conclusion was that people took the wrong action because the alarms did not provide an estimate of the time remaining until the explosion, which could help them decide how they should behave (an article, Hebrew).

Requirement specification

The requirements from the alarm system should focus on those intended to ensure that the people can trust the system, and those intended to provide the people with the information they need in order to know how they should behave safely.

- In order that people can trust the system, it should generate an alarm each time an explosion might be heard, and the alarm generation should be reliable.
- In order that people understand the meaning of the alarms for them, and to avoid hysteric responses, the alarm should indicate the risk level of the expected explosion.
- In order to enforce proper behavior, the alarm should provide information about the expected location, and the time remaining until the explosion.

Propose solutions and show feasibility

Possible solutions exist in many systems, including annunciations by radio, using cellular phones and at home (about thunderstorms). An example of a system that indicates an estimate of the risk level is that of the warnings when driving backwards.

Design and implement.

Based on these lessons, a new alarm system was developed, which provides the people with prediction of the location (an article, Hebrew). Also, in the new system, the authorities provided maps indicating the average expected time from beginning of the alarm until the explosion.

Apparently, people find it difficult to follow or estimate the time elapsed since the beginning of the alarm, and to predict the exact time of the explosion. Probably, at least some of the casualties during our recent battles with the Hamas could have been prevented, should the alarm include an indication of the time left until the explosion, in real time. Hopefully, such indication will be provided by the next versions of the alarm system, so that people can know how to respond properly (an article, Hebrew).