

PCT '08
Honolulu
January 14th, 2008
Panel M.1.2
Non-Stop Networks: Solutions for Eliminating
Downtime of Business-Critical Data Networks

Major events including hurricanes Katrina and Rita have emphasized vulnerabilities of the communications infrastructure and exposed the weakness of terrestrial communications. Smaller incidents that happen much more frequently, including those caused by construction accidents or human error, also pose a threat to business networks. Whether protecting against catastrophic events or short-term outages, VSAT satellite networks and hybrid satellite/terrestrial technologies are ideally suited as a risk mitigation platform for organizations with high uptime requirements. This panel will provide an overview of how end-user CXOs and government officials can assess the risk of their telecom infrastructure and evaluate new solutions to ensure redundant communications.

Chair:

ANDREAS GEORGHIOU, CEO, SpaceNet Inc., USA

Speakers:

LARRY BECKWITH, Senior VP of Information Systems, Bob Evans Farms, USA

BRYAN A. MCGUIRK, President, Media & Enterprise Solutions, SES Americom, USA

JOHN REPKO, CIO, Covance, USA

SERGIO ANTOCICCO, Chairman, INTUG

Non-stop networks

A methodology for reliability assessment

Sergio Antocicco
Chairman, INTUG

Executive summary

Methodologies for reliability assessment, from single equipments to complex systems, were developed in 1940 by Wernher von Braun's team. After the II W war, those methodologies were adopted in various sectors, from military to nuclear. Today, safety and security issues are of paramount importance for telecommunications infrastructures and can be addressed in a scientific way using methodologies developed for reliability assessment. The paper recalls the basic concepts of reliability, availability, maintainability, and discusses the various steps for their assessment. The telecommunications infrastructure, designed and implemented for the Italian Control Room devoted to the handling of the Millennium Bug problem, is presented and discussed as a Case Study.

Introduction

In 1940, Wernher von Braun, the German Rocket Designer, while developing V-1 and V-2 rockets, experienced severe problems due to the unreliability of some components.

Eric Pieruschka, a German mathematician working in the Von Braun team, showed that the rocket's reliability was equal to the product of the reliability of its components and not simply to the reliability of the weakest component.

That was the basis of the modern predictive reliability model.

Key concepts synthesis

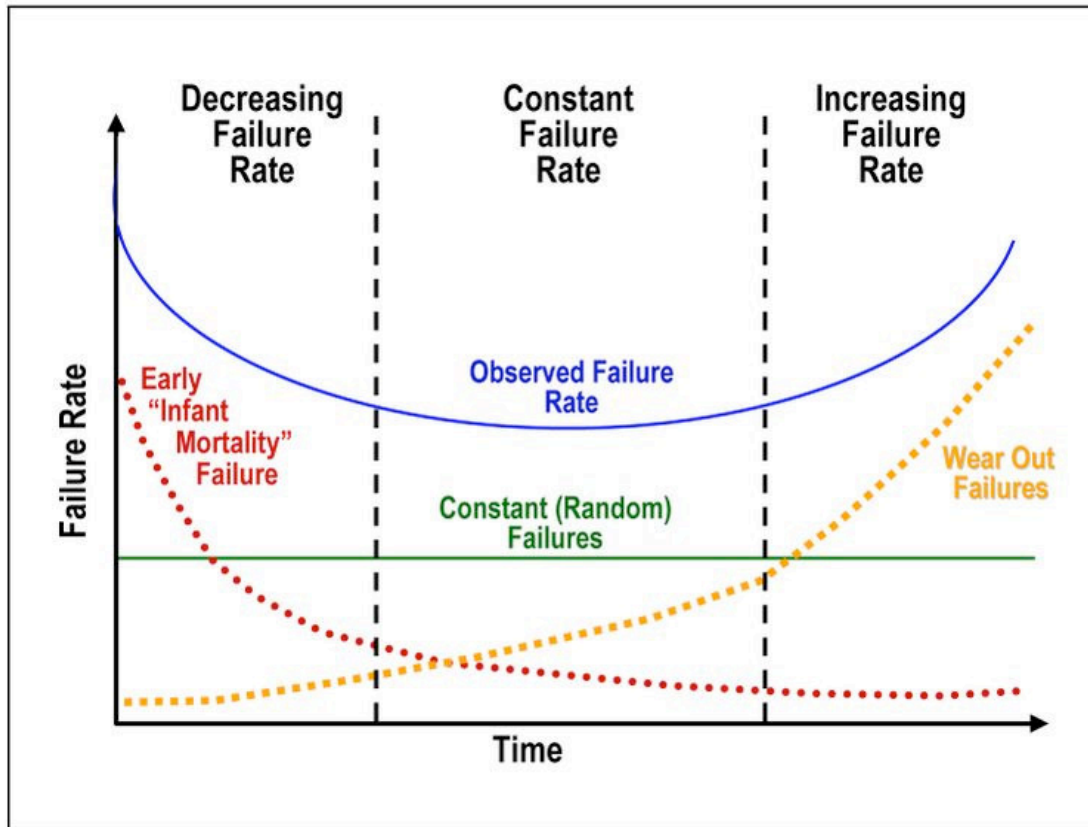
Capability

Capability is the power or ability to generate an outcome. The designer is often focused on performance improvement and cost reduction of a specific piece of equipment and does not consider other issues.

Fault

A fault is an incorrect system state resulting from failures due to several reasons (hardware or software, system components, design errors, operating errors)

Bathtub curve



MIL (MILITARY) Specification devices are those already tested for some hours in order to detect "Infant Mortality" failures. Requiring MIL Spec components can be appropriate for strategic systems.

Electronic components show rather constant failure rate, over the years, while mechanical devices go to the "wear out" area much faster.

Failure rate is simply the inverse of the mean time between failure (MTBF), expressed for example in hours.

Reliability

Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time [IEEE 90].

In simpler words, it is the probability that a given component (or system) will succeed within its mission time, with no failures.

A commonly used measure of reliability for repairable systems is the Mean Time Between Failures (MTBF). The equivalent measure for non-repairable items is Mean Time To Failure (MTTF).

The equation representing the reliability is:

$$\text{Reliability} = e^{-\text{Time}/\text{MTBF}}$$

MTBF and MTTF are normally expressed in hours.

MTBF and life expectancy

MTBF is not to be confused with life expectancy. MTBF is an indication of reliability. How long the device will last is entirely dependent on its life expectancy. A device with a MTBF of 100,000 hours may have a life expectancy of 2 years while one with a MTBF of 50,000 can have a 5 year life expectancy. The first is more reliable if replaced every 2 years. Another way to look at this is: if there are 1,000 units of the device with a MTBF of 100,000 hours and all of them are in use at the same time and any failed device is put back in working order immediately after the failure, then 1 unit is expected to fail every 100 hours.

Availability

Availability is the degree to which a system or component is operational and accessible when required for use [IEEE 90].

Maintainability.

Maintainability is defined as the measure of the ability of an item to be restored or retained in a specified condition.

Therefore, maintainability is a measure of how effectively and how quickly system operation can be restored following a failure, through corrective maintenance.

Reliability and availability are connected, but they are not synonymous: two equipments or systems can have the same reliability, but may differ in availability, due to different times for repairs.

Mean Time To Repair (MTTR) can be reduced if skilled personnel performs maintenance or if, at design level, easy ways for identifying components or systems in fault state were provided. When a local red light or a remote diagnosis identifies the component in fault, the maintenance can be performed by people non-very skilled and at a faster rate.

MTTR, too, is normally expressed in hours.

Redundancy

Redundancy is the duplication of critical components of a system with the aim of increasing the system reliability. In many safety-critical systems, some critical functions are simultaneously supplied by two or more elements. A fault in one element is not sufficient for a general failure. In some situations a voting logic is used for detecting fail-safe faults.

Diversity

Diversity, in this context, is the use of different physical principles for supplying a specific service. For instance, the temperature can be measured by a potential difference in a thermocouple or by a resistance variation in a thermistor.

Fault-tolerant systems

Fault-tolerant design refers to a method for designing a system such that if some part of the system fails, the system will continue to operate, possibly at a reduced level, rather than failing completely. In that case, the system can reduce its performance or throughput, but is still operational.

Why non-stop networks

High speed networks can provide performances similar to (or better than) local buses of Personal Computers. A remote disk could work faster than the local disk; it means that we can distribute business-critical data in dispersed locations, simply identified by IP addresses. This increases dramatically the security level.

That's another reason for requiring non-stop networks.

Reliability assessment

The reliability assessment can be done at various levels: from a single component to the whole system.

For single components, manufacturers measure the MTBF, MTTF and MTTR on the basis of historical fault data or predict them on the base of data relevant to similar components.

The whole system reliability assessment is, very often, predictive and can be done after some targets are defined.

It is necessary to define the specific fault, or class of faults for which we want to assess the probability of events.

Two situations are commonly used in the safety equipments for the nuclear sector: fail-safe and fail-to-danger.

Fail-safe is a fault determining a situation of wrong alarm.

Fail-to-danger is a fault preventing alarm in a dangerous situation.

For telecommunication networks we should define some more situations to be investigated; for each, the reliability value should be assessed.

Today, the most advanced Operators provide reliability figures for their networks; but they refer to specific networks. Those data are very useful for assessing reliability in large corporate networks, where several Operators are involved.

For a non-stop telecommunications network we must define which situation we want to monitor and it seems clear: we must prevent the circumstance of ALL networks carrying business-critical data being down at the same time.

In very complex networks, where many interactions among the various components take place, the use of mathematical tools, such as Monte Carlo analysis, helps.

If we read the title of the panel “Solutions for Eliminating Downtime of Business-Critical Data Networks” we can say that, in a probabilistic approach, this target is NOT achievable, simply because no events have zero probability.

But we can assess the probability of having all links unavailable at the same time, by performing the reliability assessment of several solutions and comparing them.

Each solution can be evaluated taking into consideration costs of implementation and operation and reliability prediction.

In the current situation, in which terrorism is a major concern, security must be specifically considered.

Therefore, the reliability assessment processes should not be made public; access to the system structure, location and characteristics of components should be restricted.

Case Study

For the Year 2000 roll-over all Governments decided to put in place a National Y2k Control Room to monitor the situation.

The Italian Prime Minister and Cabinet, appointed me to design and manage the telecommunications infrastructure for the Italian Control Room.

Due to budget and time constraints, I suggested adapting for the purpose a large meeting room in Rome, located within the premises of the Italian equivalent of the Central Intelligence Agency.

The room was already connected via encrypted links, with the Prime Minister's Palace (Palazzo Chigi) and with the NATO Headquarter and well organised from a security point of view.

Reliability assessment techniques and principles were used for the infrastructure design.

Redundancy and diversity were largely applied: analogue lines on copper, digital lines on fibre, radio links (short waves and microwaves), satellite services from GlobalStar were all mixed together.

Companies and organisations managing pervasive internal networks (State Police, Carabinieri, Guardia di Finanza, Flight Control, Airports, Port Authority, Railways, expressways, electricity, oil and gasoline) were involved and terminals of all networks were made available in the Control Room.

In practice, three international telecommunications Operators networks were accessible through independent links: Telecom Italia, France Telecom and British Telecom.

Mobile Operators assured preferential services (dedicated antennas).

Satellite links provided by Globalstar were available to major Utilities at the local level (Milan, Turin, Naples) and to the most critical bodies (already linked via other infrastructures) for assuring diversity, not only redundancy.

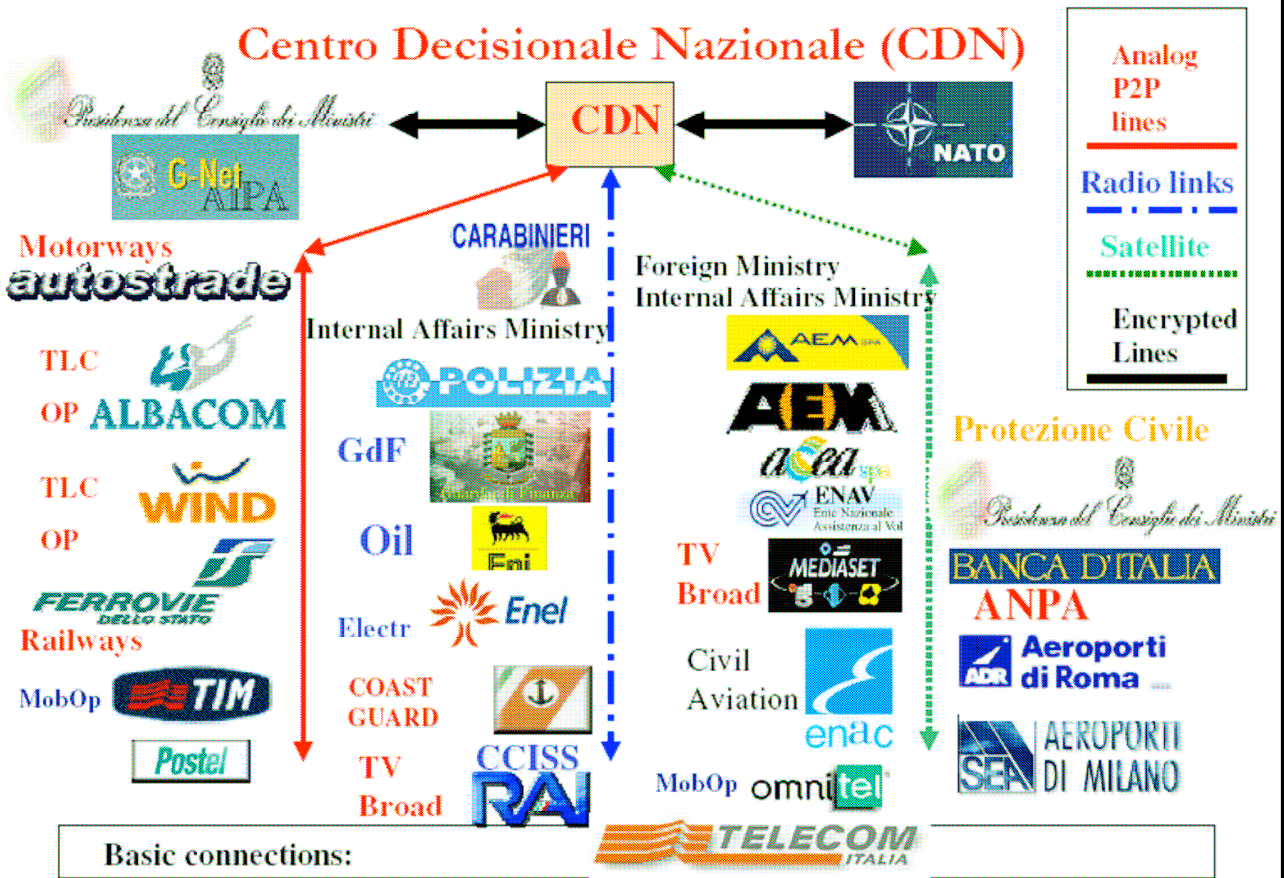
With such an infrastructure, it was possible to get in touch with every railway station, every expressway barrier and every electricity, gas, oil production and distribution center all over Italy (as for oil, the link extended as far as Algeria).

It was possible to contact every patrol car, every large ship, every Control Tower of major airports.

We were able to let 56 passengers on board trains that, having been delayed, did not reach the final destination in time for the midnight, to have a drink and a cake.

The results were absolutely satisfactory.

Connections between Control Centers and Centro Decisionale Nazionale (CDN)



Conclusions

In theory, a non-stop network doesn't exist.

In practice, we can define a reliability threshold similar to the one of events the occurrence of which we consider acceptable (being hit by a meteorite, for instance).

Therefore, if we design an infrastructure using the reliability assessment methodology as guiding principle, we can offer decision makers all relevant information for a conscious choice.