تحمل‌پذیری اشکال

Fault Tolerance

Fault Tolerance

- ***What?***
- ***Why?***
- ***How?***
- ***Where?***
- ***When?***

کاربرد بحرانی-ایمن در زندگی بشر

- سیستم‌های کنترل صنعتی
- صنعت خودرو (سیستم‌های کنترلی بکار رفته در اتومبیل‌ها)
- کاربردهای هواپیمایی
- هدایت موشک‌ها
- زیردریایی‌ها
- سیستم‌های مخابراتی
- قطارها و متروها
- ماهواره‌ها
- تجهیزات پزشکی
- آسانسورها
- دوربین‌های دیجیتال، نمابر، گوشی‌های موبایل، تلویزیون، ماشین رخت‌شوئی و ....

Safety-Critical Systems

Fault Tolerance

تحمل‌پذیری اشکال چیست؟

تحمل اشکال / خطا در حضور آنها

Fault Tolerance

چرا تحمل‌پذیری اشکال

در

کاربردهای بحرانی–ایمن ؟

نمونه‌هایی ازحوادث واقعی

انفجار موشک آریان ۵

در تاریخ چهارم ژوئن سال ۱۹۹۶ میلادی، فضاپیمای بدون سرنشین آریان ۵ توسط سازمان فضایی اروپا به هوا پرتاب شد و در کمتر از **۴۰ ثانیه** پس از پرتاب در آسمان کورو در کشور فرانسه منفجر شد. این اولین پرتاب این فضاپیما بود که پس از یک دوره تلاش **۱۰** ساله و صرف هزینهٔ **۷** میلیارد دلاری انجام می‌شد، ارزش قطعات باقیمانده پس از انفجار **۵۰۰** میلیون دلار تخمین زده شد. گروه تجسس پس از دو هفته بررسی دریافتند که دلیل این فاجعه از دست رفتن اطلاعات مربوط به ارتفاع و سرعت عمودی فضاپیما در ثانیه ۳۷ام پس از پرتاب بوده است و دلیل آن **رخدادن اشکال در تبدیل ۶۴ بیتی ممیز شناور به ۱۶ بیتی ممیز ثابت** گزارش شد.

http://www.ima.umn.edu/~arnold/disasters/ariane.html

http://www.cse.unsw.edu.au/~se4921/PDF/ariane5-article.pdf

http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html

Mission-Critical Applications Require Robustness

- Failure Reason:
  - **Efforts to reduce system costs led to the failure**
    - Re-use of Reference System software from Ariane 4
  - **Improperly handled exception caused by variable overflow during new flight profile (that wasn't simulated because of cost/schedule)**
    - 64-bit float converted to 16-bit integer assumed not to overflow
    - Exception caused dual hardware shutdown (because it was assumed software doesn't fail)

Mission-Critical Applications: Require Robustness

- What really concluded here?
  - The narrow view:
    - it was a software bug
  - The broad view:
    - the loss was caused by a lack of system robustness in an exceptional situation
- Many embedded systems must be *robust*

Embedded System failures: MIM-104 Patriot

- Is a surface-to-air missile (SAM) system
- During Operation Desert Storm failed to track and intercept an incoming Scud
- This Scud subsequently hit an Army barracks, killing 28 Americans in Dharan, Saudi Arabia, during Persian Gulf War 1991
- http://www.fas.org/spp/starwars/gao/im92026.htm
- http://archive.gao.gov/t2pbat6/145960.pdf

Embedded System failures: MIM-104 Patriot

- The MIM-104 Patriot Missile Bug
  - Caused by a **software error** in the systems clock
    - (inaccuracy of using integer representation of Real values)
  - At the time of the incident, the Patriot battery had been operating continuously for over 100 hours.
  - By then, the inaccuracy was serious enough to cause the system to look in the **wrong place** for the incoming Scud.
    - (1/3 second, ~ 700m)
  - After being ”on” for just one hour, the system calculates the location wrong by 7 meters!
  - Rocket to be detonated (Scud) travels at speeds of 2,000 to 2,200 meters per second …

نمونه‌هایی ازحوادث واقعی

سقوط پرواز هوایی VASP

در تاریخ دوم فوریه سال ۱۹۹۵ میلادی پرواز شماره ۹۵۷ خط هوایی VASP شهر سائوپائولو در کشور برزیل را به مقصد بوینس آیرس در آرژانتین ترک کرد. یکی از چرخ‌های این هواپیما پس از بلند شدن جمع نشد و این موضوع باعث فشار آمدن به یکی از موتورها و از کار افتادن هر دو موتور و در نهایت سقوط هواپیما شد. علت اصلی این حادثه پس از بررسی‌های به عمل آمده **اشکال در پردازندهٔ کنترل کنندهٔ چرخ‌ها** ذکر شد.

http://www.airdisaster.com/cgi-bin

نمونه‌هایی ازحوادث واقعی

برخورد پروازهای هوایی DHL و Bashkirian

اول جولای سال ۲۰۰۲ میلادی، جهان شاهد **برخورد دو هواپیمای بویینگ** از خط هوایی **DHL** (شماره پرواز ۶۱۱) و **توپولف** از خط هوایی **Bashkirian** (شماره پرواز ۱۵۴) در شمال دریاچه کنستانس (مرز دو کشور سوییس و اتریش) بود. هر دو پرواز در سطح FL360 و زیر نظر کنترل پرواز سوییس انجام می‌شد، کنترل پرواز به هواپیمای توپولف دستور داد که برای جلوگیری از برخورد با پرواز DHL به سطح FL350 برود، اما هواپیمای توپولف جوابی نداد. کنترل پرواز پس از **۴۰** ثانیه **مجدداً** این دستور را صادر کرد و هواپیمای توپولف پس از ارسال پاسخ، شروع به کاهش ارتفاع خود کرد، اما متأسفانه در این مدت دستگاه **اتوماتیک** جلوگیری از برخورد هواپیمای بویینگ، خلبان این هواپیما را وادار به کاهش ارتفاع کرده بود و به این ترتیب هر دو هواپیما به ارتفاع FL350رفتند و در آنجا با یکدیگر برخورد کردند. **علت اصلی این حادثه خرابی موقتی پردازندهٔ کنترل کنندهٔ ارتباط** در هواپیمای **توپولف** تشخیص داده شد.

http://www.airdisaster.com

نمونه‌هایی ازحوادث واقعی

خرابی ماهوارهٔ Equator-S

در اول ماه مه سال ۱۹۹۸ میلادی ارتباط ماهوارهٔ Equator-S در حدود ۶ ساعت تمام به دلیل اشکال در پردازندهٔ ماهواره قطع شد. به احتمال بسیار زیاد، دلیل آن رخداد اشکال SEU بوده است که در اثر برخورد ذرات شتابدار به پردازندهٔ کمکی رخداده است.

پردازندهٔ اصلی نیز در دسامبر سال ۱۹۹۷ دچار همین معضل شده بود.

http://www.mpe.mpg.de

نمونه‌هایی ازحوادث واقعی

مرگ بیماران در سیستم رادیوتراپی Therac-25

بین ۱۹۸۵ تا ۱۹۸۷

این سیستم توسط شرکت انرژی اتمی کانادا و شرکت CGR فرانسه برای کاربردهای پزشکی و رادیوتراپی تولید شده بود که به دلیل وجود **اشکال** در **نرم‌افزاری** که برروی **میکروکنترلر** این سیستم به اجرا در می‌آمد، اشعهٔ تابیده شده به بیماران بیش از حد مجاز بود و موجب از دست **رفتن جان تعدادی بیمار** گردید.

http://computingcases.org/case_materials/therac/therac_case_intro.html

http://en.wikipedia.org/wiki/Therac-25

نمونه‌هایی ازحوادث واقعی

مرگ به دلیل اشتباه سیستم کنترل آسانسور

در ۵ ژوئن سال ۱۹۸۹ در کشور کانادا شهر اتاوا شخصی هنگام داخل شدن به آسانسور توسط درب آسانسور که بسته می‌شود گرفتار می‌شود و سپس آسانسور در حالیکه درب آن به دلیل گیرکردن شخص کاملاً بسته نبوده است پیش از آنکه شخص مذکور بتواند کاری انجام دهد چندین بار به بالا و پایین حرکت می‌کند که موجب کشته شدن شخص مذکور می‌گردد. مشکل مذکور به دلیل بروز اشتباه در بخش کنترل الکتریکی آسانسور بوده است.

The Risk Digest, vol. 8, issue 77,

http://catless.ncl.ac.uk/risks/8.77.html

Software can also kill people

- **London Ambulance Failure**
- **1992**, **October 26**: the Computer Aided Dispatch system of the **London Ambulance** Service **broke down** right after its installation, paralyzing the capability of the world's largest ambulance service to handle **5000** daily requests in carrying patients in emergency situations.

  [SWTR93a]

مشکلات نرم‌افزاری

گزارش مرکز آمار ایالت متحده آمریکا (۱۹۹۷)

- از هر ۳ سیستم نرم‌افزاری، ۱ سیستم از کار می‌افتد.
- ٪۵۰ سیستم‌های نرم‌افزاری بزرگ، از کار می‌افتند.
- ٪۷۰ سیستم‌ها دچار مشکل عملیاتی می‌شوند.

رعد و برق، اطلاعات کاربران گوگل را پاک کرد

- جمعه ۲۹ مرداد ۱۳۹۴ منبع: ایرنا به نقل از رویترز
- گوگل اعلام کرد: پس از اصابت چهارمرتبه **صاعقه** به مرکز داده (دیتا سنتر) در **بلژیک**، بخشی از اطلاعات ذخیره شده این شرکت روی دیسک‌های سخت یکی از دیتاسنترها از بین رفت.
- این دیتاسنتر برای ارائه خدمات موتور پردازش گوگل مورد استفاده قرار می‌گرفت (Google Compute Engine).
- ممکن است صاعقه به تجهیزات الکتریکی و ارتباطات الکترونیکی ساختمانی که از دیتاسنتر فاصله دارد، اصابت کند و با وجود این، اطلاعات ذخیره شده در دیتاسنتر را تحت تأثیر قرار دهد. در واقع، **کابل برق می‌تواند صاعقه را تا چند کیلومتر منتقل کند** و به تمام تجهیزات متصل به آن آسیب وارد کند.

استنکاف افسر روسی از انجام وظیفه‌اش

- باید خیلی خوشبخت باشیم که یک افسر روسی از انجام وظیفه‌اش استنکاف کرد، وقتی در سال ۱۹۸۳ مشاهده کرد که نشانه‌های کامپیوتری تأیید می‌کند که چندین فروند موشک اتمی از آمریکا به سوی اتحاد جماهیر شوروی شلیک شده است.
- این رویداد پس از حمله موشکی شوروی به یک هواپیمای مسافربری رخ داده بود که بیش از ۲۵۰ نفر که بسیاری هم آمریکایی بودند کشته شدند و فضای میان دو کشور به شدت متشنج بود.
- مطابق دستورات نظامی، سرهنگ پتروف که فرمانده وقت آن قرارگاه اتمی بود، پس از دیدن آن نشانه‌ها باید مقدمات پاسخ اتمی علیه آمریکا را فراهم می‌کرد، ولی به دلایلی گمان می‌کند که این نشانه‌ها ناشی از **خطای دستگاه** است و پس از مدتی هم صحت این گمان تأیید می‌شود.
- اگر حمله اتمی شوروی رخ داده بود، آمریکایی‌ها هم مقابله‌به‌مثل می‌کردند و معلوم نبود که امروز جهان با چه وضع وحشتناکی مواجه بود.

تحمل پذیری اشکال – چرا؟

جمع‌بندی:

- وابستگی روز افزون زندگی بشر به کامپیوتر
- جلوگیری از به خطر افتادن جان انسان‌ها
- جلوگیری از وقوع آسیب‌ها محیطی
- جلوگیری از وقوع زیان‌های مالی

Reliability قابلیت اطمینان

- The reliability, R(t), of a system is a function of time, defined as the conditional probability that the system will perform correctly throughout the interval [t0, t1], given that the system was performing correctly at the time t0.

- In applications in which **repair** is impossible, T can be extremely ***long*** (≈ 10 years)
- In other applications, i.e., aircraft flight control, T can be ***several hours***. Here, R(t) ≥ 0.9999999

Availability

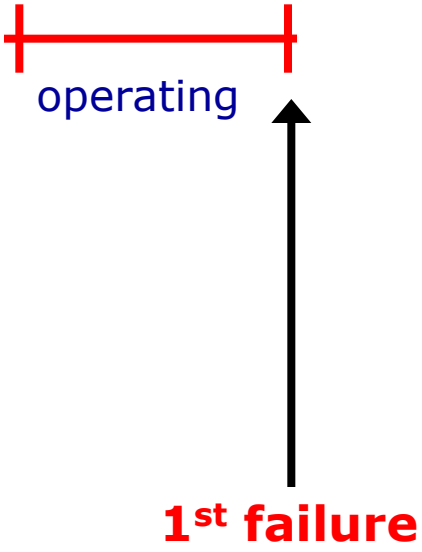
دسترس پذیری

- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.

Availability

دسترس پذیری

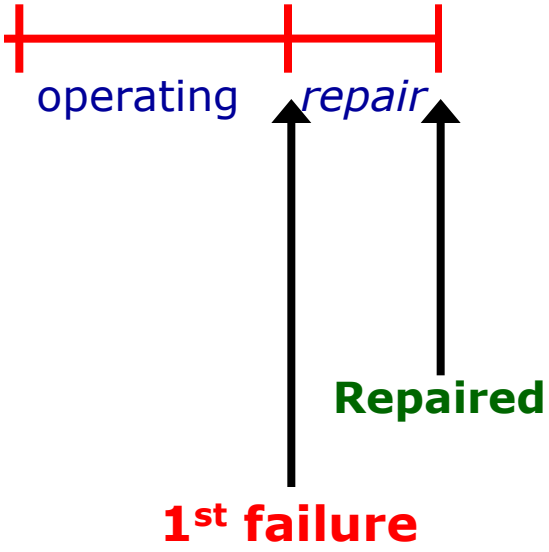
- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.



Availability

دسترس پذیری

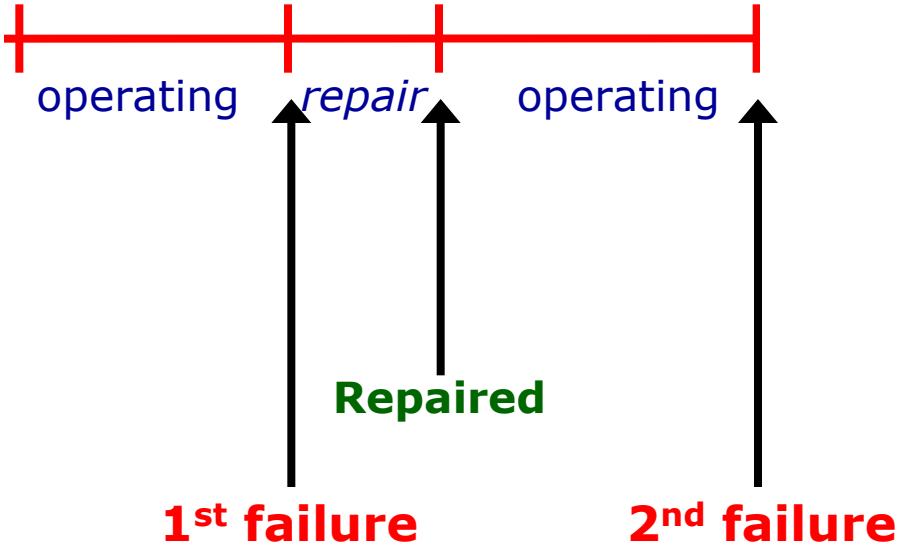
- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.



Availability

دسترس پذیری

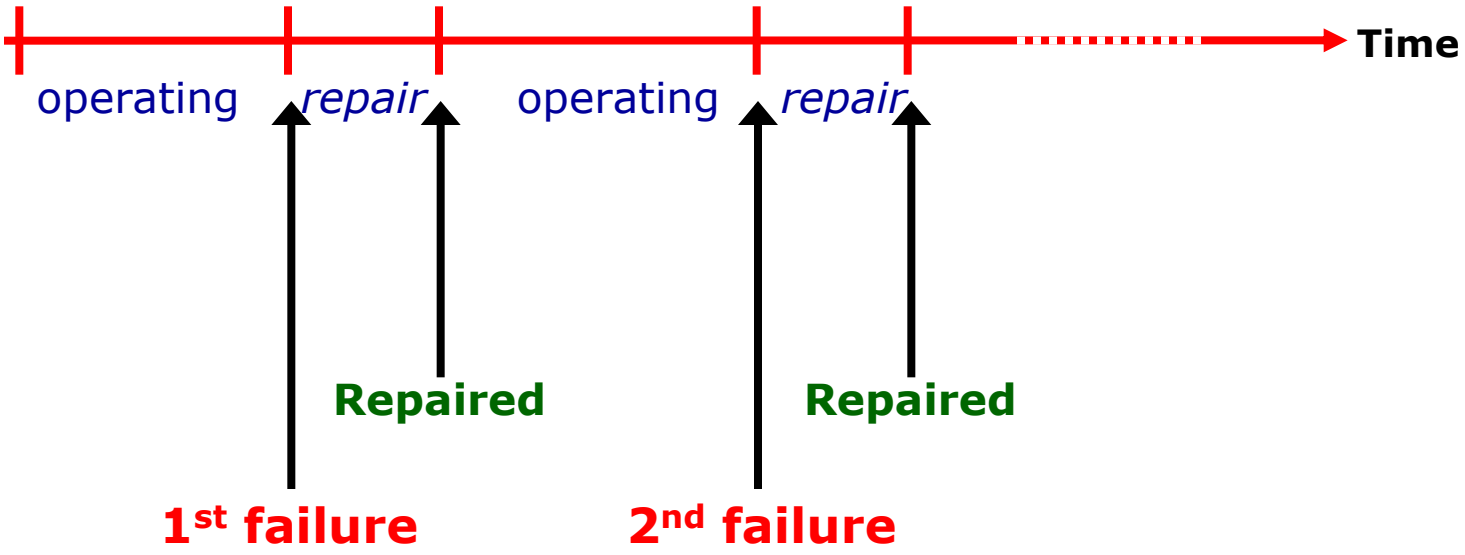
- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.



Availability

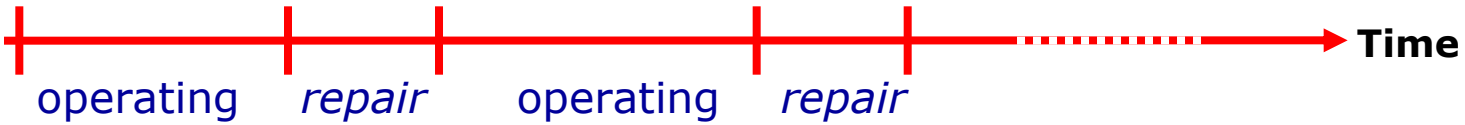
دسترس پذیری

- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.



Availability دسترس پذیری

- The availability, A(t), is a function of time, defined as the probability that system is operating **correctly** and is **available** to perform its function at the **instant** of time t.



- The availability depends on:
  - how **frequent** the system becomes inoperable.
  - how **quickly** it can be repaired.

- ***Example Applications:***
  - Transactions processing systems
    - Airline reservation.

Maintainability قابلیت نگهداری

- Maintainability, M(t), is the probability that a failed system will be restored to an operational state **within** a specified **period of time,** t.

- The restoration process includes:
  - Locating the problem
  - Physically repairing the system
  - Bringing the system back to its operational condition

Safety

ایمنی

- Safety, S(t), is the probability that a system will **either** perform its functions **correctly,** or will **discontinue** its function in a manner that does not disrupt the operation of other systems or compromise the safety of any **people associated** with the system.

- Safety is a measure of the **fail-safe** techniques of a system

Integrity

تمامیت

- Integrity is the non-occurrence of improper alternations of information.

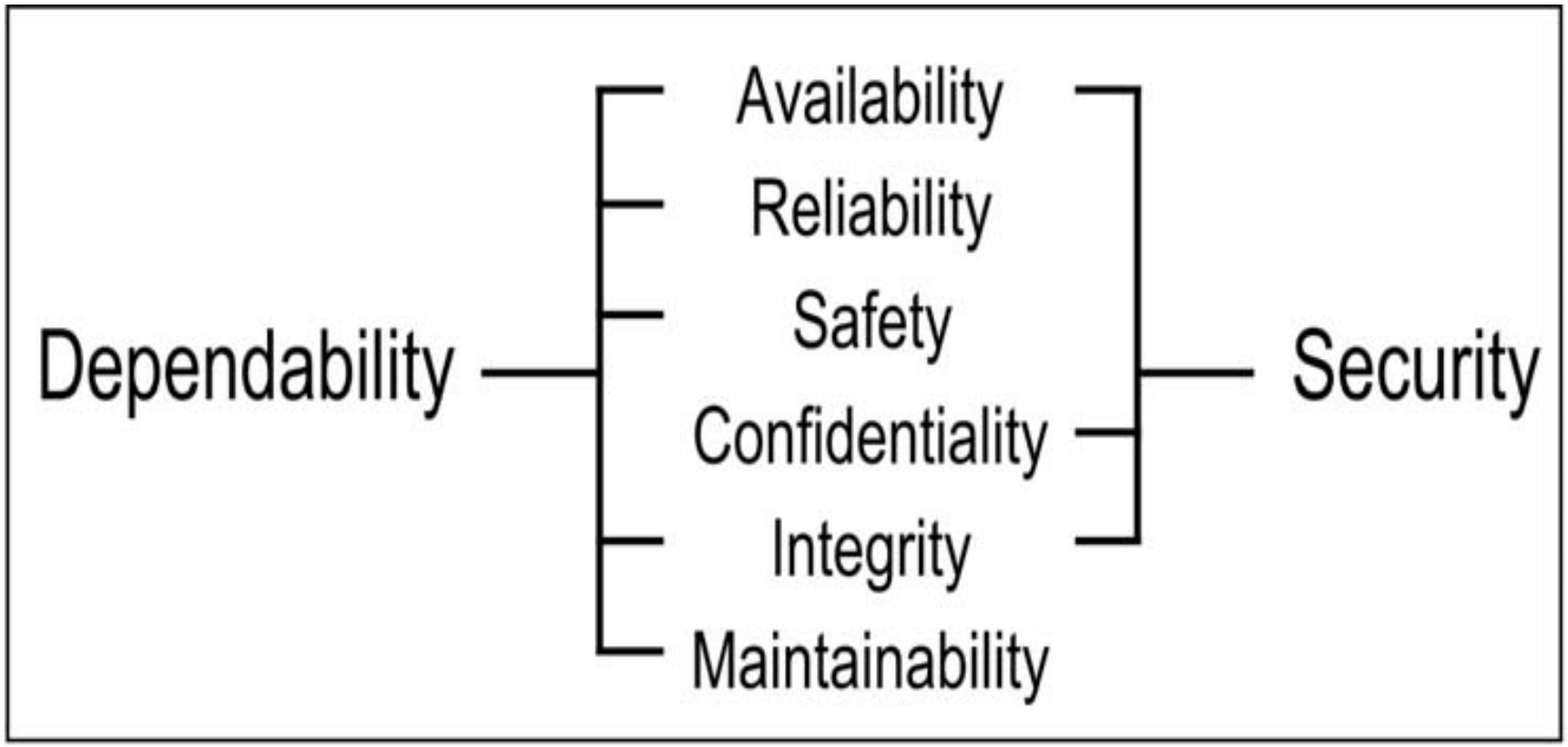
Dependability

- **The term dependability encompasses all the above concepts.**
- ***Laprie:***
  - Dependability is the ability to deliver service that can justifiably be trusted.

Confidentiality محرمانگی

- Confidentiality is the non-occurrence of unauthorized disclosure of information

Dependability & Security Attributes



IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 1, NO. 1, JANUARY-MARCH 2004

Performability قابلیت کارائی

- The performability of a system is a function of time, P(L , t), defined as the probability that the system will be **at**, or **above**, some **level** of performance, L, at the **instant of time** t.

- **Graceful degradation** is closely related to performability.
  - Graceful degradation is the ability of a system to automatically decrease its level of performance to compensate for hardware and software faults.

Performability vs. Reliability

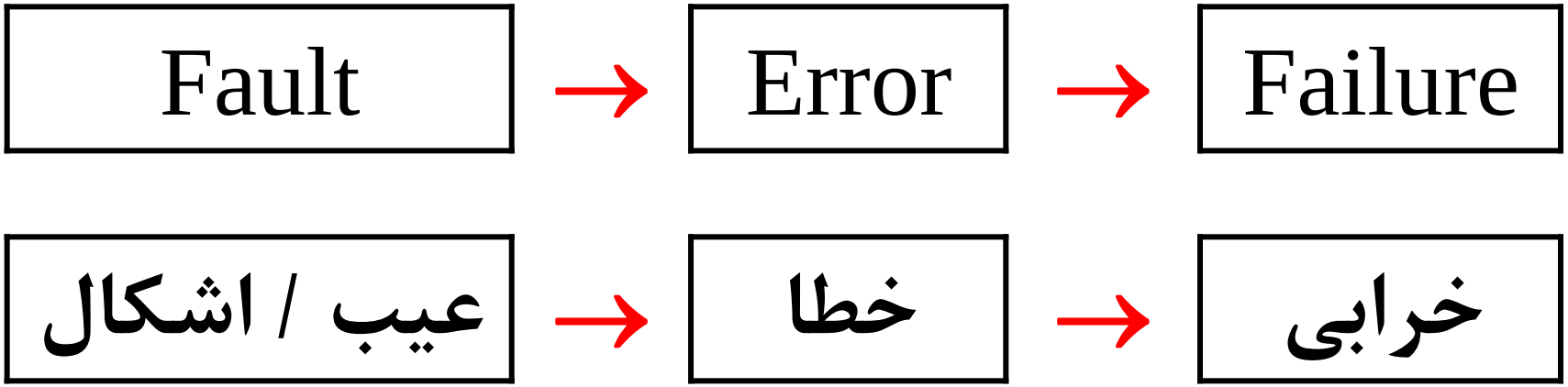
- P(L , t) is a measure of the likelihood that some **subsets** of the functions are performed correctly.
- R(t) is a measure of the likelihood that **all** of the functions are performed correctly.

Testability آزمون پذیری

- Testability is the ability to test for certain attributes within a circuit/system.

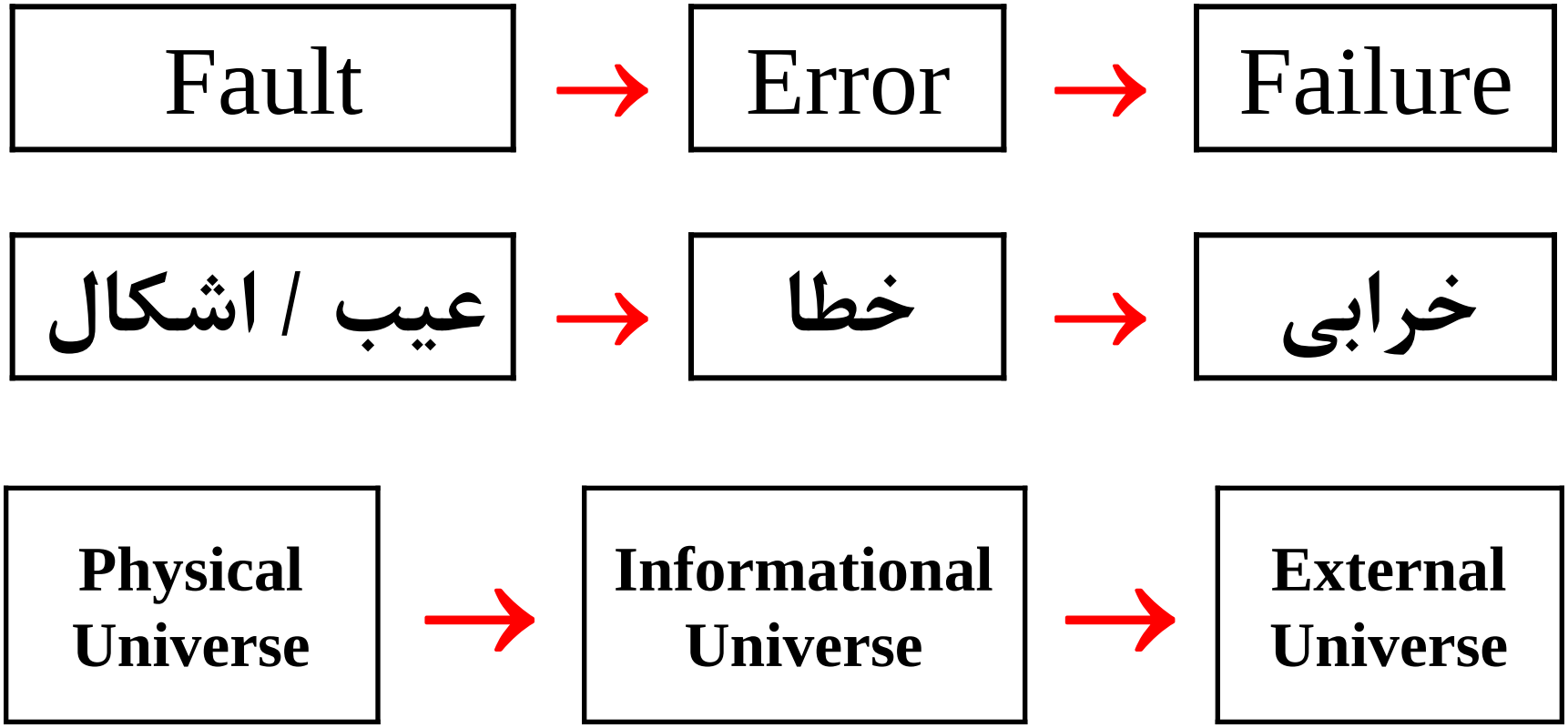
- Testability is related to **Maintainability**, because of the importance of minimizing the time required to identify and locate problems.

زنجیره علت و اثر

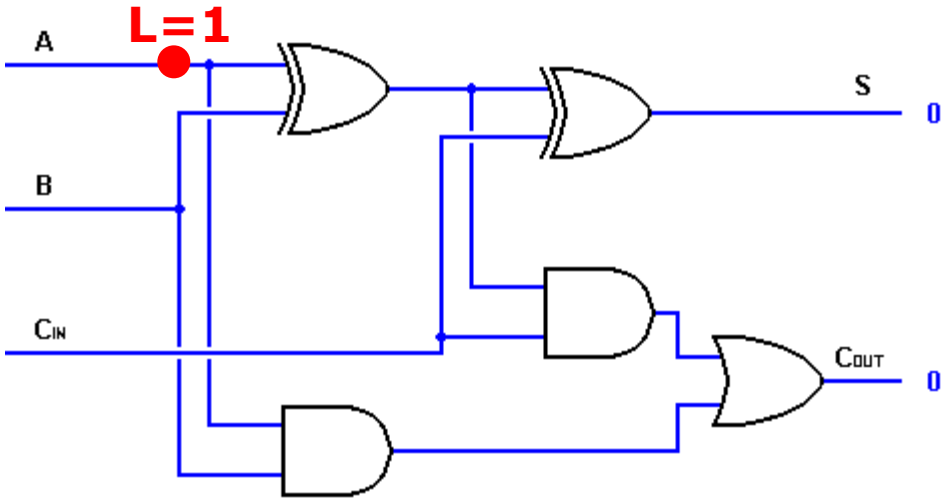


- **Failure**
  - هرگاه یک سیستم کار مورد انتظار را صحیح انجام ندهد یک **Failure** رخ داده است.
- **Error**
  - علت یک **Failure** وجود یک **Error** است.
- **Fault**
  - علت یک **Error** وجود یک **Fault** است.

مدل سه فضایی

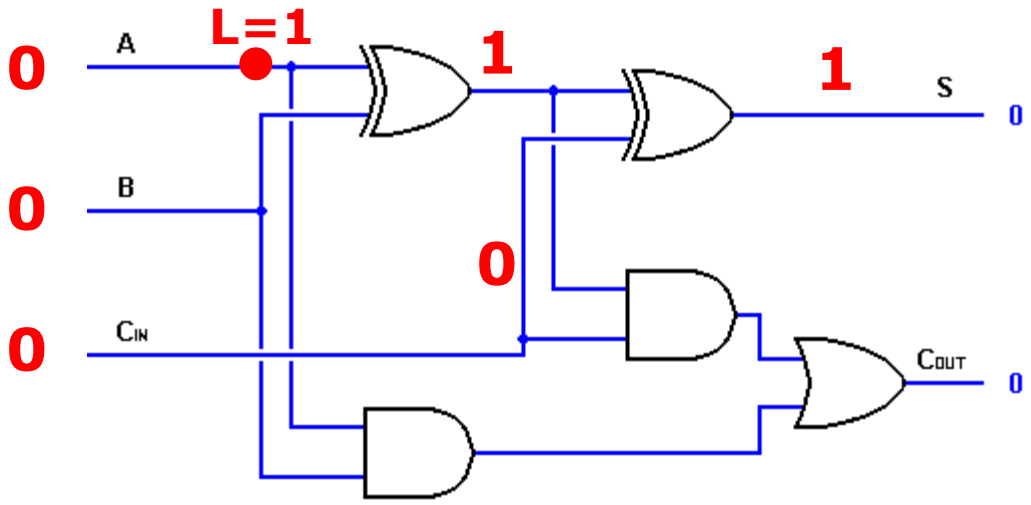

Fault
Error
Failure
عیب / اشکال
خطا
خرابی
Physical Universe
Informational Universe
External Universe

Example 1: Full Adder



A	B	Cin	S	Cout
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Example 1: Full Adder



A	B	Cin	S	Cout
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	0	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

A	B	Cin	S	Cout
1	0	0	*1*	0
1	0	1	*0*	*1*
1	1	0	*0*	*1*
1	1	1	*1*	1
1	0	0	1	0
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

Example 2

- **توقف حرکت اتومبیل**
- شرح : اتومبیلی را در نظر می‌گیریم که بر روی سطح یکی از چرخ‌هایش سوراخ کوچکی ایجاد شده است، این سوراخ سبب کم شدن فشار باد آن چرخ می‌شود. این عامل موجب انحراف در مسیر حرکت و در نهایت موجب توقف اتومبیل می‌شود.

- **Fault** : سوراخ موجود در چرخ
- **Error** : کم شدن فشار باد لاستیک
- **Failure** : توقف اتومبیل

http://www.ece.ucsb.edu/~parhami/pubs_folder/parh97-ieeetr-defect-fault-etc.pdf

Example 3

- **یک سازمان کوچک را در نظر بگیرید:**
  - **Fault**: خطاهایی در سیاست ترفیع کارمندان سازمان که می‌تواند باعث ترفیع‌های نادرست شود، بعنوان Fault در نظر گرفته می‌شود.
  - **Error**: نارضایتی‌های ناشی از آن بتدریج وقوع سوء عمل کارمندان شده و نهایتاً منجر به کاهش کارایی سازمان می‌شود.
  - **Failure**: عدم دستیابی سازمان به اهداف خود.

Example 4

- **اتومبیلی را در نظر بگیرید**
- اتومبیل به علت وقوع fault در کامپیوتر مرکزی (ECU) آن، سرعتی که صفحه‌ی کیلومتر آن نشان می‌دهد، کمتر از مقدار واقعی است، در این صورت:

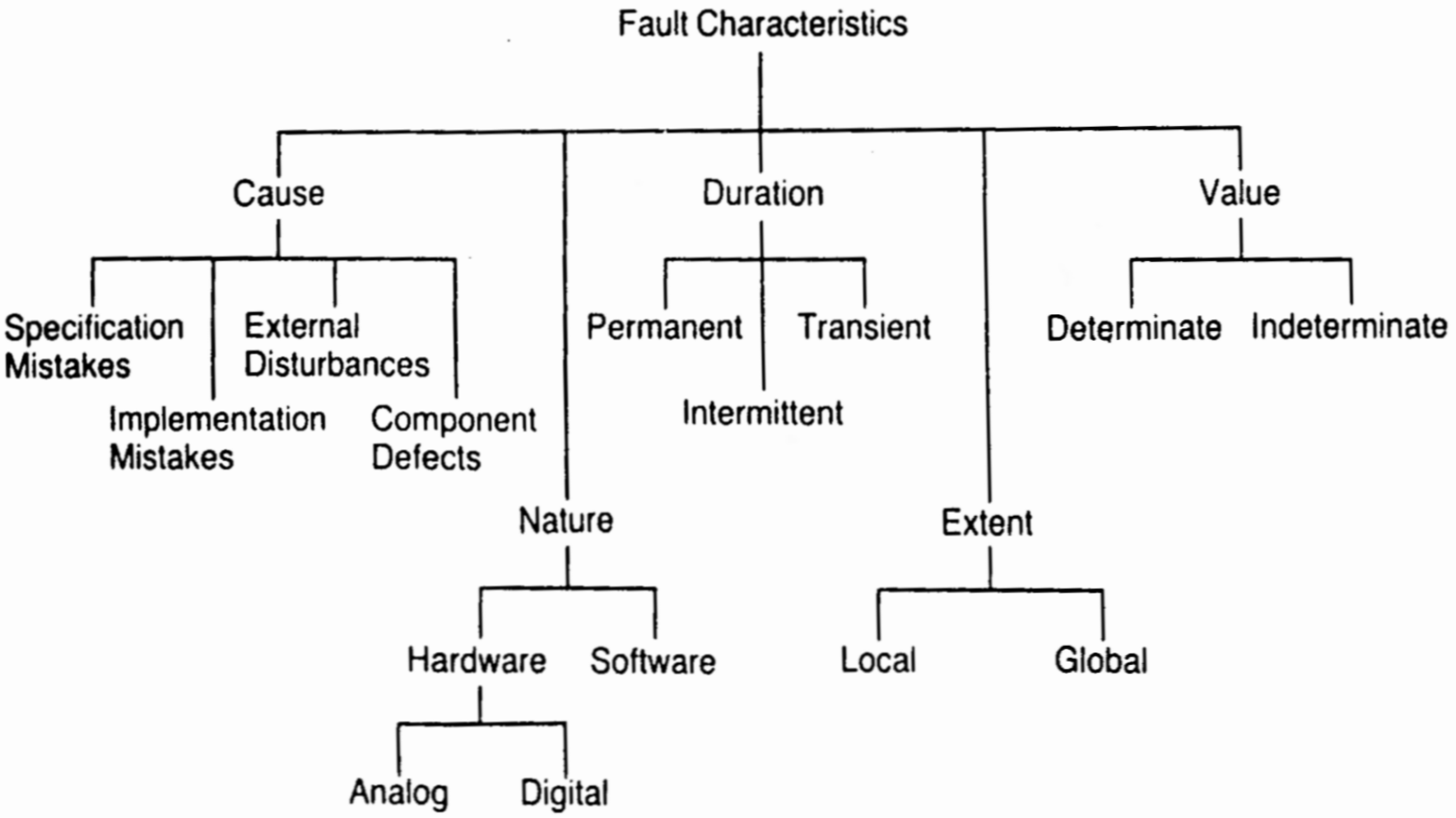
- Fault: اشکال در ECU
- Error: افزایش فشار پدال گاز توسط راننده
- Failure: تصادف با اتومبیل دیگر

Causes of Faults

- یک اشکال می‌تواند بوسیله عوامل مختلفی در اجزای نرم و سخت یک سیستم بوجود آید. این اشکال می‌تواند در چهار حالت بوجود آید.

1. During Specification & Design
2. During Implementation/Test
3. External to the components
4. Component defect

Fault Characteristics



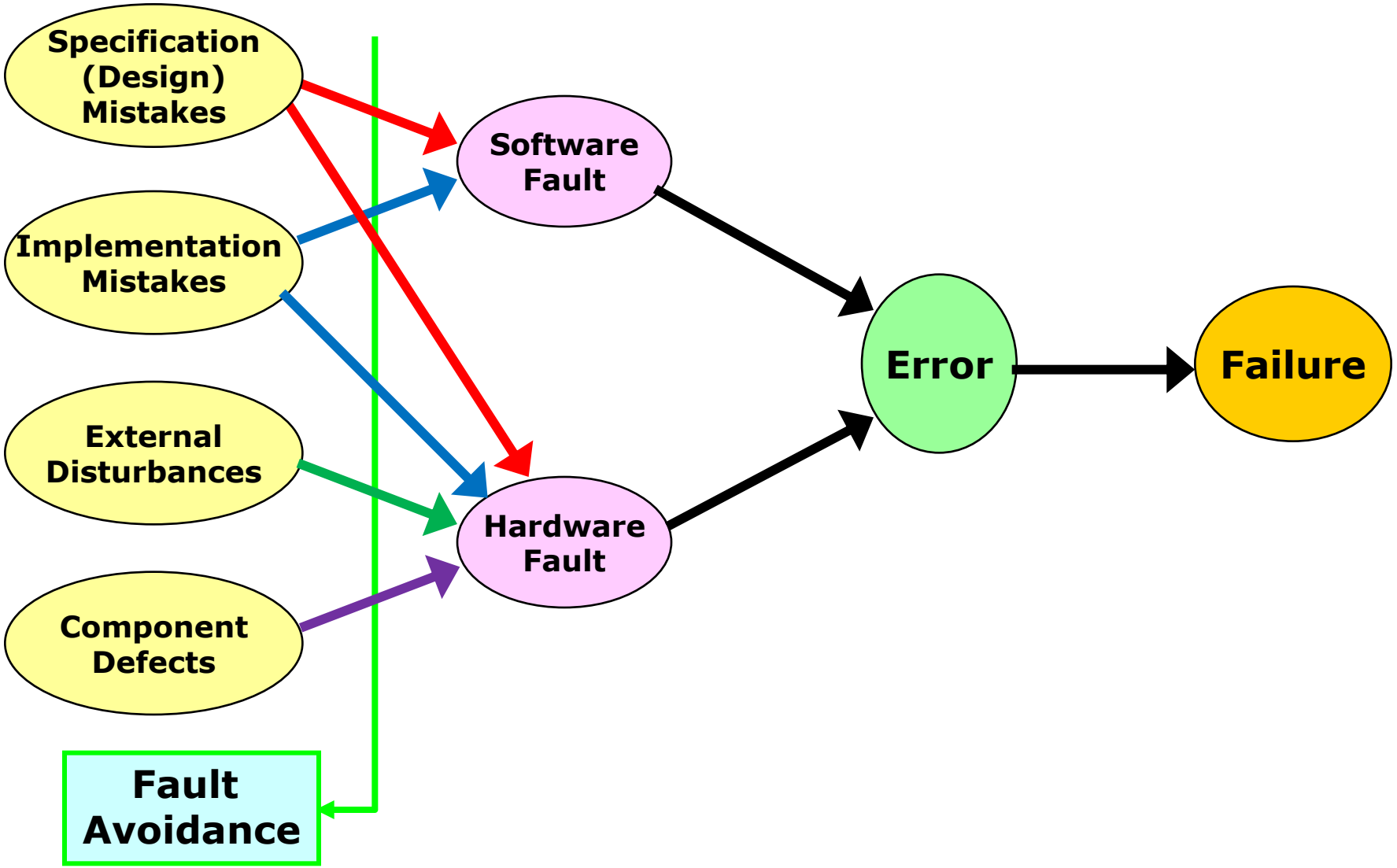
Primary techniques against faults

- ***Fault avoidance***
- ***Fault masking***
- ***Fault tolerance***

Primary techniques against faults

- ***Fault Avoidance***
  - **Attempts to prevent a fault in the first step.**
    - **Specification & Design reviews**
    - **Component screening**
    - **Functional testing**
    - **Shielding**

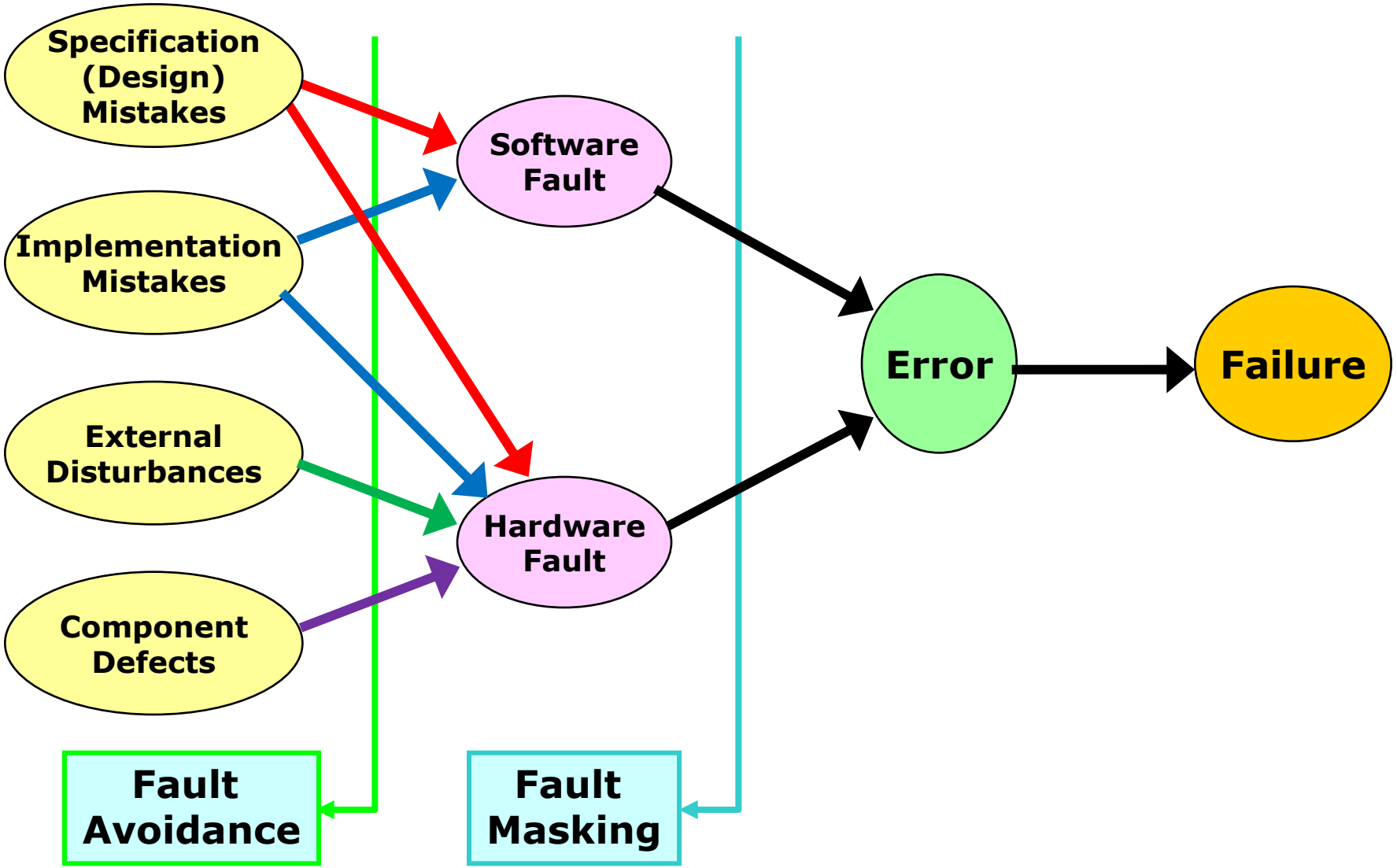
Cause and Effect Relationship



Primary techniques against faults

- ***Fault Masking***
  - **Attempts to prevent a fault in an operational system from introducing errors into informational structure of that system.**
    - **Error correcting memories**
    - **Majority voting**

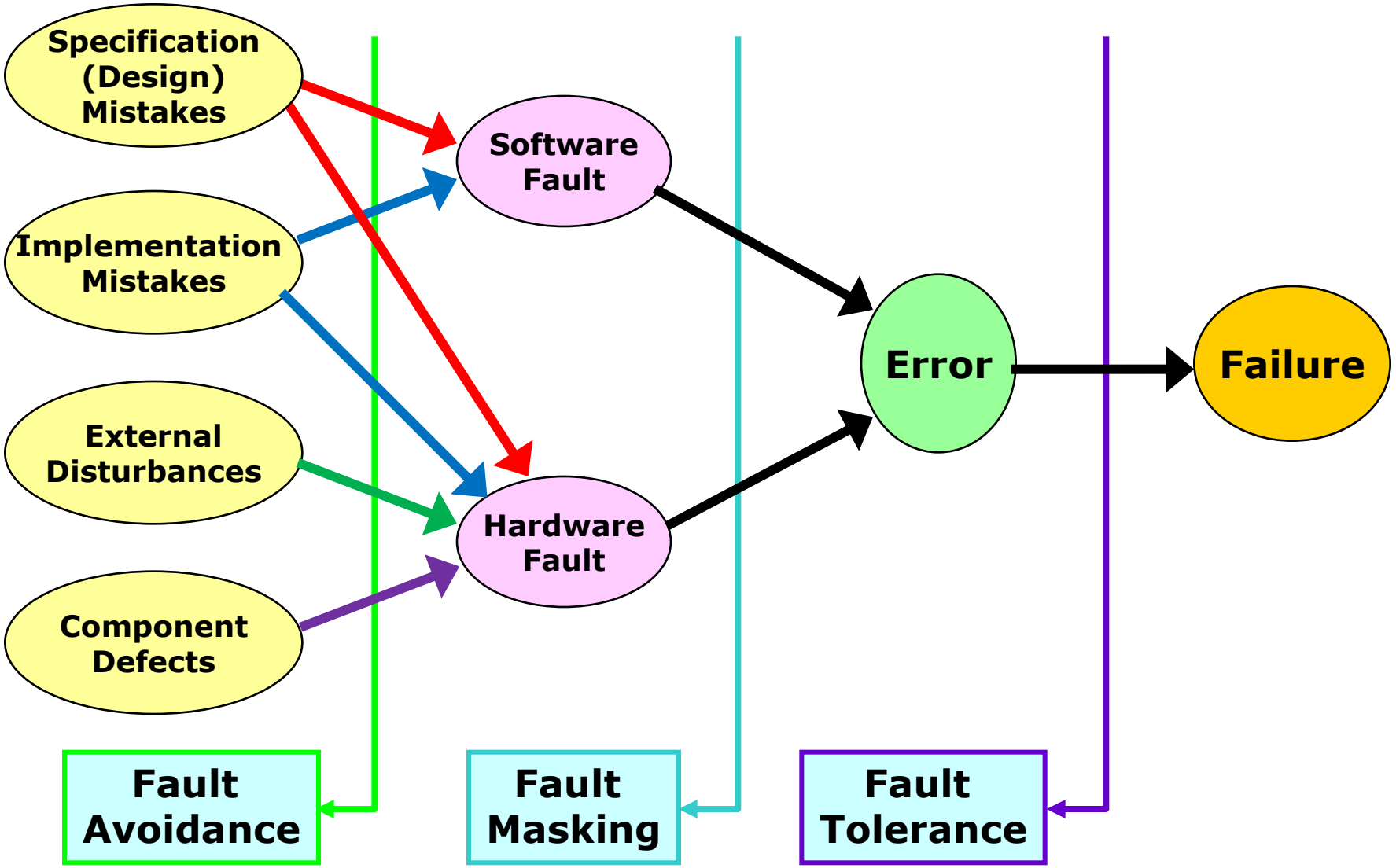
Cause and Effect Relationship



Primary techniques against faults

- ***Fault Tolerance***
  - **Attempts to provide a system to continue to perform its expected tasks after the occurrence of faults.**
    - **Fault detection**
    - **Fault location**
    - **Fault containment**
    - **Fault recovery**

Cause and Effect Relationship



Fault Tolerance

How?

BY

Redundancy

افزونگی

Redundancy

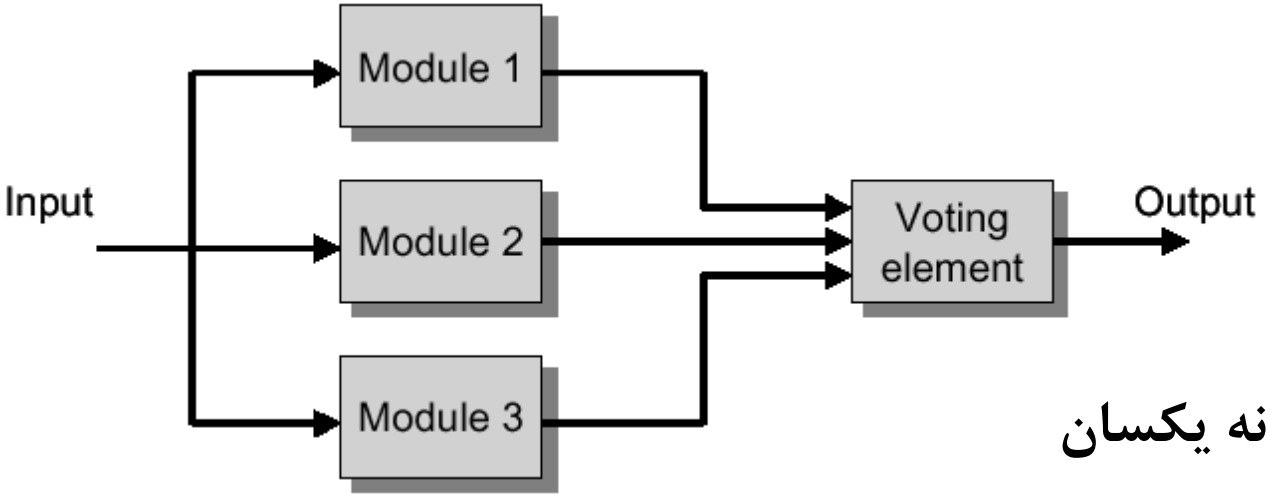
- ***Fault Tolerance*** and ***Fault Masking*** are achieved by using ***Redundancy*****.**
  - **Redundancy is the addition of HW/SW resources, information or time beyond what is needed for normal system operation.**

Types of Redundancy

- Hardware Redundancy
- Software Redundancy
- Information Redundancy
- Time Redundancy

- Redundancy Interrelationship:
  - Extra SW → Extra Memory → Extra Time

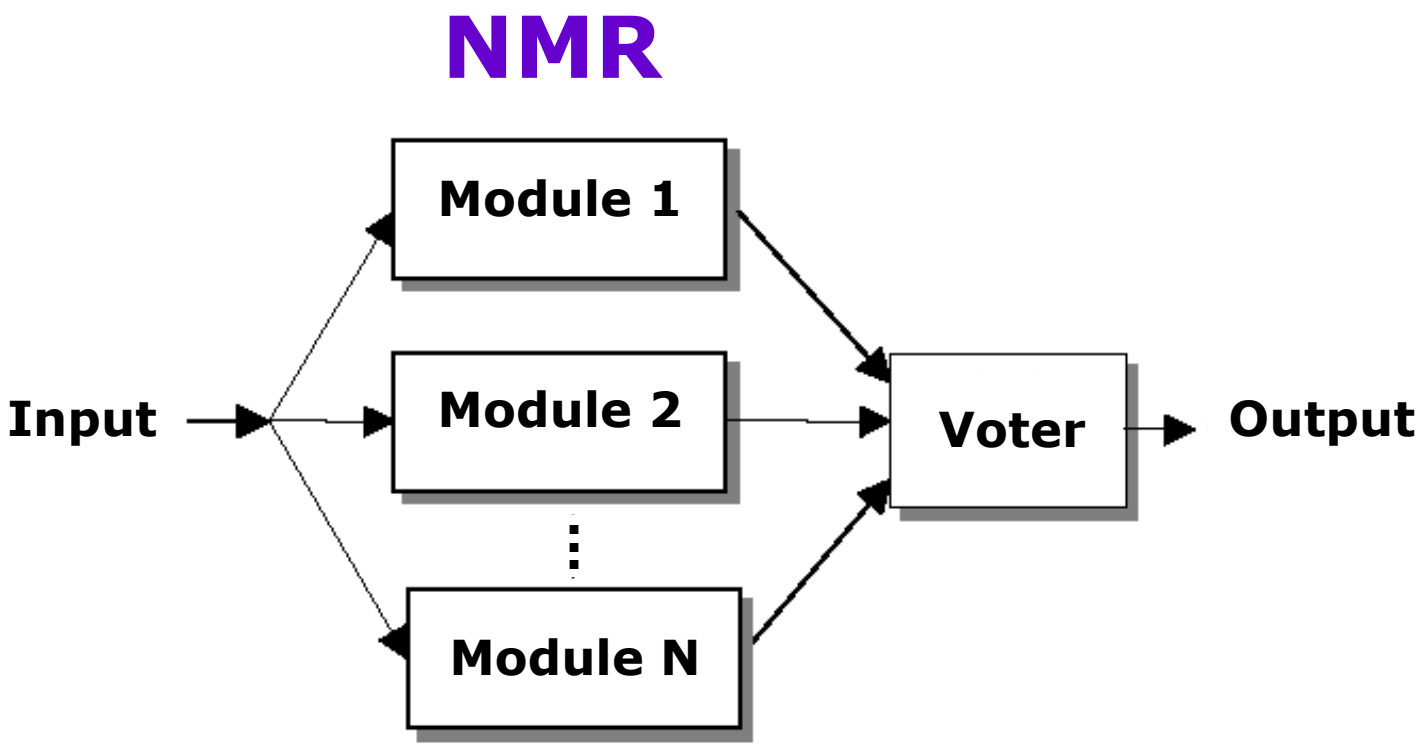
Triple Modular Redundancy افزونگی سه پیمانه‌ای



TMR

- استفاده از سه پیمانه یکسان
- استفاده از یک رأی‌گیرنده
- ورودی یکسان به سه پیمانه
- ورودی همزمان به رأی‌گیرنده
- رأی اکثریت توسط رأی‌گیرنده
- پنهان شدن **fault** در یکی از واحدها توسط واحدهای دیگر
- استفاده در سطوح مختلف (ریزپردازنده – حافظه – گذرگاه ....)

N Modular Redundancy افزونگی N پیمانه‌ای



- پنهان کردن *بیش از یک* ***fault*** توسط واحدهای دیگر

The End