四维一体的可靠性系统工程发展模式

4-D Development Mode of Reliability System Engineering

School of Reliability & Systems Engineering

可靠性与系统工程学院

BeiHang University， China

北京航空航天大学

Outline

- Who are we?
- Reliability system engineering (RSE)
- 4-D Development Mode
- Software Reliability work with 4-D Mode
- Communication with industry

Who are we?

- A school at BeiHang University, which focuses on reliability systems engineering.
- Reliability Engineering Institute of BeiHang University
- Reliability Engineering Center for Aviation Industry Corporation of China
- ……

4-est in China reliability area

Our school is the leader of reliability system engineering in China

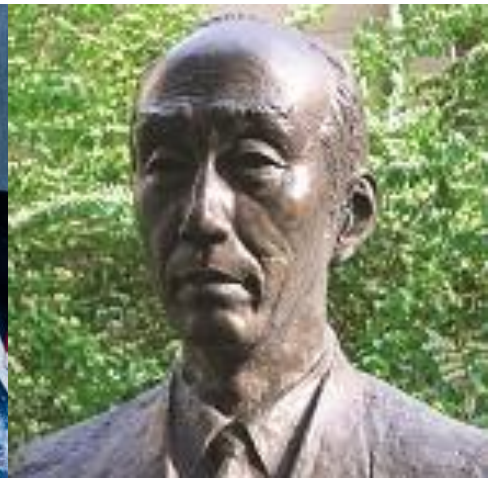
- **Earliest**
- **Most famous**
- **Widest**
- **Strongest**

Since 1985

Covering:

- Research fonding, more than 2500 million US dollar
- Number of Projects, more than 500
- Talent, 75% PhD
- Theory, Techinque, Application

The Research Prof. Yang Weimin, the leader of reliability people in China



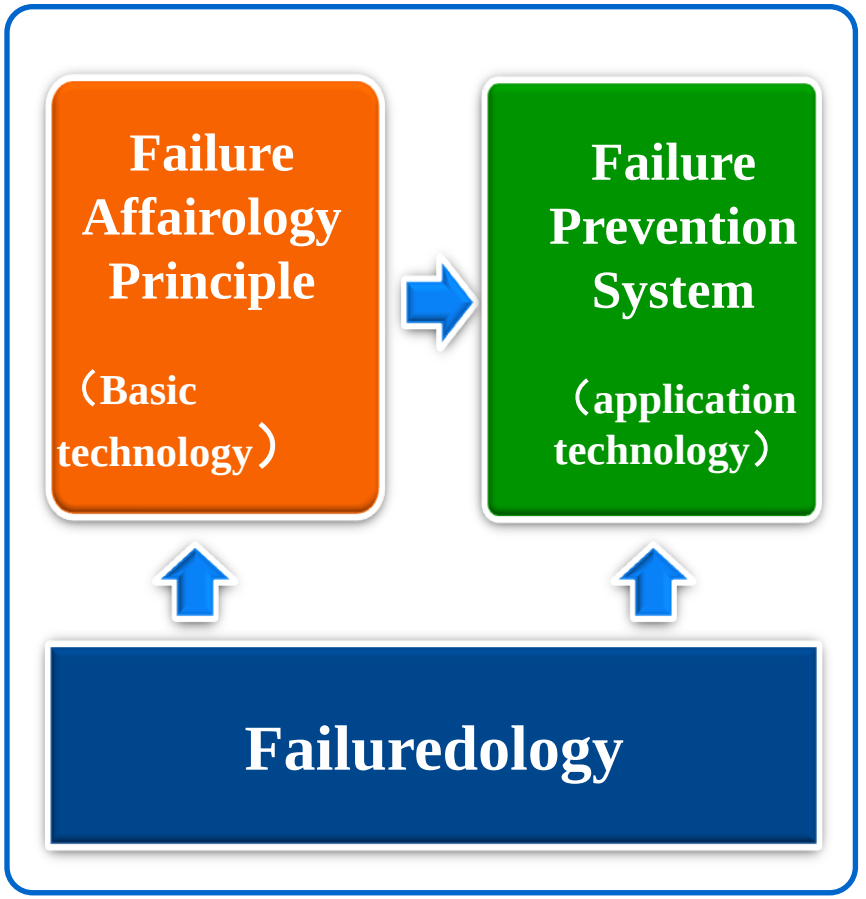
Component…

Reliability Systems Engineering

Reliability Systems

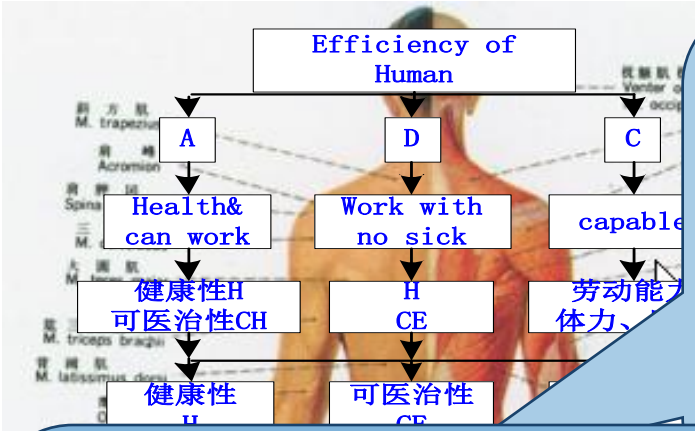
It is an integrated engineering technology which takes failure as the core issue, revealing the law of failure and providing techniques in failure prevention, failure control and repair, with systematic engineering theory and methods in the entire life cycle of the complex systems

《 China's military encyclopedia 》



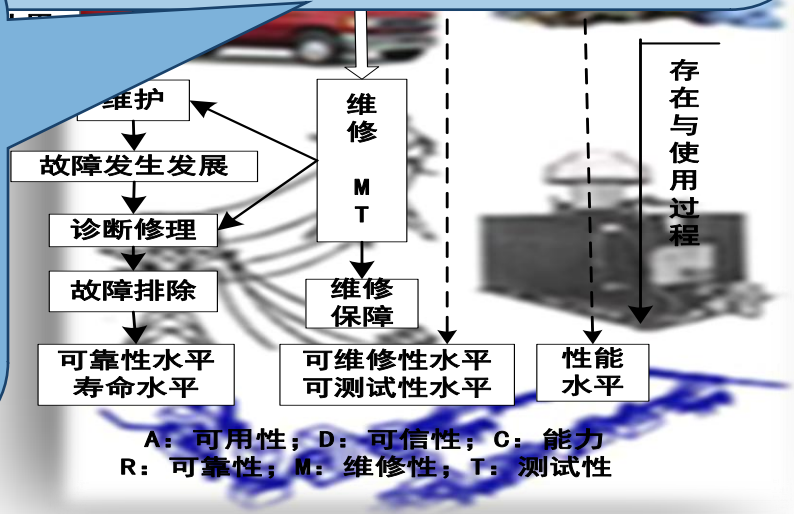
Reliability Systems Engineering

Reliability system engineering VS Health system engineering



Traditional Chinese Medicine ensures the health of human body by the principle “Prevention，Diagnosis, Prognostics and Treatment”

Similar to the body's immune system, RSE ensures that equipments operate without failures during the total life cycle

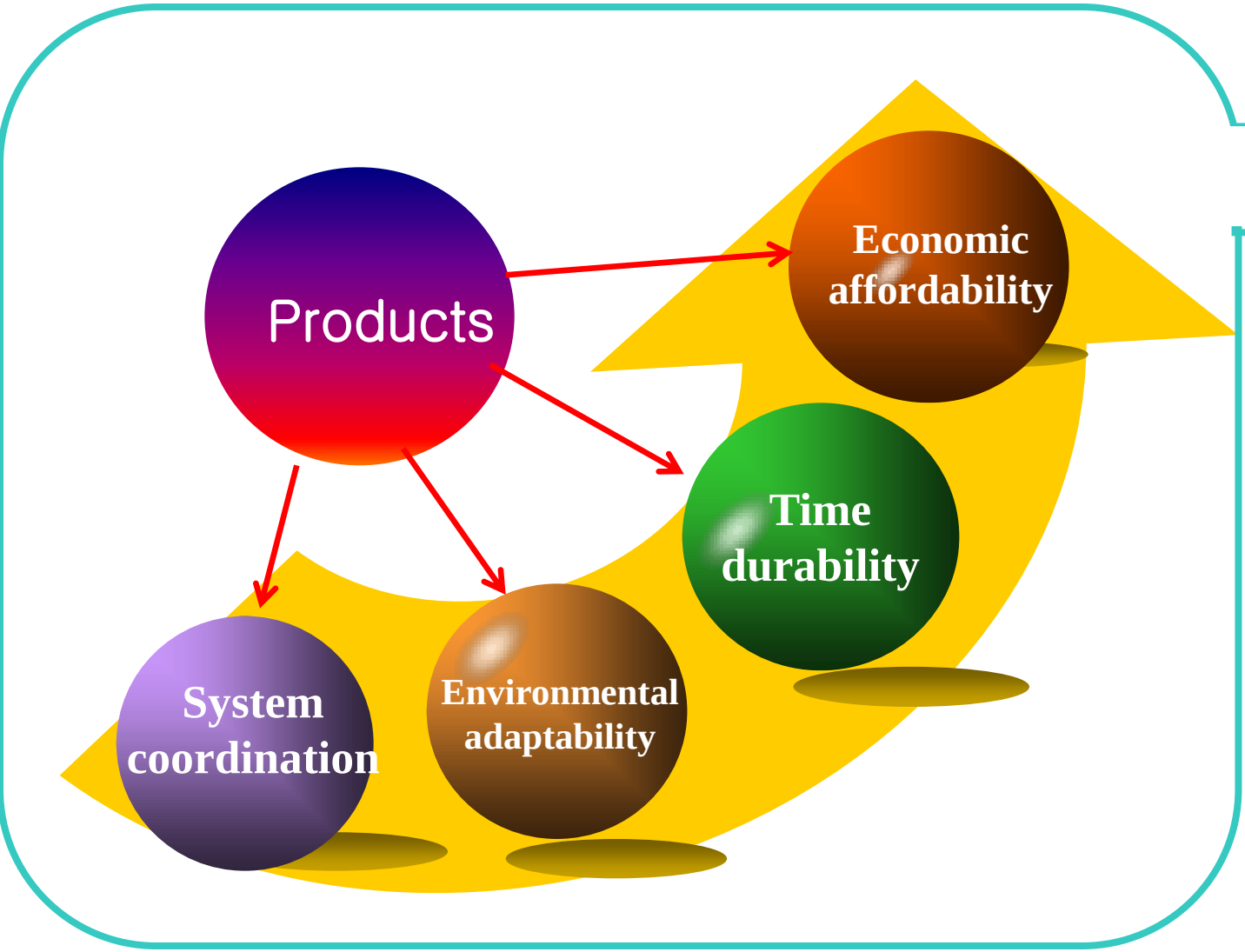


防 Prevention

诊 Diagnosis

治 Treatment

Technical Connotation of RSE



RSE

A multiplier of function and performance

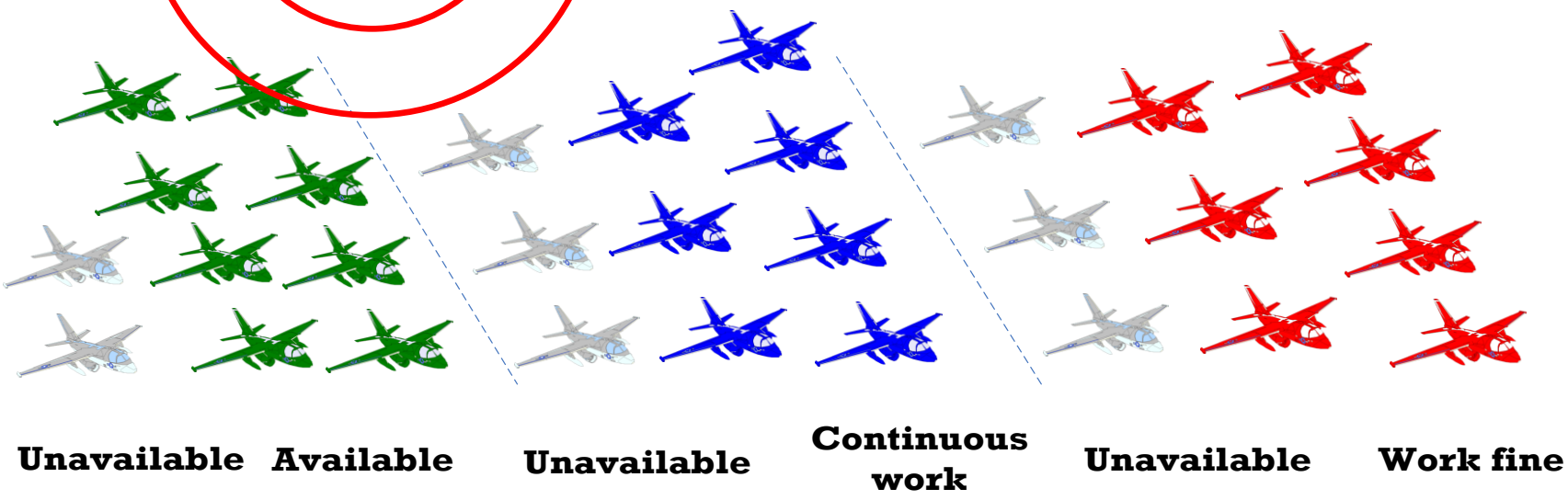
Efficiency

- Efficiency（E）is the comprehensive expression of system availability（A) dependability(D) and capability(C).
- E=A• D • C

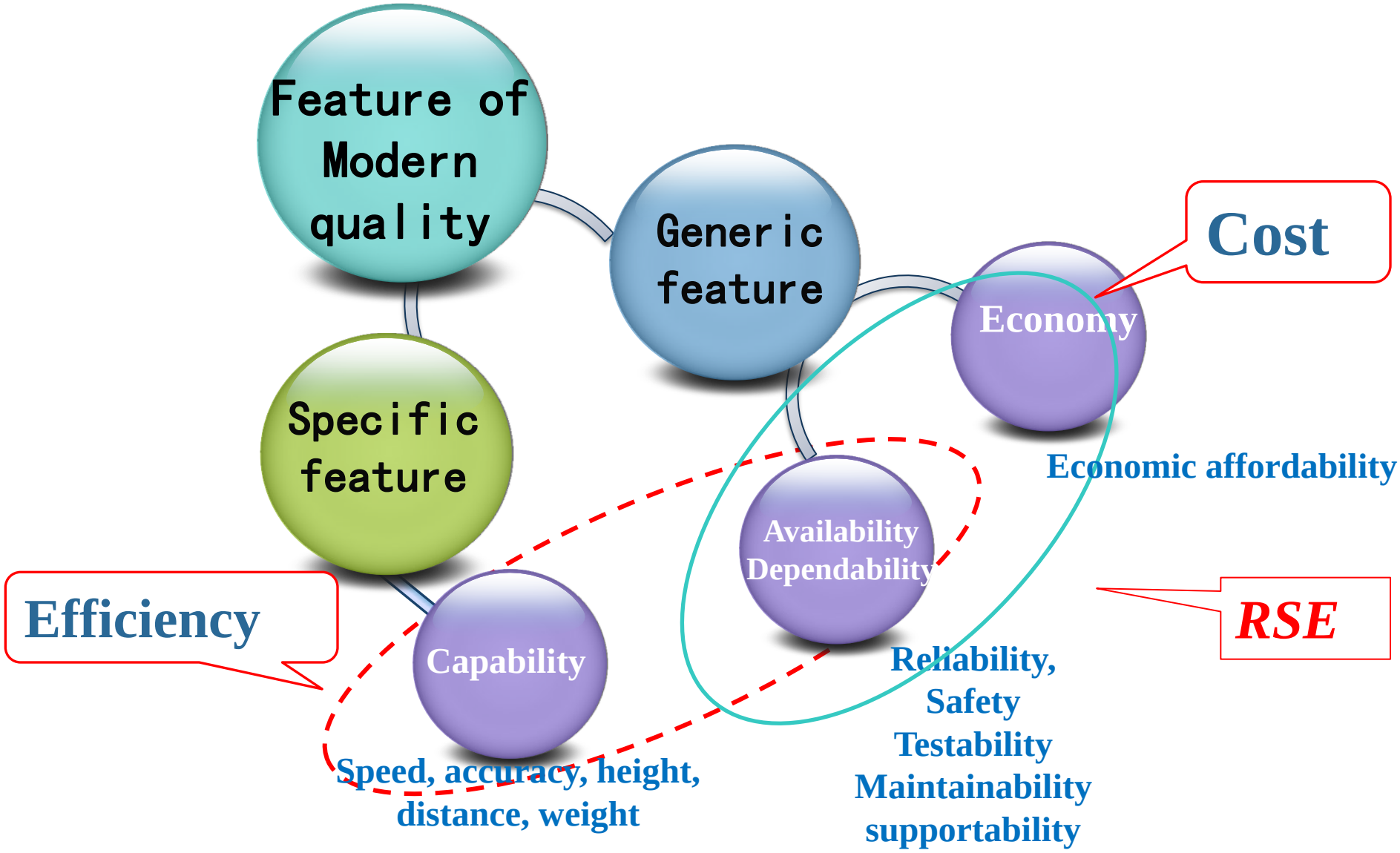
RSE

Chairman Mao said:

召之即来	来之能战	战之能胜
Come at any moment	Work continually in the mission	Complete the objectives
High availability	High dependability	High capability



Position of RSE in modern quality

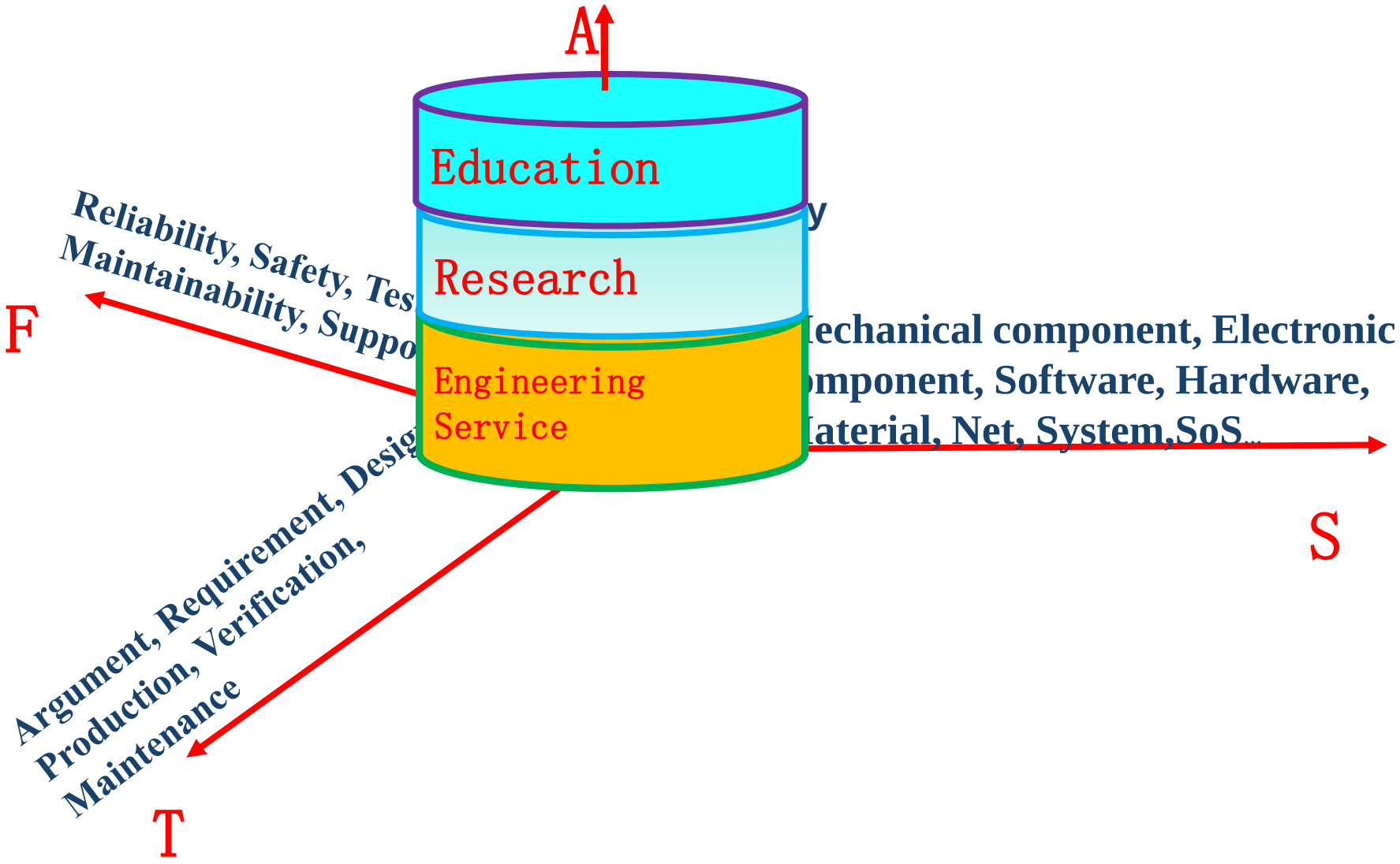


4D-Mode for RSE

$$\text{RSE Framework} = S \times T \times F \times A$$

- **S is the set of components in System-wide.**
  - **S={Component, Part, Software, Hardware, Material, Net, System, SOS,…}**
- **T is the set of Total Life Cycle of products**
  - **P={Argument, Requirement, Design, Production, Verification, Maintenance...}**
- **F is the set of the Full-features of products**
  - **F={Reliability, Safety, Testability, Maintainability, Supportability}**
- **A is the set of all around knowledge and work**
  - **A={Theory,Technology,Tools,Practice;Education,Research,Consultation, Service}**

4D-Mode

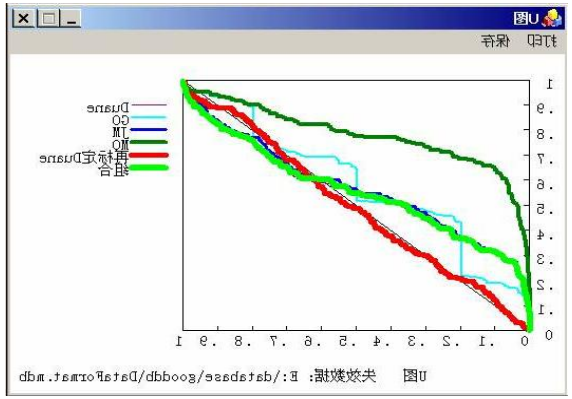

A
Education
Research
Engineering
Service
F
Reliability, Safety, Tes
Maintainability, Suppo
echanical component, Electronic
mponent, Software, Hardware,
aterial, Net, System,SoS…
S
T
Argument, Requirement, Desig
Production, Verification,
Maintenance

Example of RSE in System-wide

Component

- Electronic components destructive physical analysis(DPA)
- VLSI circuit test
- …

Software

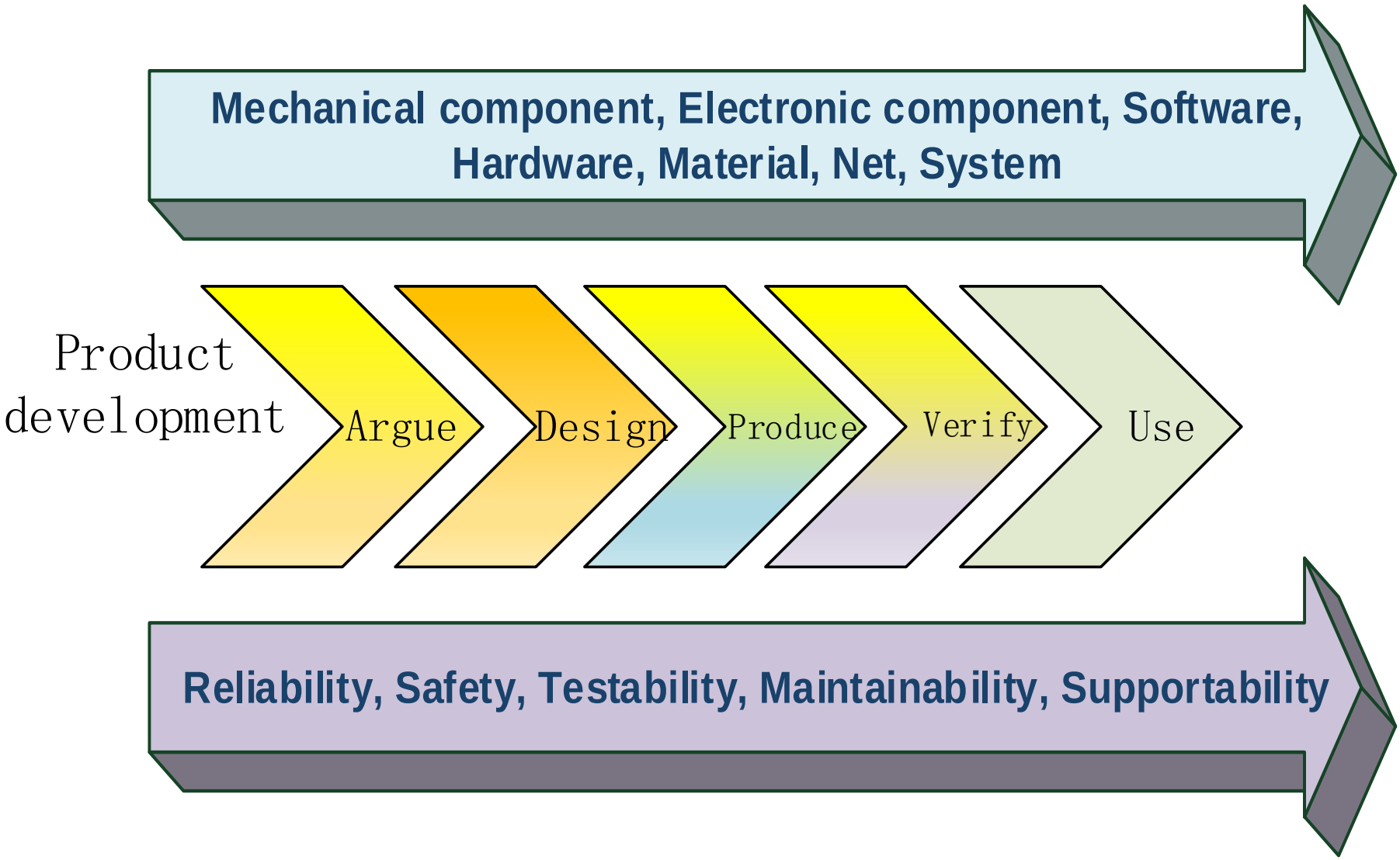


- Embedded software test
- Software reliability assessment
- …

Hardware

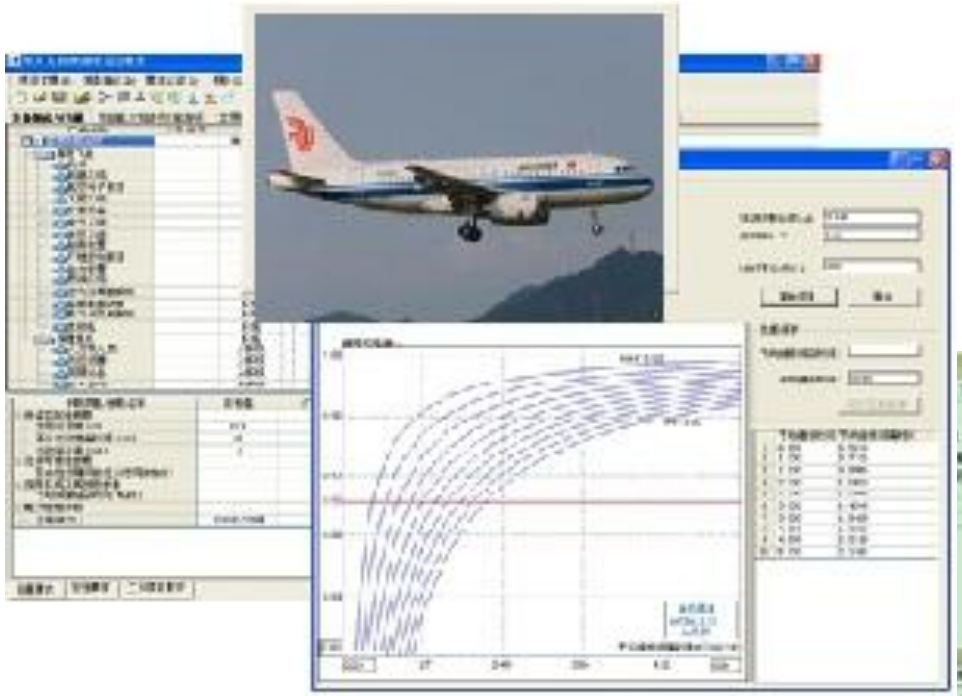
- Reliability / environmental test(Temperature, Humidity Vibration, and Altitude)
- Reliability Enhancement Testing
- …

RSE solution example in total life cycle



RSE in argument phase

Argument for reliability, safety and maintainability

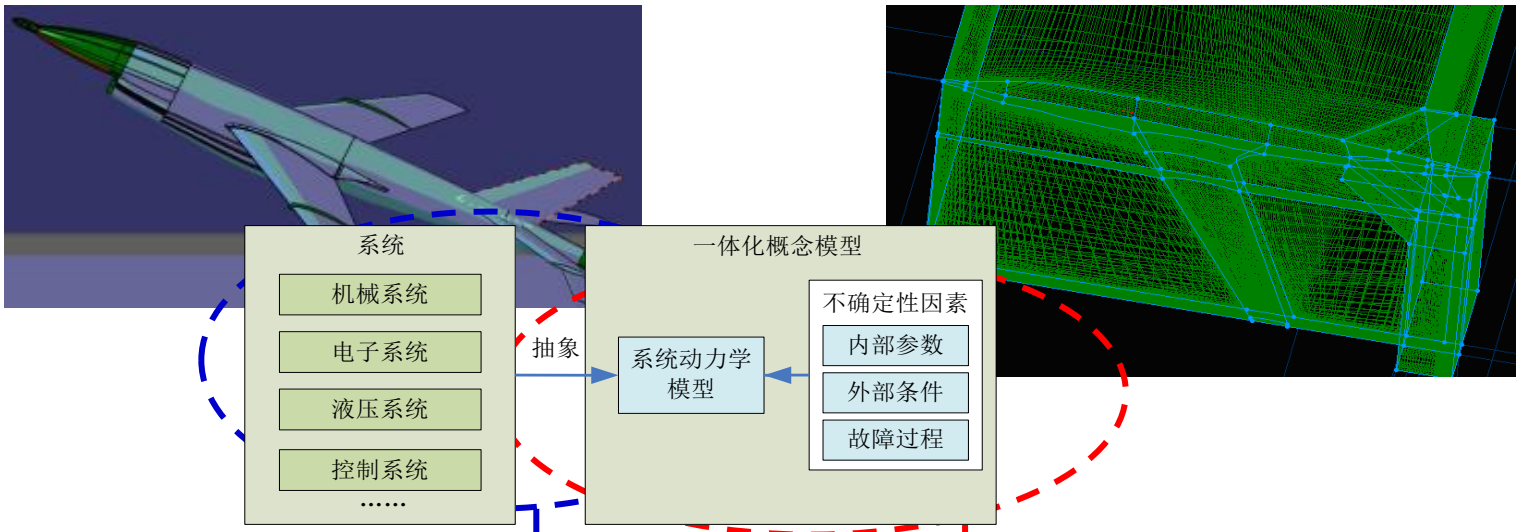


Simulation argument for RMS

Argument for the requirement of RMS

RSE in design phase

Reliability and performance integration design （for system）



$$\dot{x}(t) = Ax(t) + Bu$$
$$y(t) = Cx(t) + Du$$

ζ(t)－故障随机过程；

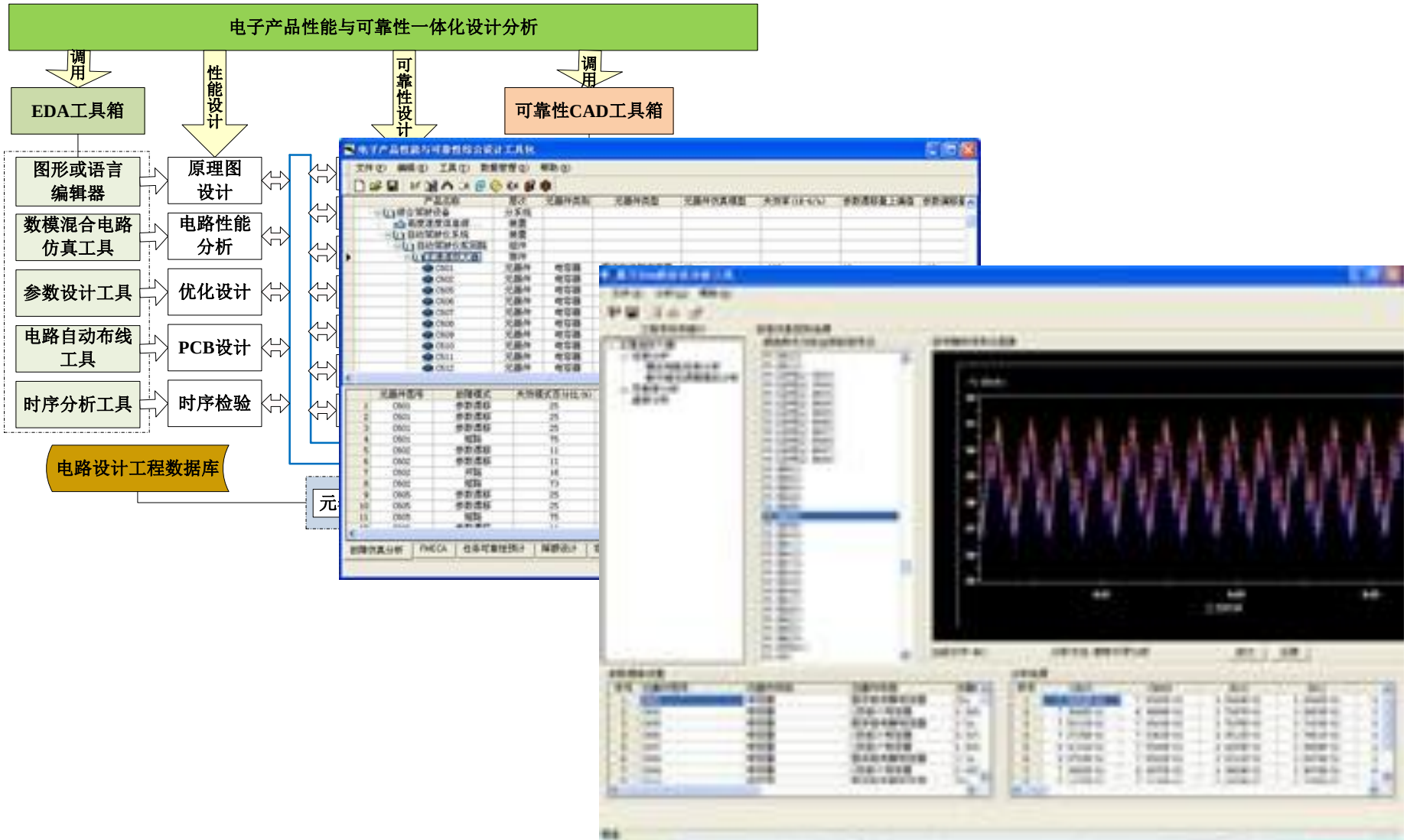
ω(t)－外部扰动随机过程；

ΔA、ΔB、ΔC、ΔD-内部参数不确定性。

$$\dot{x}(t) = [A(\zeta(t) + \Delta A(\zeta(t))]x(t) + [B(\zeta(t)) + \Delta B(\zeta(t))]u + E(\zeta(t))\omega(t)$$
$$y(t) = [C(\zeta(t) + \Delta C(\zeta(t))]x(t) + [D(\zeta(t)) + \Delta D(\zeta(t))]u + F(\zeta(t))\omega(t)$$

RSE in design phase

Reliability and performance integration design （for electronic products）



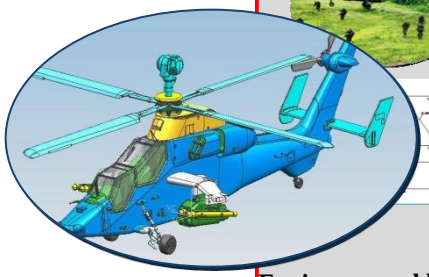
RSE in Total life cycle

Reliability simulation

Simulation Reliability

Case analysis

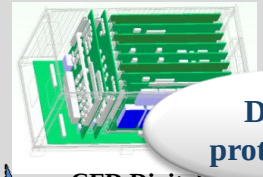
Multi task phase



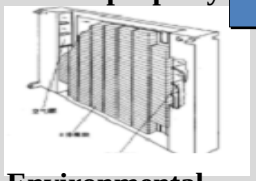
Environmental loads

Digital prototyping

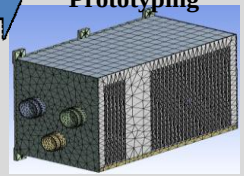
Material property



CFD Digital Prototyping

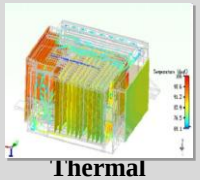


Environmental conditions



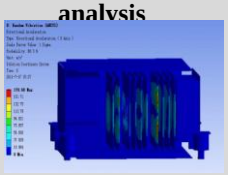
FEA Digital Prototyping

Stress analysis

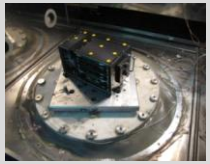


Thermal analysis

Thermal verification

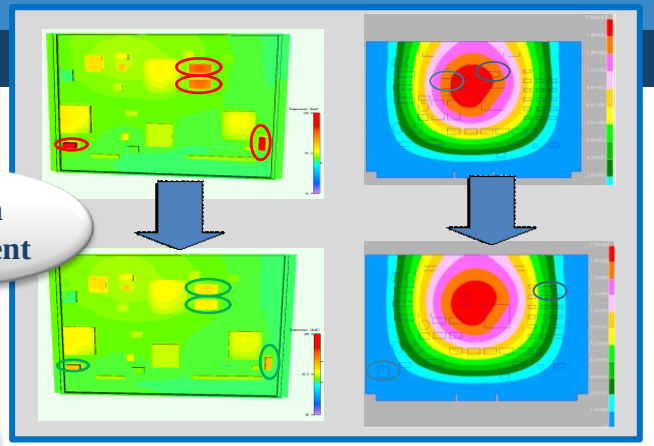


Vibration analysis



Vibration collation

Design refinement



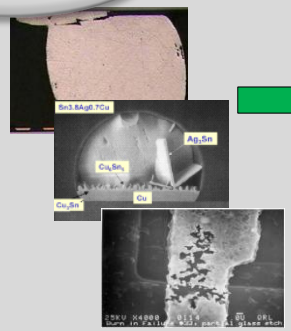
Reliability analysis& evaluation

Failure distribution

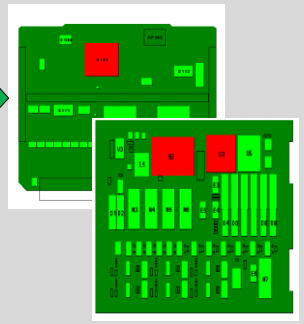
$$MTTF = \frac{\sum_{i=1}^{N} TTF_i}{N}$$

Reliability evaluation

Failure prediction



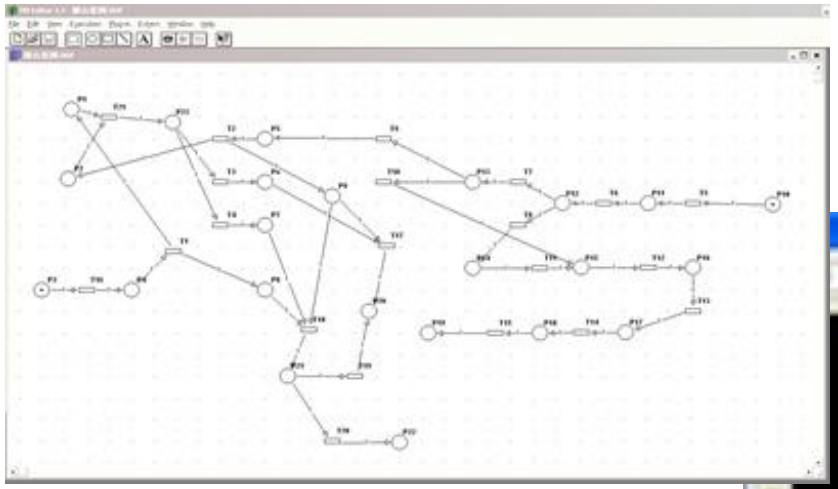
Failure mechanism



Failure point

RSE in design phase

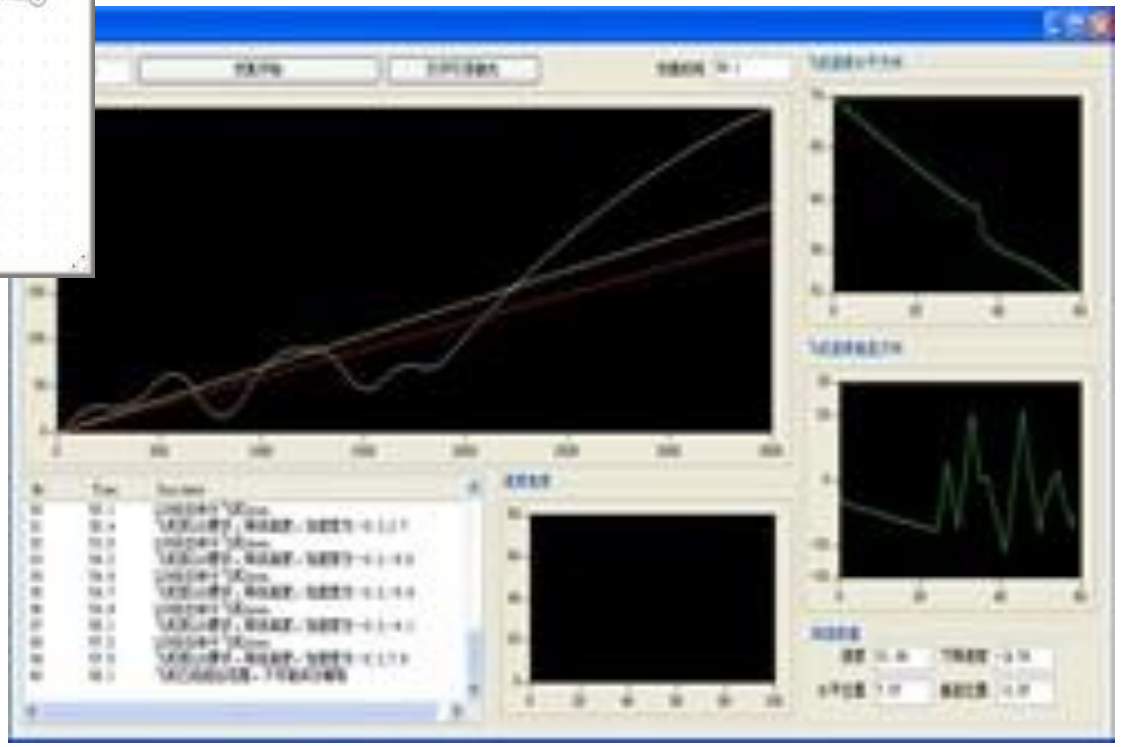
Safety design and analysis



The accident inference and prediction

FTA;FHA;ETA;

PSA……



Safety simulation of the aircraft approach process

RSE in Total life cycle

Testability simulation

Function division

FMEA

CA

Data preparation

Models

simulation

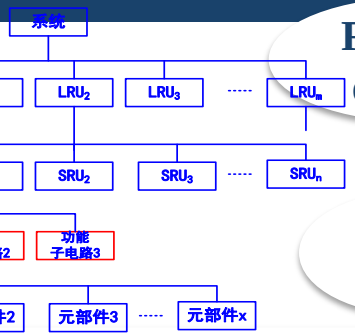
Testability

IETM etc.

Diagnosis tree

FDR/FIR

D-matrix



初始约定层次： 任务： 审核： 第 页·共 页
约定层次： 分析人员： 批准： 填表日期：

代码	产品或功能标志	功能	故障模式	故障原因	任务阶段与工作方式	故障影响			严酷度类别	故障检测方法	设计改进措施	
						局部影响	高一层次影响	最终影响				

$$C_r=\sum_{j=1}^{N}C_{mj}=\sum_{j=1}^{N}\alpha_j\cdot\beta_j\cdot\lambda_p\cdot t$$

- 结构信息
- 对外接口关系
- 内部信号流信息
- 故障流信息
- 测试信息
- 功能绑定信息

结构信息

XX系统
XX设备
XX板
XX单元
XX单元
XX单元
XX板
XX单元
XX单元
XX单元

内部信号流信息

编号	本单元的端口名称	信号传递方向（相对本单元）	连接单	
1	VCC	输入←	电源板	
2	GND	输入←	电源板	GND

故障流信息

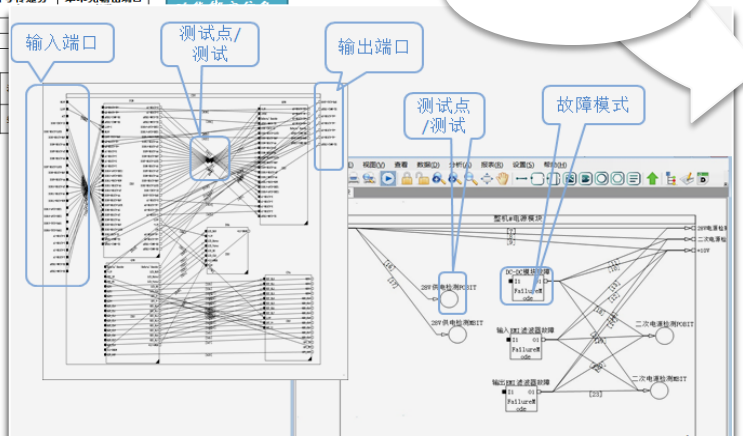
故障模式编号	故障模式名称	故障率（10⁻⁶/h）	流出的输出端口名称
XX-PM01	输出电压值异常	3.13	VCC

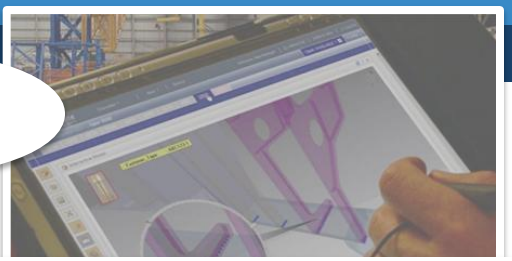
对外接口关系

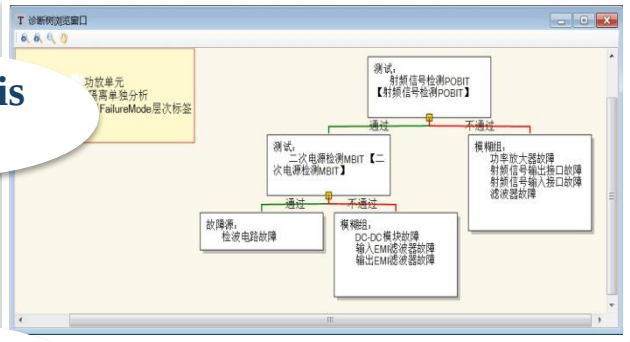
本单元的输入端口	信号传递方	本单元输出端口
A1in		
A2in		

测试信息

测试类别	测试编号
加电BIT	XX-POBIT01







$$FDR=\frac{\lambda_D}{\lambda}=\frac{\sum\lambda_{Di}}{\sum\lambda}\times100\%$$

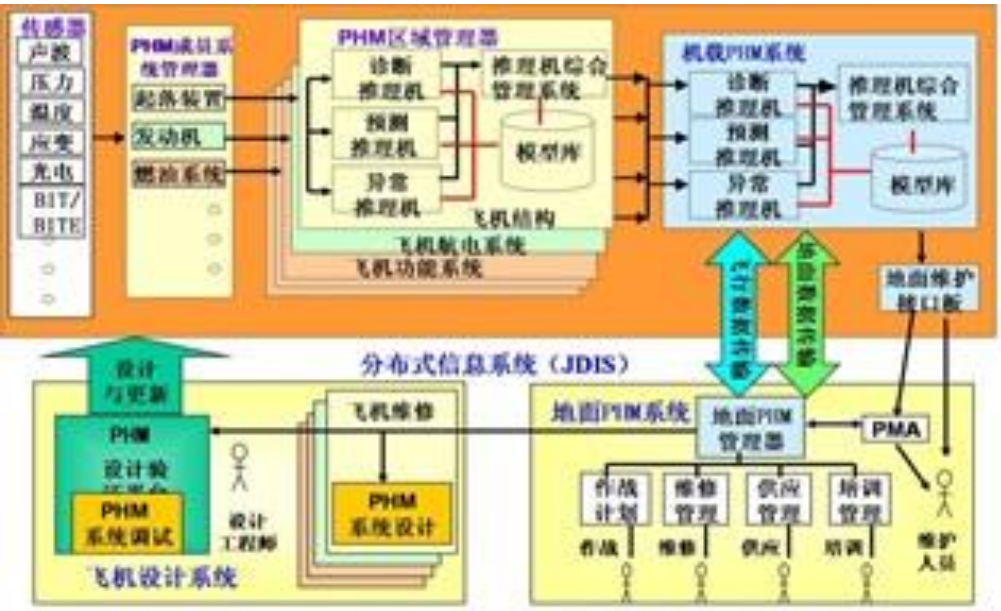
$$FIR=\frac{\lambda_L}{\lambda_D}=\frac{\sum\lambda_{Li}}{\sum\lambda_D}\times100\%$$

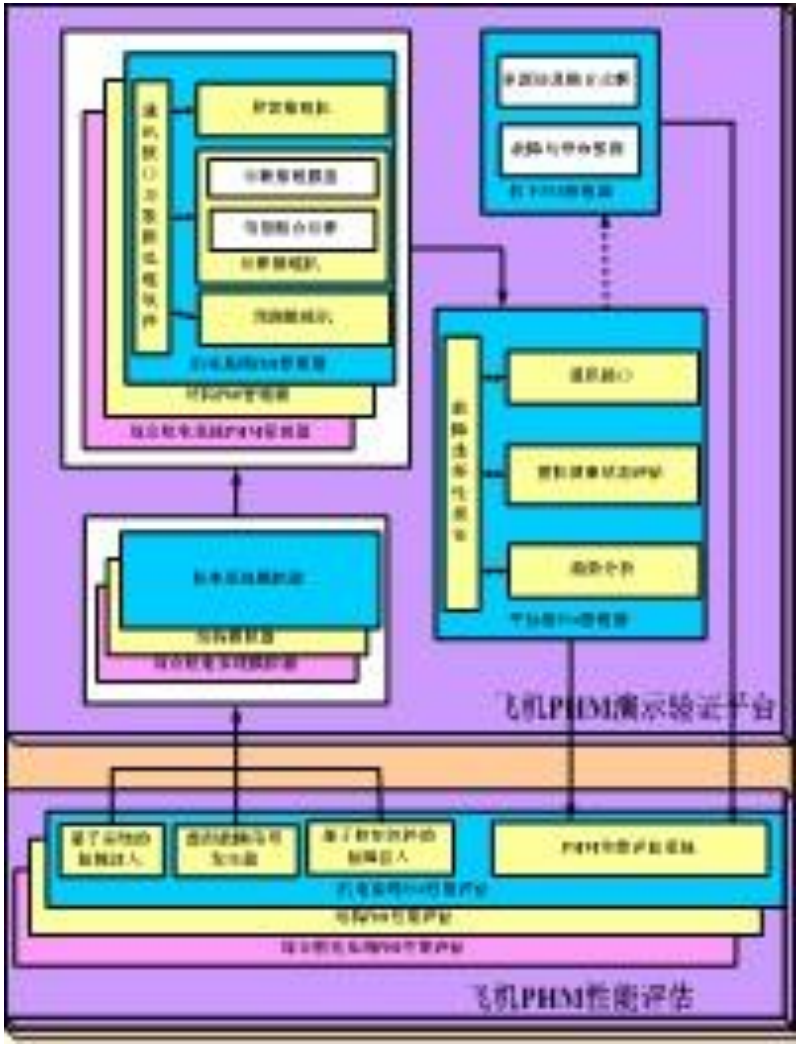
故障源数量：4 测试数量：4 (G:一般故障 F:功能故障)

全路径	MTBF	A系统 #启动控制器 #CPU模块 #CPU测试(A-CPU-POBIT01) #CPU测试(A-CPU-POBIT01)	A系统 #启动控制器 #CPU模块 #CPU测试(A-CPU-MBIT01) #CPU测试(A-CPU-MBIT01)	A系统 #启动控制器 #CPU模块 #看门狗功能测试(A-CPU-POBIT02) #看门狗功能测试(A-CPU-POBIT02)	A系统 #启动控制器 #CPU模块 #看门狗功能测试(A-CPU-PBIT01) #看门狗功能测试(A-CPU-PBIT01)
A系统#启动控...	1	0	0	0	0
A系统#启动控...	1	0	0	0	0
A系统#启动控...	0.1	1	1	0	0
A系统#启动控...	0.1	0	0	1	1

RSE in design phase

Prognostic and health management

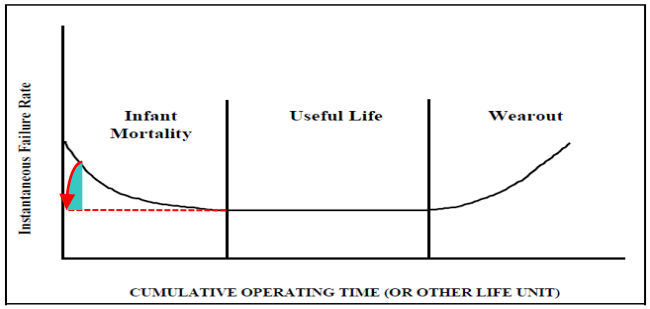


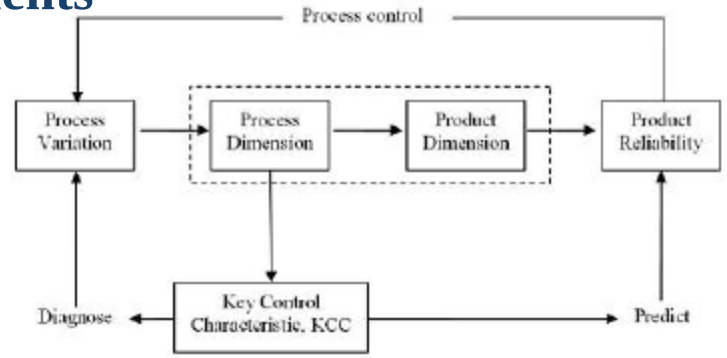


RSE in production phase

Process reliability

- **Process reliability is a method for identifying and controlling manufacturing defects, which have significant cost reduction opportunities for product infant reliability improvements**





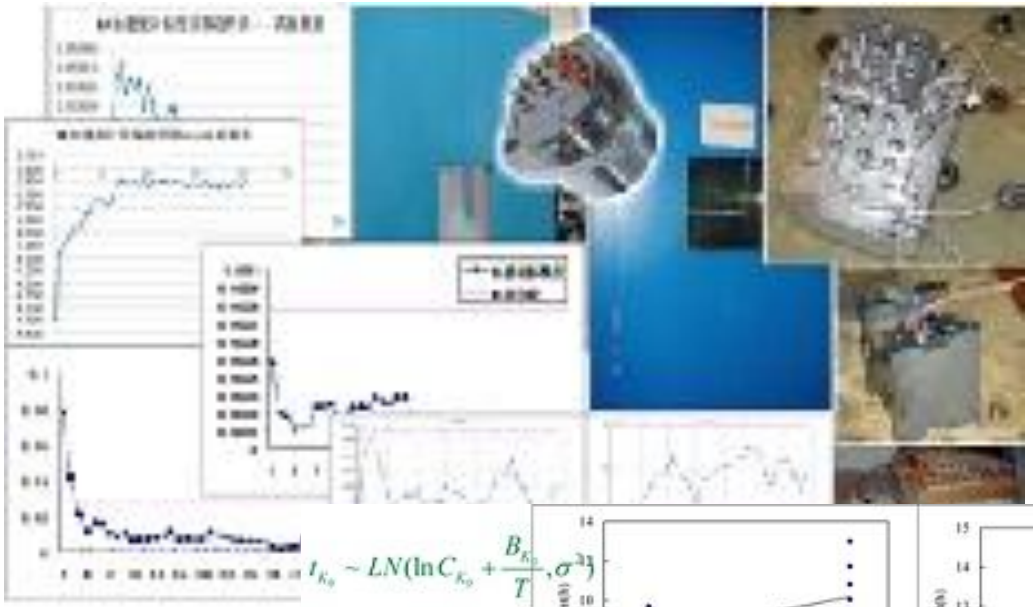
- Tools

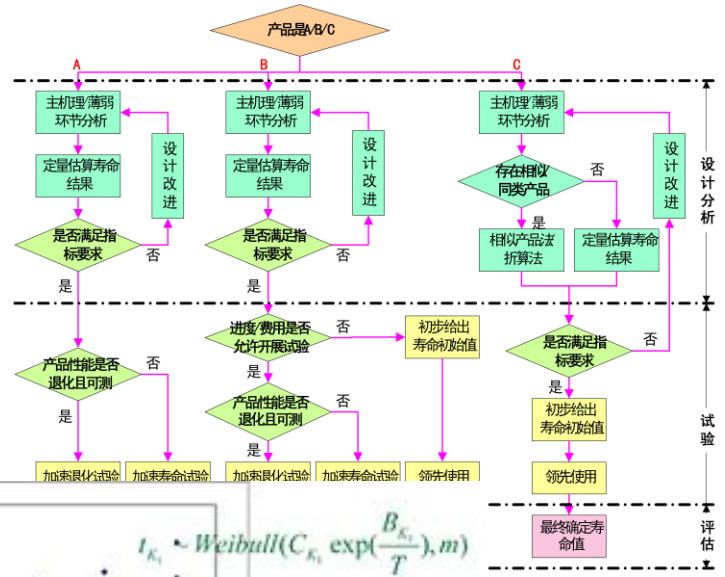
MIS of Process defects data

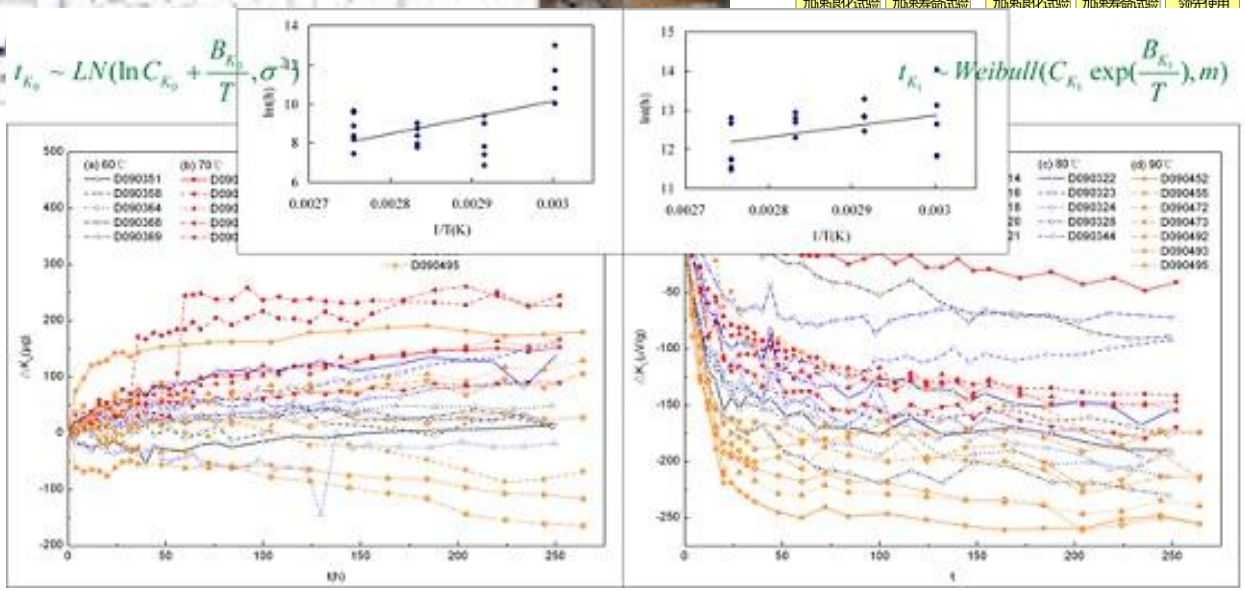
Analyzing tool of Process variation

RSE in verification phase

Environmental Reliability Qualification Testing

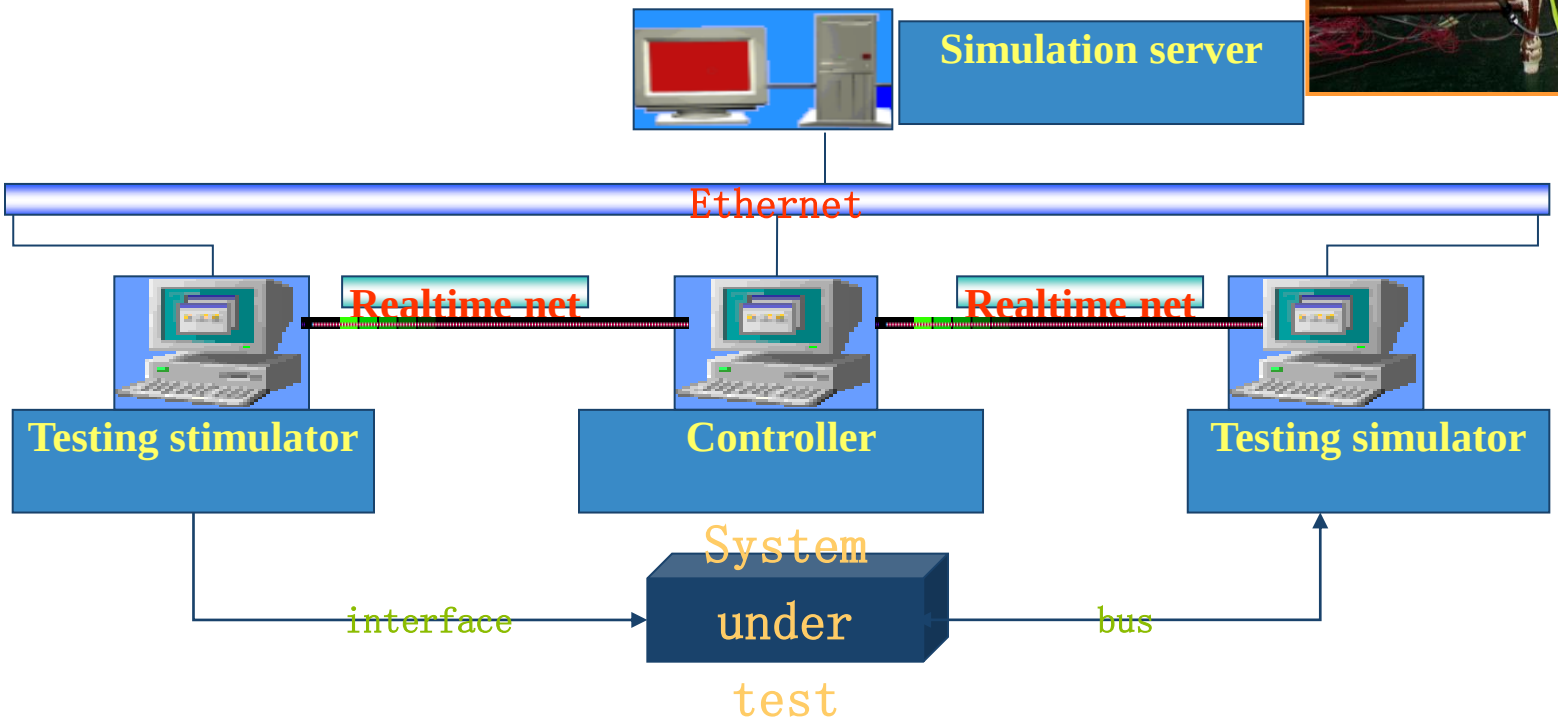






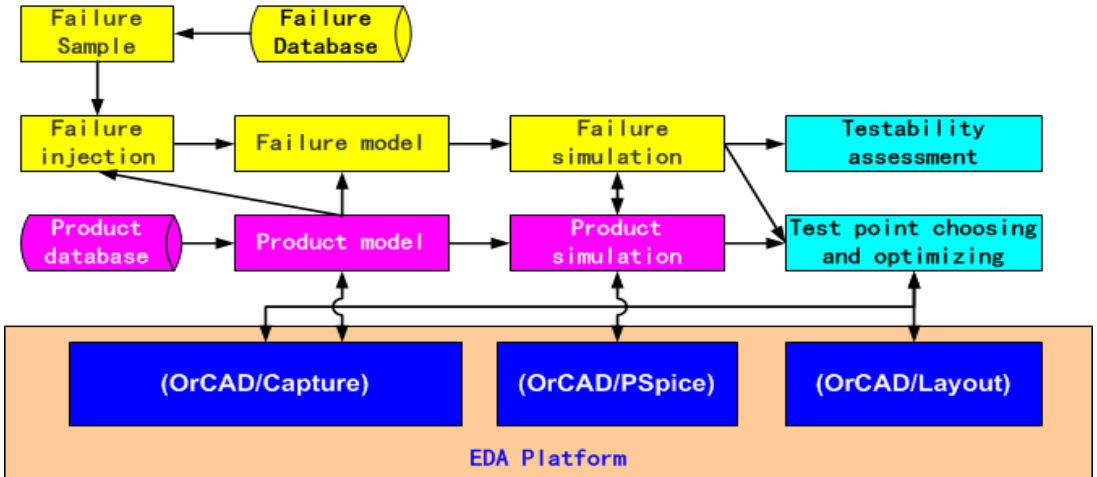
RSE in verification phase

Embedded software reliability simulation testing



RSE in verification phase

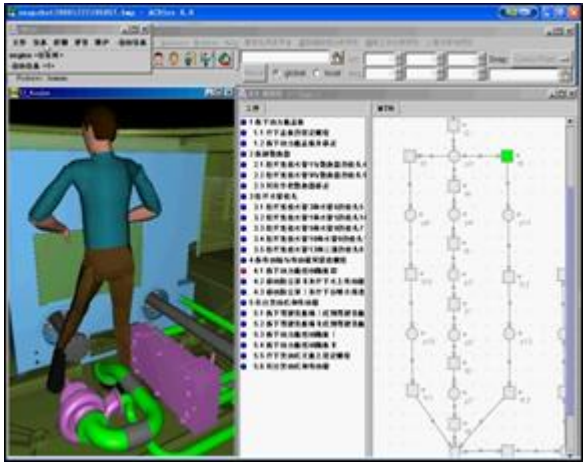
Simulation verification for testability (infield)

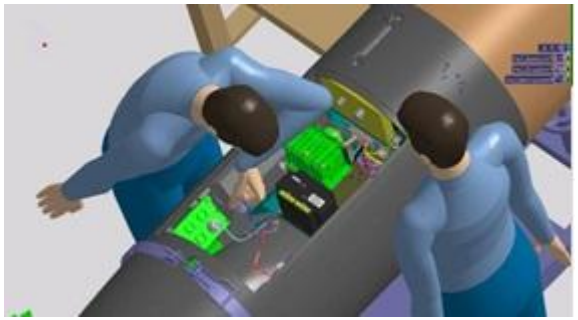


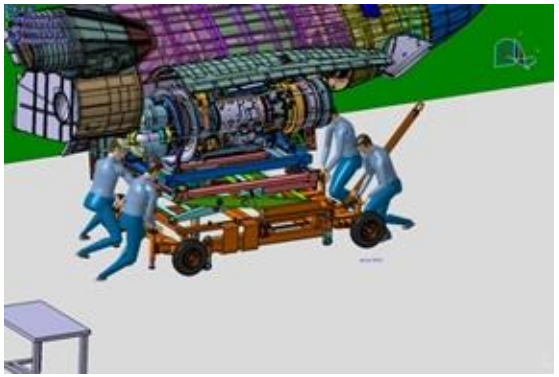
- **Failure injection**
  - Failure injection for bus
    - MIL-1553B
    - CAN
    - ARINC429
    - RS422、RS232
    - IO、TTL
  - Failure injection with probe
  - Software failure injection
    - DSP：CCS
    - ARM：Linux
    - FPGA：Xilinx ISE
    - SCM：Keil C
    - ……

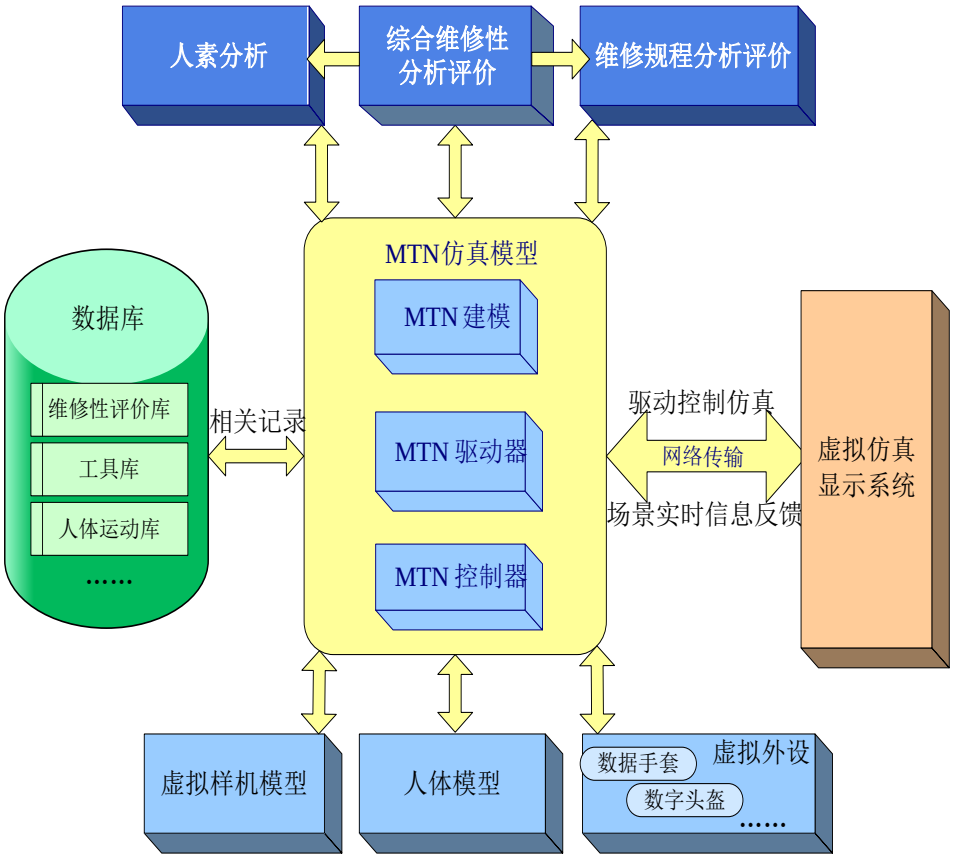
RSE in verification phase

Maintainability analysis and evaluation with virtual maintenance





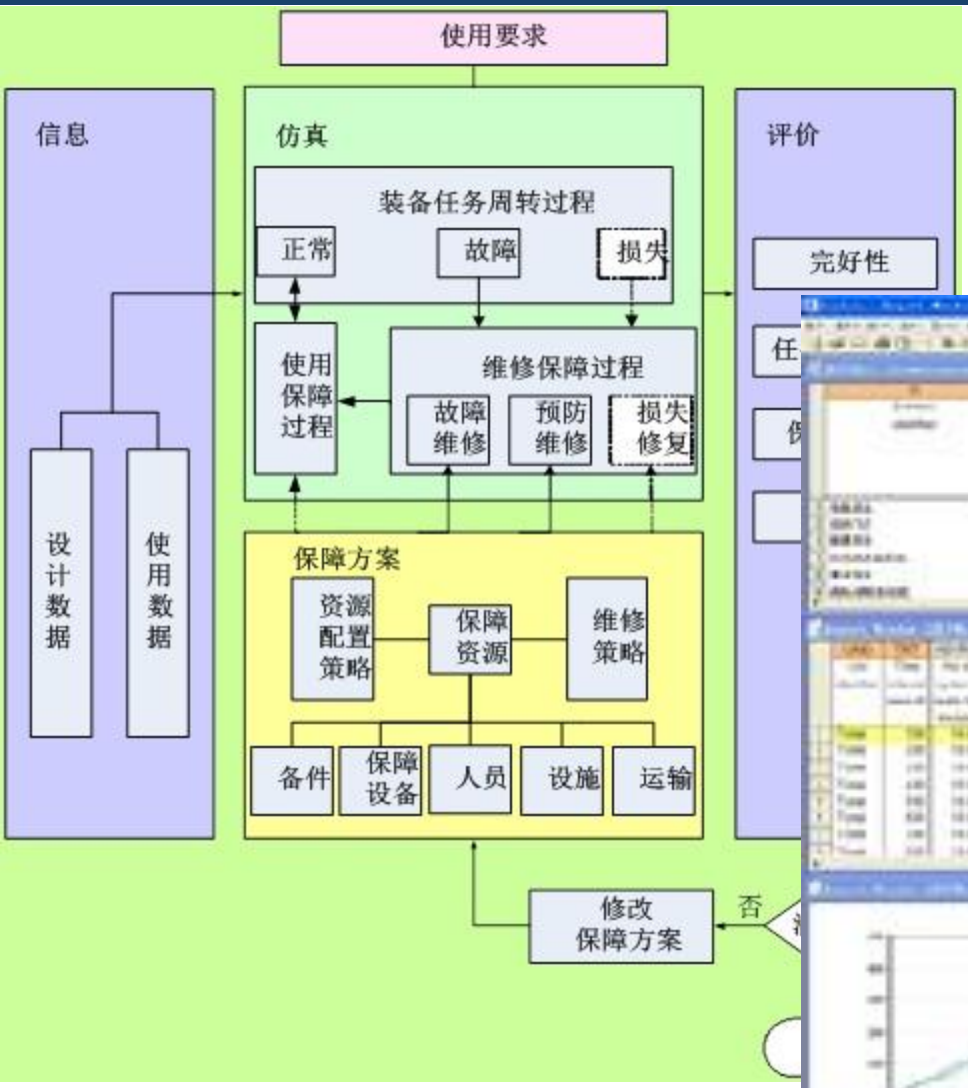


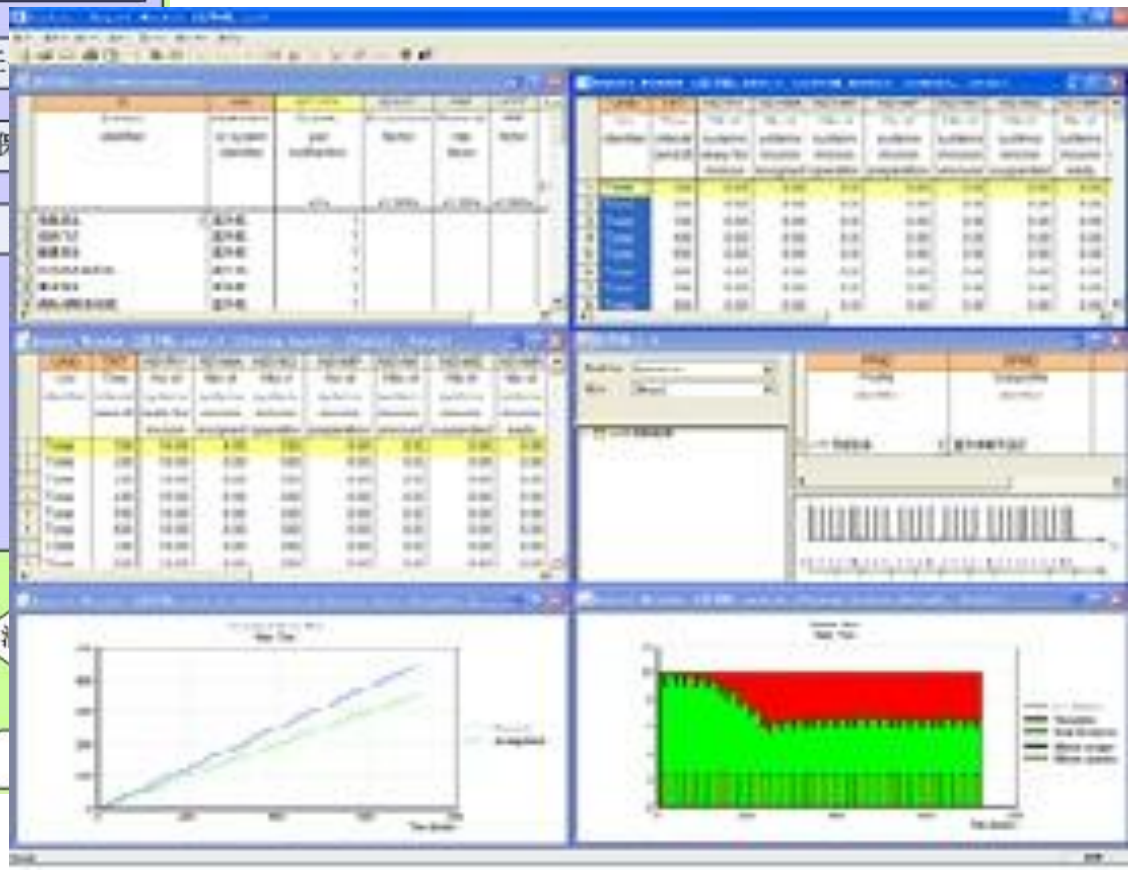


Virtual maintenance task analysis system

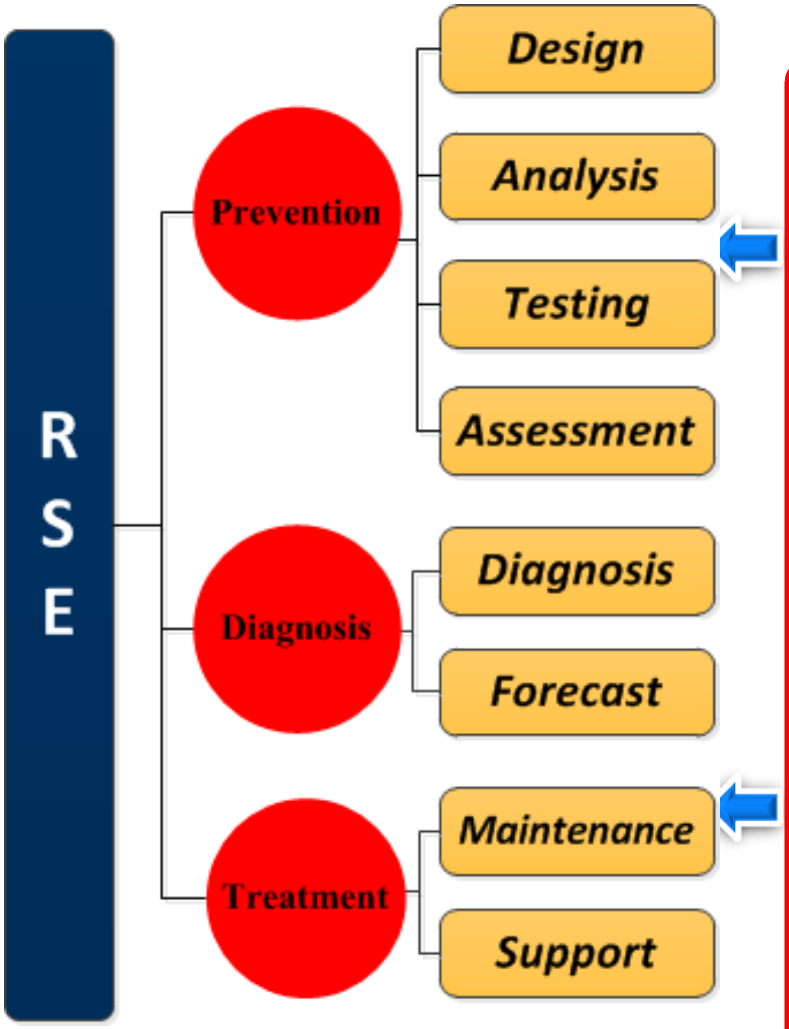
RSE in usage phase

Simulation for supportability





RSE in Full-Feature



Technical Advantage

- Electronic product reliability prediction based on POF
- Mechanical product reliability analysis
- FMECA
- Reliability Enhancement Testing
- reliability evaluation with Small sample
- Software reliability simulation testing for embedded software
- The system maintainability modeling
- maintainability analysis and evaluation based on the digital model
- Fault diagnosis ability evaluation for test configuration
- Testability modeling of On-off type polymorphism system
- Performance simulation model and evaluation for supportability
- Safety design criteria for space plane
- Safety constraint state space and accident derivation
- ….

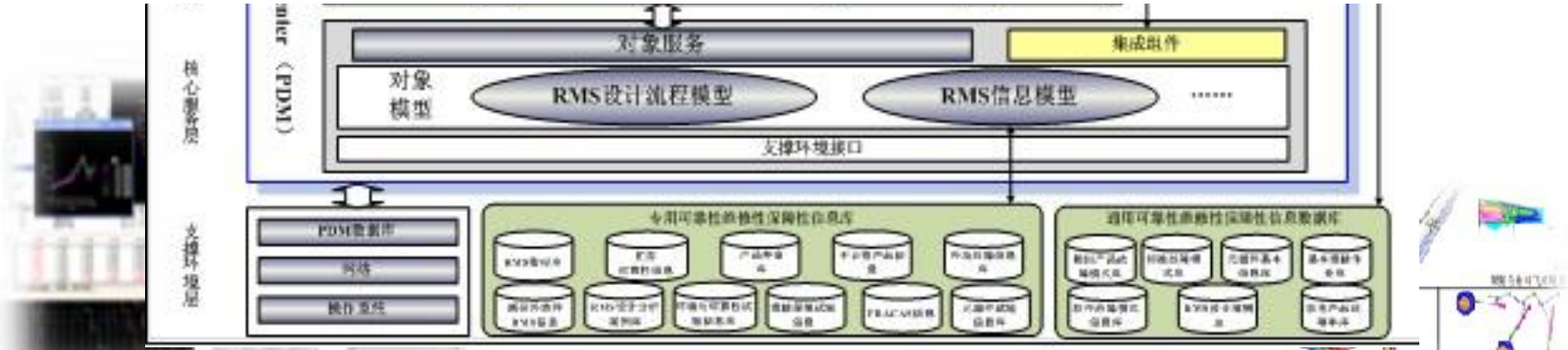
Example of RSE in Full-Feature

Integration technology of Reliability, safety, testability, supportability and maintainability

46 Tools. Supporting reliability, safety, maintainability, supportability, testability work

18 databases. More than 130 thousand reliability , safety, maintainability, supportability and testability data

Integrated with development process of products

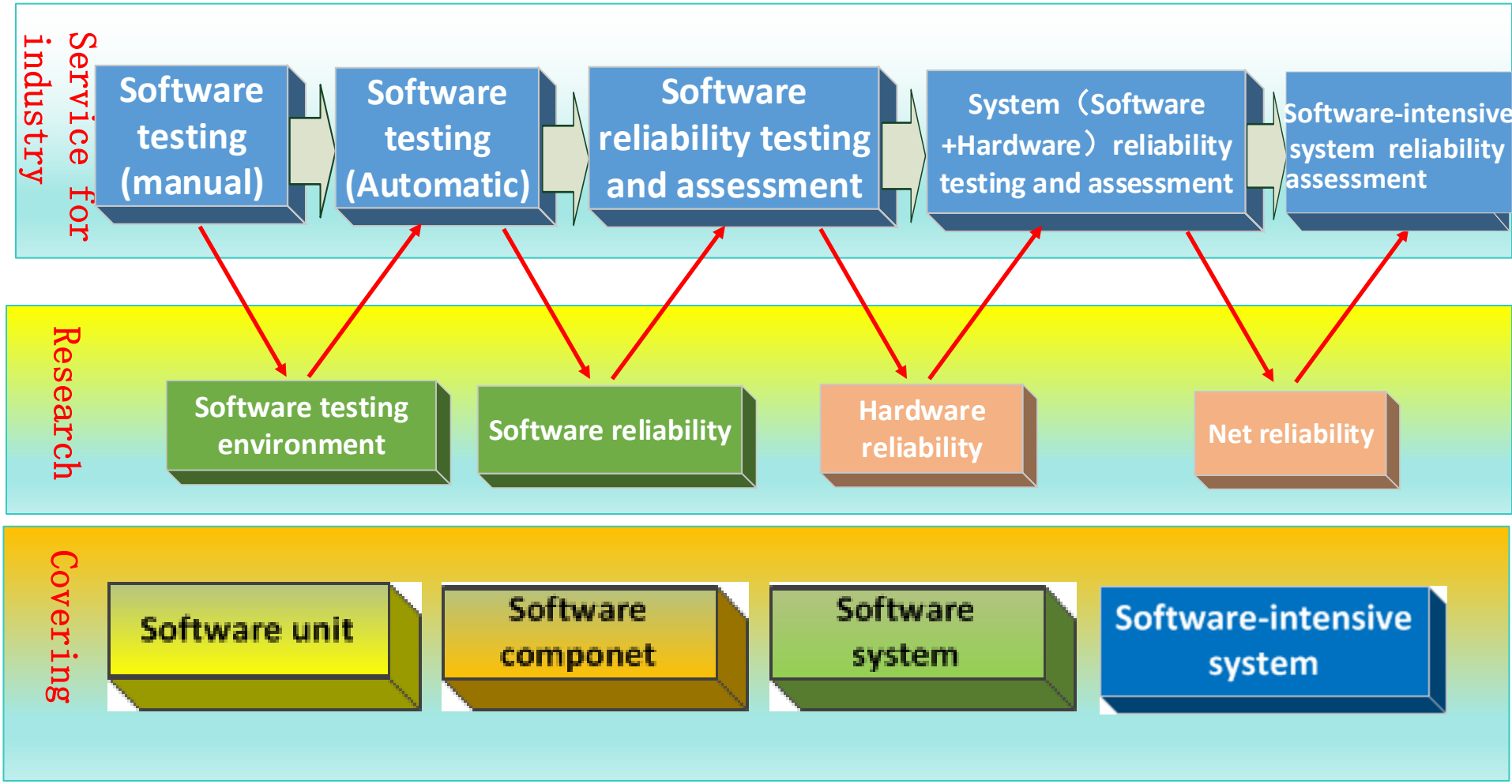


Software reliability work in 4-D Mode

System-wide

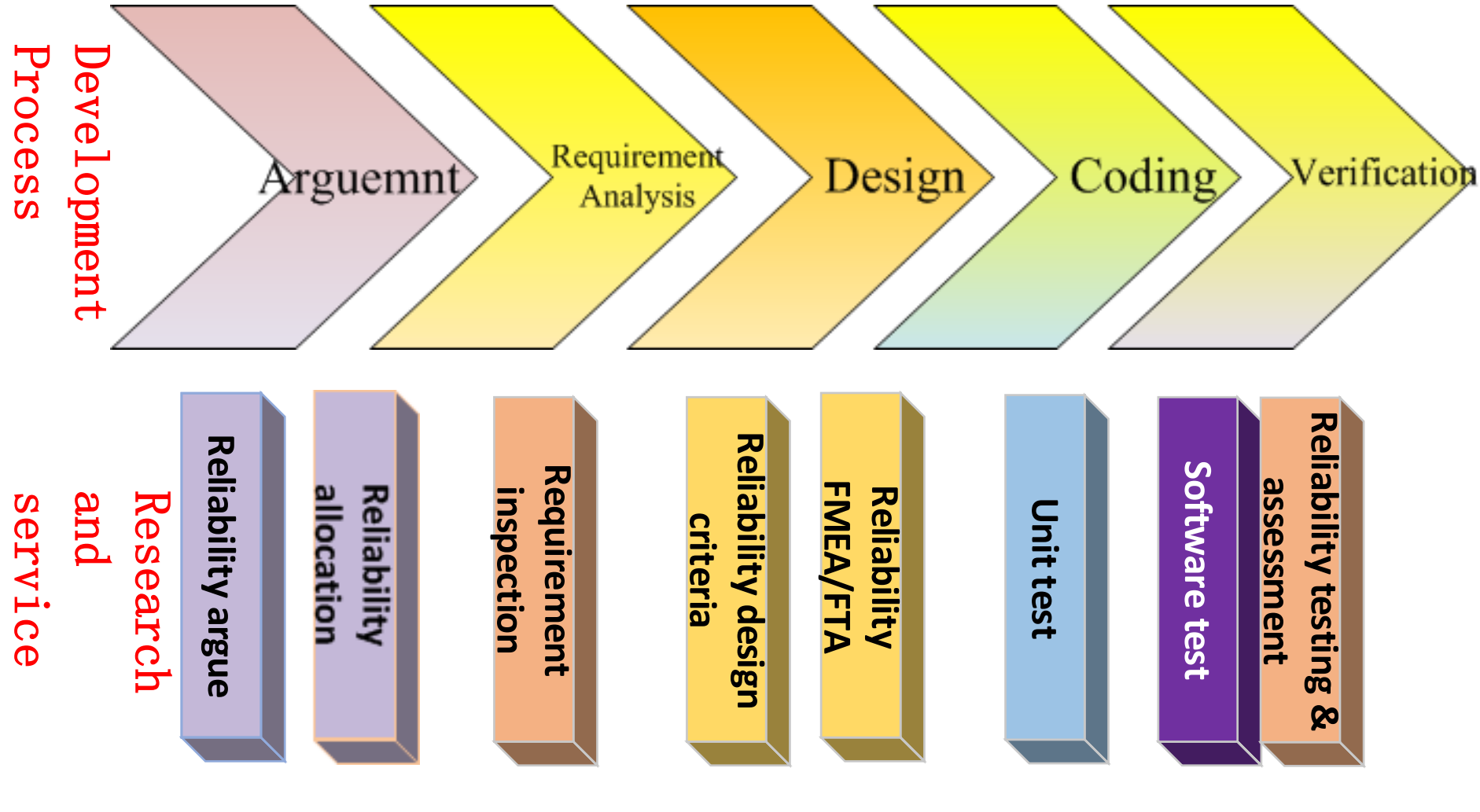
From software unit to software-intensive system

From qualitative to quantitative



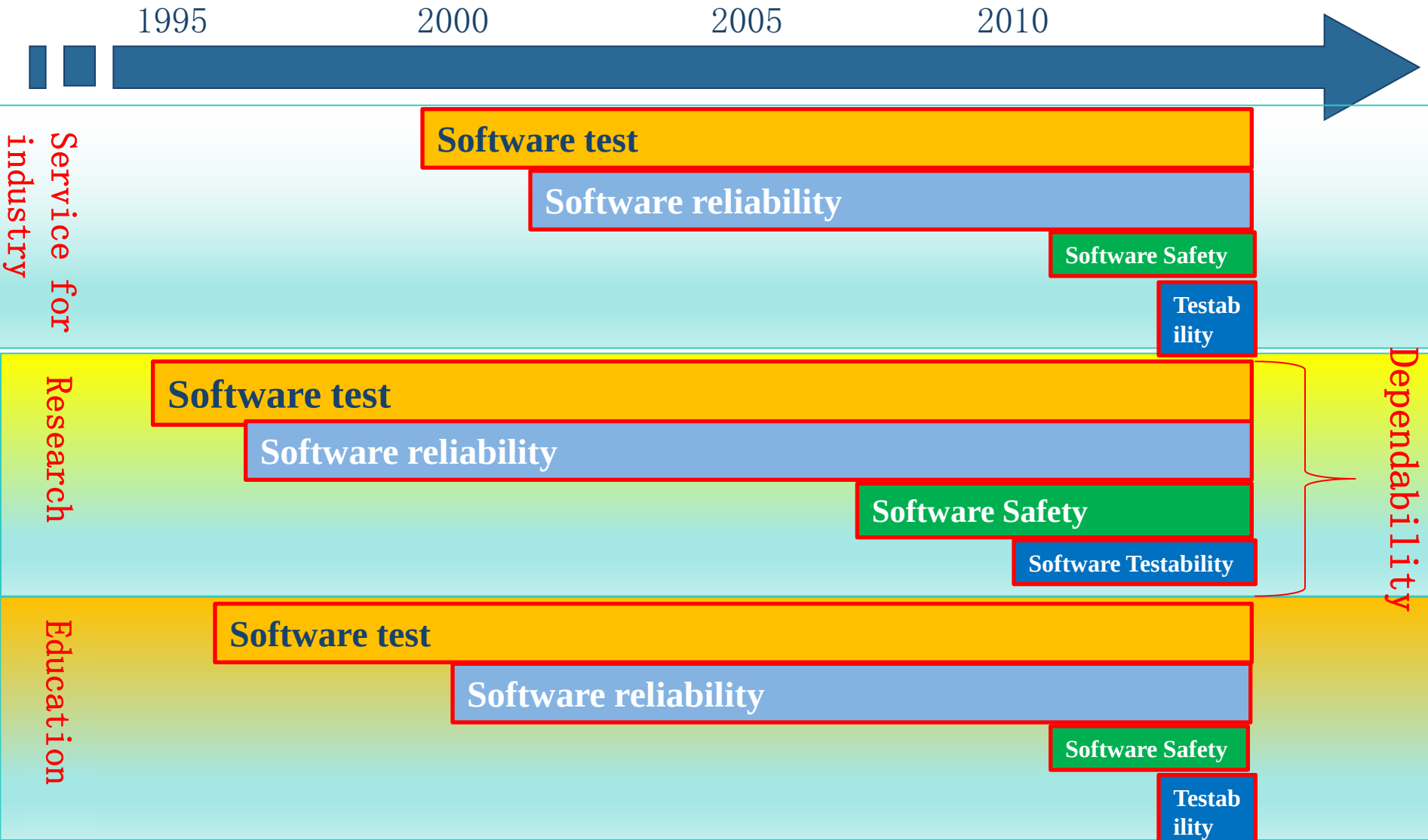
Total Life Cycle

From verification only to total life cycle support



Full feature

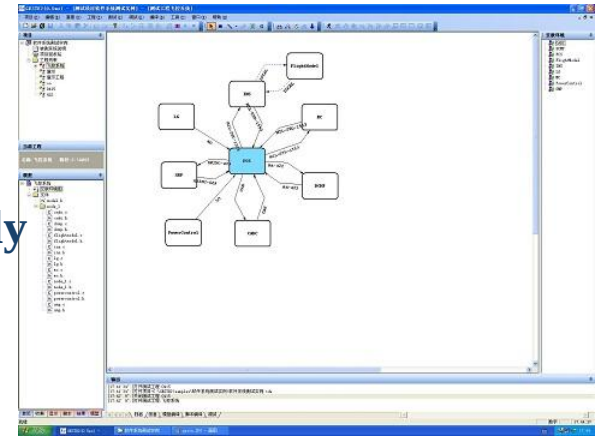
From software reliability to software dependability

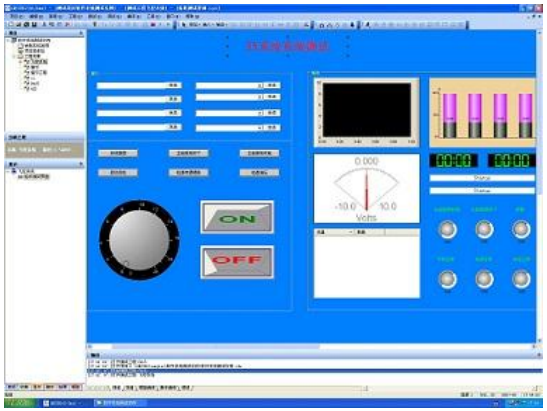


Some developed tools for software reliability

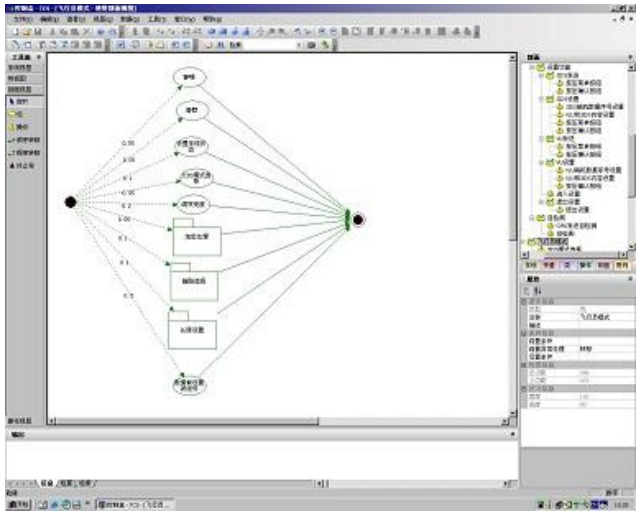
General Embedded Software Simulation Testing Environment

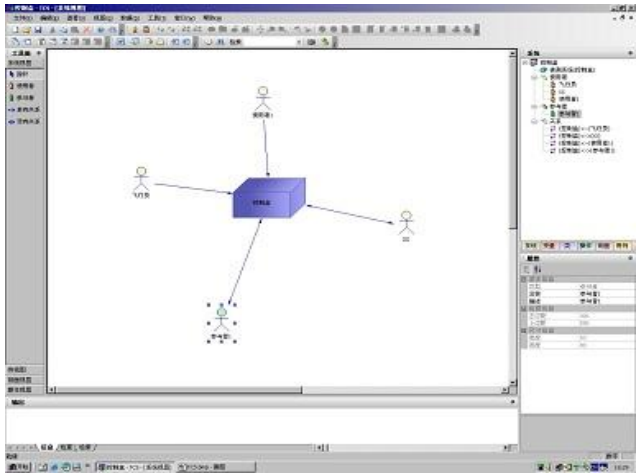
- Building testing environment for different embedded software quickly
- Generating simulation model code automatically
- Testing embedded software with GUI
- Simulation time cycle= 1 ms





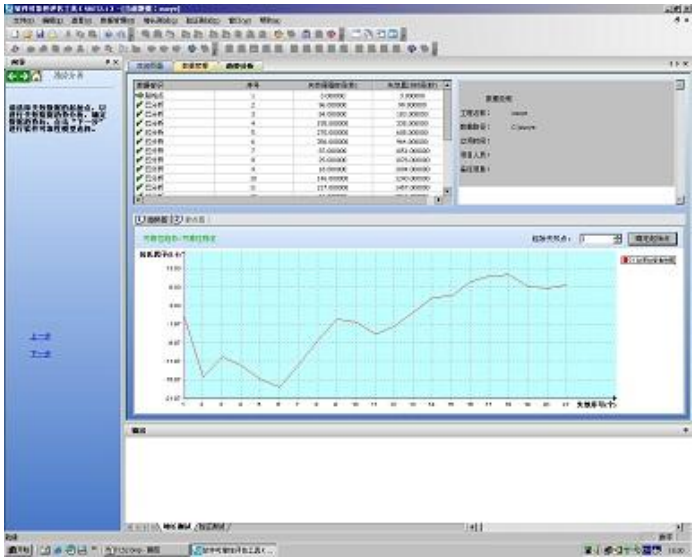
Software reliability testing profile building and test case generation tool (TCS)

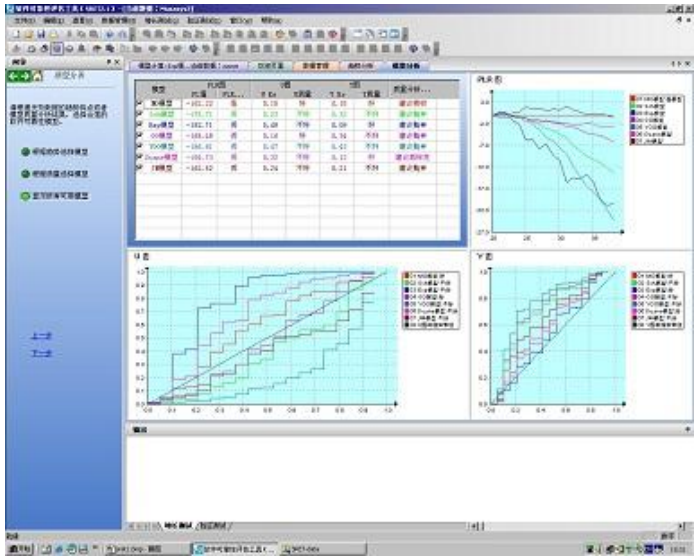




- Building software reliability testing profile with drawing
- Complex input restrictions modeling support
- Analyzing input variables with GUI
- Checking restriction relationships automatically
- Generating test cases automatically
- Generating testing reports automatically

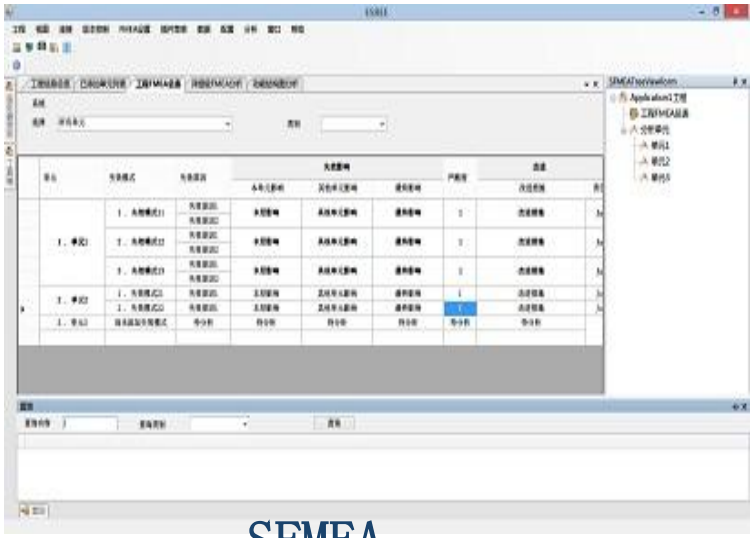
Software reliability evaluation tool



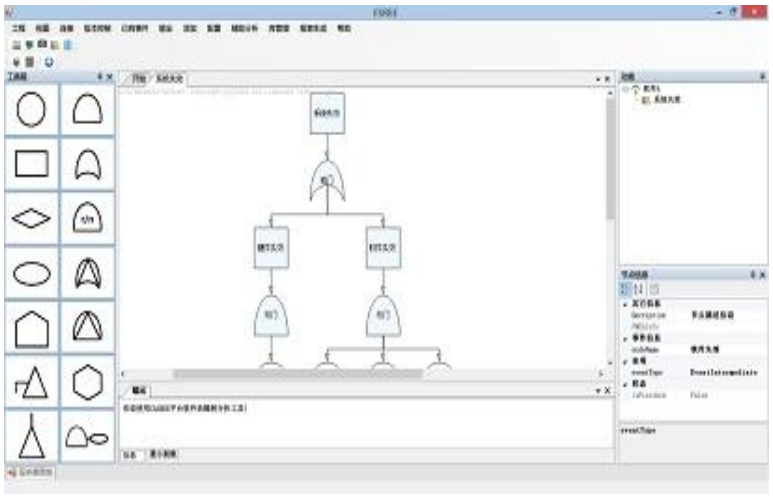


- Managing failure data
- Analyzing reliability tendency automatically
- Evaluating the quality of software reliability models
- Choosing the best software reliability model
- Software reliability calculator
- Generating software reliability evaluation reports

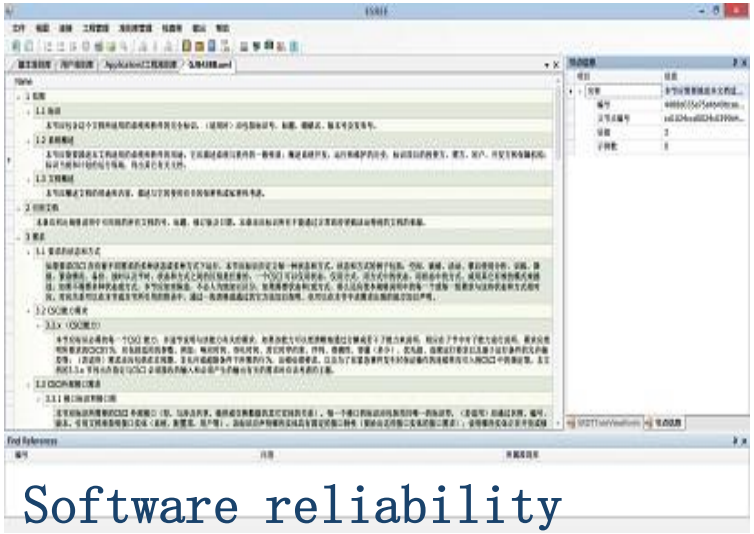
Other software reliability tools



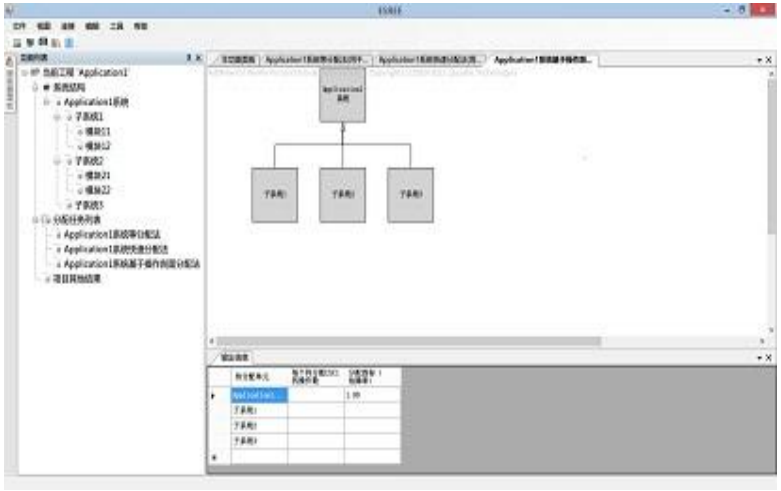
SFMEA



SFTA



Software reliability design criterion tool



Software reliability distribution tool

Some software reliability research in progress

Software Dependability

- Complex software failure mechanism and failure propagation law
- Software dependability modeling and analysis
- Software prognostic and health management
- Accelerated software dependability demonstration
- Software dependability evaluation for small sample
- …

Net reliability

- Net failure mechanism and failure propagation law
- Net failure models
- Arithmetic and theory for net performance reliability
- Net reliability accelerated testing
- …

Reliability and safety for software-intensive system

- Software-intensive system safety control and evaluation
- Software-intensive system failure mechanism
- Software-intensive system reliability simulation
- Software-intensive system reliability comprehensive evaluation and demonstration
- …

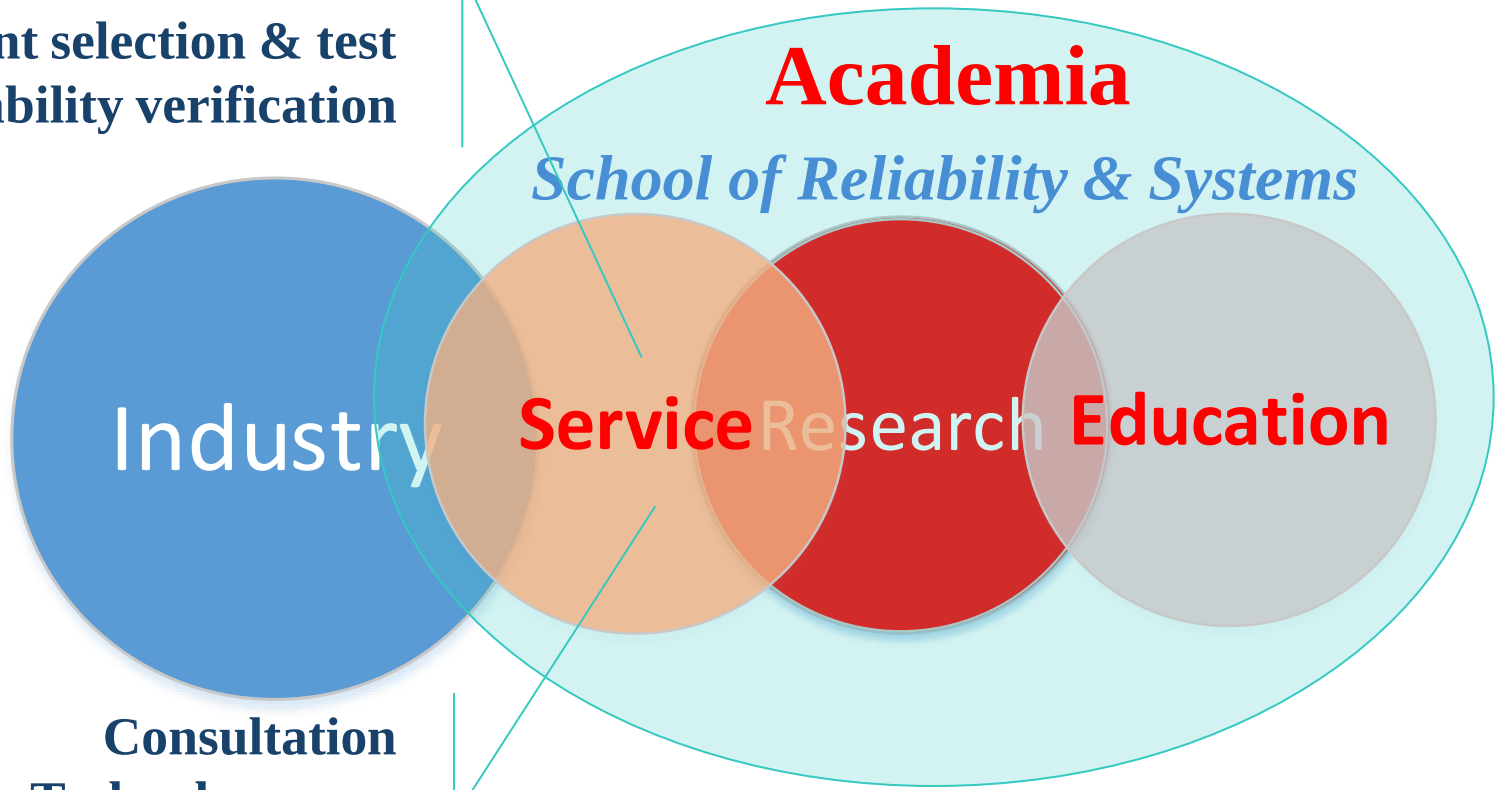
Communication and cooperation with industry

How?

- Joining industry activity directly
- Adaptable organization structure
- Academic exchange platform
- Demonstration case for new technology application
- Tools and platform support
- RSE capability

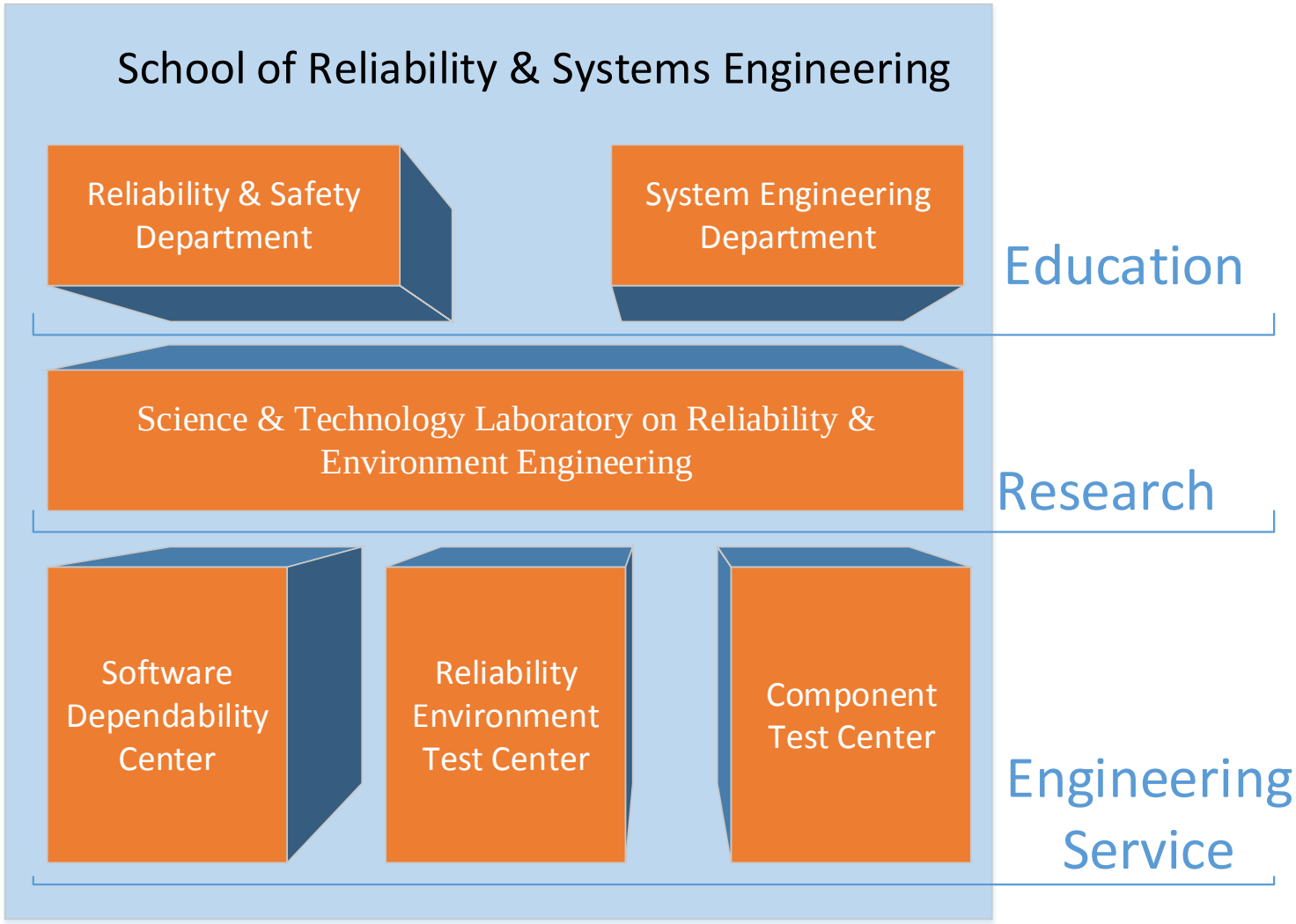
Joining industry activity directly

Reliability test
Software test
Component selection & test
Testability verification



Consultation
Technology case
Tools & Platform
Top reliability plan
Training

Adaptable organization structure

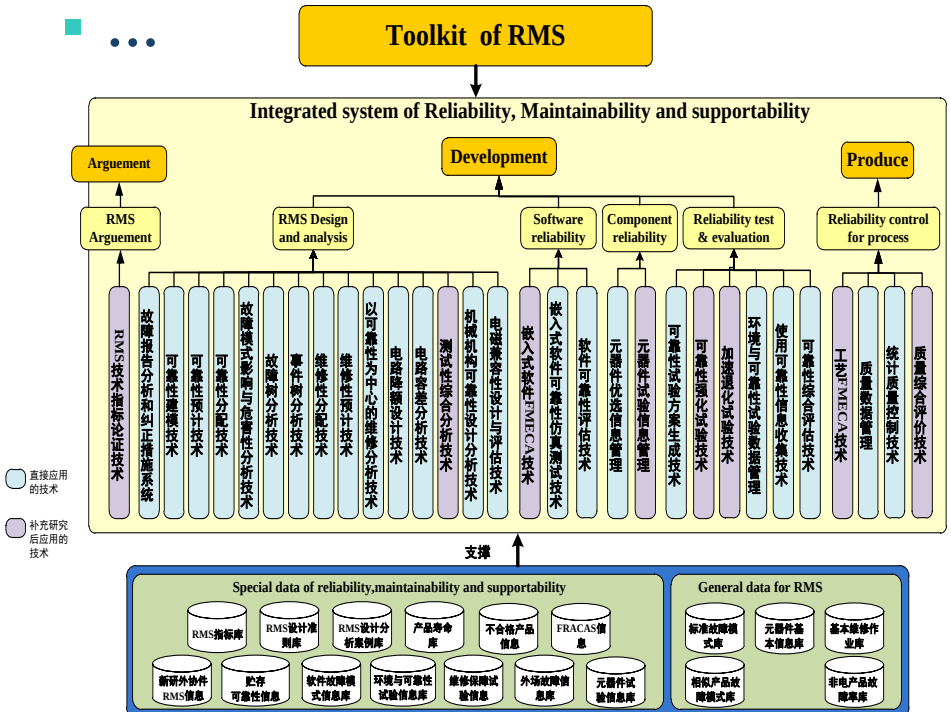


Academic exchange platform affiliated with our school

- **Academic exchange platform**
  - **Reliability Engineering Committee of China Society of Aeronautics and Aeronautics**
  - **International Conference on Reliability Maintainability & Safety**
  - **International education forum of reliability and system engineering**
  - **Reliability academic annual meeting of CSAA**
  - **…**

Tools and platform support

- **Transforming the research results to new tools and platforms and apply them in industry**
  - Software reliability simulation testing and assessment platform
  - Reliability and performance integration design platform
  - RMS Integration platform
  - General embedded software simulation testing environment
  - …



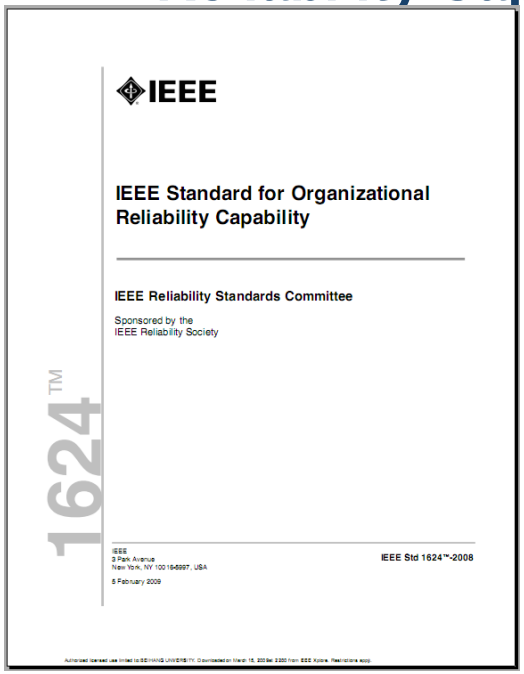
Demonstration case for new technology application

Demonstration case for new technology application

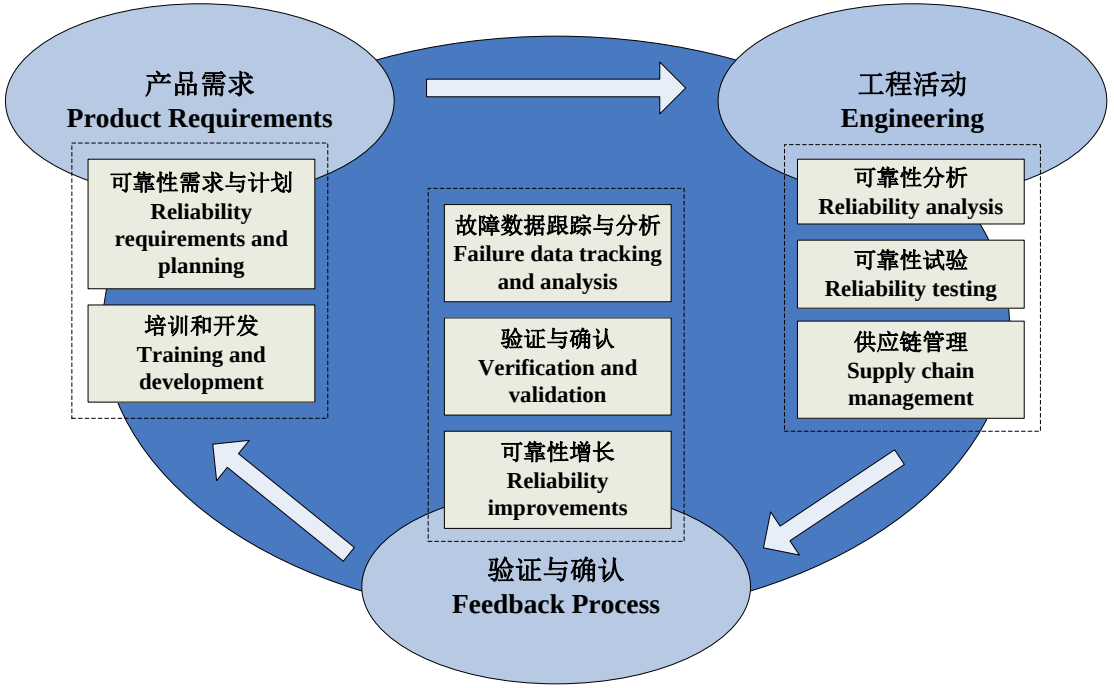
- Taking part in the development of a product, and apply the new technique in a full process.
- Analyzing the process data and write a detailed application guideline
- Guiding some in the industry to apply the new technique step by step
- Typical demonstration cases
- …

RSE capability maturity model Integration

- **Organization Reliability Capability (ORC)& Capability Maturity Model Integration（CMMI）**
  - **IEEE Std 1624-2008: IEEE Standard for Organizational Reliability Capability.**

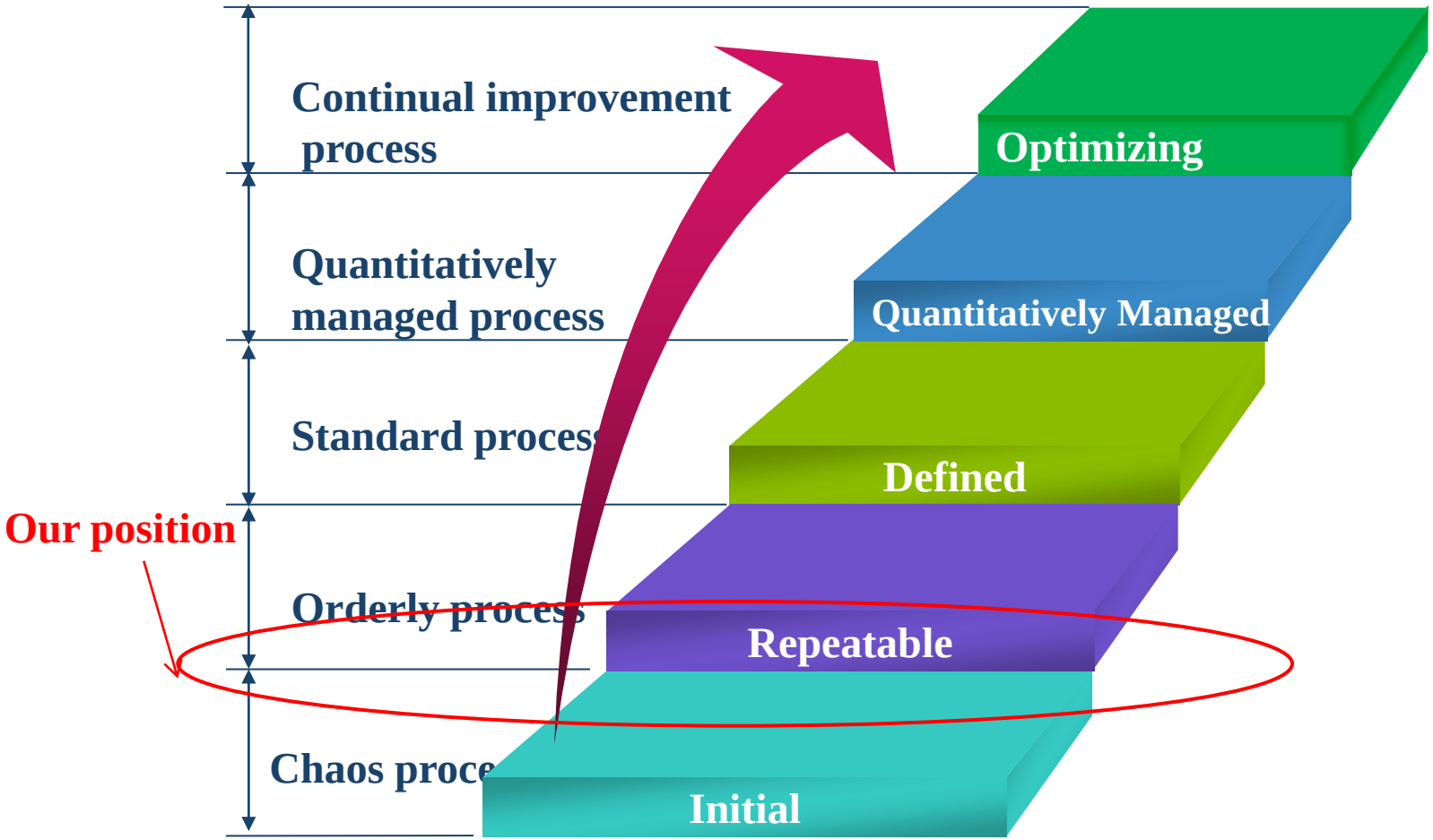


IEEE Std 1624-2008



Key practice for ORCMMI

RSE capability maturity model Integration (RSECMMI)



Thinking and suggestion

Comparing with the 4-D development mode of RSE in China, which emphasizes integrating and optimizing the full-features, and aims at the high efficiency, low cost, and healthy pregnancy and scientific nurture like human being, the process is similar to the software, which focuses on dependability, including reliability, safety, security, testability and supportability too.

RSE → Systematization, Relationship, Coordination, and Optimization → **Software Dependability**

From personality to whole
From quantitative change to qualitative change
From independence to fusion
From synchronization to optimization.

Thank you !

Q & A