ICAO

中国民用航空局
空中交通管理局
Air Traffic Management Bureau. CAAC

LIFE CYCLE MANAGEMENT OF ATM AUTOMATION SYSTEM

Presented by China

CONTENTS

01 System lifecycle is assessed solely based on operational time

When the system is decommissioned, some equipment may still perform well and remain usable, whereas other components might have been discontinued shortly after deployment.

The software should be continuously optimized, upgraded, and adjusted throughout the system's lifecycle. system software from the same vendor will undergo a stepwise, spiral evolution of continuous enhancement. Most features iteratively improve by building upon previous designs rather than being refactored from scratch.

(*According to the Regulations on the Use and Management of CNS Equipment in Civil Aviation ATC Systems, automation system hardware can be upgraded every six to eight years based on market conditions and spare parts availability.*)

02 Identical maintenance strategies applied indiscriminately throughout the operational lifecycle phases

Customized Maintenance Strategy

Differentiated maintenance programs based on performance characteristics and technical features in periodic maintenance and planed inspections.

03 Excessive maintenance

Sheer volume of system components, leading to unnecessary procedures while critical tasks remain unaddressed

scientific management methodologies, safety, reliability, sustainability, technological advancement, and operational efficiency.

CONTENTS

02. Life Cycle of ATM Automation System

Planning

- Performing requirements analysis and planning
- Developing technical specifications
- Conducting supplier selection
- Establishing budget and timeline
- Defining system retirement objectives

Development

Customizing/developing hardware components

- Developing and testing application software
- Conducting system integration and joint debugging
- Configuring device firmware
- Developing system interfaces

Validation

- Executing Factory Acceptance Testing (FAT)
- Performing Site Acceptance Testing (SAT)
- Obtaining safety certification
- Ensuring regulatory compliance

Deployment

- Executing on-site installation and integration
- Migrating data and configuring systems
- Conducting personnel training
- Implementing parallel operation
- Performing final operational cutover

Operations

- Implementing 24/7 real-time monitoring
- Executing preventive maintenance programs
- Managing change control processes
- Maintaining Configuration Management Database (CMDB)
- Performing vulnerability management

Decommissioing

- Developing decommissioning plans
- Archiving and migrating historical data
- Destroying sensitive data using certified methods
- Implementing environmentally compliant equipment disposal
- Decommissioning assets in financial systems

。

02. Life Cycle of ATM Automation System

Life Cycle Management of Automation System

Pre-Operational phase

Construction Preparation Phase

- **Planning**
- Development
- V&V
- Implementation

Service Phase

Hardware Management

- Early Failure Period — 1-3 years post-commissioning
- Random Failure Period — 4-8 years post-commissioning
- Wear-out Failure Period — 9-12 years post-commissioning

Software Management

Early Failure Period

Software Service Phase:

- operational environment
- operational requirement
- parameter adjustment
- maintenance operations

- Perfective Maintenance
- Adaptive Maintenance
- Corrective Maintenance

Final Phase

- Continuous Monitoring Failure Node Prediction
- Adequate Spare Parts Inventory Advance Maintenance
- Condition-Based Updates, Retrofits, and Rebuilds
- Decommissioning

Equipment malfunction or degraded technical performance may lead to automation system service interruptions， reliability reduction, and significant safety risk escalation

01 Background

01

Reliability-Centered Maintenance (RCM) is a maintenance strategy that determines the necessary maintenance **content**, **type, interval, and level** through logical decision-making, with the goal of optimizing maintenance activities.

02

This study introduces lifecycle management of ATM automation system. By applying RCM theory, it quantitatively analyzes the operational status of system hardware and software during service, develops logical decisions and maintenance outlines, optimizes the O&M strategy, reduces maintenance workload by 40%–70%, and extends service life by 40%.

ICAO Annex 10： **"Operational status requires continuous availability monitoring"**

CONTENTS

3.1 Life Cycle Management of ATM Automation System — Pre-operational Phase

The preparatory stage of ATM automation system construction

—— Determine the inherent reliability level of the system

Planning & Definition

Conduct thorough planning and preparation
Propose comprehensive, rational, and clear functional **requirements**
Minimize defects and vulnerabilities

Development & Integration

Technical standards should be strictly enforced to ensure rigorous system architecture design, reasonable resource allocation.
Ensure system performance complies with operational requirements

Verification & Validation

Deployment & Implementation

fully participate in equipment installation and debugging
Promptly identify and resolve issues
Scientifically sound implementation plan
Transition

3.2 Life Cycle Management of ATM Automation System — Service Phase

The service phase refers to the phase from the commissioning and operational use of the automation system to its gradual aging and eventual significant decline in reliability.

—— Apply RCM methodology to guide system operation and maintenance management

01 Hardware Service Phase Management

02 Software Service Phase Management

Key Metrics
Assess System Reliability

- **MTBF** – Mean Time Between Failures
- **λ** – Failure Rate
- **MTTR** – Mean Time To Repair

Quantitative reliability analysis for both hardware and software systems

MTBF: Higher values indicate **superior reliability**

λ: lower failure rate denotes **higher device reliability**

MTTR: Smaller values signify higher maintenance **efficiency and faster** recovery

3.2.1 Hardware Service Phase

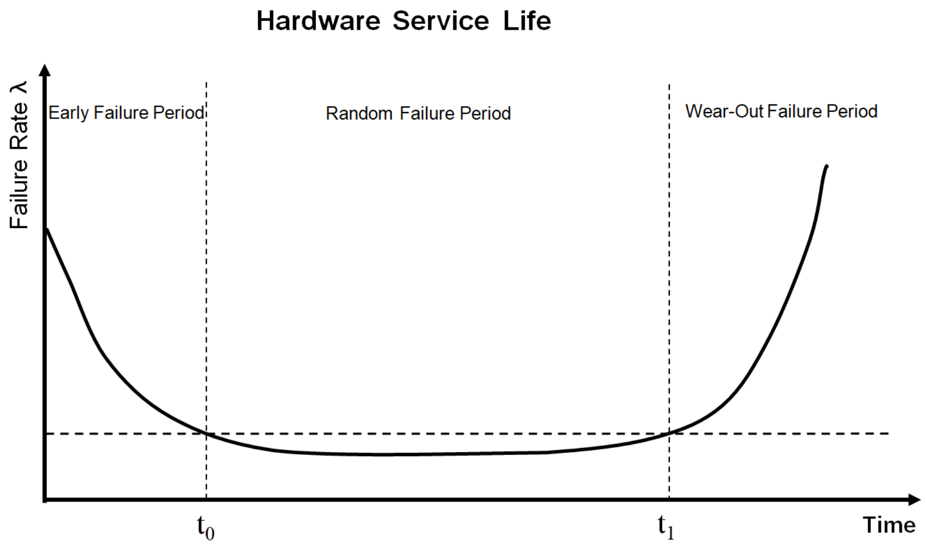


Fig. 2 Bathtub Curve of Hardware Failure Rate

Early Failure Period

- The stage following the official commissioning and operation of the automation system (1-3 years).
- The failure rate is generally high, primarily due to factors such as **system design flaws**, **poor assembly**, or **improper operation** by on-site personnel.

Random Failure Period

- After the system has adapted and stabilized following the early failure period (4-8 years).
- The system demonstrates consistent and reliable performance, exhibiting the lowest failure rates in its lifecycle.

Wear-out Failure Period

- The operational stage where prolonged service leads to **excessive component wear, fatigue, and rapid degradation** (9-12 years).
- The equipment gradually loses the performance level it had during initial stable operation, and the failure rate increases rapidly.

3.2.2 Implementation of RCM theroy in Hardware Service Phase

3.2.2.1 Historical Hardware Failure Data Analysis

The failure data and annualized failure rates of 156 workstations in an ATM automation system from 2013 to 2024 are presented in Table 1.

Based on the fitted failure rate data, the resulting failure rate curve aligns with the characteristics of the bathtub curve.

Equipment Service Year(s)	2013	2014	2015	2016	2017	2018
Total Failures (unit-events/year)	27	13	6	4	3	3
MTBF(h)	50613	105120	227760	341640	455520	455520
Annualized Failure Rate λ (%)	0.0020	0.0009	0.0004	0.0003	0.0002	0.0002
Equipment Service Year(s)	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**
Total Failures (unit-events/year)	3	7	16	23	31	41
MTBF(h)	455520	195222	85410	59415	44082	33330
Annualized Failure Rate λ (%)	0.0002	0.0005	0.0011	0.0016	0.0022	0.0030

Tab. 1 Failure Statistics of Workstations in an Automation System

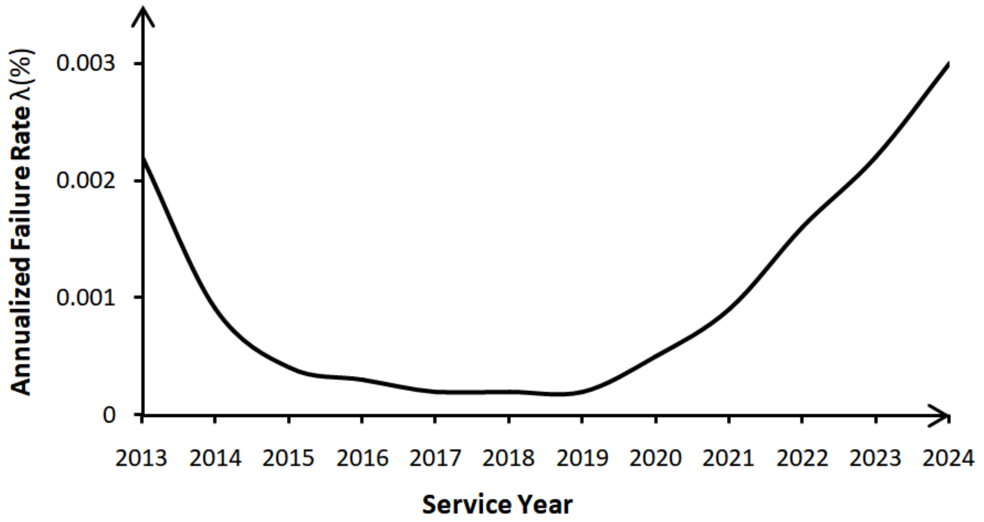


Fig. 3 Failure Rate Curve for Workstations in the Automation System

- From the 8th year of service, the failure rates increase rapidly.
- Combined with the bathtub curve analysis, this indicates that the workstation has transitioned from the random failure phase to the wear-out failure phase, and there is reason to expect that the failure rate will continue to rise in the future.

3.2.2 Implementation of RCM in Hardware Service Phase

3.2.2.2 Failure Consequence Classification and Maintenance Decision-Making

According to RCM theory, failure consequences are classified into four categories:
A1-Safety and Environmental Consequences,
A2-Hidden Failure Consequences,
A3-Operational Consequences,
A4-Non-operational Consequences.

Based on the severity of failure impacts, the corresponding Logic Decision Diagram is structured.

Based on this diagram and failure rates, the maintenance outline for workstation functional modules is developed as shown in Table 2.

<table>
<tr><th rowspan="2">Failed Module</th><th colspan="4">Logical Response (Y/N)</th><th rowspan="2">Maintenance Approach</th><th rowspan="2">Failure Description</th><th rowspan="2">Maintenance and Spare Parts Recommendations</th></tr>
<tr><th>A1</th><th>A2</th><th>A3</th><th>A4</th></tr>
<tr><td>CPU</td><td>N</td><td>Y</td><td>Y</td><td>N</td><td rowspan="3">Primary: Condition-Based Maintenance
Secondary: Corrective Maintenance</td><td rowspan="3">Low failure rate
Severe consequences
Periodic inspections</td><td rowspan="3">Memory expansion</td></tr>
<tr><td>Hard Disk</td><td>N</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>Memory</td><td>N</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>Network Interface Card</td><td>N</td><td>Y</td><td>Y</td><td>N</td><td rowspan="4">Primary: Corrective Maintenance
Secondary: Condition-Based Maintenance</td><td rowspan="3">Low failure rate
Minor impact
Difficult to detect proactively</td><td rowspan="3">Replace spare parts
Maintain minimum inventory</td></tr>
<tr><td>Graphics Card</td><td>N</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>Power Supply Unit</td><td>N</td><td>Y</td><td>Y</td><td>N</td></tr>
<tr><td>Cooling Fan</td><td>N</td><td>Y</td><td>N</td><td>Y</td><td>High failure rate
Minor impact
Difficult to detect proactively
Ensure cleanliness</td><td>Replace spare parts
Maintain sufficient inventory</td></tr>
</table>

Tab. 2 Workstation Maintenance Program

3.2.2 Implementation of RCM in Hardware Service Phase

3.2.2.3 Major concepts of RCM theory

Modular Maintenance: memory expansion, optimization of spare parts inventory, and improvement of the operating environment—**equipment reliability can be restored to the random failure period level**. Customized procedures.

Reliability Prioritization: The above analysis and maintenance results indicate that implementing a **precision maintenance strategy can extend the reliable operation** period during the random failure phase and defer the hardware upgrade window to after 10 years, thereby **effectively optimizing the lifespan**.

Data-Driven Decision-Making: The outcomes of RCM can also feed back into the lifecycle management, **optimizing maintenance strategy**. *By comparatively analyzing MTBF data of different models from the same brand and across brands under the same operating conditions, more suitable hardware can be identified for local operational needs.* This **provides valuable guidance for equipment selection** during the early system design and procurement phases.

3.2.2 Implementation of RCM in Hardware Service Phase

3.2.2.4 Insights – Flexible maintenance strategy

High-Failure-Rate Components

May undergo *preemptive replacement* in accordance with reliability thresholds

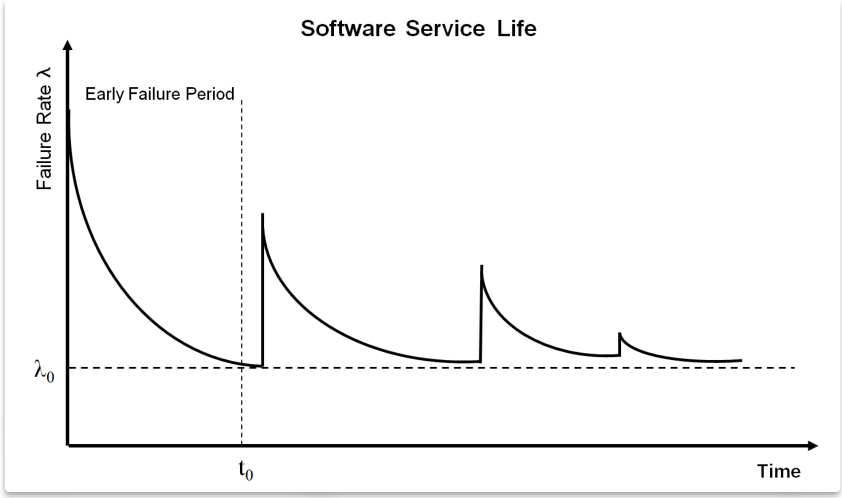
Performance-Degraded Hardware

Enable *targeted upgrades* for equipment experiencing capacity shortfalls due to prolonged operation or increased processing loads **(servers)**

Commercial Off-the-Shelf (COTS) Products

Optimize inventory buffers through *failure pattern analysis*, ensuring adequate sparing for fast-obsoleting items

3.2.3 Software Service Phase



Modified Bathtub Curve of Software Failure Rate

1

In the early stage of deployment, due to unclear initial requirements, design flaws, coding errors, insufficient testing, and incomplete configuration, software vulnerabilities tend to emerge in clusters, resulting in a peak failure rate.

2

As maintenance progresses and these vulnerabilities **are gradually resolved,** the failure rate decreases and remains low for a period.

3

Due to **changes** in the operating environment, evolving **air traffic control demands**, **parameter adjustments**, and maintenance personnel operations, **new vulnerabilities may be introduced**, bringing both direct and secondary risks to software operation. These vulnerabilities are typically hidden and difficult to detect, meaning failures tend to occur suddenly and without prior warning. This necessitates **a new round of maintenance** to address the issues.

4

The inflection point for increased failure rates is closely related to factors such as the frequency of requirement changes, the operational status of hardware and software, and the capabilities of maintenance personnel. It can be predicted using Mean Time Between Failures (MTBF).

3.2.4 Implementation of RCM in Software Service phase

3.2.4.2 Classification of Software Maintenance Activities and Maintenance Strategies

Software management data was collected from 2018 to 2024.

	2018	2019	2020	2021	2022	2023	2024
Technical Modifications	16	22	29	17	14	12	17
Software Patch Installation	0	3	5	2	3	0	4
New Software Deployment	0	3	3	2	1	1	1
Platform Reboot	2	4	7	6	4	0	2
Software Failure	4	11	12	8	6	5	4

Tab. 4 Maintenance Workload Statistics for Automation System Software

3.2.4 Implementation of RCM in Software Service phase

3.2.4.1 Historical Software Failure Data Analysis

Based on the severity of the consequences, the software failures has been classified into four levels:

Failure Level	Definition	Failure Statistics						
		2018	2019	2020	2021	2022	2023	2024
S1 Catastrophic Failure	Complete loss of core system functionality.	0	0	0	0	0	0	0
S2 Critical Failure	Severe degradation of a major operational function.	0	0	0	0	0	1	0
S3 Moderate Failure	Partial impairment of a non-critical function; resolvable without affecting primary operations.	2	3	8	3	2	2	0
S4 Minor Failure	No functional impact, but causes slight operational inconvenience.	2	8	4	5	4	2	4
MTBF（h）		2190	796	730	1095	1460	1752	2190
Annualized Failure Rate λ（%）		0.05	0.13	0.14	0.09	0.07	0.06	0.05
7-year MTBF（h）		1459						

Tab. 3 Statistical Table of Automation Software Failure Classification

The software operated stably over the past 7 years with no S1 failures.

S3 Failures: MTBF=3,066 h (~127 days)

Failures mainly concentrated in core data processing module:

- FDP program issue that caused inbound flights from a specific direction to remain continuously uncorrelated;
- Frequent unexplained ICC process alarms on the front-end processor, which triggered automatic radar channel switching.

S4 Failures: MTBF=2,108 h (~ 87.8 days),

mostly related to the system monitoring and O&M modules, such as:

- logic error in the heartbeat signal sending process, causing frequent false alarms in the monitoring system;
- The FDP server's crontab missing the scheduled logmanage script, leading to the server's disk usage exceeding 70%.

3.2.4 Implementation of RCM in Software Service phase

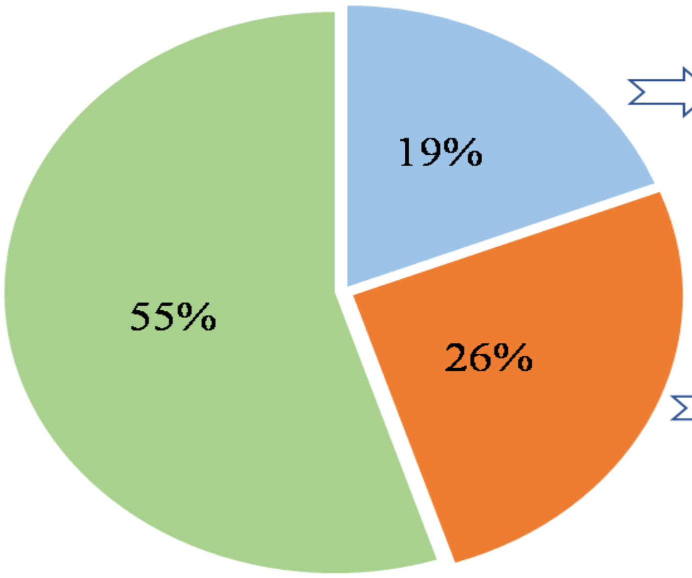
3.2.4.2 Classification of Software Maintenance Activities and Maintenance Strategies

Software Maintenance Workload

Software update activities aimed at expanding functionality and enhancing performance in response to new user requirements.

Software updates drive the evolution of the software lifecycle, which is categorized by time span into:
1. Short-term requirement updates (addressing immediate regulatory needs)
2. Medium-to-long-term requirement planning (focusing on cutting-edge technology applications)

Software updates and manual operations may introduce new vulnerabilities, posing both direct and secondary risks to system operations.
Primary: corrective maintenance
Secondary: condition-based maintenance



Maintenance activities conducted to identify and rectify software defects, correct erroneous configurations, and eliminate operational errors, primarily addressing pure software failures.

Primary: corrective maintenance
Secondary: scheduled maintenance、condition-based maintenance

Maintenance activities performed to adapt to external environmental changes, primarily addressing hardware capacity deficiencies that result in software performance degradation/crashes, data acquisition failures, or operational interruptions.

Primary: scheduled maintenance
Secondary: corrective maintenance、condition-based maintenance

Corrective Maintenance   Adaptive Maintenance   Perfective Maintenance

Fig. 5 Pie Chart of Software Maintenance Workload Distribution

3.2.2 Implementation of RCM in Software Service Phase

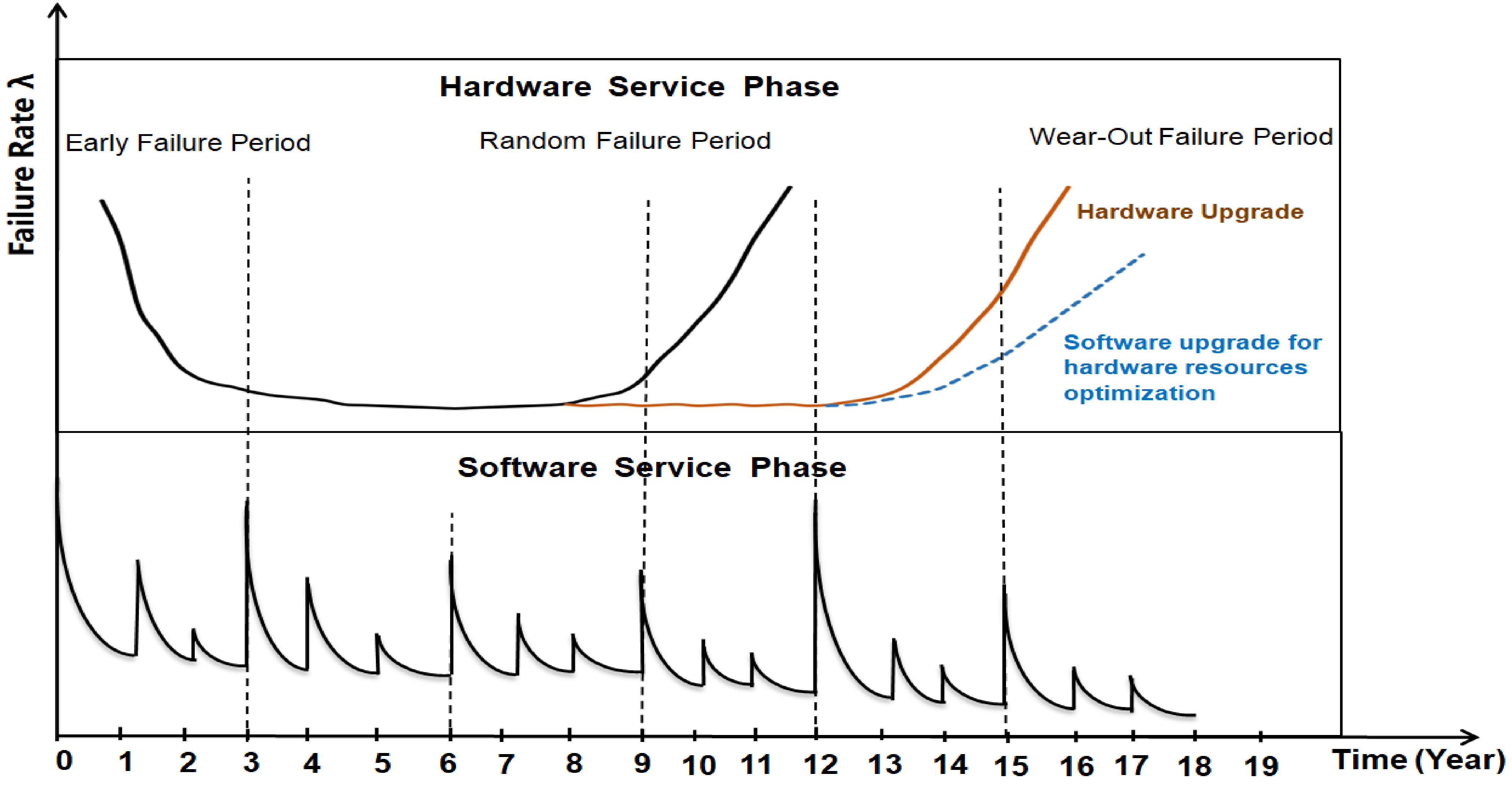
3.2.2.3 Insights – Major concepts of RCM theory- Reliability maintenance strategy

- Failure Mode Repository :*Establishing a failure database enables rapid fault diagnosis and resolution by maintenance teams.*
- **Strict Change Management & Quality Assurance**: *Any modification to the production environment must undergo a rigorous process of request, evaluation, testing, and approval.*
- **Data-Driven Preventive Management:**

  quantitative analysis of high-frequency and high-impact issues across different software failure levels, maintenance teams can accurately identify critical weak points in the software and develop targeted optimization strategies.
- **Hardware Independence:** to *Reduce hardware dependencies via modular architectures*
- **Maintenance Execution & Feedback Loop**

  Dynamic Strategy Adjustment, Contingency Execution, Closed-Loop Optimization

What we plan


Failure Rate λ
Hardware Service Phase
Early Failure Period
Random Failure Period
Wear-Out Failure Period
Hardware Upgrade
Software upgrade for hardware resources optimization
Software Service Phase
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
Time (Year)

3.2 Life Cycle Management of ATM Automation System — Final Phase

The final stage refers to the phase when an ATM automation system continues to operate and provide services despite nearing or exceeding its designed or normal service life. During this stage, component precision deteriorates or performance fails, leading to service interruptions or reduced system reliability, and **a significant increase in safety risks**

01 Based on RCM analysis results from the service period, predict wear trends and forecast the timing, location, and impact of potential failures.

02 For components with high failure rates or critical importance, ensure spare parts are well-stocked and conduct preemptive maintenance.

03 Depending on the situation, consider upgrading, retrofitting, or rebuilding the system to maintain its reliability level.

04 If the system's performance no longer meets operational requirements, decommissioning should be carried out.


CONTENTS

4. Summary and Outlook

01

Lifecycle management of automation systems spans every stage from inception to retirement, ensuring optimal performance and value throughout the system's lifespan.

02

The study **quantitatively analyzed the reliability of both hardware and software**, optimized maintenance strategies, and effectively **improved system reliability, resource utilization, operational efficiency, and reduced maintenance costs**—offering practical insights for full lifecycle management.

03

RCM is suitable for hardware maintenance, while for software oriented ATM Automation system, need to further investigate comprehensive management model that is **reliability-based, agility and resilience-centered, and supported by full-process management.**

4. Summary and Outlook --Future Plan

Targeted research will be conducted on MTTR (Mean Time To Repair), focusing on collecting data such as maintenance team response time, preparation time, fault assessment time, spare parts acquisition time, disassembly time, replacement time, etc.

Develop intelligent tools for collecting operational metrics such as CPU usage and other runtime data to enhance the analysis of system performance and health status.

Collect more operational and failure data from servers and workstations to analyze performance and failure rate trends, providing data support for future hardware upgrade projects.

Invite States/Administrations interested in the lifecycle management of ATM automation systems to jointly explore optimization and analysis methods and share management experiences.

Thanks!

Looking forward to progress together !