End-to-End Integrated Systems Management Tools:

Enabling Cost-effective Enterprise 3G IKC2 Configuration Management

ABSTRACT

The management of Third Generation Integrated Knowledge-based Command and Control (IKC2) systems configuration and performance is becoming increasingly challenging in a more complex networked environment with fast-changing infrastructure. In this management process, there is primarily a need to strike a balance among the maintenance of the systems' integrity, stability, and their ability to adapt to any emerging cyber threats. Users are required to have the knowledge of an accurate and complete inventory of infrastructure components residing within the system of systems to carry out periodic and frequent systems updates. These include installing system security updates, anti-virus file patches as well as server and network software updates. Most importantly, users need to be fully aware of any configuration discrepancy to respond in a timely and proactive manner. These tasks require considerable resources and time. This article describes how advanced technological tools are being explored for better systems management efficiency and cost-effective configuration management. The key objective is to achieve an end-to-end integrated systems management and enterprise-wide configuration management database for the IKC2 system of systems. The article also highlights promising results of implementing an automated configuration management tool suite to improve work efficiency and optimise resources.

Tay Yeow Koon
Sng Kok Seng
Ashley Tong Kian Aik
Goh Pei Ming

End-to-End Integrated Systems Management Tools: Enabling Cost-effective Enterprise 3G IKC2 Configuration Management

INTRODUCTION

Configuration management is a management discipline that focuses on establishing and maintaining the consistency of a system's performance and its functional and physical attributes with its specified operational requirements. Configuration management for Integrated Knowledge-based Command and Control (IKC2) systems entails the management of their security and integrity requirements through the control of changes made to their hardware, software, interface and documentation throughout their life cycle. The task of configuration management is fast becoming highly challenging in the designing of the IKC2 system of systems (SoS) for the Third Generation Singapore Armed Forces (SAF). First, personnel who are performing the configuration management must possess considerable professional skills and knowledge. They must be able to cope with the increased level of SoS integration and with added complexities in terms of a larger scale of heterogeneity and interaction, as well as a wider diversity of operating platforms, applications and services. Second, greater systems flexibility, adaptability and availability are needed to support operations in modern warfare. These requirements also have to be met with limited resources and budget.

CHALLENGES

As the SAF moves towards implementing a highly integrated SoS operating environment, configuration and performance management such as network fault isolation and software inventory verification are becoming more complicated. This is due to the sheer number and diverse range of the system configuration items involved. For example, installing and setting up software for a large number of client stations and checking their software versions could require significant effort from the systems administrator. This is more so when the equipment in the systems is geographically dispersed, and when more applications and services are being deployed. Similarly, maintenance tasks involve more rigorous software verification testing, patch testing, installation and distribution. These can be time consuming and tedious. Resources are further strained when security patches or virus definition files need to be updated frequently. Unmanaged or unintended changes have also been identified as one of the causes for unplanned systems downtime. Therefore, human error and the downtime due to the labour-intensive troubleshooting processes could impact systems readiness.

Furthermore, the continual process of integrating newly deployed systems as well as phasing out legacy systems remains a major challenge. How does one ensure that the systems integration is carried out seamlessly? For systems integrity and reliability, the need to ensure accuracy, relevance and consistency in configurations while integrating systems and optimising the cost of software maintenance and network infrastructure has always been a great challenge. In addition, there is a routine to track the usage of software licenses used in the systems and to manage and re-distribute the licenses holistically when there are changes in user configuration.

In the rapidly growing IKC2 network, the demand for more manpower or budget to cope with these tasks is unsustainable in the long term.

TECHNOLOGY OF INTEGRATED SYSTEMS MANAGEMENT TOOLS

Integrated Systems Management Tools (ISMT) are being explored to overcome the challenges. ISMT comprise a wide range of commercial-off-the-shelf software products that are developed to perform functions such as configuration management, incident management and availability management. In the past, exploitation of the technology was carried out in a disparate and less coherent manner due to its lower level of maturity.

Since 2007, the usefulness of the technology as an integrated solution for business service management (BSM) has become more widely publicised. This trend is primarily attributed to the evolution of ITIL®[1] and the broadening of the technology landscape and areas of application. Simply put, ISMT are employed to improve management effectiveness and efficiency. As depicted in Figure 1, systems tools developed for each layer of service domain can provide management capability specific to the domain. For instance, systems tools associated with the network layer can provide the user with the capability to monitor and track linkages as well as the traffic status of a network of equipment automatically. This in turn reduces the resources, effort and cost required by the user to manage the network. As the technology progresses and more software products become available over the years, the capability objective is to provide an end-to-end integrated solution that strings together the full suite of systems tools developed for the various layers. It is this increased level of technological maturity we are leveraging to enhance our capability in systems and configuration management for Third Generation IKC2 systems.

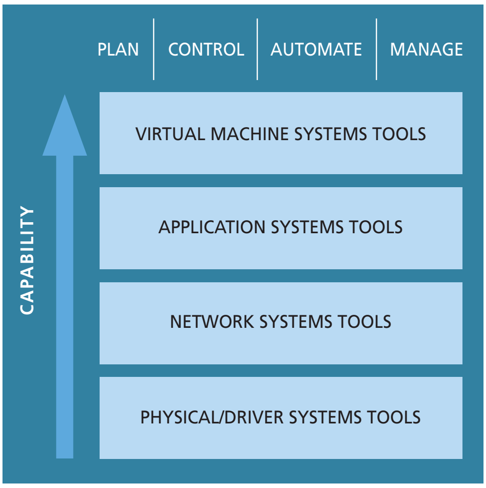

PLAN
CONTROL
AUTOMATE
MANAGE
CAPABILITY
VIRTUAL MACHINE SYSTEMS TOOLS
APPLICATION SYSTEMS TOOLS
NETWORK SYSTEMS TOOLS
PHYSICAL/DRIVER SYSTEMS TOOLS

Figure 1. Technology of ISMT

PILOT IMPLEMENTATION

Key Considerations

A pilot implementation of ISMT has been carried out for selected IKC2 systems. The primary considerations covered the systems' deployment requirements, infrastructure and bandwidth availability. For example, to facilitate rapid deployment, software tools are usually required to be easily installed or restored during systems set-up. The tools should also be easily configurable by the user to cater for changes in IP/MAC addresses and other changes in the network configuration during deployment. Hence, ISMT that are adopted will have to cater for the dynamic operating environment and its constraints.

Most importantly, the objective of the pilot implementation is to provide major stakeholders with an automated and integrated technological solution to improve operational readiness, service support and systems management efficiency.

Focus Areas and Functional Scope

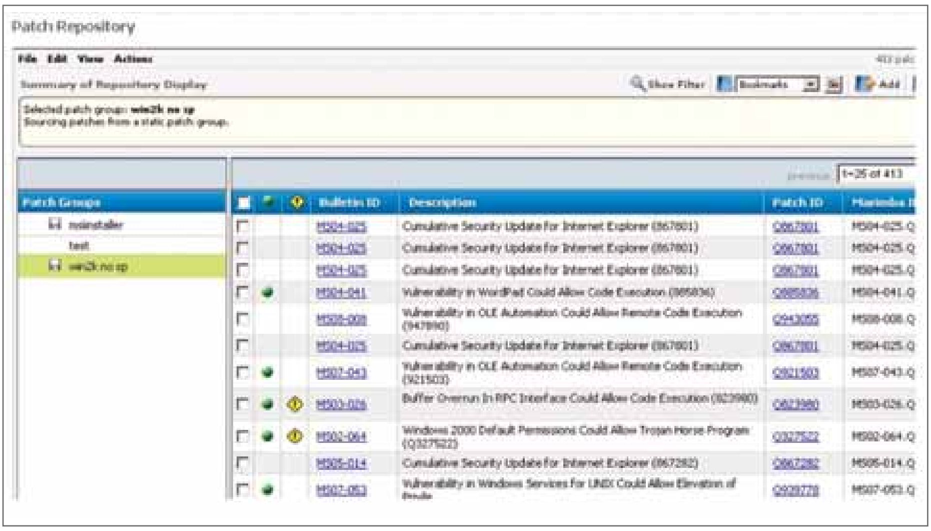
Following the identification of areas with the greatest potential for systems improvement, several ISMT were evaluated to fulfill the objective. A suite of tools deemed most cost-effective was deployed to provide the following capabilities:

Configuration Management. For systems run-up or configuration alteration, the ISMT run an automated configuration and baseline detection as well as recovery capability. They are able to provide verification checks on the hardware and software inventory of the systems and to detect any deviation from the default baseline configuration. The systems administrator can closely monitor this automatic verification scan of the inventory via a remote terminal. Depending on the administrative policy set, the tools can perform automatic repair and restore any affected software to the baseline state. Without the tools, any configuration glitch would have taken the systems administrator or engineer hours to perform troubleshooting or fault isolation.

Patch Management. ISMT enable the systems administrator to disseminate software packages such as security patches from a centralised location to many remote clients at once. Besides allowing the administrator to collate patches into patch groups before distribution, the tools also provide the status of the patch installation after the distribution, as shown in Figure 2. The tools not only automate the labour-intensive patch processes, but also provide the historical status of software patching to facilitate audit processes.

Assets Management. The tools enable resources usage and trend patterns to be centrally monitored. Detailed log reports can also be generated for documentation and resource planning.

Performance and Availability Management. As shown in Figure 3, the tools incorporated into systems facilitate performance and availability management by providing the systems administrator with statistical information on the underlying systems operations. The information is analysed in real time to allow online application and systems health monitoring. When the performance falls below a predetermined threshold level, an early warning is sent to the systems administrator. Such information on the profile of the applications, transactions and resources usage enables the systems administrator or engineer to take pre-emptive action in a more timely manner. The information also facilitates the service support team to carry out predictive or on-condition maintenance when necessary.



Selected patch group: **win2k no sp**
Sourcing patches from a static patch group.

Patch Groups
nsinstaller
test
win2k no sp

□	●	⚠	Bulletin ID	Description	Patch ID	Marimba I
□			MS04-025	Cumulative Security Update for Internet Explorer (867801)	Q867801	MS04-025.Q
□			MS04-025	Cumulative Security Update for Internet Explorer (867801)	Q867801	MS04-025.Q
□			MS04-025	Cumulative Security Update for Internet Explorer (867801)	Q867801	MS04-025.Q
□	●		MS04-041	Vulnerability in WordPad Could Allow Code Execution (885836)	Q885836	MS04-041.Q
□			MS08-008	Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)	Q943055	MS08-008.Q
□			MS04-025	Cumulative Security Update for Internet Explorer (867801)	Q867801	MS04-025.Q
□	●		MS07-043	Vulnerability in OLE Automation Could Allow Remote Code Execution (921503)	Q921503	MS07-043.Q
□	●	⚠	MS03-026	Buffer Overrun In RPC Interface Could Allow Code Execution (823980)	Q823980	MS03-026.Q
□	●	⚠	MS02-064	Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522)	Q327522	MS02-064.Q
□			MS05-014	Cumulative Security Update for Internet Explorer (867282)	Q867282	MS05-014.Q
□	●		MS07-053	Vulnerability in Windows Services for UNIX Could Allow Elevation of	Q939778	MS07-053.Q

Figure 2. Patch repository by ISMT

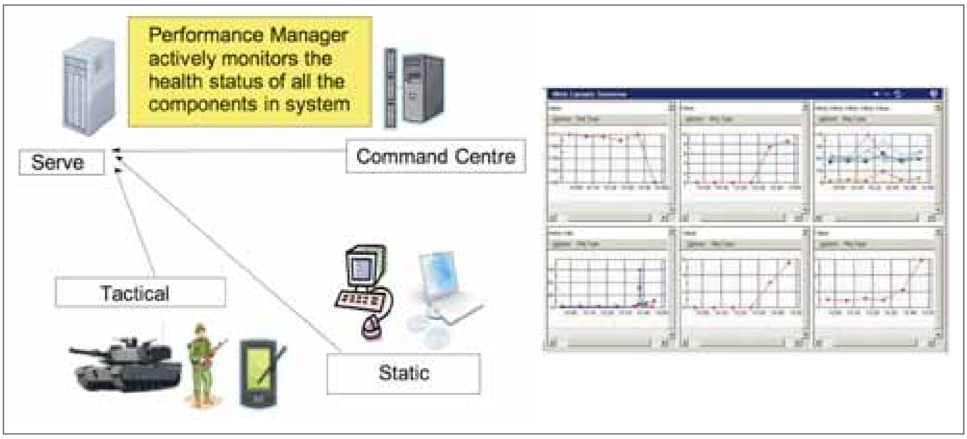

Performance Manager actively monitors the health status of all the components in system
Serve
Command Centre
Tactical
Static

Figure 3. Performance and availability management

Measurement of Result

Data collection and measurement were carried out to gauge the outcome of the implementation. For a set of routine configuration control tasks shown in Table 1, the number of manhours required by the systems administrator to perform the tasks was recorded before and after the implementation. The measurement results show that an automation of the tasks using ISMT reduced the number of manhours required by around 90%. This reduction is highly significant as it not only reduces operations & support (O&S) costs but also enables stakeholders to do more with fewer resources.

Benefits and Added Capabilities

Apart from the time savings, the ISMT also helped the systems administrator and manager to provide technical support services and improve their responsiveness to operational requirements. The benefits and added capabilities are summarised in Table 2.

Task	Average number of manhours needed before implementation	Average number of manhours needed after implementation
Hardware Configuration Inventory Collection	18	2
Software Configuration Inventory Collection	30	2
Software Configuration Baseline Detection and Recovery	18	4
Software Deployment (e.g. patch distribution)	33	2

Table 1. Time savings achieved by using ISMT for configuration

Tasks and Description	*Systems Administrator*	*Systems Manager*
Maintenance • Regular preventive maintenance (e.g. boot and shutdown systems when needed, backup database) • Installing and verification of baseline software • Systems monitoring and tuning (e.g. kernel, networking software and server)	**Configuration Control** • Automate regular tasks (e.g. Auto-remediation) • Auto-remediation • Automatic verification for compliance to baseline • Maintain consistent hardware builds and software installations • Capture and track configuration records for faster turnaround for defects	**Configuration Management** • Accurate, consistent and complete documentation of baseline configuration • Collation of compliance • Improve governance • Use data to identify root cause of failures and generate reports
Monitoring • Monitor temperature, humidity, electrical systems and uninterrupted power supplies • Maintain printer and disk space network, servers and workstations, performance, and security, and all log files regularly	**Online Application/ Network Monitoring** • Monitor all applications, servers and network connectivity proactively • Alert the systems administrator to incidents and potential for faster turnaround	**Performance Management** • Establish performance baselines to set thresholds for performance related problems • Enable trending for capacity and performance management • Trending Analysis
Assets Management • Track hardware and software assets • Aid purchase management, contracts management with software compliance and licences, etc	**Assets Tracking** • Up-to-date reports of asset listing	**Assets Management** • Manage and track all the assets at systems level • Provide visibility into asset costs
Service Operations • Incident management • Request fulfilment • Problem management • Knowledge base	**Incident Management** • Tracking of requests delivered for management reporting • Knowledge base of incidents • Timely incident report	**Incident and Event Management** • Maintain knowledge base of incidents and problems • High traceability • Maintain service contracts

Table 2. Sample of benefits and added capabilities from using ISMT

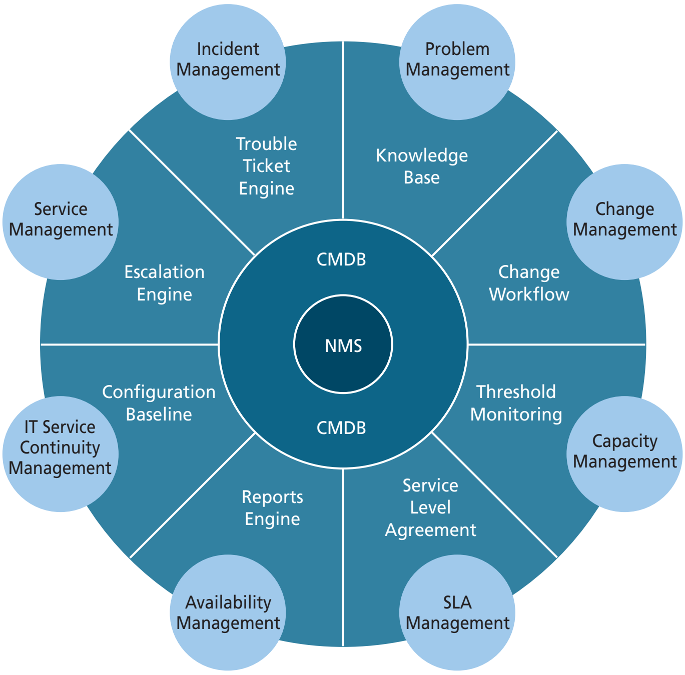


Figure 4. CMDB integrates BSM processes in the ITIL® framework

CONFIGURATION MANAGEMENT DATABASE FOR ENTERPRISE-WIDE SYSTEM OF SYSTEMS AND SERVICES MANAGEMENT

What is Configuration Management Database?

Configuration management database (CMDB) is a repository of information relating to all the configuration items (CI) of an IKC2 system. The CMDB records CIs and details the important technical and operational attributes and their relationships. A well-configured CMDB can monitor CIs – their location, status, and relationship to one another – and consolidate disparate data sets. It also provides a single source of accurate information about data in the IKC2 environment. Under the ITIL® framework, CMDB is a core component that integrates the various BSM processes, as shown in Figure 4.

SoS Configuration and Integration Management

CMDB can be leveraged as a technological tool to bring the IKC2 SoS capability to the next level. For example, with all the CI information of the SoS captured, the CMDB provides an accurate, consistent and complete picture of the SoS configuration and the relationships among the CIs at the various operational layers. At the top layer, it is possible to know the relationships and interdependency among individual systems for integration and operational assessment. At the intermediate layer, the relationships among the CIs, shared infrastructure and resources can be viewed to identify the level of usage of the shared resources and for asset optimisation.

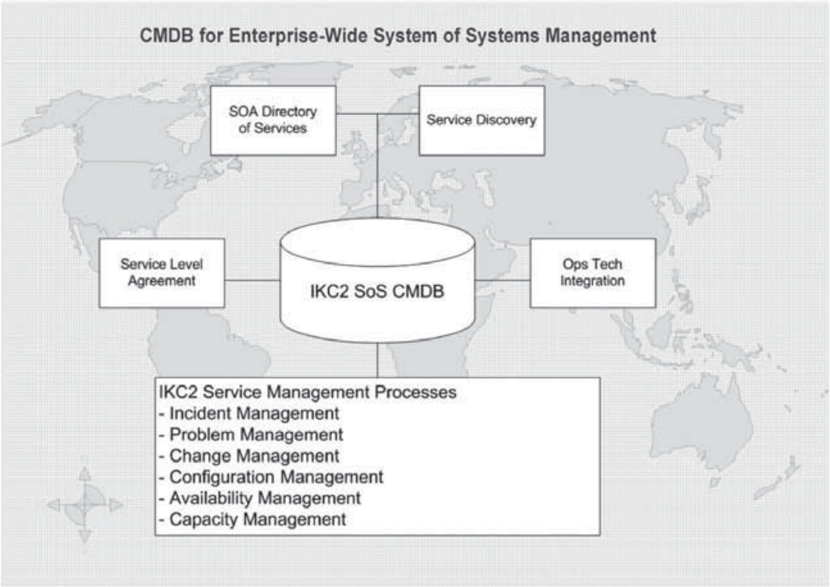

CMDB for Enterprise-Wide System of Systems Management
SOA Directory of Services
Service Discovery
Service Level Agreement
IKC2 SoS CMDB
Ops Tech Integration
IKC2 Service Management Processes
- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Availability Management
- Capacity Management

Figure 5. CMDB for enterprise-wide IKC2 SoS management

Greater Ops-Tech Integration and Service Level Agreement

As depicted in Figure 5, CMDB can also serve as a collaborative platform for closer operations-technology integration. The provision of comprehensive configuration data information enables the Integrated Systems Management team to manage application service delivery from user perspectives and provide speedy detection of root causes of problems. By comparing data collected on systems and transaction performance against service level targets, the management team can leverage CMBD to provide O&S services of better quality and improve the Service Level Agreement with customers to meet enterprise-wide IKC2 requirements.

Service Discovery and Service Management for Service-Oriented Architecture

We can also optimise the CMDB framework to increase the IKC2 systems capability. Under the Service-Oriented Architecture (SOA), CMDB can categorise the broad range of services and applications provided to the IKC2 systems under CIs. The relationships among the services and their linkage to common sources or shared infrastructure are registered and monitored in the CMDB. With the ability to discover information about the CIs automatically (auto-discovery) and track changes, the CMDB can be used to provide a directory of services and service discovery. It enables stakeholders to integrate services across various operational domains and to plan and manage them.

CONCLUSION

ISMT have been exploited to address the challenges of managing the complexity of Third Generation IKC2 systems. The implementation of ISMT for selected IKC2 systems has yielded positive results. The next step is to continually employ the latest ISMT and CMDB technology to develop an enterprise-wide IKC2 SoS management capability. A well-configured CMDB will enable stakeholders to monitor CIs of the SoS easily and provide them with a global picture of accurate information in the SoS environment. Having this control will strengthen the value of the service that IKC2 systems provide to the SAF. Furthermore, a CMDB framework equipped with service directory and service discovery capabilities can be leveraged to support the SOA requirement across various domains. It will not only reduce the Total Cost of Ownership to manage the IKC2 SoS operation, but also can be used as a framework to enable the SAF to achieve more with fewer resources.

REFERENCES

Bishop, Tom. 2007. ITIL and the CMDB: Better Service Management Equals Greater Business Value. BMC Software.

Lee, Jacqueline, Melvyn Ong, Ravinder Singh, Andy Tay, Yeoh Lean Weng, John J. Garstka and Edward Smith, Jr. 2003. 'Realising Integrated Knowledge-based Command and Control: Transforming the SAF'. POINTER Monograph No. 2, Singapore Armed Forces.

Phoenix Business and Systems Process Inc. Services ITIL Implementation and Advanced Training. http://www.pbandsp.com/services/ITIL.html (accessed 26 June 2009)

Richardson, James P., Lee Graba and Mukul Agrawal. 2004. Computing and Communications Infrastructure for Network-centric Warfare: Exploiting COTS, Assuring Performance.

Wikipedia, the free encyclopedia. Configuration Management. http://en.wikipedia.org/wiki/Configuration_management (accessed 26 June 2009)

ENDNOTES

[1] The Information Technology Infrastructure Library (ITIL) is a set of industrial concepts and best practices for managing IT infrastructure, operation and services. It provides a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom's Office of Government Commerce.

BIOGRAPHY

Tay Yeow Koon is Deputy Director (Systems Management – Operations & Support). He manages all Operations & Support (O&S) matters and oversees the systems management of Command, Control, Computing Intelligence systems of the Ministry of Defence and Joint Services. Yeow Koon has extensive experience in the Command, Control, Communications, Computers and Information Technology domain involving diverse users from the Singapore Armed Forces and homefront security agencies including the Singapore Police Force and Singapore Civil Defence Force. Yeow Koon holds a Bachelor degree of Computer Science from the National University of Singapore (NUS) and completed the General Management Programme at Harvard Business School in 2009.

End-to-End Integrated Systems Management Tools:

Enabling Cost-effective Enterprise 3G IKC2 Configuration Management

Sng Kok Seng is a Senior Principal Engineer (Systems Management). He is involved in developing systems engineering processes, technological solutions and best practices to enhance the operational readiness and cost-effectiveness of Command and Control Information Systems. Kok Seng also provides technical advice and support to acquisition and development project teams in systems design for reliability, maintainability and supportability, as well as in the development of Integrated Logistics Support (ILS). He is currently a member of the Systems Engineering Technical Committee of the Institution of Engineers, Singapore. Kok Seng obtained a Bachelor degree in Electrical Engineering (Honours) and a Master of Science degree in Electrical Engineering from NUS in 1988 and 1994 respectively.

Ashley Tong Kian Aik is an Engineer (Systems Management). He is involved in the monitoring and projection of systems performance, serviceability, reliability and availability. Ashley also provides support to acquisition project teams from the ILS perspective. He has led several teams in aspects such as change management, configuration control management, and O&S engineering support in the areas of troubleshooting, incident investigation as well as systems recovery, modification, upgrade, retirement planning and disposal. Ashley is a member of the Singapore Computer Society and is a Certified IT Project Manager (Associate). He obtained a Master of Information Technology degree from the University of Sydney, Australia in 2004.

Goh Pei Ming is an Engineer (Systems Management). She tracks and manages systems performance and trends in failure data to highlight any sustainability and supportability issues. Pei Ming also manages resources such as spares, manpower as well as the renewal and establishment of contracts. She provides ILS support and consultation from the O&S perspective to the project team, and contributes to the planning and management of systems upgrades, modification and decommissioning. Pei Ming graduated with a Bachelor degree in Computer Engineering (Honours) from NUS in 2008.