

SUITABILITY TEST REPORT

for

**Auto-trol
KONFIG™, Version 3.0
Solaris**

Network Manager Component

April 24, 1998

Prepared by



National Product Line Asset Center
1000 Technology Drive, Suite 1000
Fairmont, WV 26554

1.0 SCOPE

1.1 Introduction

This Suitability Test Report (STR) defines and records the test preparation and test results from suitability testing of the KONFIG™ enterprise-wide physical network management applications developed and marketed by Auto-trol.

KONFIG Network manager provides large organization with a centralized data repository for documenting enterprise-wide data, voice and video networks. The KONFIG network data model simplifies network design, configuration management and problem resolution, in addition to performing asset and inventory management. KONFIG is database-driven, storing all network data in ORACLE and automatically generating graphic network views from the data. KONFIG's centralized data repository eliminates redundant data, improves data reliability, ensures data integrity, and facilitates data sharing across business areas. As a result KONFIG can help reduce network downtime, improve worker productivity, cut expenses and increase profits.

Criteria for which an SMP or LNMP is required have received a "No" Test Result due to their reliance on another Network Manager (another product in the same component) product to meet the criteria.

1.2 Test Environment

KONFIG™ was suitability tested against command center product line requirements and architectural constraints, utilizing a test network comprised of four models (i.e., one SUN Ultra 1, one PC running Windows 95, and 2 printers). The results of the testing are documented in this report.

Base Package:

Part Name	Version No.	Manufacturer
KONFIG	3.0	Auto-trol Technology

To complete suitability testing, the following optional parts were required. These require the purchase of separate licenses.

Part Name	Version No.	Manufacturer
Oracle DBMS	7.3	Oracle
ATTCLm		Auto-trol Technology

2.0 SYSTEM REQUIREMENTS

Contact vendor for details.

3.0 TEST RESULTS

The results obtained during testing of the Auto-trol product KONFIG™ are shown in the following table. The table contains the *Criteria Number*, *Criteria Description*, *Test Result*, *Explanation*, and *Test Method*. The test methods used to perform the suitability testing included:

Inspection - consists of investigation, without the use of special equipment or procedures, to determine compliance with requirements. Inspection may include comparison of requirements to the vendor supplied product, documentation, and/or information.

Test - is the evaluation of functional operation by use of equipment or instrumentation, simulation techniques, and the application of established principles and procedures to determine compliance.

4.0 CRITERIA SOURCE REFERENCES

The criteria used in the suitability testing process were developed from the following source references:

- Generic Command Center Architecture (GCCA) Report for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision A, 5 April 1993.
- Qualified Product List (QPL) Capstone Test Plan for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision 0.1, 29 June 1995.
- Network Manager Class Requirements for the Portable, Reusable, Integrated Software Modules (PRISM) Program, Revision 1.0, 7 July 1995.

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
1.0	Architectural Characteristics			
1.1	The Network Manager should be capable of working in small (0-50 nodes), medium (50-150 nodes), and large (over 150 nodes) networks.	Y		Inspection
1.1.1	The NM should be capable of handling the magnitude of management information that could be generated in a large (i.e., over 150 nodes) network.	Y		Testing
1.2	The NM should be able to provide a hierarchical view of all devices managed by the NM. This view should be represented as a hierarchical map that incorporates explodable icons, which can spawn a sub-map that represents another level of detail. At the lowest level, icons should represent specific devices from which status information can be accessed.	Y		Testing
1.3	The NM should allow grouping of devices based on functionality, location, security, or any other user-defined category, and perform management on those groups.	Y		Testing
1.4	The NM should support manager-to-manager transmissions of: Access control information. Device status change information. Network configuration changes. (Others?).	N		Inspection
1.5	The NM should provide for functionality which is contained in separate modules which allows the user to choose those functions required and avoid inclusion of non-required functions.	Y		Testing
1.5.1	The user of the NM software should be able to make software configuration changes (based on changes in the environment) without vendor technical support.	Y		Inspection
1.6	The NM should be capable of distributing its manager/agent processes among multiple network devices.	Y		Inspection
1.7	The NM should be capable of running on multiple platforms.	Y		Inspection
2.0	System Interface Criteria			
2.1	The NM should support a graphical representation of the network. Comment: This requirement deals with the topology (e.g., token ring, star, bus, node, etc.) of any given level of geography.	Y		Testing
2.1.1	The NM should support the ability to provide a hierarchical map.	Y		Inspection
2.1.2	The NM should support the ability to represent unmanageable devices in the map.	Y		Testing
2.1.3	The NM should support the ability to show both physical and logical maps.	Y		Inspection
2.1.4	The NM should support the ability to tailor the icons that represent the network and network interfaces.	Y		Testing
2.2	The NM should provide an interface to access the information off of the Directory Server when one exists.	Y		Inspection
3.0	Security Features			

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
3.1	The NM should provide a means to identify and authenticate users via user identification and passwords.	Y		Testing
3.2	The NM should provide user access controls.	Y		Inspection
3.2.1	The NM should provide the capability to restrict access to applications.	Y		Inspection
3.2.2	The NM should provide the capability to restrict access to files.	Y		Inspection
3.2.3	The NM should provide the capability to restrict access to queues and other resources.	Y		Inspection
4.0	Implmentation Constraints			
4.1	If Unix-based, the NM should support current POSIX requirements (FIPS Pub 151).	Y		Inspection
4.2	If Unix-based, the NM product should use the X-windows standard.	Y		Inspection
4.3	If Unix-based, the NM should support the Open Software Foundation (OSF)/MOTIF graphical user style guide.	Y		Inspection
5.0	Configuration Management			
5.1	The NM should provide the capability to define new managed object types. The definition should include attributes, including the range and types of values to which the attributes can be set.	Y		Testing
5.2	The NM should provide the capability to set SNMP parameters and process allocation.	N	Requires Third Party Logical Network Management Platform (LNMP).	Inspection
5.3	The NM should provide the capability to modify the relationships (i.e. roles) of network resources.	N	Requires Third Party Logical Network Management Platform (LNMP).	Inspection
5.4	The NM should provide the capability to remotely examine device statistics, threshold values, and Local Area Network (LAN) connections.	N	Requires Third Party Logical Network Management Platform (LNMP).	Inspection
5.5	The NM should provide the capability to specify initialization and shutdown procedures for network devices.	Y		Testing
5.6	The NM should provide for graceful degradation and restoration of the network.	N		Inspection
5.7	The NM should provide the capability to verify each user's authorization for performing either specific or categories of configuration management functions.	Y		Testing
5.8	The NM should be capable of reporting on configuration status.			
5.8.1	The NM should provide the capability of agent systems to report configuration changes to their managers as these changes occur.	N	Requires a Third Party Product Logical Network Management Platform (LNMP) or System Management Platform (SMP).	Inspection
5.8.2	The NM should provide the capability to poll their agents in order to determine each agent's (or agent system's) configuration status.	N	Requires a Third Party Product Logical Network Management Platform (LNMP) or System Management Platform (SMP).	Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
6.0	Performance Management			
6.1	The NM should provide the capability to monitor performance.	N	Requires a Third Party Logical Network Management Platforms (LNMPs)/System Management Platforms (SMPs).	Inspection
6.1.1	The NM should provide the capability to monitor the workload of networked devices (e.g., resource utilization).	N	Requires a Third Party Product Logical Network Management Platform (LNMP).	Inspection
6.1.2	The NM should provide the capability to generate event reports as utilization approaches capacity.	N	Requires Third Party Product (Logical Network Management Platform (LNMP))	Inspection
6.1.3	The NM should provide the capability to report on other (i.e. other than utilization capacity) events. The report should specify the event type.	N	Requires Third Party Product (Logical Network Management Platform (LNMP))	Inspection
6.2	The NM should provide the capability to execute performance tests and to collect the results from those tests inputted to the Diagnostic Testing Function provided under Fault Management.	N	Requires Third Party Product (Logical Network Management Platform (LNMP))	Inspection
6.3	The NM should provide the capability of monitoring resource allocations for any resource on the network.	N	Requires Third Party Product (System Management Platform (SMP)).	Inspection
6.4	The NM should provide the capability to set or modify resource attribute values.	N	Requires Third Party Product (System Management Platform (SMP)).	Inspection
6.5	The NM should provide the capability to allow NM operators to specify performance tuning methods.	N	Requires a Third Party Product System Management Platforms (SMPs).	Inspection
6.6	The NM should provide the capability to generate performance reports based on user specified criteria.	N	Requires a Third Party Product Logical Network Management Platform (LNMP). KONFIG allows user to specify the criteria. However, the LNMP must provide the data to KONFIG.	Testing
6.6.1	The NM should provide the capability to specify the format of all reports.	Y	Requires a Third Party Product Logical Network Management Platform (LNMP). KONFIG allows user to specify the criteria. However, the LNMP must provide the data to KONFIG.	Testing
6.7	The NM should provide the capability to test resource capacity.	N	Requires Third Party Product (System Management Platform (SMP)).	Inspection
7.0	Fault Management			
7.1	The NM should provide the capability to monitor the events and errors.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection
7.2	The NM should provide the capability to log events and errors, to record reports within the managed system that generated the event, (e.g., logging) or error, and then retrieve these reports remotely.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection
7.3	The NM should provide the capability to forecast anticipated faults by allowing the user to set thresholds, which represent performance limits of networked devices.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
7.4	The NM should provide the capability to activate diagnostic and testing procedures.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection
7.5	The NM should provide the capability to report results from Diagnostic and Testing procedures.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection
7.6	The NM should provide the capability to analyze the results of diagnostic testing.	N		Inspection
7.7	The NM should provide the capability to report failures.	N	Requires Third Party Network Management Product (LNMP or SMP) to perform this function.	Inspection
7.8	The NM should provide the capability to terminate failures.	N		Inspection
7.9	The NM should provide Diagnostic Tests.			
7.9.1	The diagnostic tests should include Connectivity Tests.	N		Inspection
7.9.2	The diagnostic tests should include Data Saturation Tests.	N		Inspection
7.9.3	The diagnostic tests should include Data Integrity Tests.	N		Inspection
7.9.4	The diagnostic tests should include Protocol Integrity Tests.	N		Inspection
7.9.5	The diagnostic tests should include Connection Saturation Tests.	N		Inspection
7.9.6	The diagnostic tests should include Response Time Tests.	N		Inspection
7.9.7	The diagnostic tests should include Imaging Loopback Tests.	N		Inspection
7.10	The NM should provide the capability to request dumps.	N	Requires Third Party Network Management Product (LNMP or SMP).	Inspection
7.10.1	The NM should provide the capability to request statistic blocks.	N	Requires Third Party Network Management Product (LNMP or SMP).	Inspection
7.10.2	The NM should provide the capability to request operational status information of managed network devices.	N	Requires Third Party Network Management Product (LNMP or SMP).	Inspection
7.11	The NM should provide the capability to track corrections to fault conditions.	N	Third Party Product Action Request System (Vendor recommends Remedy) is required to perform this function, However database used with the product does allow the tracking of corrections to fault conditions.	Testing
8.0	Security Management			
8.1	The NM should provide the capability to the NM operator (or security officer) to permit or disallow access to security related parts of the network.	Y		Testing
8.2	The NM should provide the capability to archive and retrieve security related information.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
8.2.1	The NM should provide the capability to create and delete security logs or audit trails.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection
8.2.2	The NM should provide the capability to read from and write to security logs or audit trails.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection
8.2.3	The NM should provide the capability to start and suspend logging or auditing activities.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection
8.2.4	The NM should provide the capability to monitor audit trails or security logs to identify security violation activity.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection
8.2.5	The NM should provide reporting and notification of violations or attempted violations.	Y	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology).	Inspection
9.0	Accounting Management			
9.1	The NM should be capable of recording and generating accounting information.	N	Requires an additional KONFIG module Asset Management Systems (Auto-trol Technology) and a Third Party Product SMPs.	Inspection
9.1.1	The NM should be able to gather information regarding the duration of communications resource usage.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.1.2	The NM should be able to gather information regarding the number of service data units used.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.1.3	The NM should be able to gather information regarding the quality of service provided.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.1.4	The NM should be able to gather information regarding the reason for communications termination.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.2	The NM should provide the capability of specifying accounting information to be collected.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.2.1	The NM should provide the capability to specify accounting information based on the definition of a managed object.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.2.2	The NM should provide the flexibility for the inclusion of optional attributes for accounting (Accounting Management).	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset Management System)	Inspection
9.2.3	The NM should provide the flexibility for new attributes to be specified by the NM operator.	N	Requires Third Party Network Management Product (LNMP or SMP) and an additional Module (Asset	Inspection

Criteria Number	Criteria Description	Test Result	Explanation	Test Method
			Management System)	
9.3	The NM should allow for standard procedures to retrieve accounting information and to manage the disposition of the accounting information.	N	Requires Third Party Product (System Management Platform (SMP)).	Inspection
9.4	The NM should provide the capability for NM operators to select the format the accounting information is to be presented to users, operators, and administrators.	Y	Requires a Third Party Product System Management Platform (SMP) to gather accounting information for a report. KONFIG does allow the user to specify the format of the report.	Inspection
9.5	The NM should support the ability to read accounting limits for communications resources.	N		Inspection
9.5.1	The NM should support the ability to set accounting limits for communications resources.	N		Inspection
9.5.2	The NM should support the ability to change accounting limits for communications resources.	N		Inspection
9.6	The NM should provide the capability to allow the NM operator to define metrics and accounting information units for accountable resources.	N		Inspection
10.0	General			
10.1	The NM should be a COTS or GOTS product.	Y		Inspection
10.1.1	The NM should have been used to satisfy NM requirements for at least one year in a multiplatform environment.	Y		Inspection
10.2	The NM should have proven performance, reliability, and availability characteristics (e.g., mean time between failure, response time to user inputs) and the vendor should be able to provide data supporting characteristic values claimed.	Y		Inspection
10.3	The NM should have user manuals.	Y		Inspection
10.3.1	The NM should have training support.	Y		Inspection
10.3.2	The NM vendor should provide or make available product upgrades, new versions, updates, patches, bug fixes, and maintenance releases to users, including options for implementing the changes and associated costs for the various kinds of changes.	Y		Inspection
10.4	The NM should have proven conformance to Human Factors Engineering (HFE) requirements applicable to an operational command center. (Ref, USAF Human Factors Engineering Guidelines)	Y		Inspection
10.5	The NM should provide programmatic interfaces to support detailed NM requirements.	Y		Inspection
10.6	The NM should have a proven and demonstrable installed base, where the network manager products have been installed in DoD or non-DoD applications in which products could be demonstrated.	Y		Inspection
10.7	The NM should be structured into separate functional priced items to allow users to choose the desired capabilities of the product base that satisfy their particular requirements.	Y		Inspection

