

**Unisys SafeGuard 30m and Oracle® Fail Safe  
Disaster Recovery Solutions**

---

**White Paper**

---

## Introduction

The requirements for Disaster Recovery (DR) solutions have changed dramatically in the last decade. DR scenarios once considered viable are now at risk. Metropolitan and Data Center centric solutions no longer provide the degree of reliance required in today's world. Solutions spanning local regions, countries or even continents are now required. Geo Clusters have existed for some time requiring high bandwidth and complex implementation scenarios, thus limiting their acceptance beyond the most 'sophisticated' datacenters. Today Oracle and Unisys have teamed together to provide a proven DR stack, that not only allows for near plug and play implementation but a low cost enterprise level DR that enables automated failover and recovery over unlimited distances in 30 minutes or less.

SafeGuard 30m upon completion of testing was touted by Oracle as a trouble-free certification with outstanding stability, features and ease of use.

This white paper discusses how Oracle Fail Safe and Unisys SafeGuard 30m have teamed together to certify a DR solution that meets today's needs. Features and implementation strategy are highlighted.

## Objectives

- Provide an overview of Oracle Fail Safe and Unisys Safeguard 30m.
  - Present the combined power of the two products in the DR space of today's enterprise solutions.
  - Describe system and software environment, and high level configuration details.
-

## **OVERVIEW**

### **Oracle Fail Safe**

Oracle Fail Safe is an easy-to-use high availability solution layered on top of Microsoft Cluster Server (MSCS). It is a feature of Oracle Database and is shipped with Oracle Database 10g for Microsoft Windows.

Oracle Fail Safe allows users to easily configure Oracle Database, Oracle Application Server and other Oracle resources for high availability in an MSCS environment. Once the resource is configured for high availability, Oracle Fail Safe works with MSCS to detect resource failures and restart or failover the resource to the secondary node as the user has specified.

The following Oracle resources can be made highly available through Oracle Fail Safe:

- Oracle 9i Database (9.0, 9.2) and Oracle Database 10g (10.1, 10.2)
- Oracle Intelligent Agent (Release 9.0 and 9.2)
- Oracle Management Agent (Release 10.1)
- Oracle Application Server (Release 10.1.2)

### **SafeGuard 30m**

The Unisys SafeGuard 30m solution has fully automated failover and data recovery capabilities. SafeGuard 30m is the only Microsoft certified failover solution that span distances of thousands of kilometers, compared to previous 300-kilometer limitations.

The Unisys SafeGuard 30m solution is based on best practices developed over years of experience in mission-critical computing. The SafeGuard 30m solution has been pretested and configured for unmatched reliability. Solution offerings include services, software and technology at an optimal cost.

SafeGuard 30m versatility spans the gamut of databases and application DR. Oracle Fail Safe, in conjunction with SafeGuard 30m, has the ability to provide DR solutions beyond 300-kilometers with reduced cost and increased stability and performance.

Additional key features of SafeGuard 30m:

- Replication across heterogeneous storage
  - OS-independent replication and consistency
-

- Automated recovery with extensive scripting capability
- Predictable recovery-time objective (RTO)
- Point-in-time (PiT) recovery by taking many different “snapshots” of your data
- Roll back from an instance of data corruption to the last good snapshot without copying all of the data
- An easy to use, secure, centralized management GUI connects to the Safeguard 30m components from anywhere IP access is available
- Software and hardware upgrades do not disrupt operations
- The entire system operates outside of the server-SAN-storage path (out of band)
- Easy to deploy
- An intuitive ‘wizard’ connects Safeguard 30m to MSCS
- You pay only for the data you protect
- Built in data compression and coalescing

### **Microsoft Cluster Service (MSCS)**

Windows Server 2003-based server clusters provide failover support for back-end applications and services that require high availability and data integrity. These back-end applications include enterprise applications such as databases, file servers, enterprise resource planning (ERP) systems, and messaging systems

### **The Solution**

The best solutions in any genre are those that combine elegance, simplicity, stability and ease of execution. All these qualities come together with Oracle Fail Safe and Unisys SafeGuard 30m. Independently, these solutions are powerful tools in the DR space. Together, they combine to provide the premier DR solution stack for Oracle Database customers on Windows.

Core to SafeGuard 30m is its non-intrusive architecture. Data can be intercepted either at the database or the machine level or can be implemented completely at the SAN level. The IO write is captured at the primary site via a splitter driver by the SafeGuard 30m appliance and transmitted to the target site appliance. The write is then acknowledged and written to the target side SAN (see Figure 1).

---

## Unisys SafeGuard 30m Replication Appliances

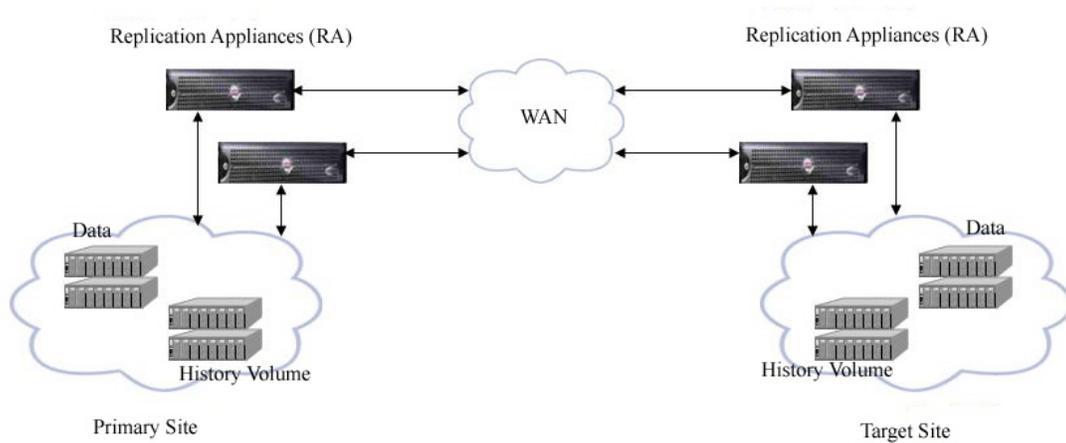


Figure 1

Unisys worked with Microsoft to develop the SafeGuard 30m solution. This solution allows for seamless clusters across thousands of kilometers. Unisys and Microsoft have to date certified SafeGuard 30m at a fail over distance of 3000 miles (see Microsoft certification link below)

<http://www.microsoft.com/windows/catalog/server/default.aspx?subID=22&xslt=detail&pgn=e33aad04-3b7a-3838-953a-bcbb6b63e639>

Oracle Fail Safe completes the stack with an easy to use MSCS-aware software solution for Oracle. When the database fails over to the target node thousands of miles away, Oracle Fail Safe takes over, once SafeGuard 30m has acknowledged the node is in sync.

## High Level Configuration

### Configure the SafeGuard 30m appliance at the primary and target locations

SafeGuard 30m hardware consists of two redundant Replication Appliances (RAs) clustered at the primary and target locations. (see Figure 1)

Configuring the RA at both locations involve:

- SAN
  - Each appliance configured with dual HBAs.
  - Zoning
    - Each RA has a zone to all storage controllers that the server uses as related to the database storage and RA history volume.
    - Zoning Configuration
      - Primary-RA-to-RA-Target
      - Server-to-RA
      - Server-to-Storage
      - RA-to-storage
  - LUNs (Note naming conventions should be identical on both nodes)
    - Create required MSCS LUNs on both nodes (quorum).
    - Create appropriate LUNs on primary and target node designated for replication ('replication pairs').
    - Create consistency groups as required\*.
    - Create history volumes LUN on both nodes\*\* to store change data on the target site.
- Network (redundancy as required)
  - Local Area Network for management of RA, Active Directory, DNS and MSCS requirements.
  - Safeguard 30m requires three VLANs between primary and secondary locations. The first is used for replication traffic, the second is used for user traffic and the final is the MSCS heartbeat.
  - DNS,NTP and DHCP server entries
- Unisys SafeGuard 30m software installation (installed after MSCS installation and configuration)
  - Install Global Recovery Sentinel (GRS) on MSCS cluster
  - Create a GRS resource in each MSC resource group the contains a replicated volume
  - Add appropriate physical disk dependencies to GRS resource(s)
  - Additional configuration includes
    - Activating licenses, setting policies, enabling consistency groups, configuring splitters etc.

\* Consistency groups logically map replication pairs and history volumes.

\*\* History volumes hold the changed blocks reducing impact to the primary

See Unisys Planning and Installation Guide Release 2.2 for details.

---

## **Configure MSCS at the primary and target machines.**

See Unisys Planning and Installation Guide Release 2.2 for details

## **Configure Oracle Fail Safe components at primary and target machines.**

Once SafeGuard 30M and MSCS are configured:

- Install Oracle Database software on a local drive on every node
- Install Oracle Fail Safe software on a local drive on every node and reboot
- Launch Oracle Fail Safe Manager and perform Verify Cluster
- Validate the configuration through Fail Safe's sample database feature
  - Create the sample database by going to the **Resources** menu item, and choose **Create Sample Database**
  - Add the database to a group with a virtual address. Click on **Resources** menu item, and choose **Add to Group**.
- Create customer database and configure for high availability.

## **Testing Overview**

Upon completion of system configuration, testing began at the Unisys / Oracle Center of Excellence (COE) in Pleasanton, CA. The test environment simulated a real life DR scenario implemented over thousands of kilometers. (See Figure 2)

### Test 1: Simple Failover and Failback

Database and tables were loaded for failing over MSCS via cluster management services. With tables updating, the switch was made and the stack began the work. MSCS signaled the failover, then SafeGuard 30m completed moving all the data from the history volumes and applied the changes to the target database. SafeGuard 30m then activated MSCS on the target node, thus triggering Oracle Fail Safe to bring up Oracle Database and services. The data changes were then checked at the target site and confirmed for accuracy. Using the same methodology, failback was tested and worked flawlessly on every execution.

### Test 2: Pulling the Plug

The system was running as originally configured with database and tables loaded. The update scripts were put into action. The primary ES7000 server was brought down hard, simulating a complete loss at the primary site. Safeguard 30m completed the transition to the target cluster, signaling MSCS. Fail Safe again brought the database and services up. The test executed successfully and was repeated for failback to the primary server with the same results.

---

Both tests took less than four minutes to complete. The tests were run multiple times, and succeeded flawlessly each time.

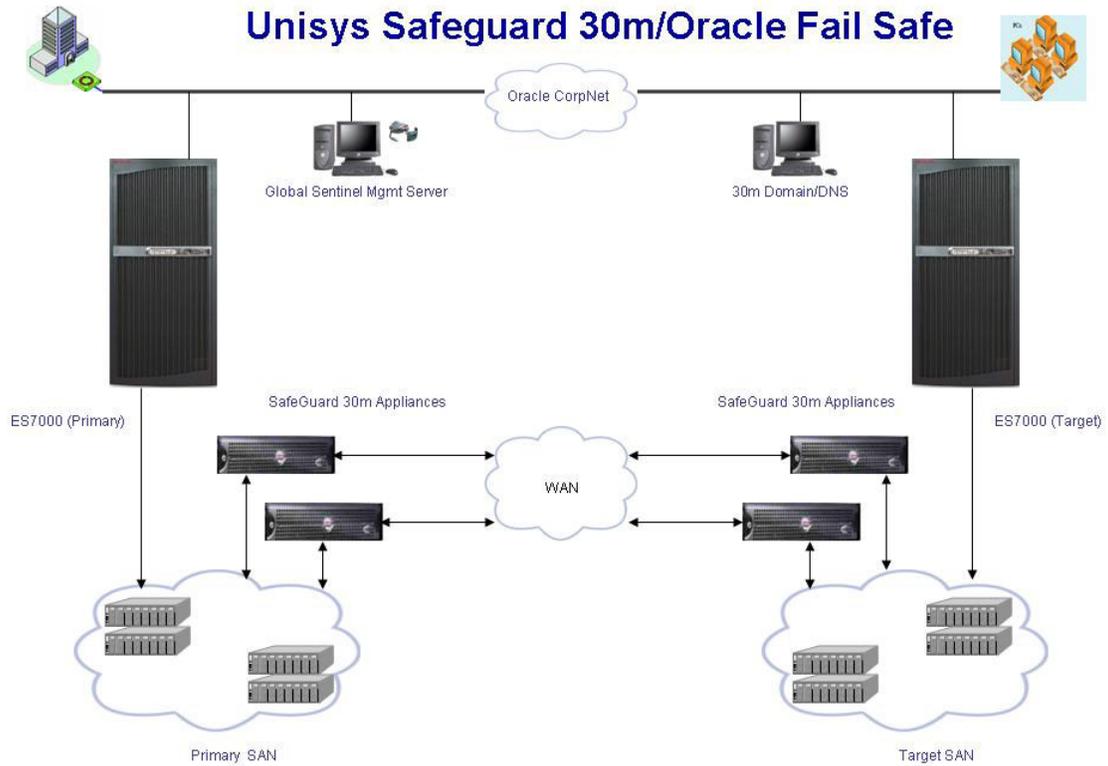


Figure 2

## **System and Software Requirements**

### **Oracle Fail Safe**

For the purpose of this white paper, Oracle Fail Safe version 3.3.4 was used.

Oracle Fail Safe supports any of the following Windows operating systems:

- Microsoft Windows Server 2003 (32bit, 64bit Itanium, 64bit AMD64\EM64T)
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

### **Unisys SafeGuard**

SafeGuard 30m supports any of the following Windows operating systems:

- Microsoft Windows Server 2003, Datacenter Edition Service Pack 1 (32-bit and 64-bit)
- Microsoft Windows Server 2003, Enterprise Edition with Service Pack 1 (32-bit and 64-bit)
- Microsoft Windows Server 2003, Datacenter Edition (32-bit and 64-bit)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit and 64-bit)
- Microsoft Windows 2000 Advanced Server (Service Pack 4)
- Microsoft Windows 2000 Datacenter Server (Service Pack 4)

Unisys supports a wide range of hardware and storage solutions with SafeGuard 30m. Please contact your Unisys representative or email: [Oracle.COE@unisys.com](mailto:Oracle.COE@unisys.com)

---

## **Additional Documentation and Links**

Unisys SafeGuard 30m homepage

[http://www.unisys.com/products/solutions\\_infrastructure/business\\_continuance/30m\\_solution.htm](http://www.unisys.com/products/solutions_infrastructure/business_continuance/30m_solution.htm)

Unisys SafeGuard 30m whitepaper

[http://www.unisys.com/eprise/main/admin/corporate/doc/SafeGuard\\_30m\\_Architecture\\_Overview\\_Final.pdf](http://www.unisys.com/eprise/main/admin/corporate/doc/SafeGuard_30m_Architecture_Overview_Final.pdf)

Oracle Fail Safe software download site:

<http://www.oracle.com/technology/software/tech/windows/failsafe/index.html>

Oracle Fail Safe documentation download site:

<http://www.oracle.com/technology/documentation/failsafe.html>

Microsoft MSCS 2003 homepage

<http://www.microsoft.com/windowsserver2003/technologies/clustering/default.aspx>

Microsoft SafeGuard Certification

<http://www.microsoft.com/windows/catalog/server/default.aspx?subID=22&xslt=detail&pgn=e33aad04-3b7a-3838-953a-bcbb6b63e639>

### **Contact Information:**

For additional information regarding the Unisys SafeGuard 30m and Oracle Fail Safe solution please email your request to:

[Oracle.COE@unisys.com](mailto:Oracle.COE@unisys.com)

Authors: Ken Young, Yee Chin, Sam Bohlin, Haruko Matsuda, Steve Siri, Rick Buchanan, Jereme Nielsen

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. All other product and service names mentioned may be trademarks of their respective owners.

Copyright © 2006 Unisys Corporation  
All rights reserved.

---

