Implementation Guide

XFRACAS

Version 2020

ReliaSoft

XFRACAS 2020 Implementation Guide

Contents

XFRACAS Implementation Guide

This document provides instructions to implement ReliaSoft XFRACAS by HBM Prenscia for your organization. This will require:

- IT support to prepare the database and web server(s) and install the website.
- Practical decisions from the individual(s) who will configure the site to meet your organization's particular needs.

To learn more about configuration options, see the XFRACAS admin help.

1 XFRACAS Architecture

XFRACAS is a web-based application that serves the needs of engineering teams of any size. Based on the .NET Framework, it is designed to be n-tier, scalable, distributable, robust and able to be deployed across multiple servers or on a single computer.

1.1 Server Requirements

If you plan to host the database and website on the same server, you will need the following:

- Windows 2008 R2 or newer
- .NET 4.6
- IIS with support for serving ASP.NET
- SQL Server 2008 or newer OR Oracle 10g or newer (32-bit and 64-bit versions of all, full version only)

If Microsoft Office is installed, it must be 64-bit.

1.2 Client Requirements

Once the website has been implemented, users can access it with any browser that supports the following doctype:

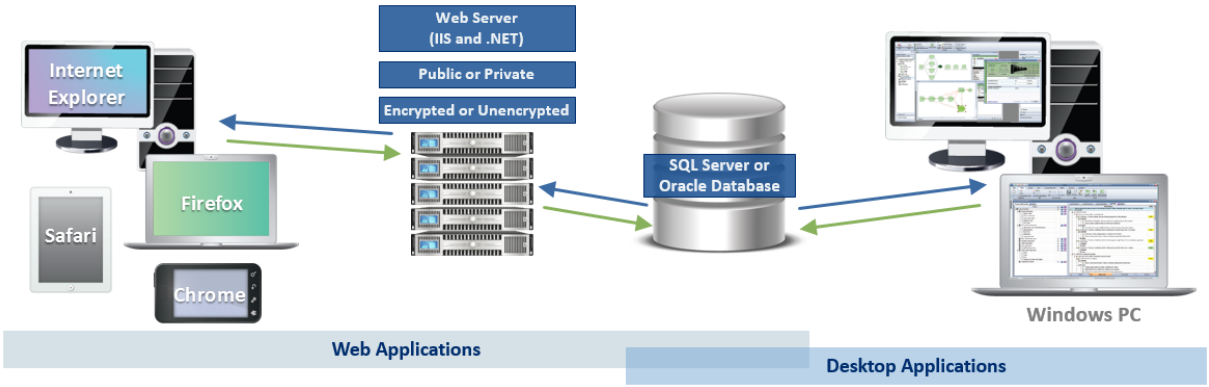
```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

This includes most common browsers (such as Internet Explorer, Chrome, Safari and Firefox) that are available for Windows, Mac and tablet operating systems.

NOTE: If you are using Internet Explorer, version 11 is required; earlier versions are no longer supported.

If the site is private (e.g., http://InternalServer/XFRACAS), an application administrator may need to provide instructions for accessing the site on the internal network from mobile devices (e.g., via VPN or some other method).

These are the same requirements as for SEP, which provides web-based access to a variety of metrics and analyses performed in ReliaSoft desktop applications (Weibull++, XFMEA, etc.). Both applications can be deployed together on the same database and web server(s).



2 Plan Your XFRACAS Implementation

Before you begin, the person who will be making practical decisions about how to configure XFRACAS for your organization will need to gather some information to prepare for the initial configuration after the website is installed. The specific configuration steps are discussed in Section 12 on page 21. Minimum data requirements are summarized here to help you plan ahead.

2.1 System-Wide Preferences

You will need to plan ahead for some of the system-wide preferences that are relevant for the initial configuration. Be prepared to answer the following questions:

- Does the website need to use Secure Socket Layer (SSL) support?
- Will the web server be configured for Single Sign-On (SSO) authentication? If so, will it use the default variable (Auth_User) or do you need to configure XFRACAS to recognize a different variable?
- Will you allow users to upload file attachments? If so, will the files be stored in the database or uploaded to the web server?
- What is the port and address for the SMTP server that will be used for e-mail notifications?

For a comprehensive list of all preferences, see "Managing Preferences" in the admin help.

2.2 Entities

XFRACAS can be configured with a single entity (where all users share the same configuration settings and data) or with multiple entities (where each entity has its own separate user permissions, settings and data).

For example, you might choose to create separate entities within XFRACAS if your organization has different business units or functional teams that require the website to be configured for different needs, processes and/or terminology. You may also need separate entities if there's a requirement to segregate some portion of the data.

- The system-wide preferences, companies, contacts and locations will be the same for all entities in the database.

- The user permissions, systems and most configuration options can be managed separately for each entity.

Your XFRACAS license determines the number of entities that you can create for your implementation.

2.3 Users and Security Groups

You will need to compile at least the minimum details for new user accounts. After XFRACAS is installed, you will be able to create user accounts via the website or import details from an XML file or Microsoft Active Directory. The minimum info required for each user includes:

- first name, last name
- domain\username (Windows login)
- e-mail address

You will also need to plan the security groups that new users will be assigned to (e.g., read-only, regular, admin). This is more efficient than assigning permissions individually to each user.

For a comprehensive list of all user categories and permissions, see "Managing Users" in the admin help.

2.4 Systems/Parts/Templates/BOM

You will need to decide how your organization will track incidents. After XFRACAS is installed, you will be able to define system configuration(s) via the website or import the data from an XML or Excel file or from XFMEA/RCM++/RBI.

2.4.1 Generic Template

If you plan to track by part number/version (not serial number) or by process/task, you only need to create generic template(s). This requires the following information:

- At least a number and name for each part (or process)
- How the parts (or processes) are related hierarchically
- User(s) who are responsible for specific parts (or processes) — this is required for at least one item and recommended for all top-level items

2.4.2 Serial Numbers

If you plan to track by specific instances of a part or system (identified by serial number when applicable), you will need to create the following:

- A generic template that identifies the types of parts and responsible users (as described above)
- A serialized configuration for each individual system that you are tracking — this requires a unique serial number at least for each top-level system

Either approach can be used to gather data for analysis in Weibull++, RGA or XFMEA. Serialized systems allow you to track issues for specific customers and collect more accurate reliability data for further analysis. However, such systems can be considerably more complicated to set up and manage.

For more information, see "Managing System Templates" and "Managing Serialized Systems" in the admin help.

2.5 Review Sample Data from Current FRACAS (if Applicable)

If your organization has previously used any other FRACAS systems or processes, you will need to do the following:

- Assemble and review sample data to help identify the specific fields you wish to configure in XFRACAS (e.g., required fields you want to continue to capture, new fields that are currently lacking, etc.).
- Compile any "pick lists" that will be available throughout the site (e.g., modes of operation, fault codes, etc.). You will be able to create these lists via the website or import them from Excel or XML.

For more information, see "Managing Details" and "Managing Lists" in the admin help.

2.6 Contacts, Companies, Locations

If you plan to use the Customer Support interface, you will also need to gather details for any contacts, companies or locations that you want to predefine in the site.

For more information, see "Managing Contacts," "Managing Companies," and "Managing Locations" in the admin help.

3 Prepare the Database Server - SQL Server or Oracle

The ReliaSoft desktop applications, XFRACAS and SEP are all designed to connect with the same database on either SQL Server or Oracle.

If you need to establish a new database, the following considerations apply for preparing the database server. Later, you will use the admin utility to either create the database or connect to an existing one. (*See Section 7 and Section 8*.)

If you are setting up for SQL Server

- Make sure you have the latest version of SQL Server running. To do this, run the following query in Query Analyzer: "Select @@version". This should return a value like "Microsoft SQL Server 2005 - 9.00.3042 (Intel X86)" or "Microsoft SQL Server 2008 R2 - 10.50.1617 (X64)," depending on which SQL Server service pack you have installed.

- Make sure you know the SQL Server Name. This is a local server name or IP address so the IIS machine with the .NET application can connect to the database. These instructions assume that you will use a default instance of SQL Server to host the ReliaSoft database (e.g., SERVERNAME). If not, you must specify the instance when you enter the server name (e.g., SERVERNAME\INSTANCENAME).

If you are setting up for Oracle

For easier support, we recommend installing the SQL Worksheet (available with the Enterprise edition) or Oracle SQL Developer (free to download from the Oracle website).

4 Prepare the Web Server - IIS

NOTE: XFRACAS cannot be installed on a server running Windows 2012 R2 if the server has Active Directory or DNS services installed.

To prepare the web server prior to installing XFRACAS, make sure the IIS Web Server role and services are installed. In addition, if applicable, prepare for SSL protection.

4.1 IIS Roles and Features

Install the Web Server (IIS) role (if it is not already installed) and make sure the following role services are also installed. (*Instructions follow this table for Windows 2016, 2012 and 2008.)*

To use the XFRACAS web service, you must also make sure **HTTP Activation** is enabled for the .NET Framework (under Features).

	Windows 2016/2012	Windows 2008
Web Server		
Common HTTP Features		
Default Document	x	x
Directory Browsing	x	x
HTTP Errors	x	x
Static Content	x	x
Health and Diagnostics		
HTTP Logging	x	x
Custom Logging	x	x
Logging Tools	x	x
Request Monitor	x	x
Performance		
Static Content Compression	x	x
Dynamic Content Compression	x	x
Security		
Request Filtering	x	x
IP and Domain Restrictions	x	x
Windows Authentication	x	x
Application Development		
.NET Extensibility		x
.NET Extensibility 4.5 or 4.6	x	
Application Initialization (if Windows Server 2016)	x	
ASP	x	x
ASP.NET		x
ASP.NET 4.5 or 4.6	x	
ISAPI Extensions	x	x
ISAPI Filters	x	x
Server Side Includes	x	x
Management Tools		
IIS Management Console	x	x

On Windows Server 2012 or 2016

Note that if you do not already have the required version of the .NET Framework installed, you will need to have the operating system installation media available when you install the Web Server (IIS role). The required file is in the sources/sxs folder.

1. Open the Server Manager.
2. Click the **Manage** menu, choose **Add Roles and Features** and proceed through the wizard.
3. On the **Server Roles** page, select **Web Server (IIS)**.
   a. *If the role is already installed, expand the node, review the services that are already installed and select additional services if applicable.*
   b. *If the role is not already installed, accept any prompts to install required features and proceed to the **Web Server (IIS) > Role Services** page where you can select the services you need to install.*
4. On the **Features** page, select **HTTP Activation** under .NET Framework Features > WCF Services for the version of .NET you are using.
5. At the end of the wizard, click **Install**.

On Windows Server 2008

1. Open the Server Manager.
2. If the Web Server (IIS) role is not installed, view the **Roles** page and, under **Roles Summary**, click **Add Roles**. Follow the wizard to install the role and services.
3. If the Web Server (IIS) role is already installed, view the **Roles > Web Server (IIS)** page. Under Role Services, review the services that are already installed. If you need to add service(s), click **Add Role Services** and follow the wizard.
4. On the **Features** page, select **HTTP Activation** under .NET Framework Features > WCF Activation for the version of .NET you are using.

4.2 SSL Certificate

If you want the website to use HTTPS for secure communication (SSL/TLS), you must have a digital certificate. Later, you will use this certificate to create the binding for the site. (*See Section 9.5 on page 13*.)

If you don't purchase a third-party certificate, you can create your own via another method, such as by generating a self-signed certificate using IIS Manager or using the Active Directory Certificate Services role installed on the server.

5 Establish a Service Account for the Application

We recommend establishing a service account (e.g., "SVC_XFRACAS") that the XFRACAS website will run as on the web server (IIS, accessing files on the server, DIU service, etc.).

If the ReliaSoft database is on SQL Server, this account will also be used to connect to the database and must meet the following requirements:

- It must be an Active Directory account (if the application is running on a different machine from SQL Server).

- Ideally, it should have a password that does not expire (recommended).

- If the database is on SQL Server, a user should be assigned to a public server role, with at least the **db_datareader** and **db_datawriter** roles for the ReliaSoft database. *(If the database does not yet exist, you will need to add the roles via SQL Server after you create it in Section 7.)*

6 Install the Website and Activate the License

After you have prepared the database and web server(s), you can log in to the web server as an administrator and perform the following steps. User Account Control (UAC) can either be left on or turned off for this installation.

1. Run the XFRACAS setup (e.g., **XFRACAS19.exe**) and follow the steps in the wizard to create the website and install the activation and admin tools.

2. From **Start**, search for **"**XFRACAS 2020 Activation**"** then run the product activation tool and follow the steps to activate your license.

The license will be registered to a specific e-mail address, which will receive the notification required to activate it. This will be the same address for all stages of license usage from development/staging to production. Choose an address that can be accessed by someone who changes the hardware on the server. If the hardware changes for any reason, the license must be reactivated to get XFRACAS back up and running.

7 Create the ReliaSoft Database (if Applicable)

If you already have a database that the website will use, skip ahead to Section 8.

7.1 Plan for Your Implementation

To create a new ReliaSoft database, you'll need to run the XFRACAS admin utility (which resides on the web server) from a Windows user account that has the following permissions:

- For SQL Server implementations, you must be able to create objects under the default database owner (dbo) schema. Be prepared to specify the server and database names.

- For Oracle implementations, you must be able to create a database. Be prepared to specify a port, host, service name or SID, schema and password.

7.1.1 Created Admin Accounts

During this process, the admin utility automatically creates two new user accounts for you—one for SEP and ReliaSoft desktop applications and another for XFRACAS—that use your Windows login and provide full admin permissions for those applications. The XFRACAS account is a special, IT/admin-only account for tasks such as updating database tables, rolling out new permissions to other admin users, performing

bulk data imports (so imported records are not assigned to a specific user), etc. It is invisible to regular users and does not count against the number of users allowed by your XFRACAS license.

7.1.2 Future Upgrades and Ongoing IT / Maintenance Tasks

We recommend performing upgrades and ongoing IT/admin tasks from the same Windows account that you used to create the database (which, by default, has the database permissions required for all ReliaSoft applications). If you cannot identify a single person in your organization who will be available to perform these tasks—both now and in the future—we recommend establishing a shared service account for this purpose.

Note that, even if you created the database from a personal user account, you can still create a shared account to use for future upgrades:

- For SEP and desktop applications, use the admin utility to create additional accounts that are assigned to the "admin" security group.
- For XFRACAS, use the website's **Admin** tools (**Admin > Configure > Security > Users**) to change the domain\username of the account that was created automatically.

Instructions for upgrading XFRACAS are provided in the Install Update guide that comes with your upgrade package.

7.2 Create or Upgrade the Database

1. Log in to Windows with an appropriate account for your implementation. (Alternatively, you can run the admin utility as that account in step 2).
2. From **Start**, search for "XFRACAS 2020 Admin" and open the admin utility.
3. Click either **New Enterprise Database** or **Upgrade Enterprise Database** and enter the details required to create or upgrade the database. For custom SQL Server or Oracle connections, you will need to provide a valid connection string.

7.3 Assign Roles in SQL Server for Application Service Account

Finally, if you created a new database on SQL Server, you must make sure the application service account (i.e., the account that the application will use to connect to the database) has the required roles assigned in SQL Server. For requirements, see Section 5 on page 7.

8 Update the XFRACAS Configuration File

After you have installed the website, activated the license and established a database, the next step is to update the configuration file on the web server.

From **Start**, search for "XFRACAS 2020 Admin" and open the admin utility. Then click **Update XFRACAS Configuration File**.

1. On the **Connection** tab:

   - **Connection Info** - Enter the required details for the database that the application will connect to. If you used the admin utility to create the database, the connection info will appear in the fields automatically. If the default connection string doesn't work for your implementation (e.g., you want to deploy XFRACAS on Azure, use SQL Authentication, etc.) you can enter a custom connection string.

     Select **Encrypt Connection String** if you want to hide the connection string information within the web configuration file.

   - **Application Service Account -** Enter the credentials for the service account that XFRACAS will run as on the web server (for IIS, accessing files on the server, the DIU service, etc.). If the ReliaSoft database is on SQL Server, this account will also be used to connect to the database. (See Section 5 on page 7.)

     Select **Encrypt Impersonation Identity** if you want to hide the credentials within the web configuration file.

     NOTE: If you choose to use encryption, the Authentication feature in IIS Manager will be unable to read the resulting web.config file. You may see an error such as "Error: Configuration section encryption is not supported." If you need to use this feature in IIS Manager, you can temporarily remove the encryption.

2. On the **Settings** tab:

   - **Command timeout** sets how long the application should wait for a command to finish. Typically, this will not need to be changed, but if you have custom SQL queries that run longer than the standard 120 seconds, you can increase this value.

   - **Request timeout** sets how long IIS waits for a request to the application to finish processing. Typically, this will not need to be changed, but if you are importing large XML files into the system and they time out during import, you can extend this to a larger value.

   - **Web Service Maximum File Size** sets the maximum size for files inserted into the import queue by the XFRACAS web service. This is set during installation to 10485760 bytes (or ~10 MB).

   - **Upload Maximum File Size** sets the maximum file size that can be uploaded to the server. This is set during installation to 10485760 bytes (or ~10 MB).

   - **Content-Security-Policy Header** determines which types of dynamic resources are allowed to load on the site. This policy is required to detect and prevent cross-site scripting (XSS) and other code-injection attacks. Typically, it will not need to be changed; however, if you decide to modify this policy, you *must* include the following directives to ensure that the site functions properly:

     - `'unsafe-inline'`
     - `'unsafe-eval'`

- For a SQL Server implementation,

  - Select **Encrypt communication** to encrypt the connection between the application and the database.

  - Select **Trust server certificate** if the server has a self-signed certificate.

  NOTE: **To encrypt the connection for an Oracle implementation, you must set the encryption type to either "requested" or "required" for the Oracle database. For more information, please consult the Oracle documentation (e.g., https://docs.oracle.com/cd/B19306_01/network.102/b14268/asoconfg.htm#i1007808).**

9 Perform Post-installation Steps (if Applicable)

After installation, you may need to configure additional settings to fit your particular implementation.

To make changes to address OWASP security concerns, see Section 10.

9.1 .NET Temporary Folder Permission

If the .NET framework was pre-existing on the IIS server (i.e., if it was already installed and not installed via the XFRACAS installation), you may encounter a server error the first time you attempt to access the website (e.g., "Could not load file or assembly 'DevExpress.Charts.v16.1.Core' or one of its dependencies. Access is denied.").

If this happens, you will need to give full permissions for the .NET temporary folder (C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.Net Files\) to the account that XFRACAS runs as (specified in the XFRACAS configuration file). You may need to take ownership of this folder before you are able to do this.

9.2 Release and Recycle Memory

For large systems or systems with a high transactional load, an "Out of Memory" error can occur when the request for pages exceeds the system's capability to release and recycle the memory with the default IIS settings. The settings provided below will force IIS to recycle the memory usage and handle it better so that the "Out of Memory" error does not occur. Note that overly aggressive settings can slow the response of the system. Typically, memory is recycled when the application pool and server are not busy. Forcing memory to recycle more often can consume processor cycle time when the application is still busy, thus slowing system performance. The following settings have been tested to prevent the error from occurring, while posing the minimum possible impact on performance.

1. In the **Connections** pane of the IIS Manager, click **Application Pools**.

2. Right-click the system's application pool and choose **Recycling** on the shortcut menu.

3. In the Application Pool Recycling Settings window that appears, specify the following settings and then click **Next**:

   - In the Fixed Intervals area, select **Regular time intervals** and enter **1740**.

- In the Memory Based Maximums area, select **Private memory usage** and enter **1,024,000**.

4. Select to log the following events and click **Finish**:

   - **Regular time intervals**
   - **Private memory usage**
   - **Unhealthy ISAPI**

9.3 Prepare to Use *.XLSX for Data Import

XFRACAS provides the option to use Excel templates (*.xlsx) to import some types of data, as an alternative to XML. To configure the web server to support this functionality, you must install a 64-bit version of Microsoft Office (2013 or newer) on the web server.

9.4 Folder for Uploaded Files

You can configure the website's Attachment window to store uploaded files on the web server (rather than in the database). If you plan to do this, you must prepare the folder where the files will be stored.

- **Option 1**: Create the folder directly within the website's IIS folder (e.g., C:\inetpub\wwwroot\XFRACAS\uploads).

- **Option 2**: Create the folder in another location on the web server (e.g., D:\storage\xfracas) and then create a virtual directory within IIS.

9.4.1 Create a Virtual Directory

To create the virtual directory for Option 2:

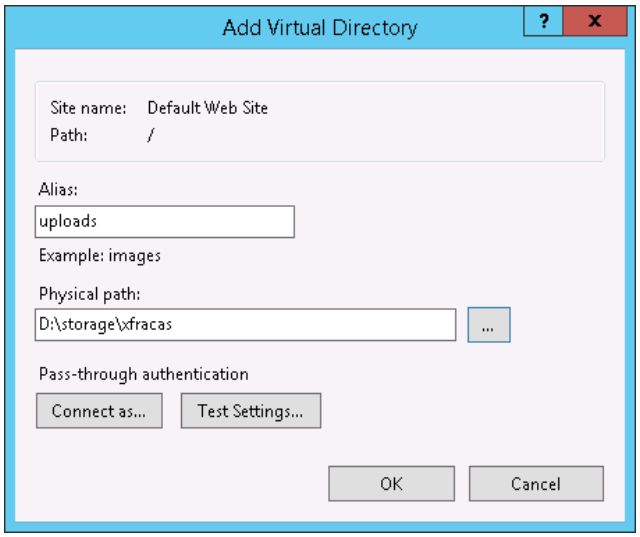
1. In the **Connections** pane of the IIS Manager, click **Application Pools** and either add a new pool or modify the default pool. *Do not modify the "XFRACAS" application pool.*

   - Leave the identity as **ApplicationPoolIdentity**.
   - Set the managed pipeline mode to **Classic**.

2. In the Connections pane, right-click the **Default Web Site** node and choose **Add Virtual Directory**. *This must be under the default web site node; do not create the virtual directory within the XFRACAS website.*

   - Set the directory alias (e.g., "uploads" or "attachments").

- Specify the physical path to the location where the files will be stored.



3. In the Connections pane, click the virtual directory and double-click **Authentication**. Make sure **Forms Authentication** is disabled.

4. In the Connections pane, right-click the virtual directory and choose **Convert to Application**. Select the appropriate application pool and click **OK**.

9.4.2 Test the Configuration

To test, you will need to set the appropriate preferences via the XFRACAS website (see Section 12.1 on page 21), open a record that allows attachments (e.g., incident), upload a file and test the download.

For example, if you created an actual folder called “uploads” within the XFRACAS website, you would use:

Attachments - Uploaded Files Filesystem Prefix	C:\inetpub\wwwroot\XFRACAS\uploads
Attachments - Uploaded Files IIS Prefix	/XFRACAS/uploads

Alternatively, if you created a virtual folder called “uploads” that stores files in another location on the web server (e.g., D:\storage\xfracas), you would use:

Attachments - Uploaded Files Filesystem Prefix	D:\storage\xfracas
Attachments - Uploaded Files IIS Prefix	http://servername/uploads

9.5 HTTPS for Secure Communication

9.5.1 Enable HTTPS

If you want to use HTTPS for secure communication (SSL/TLS) and you already have a certificate for the website (as discussed in Section 4.2 on page 7), do the following:

1. In the **Connections** pane of the IIS Manager, open the **Sites** node under the server name. Click the **Default Web Site**.

2. In the **Actions** area on the right side of the window, click the **Bindings** link and then click the **Add** button in the Site Bindings window that appears.

3. Add a site binding of type https and specify your digital certificate. Close the Site Bindings window.

4. Return to the **Connections** pane and click the **XFRACAS** site.

5. Under IIS, double-click the **SSL Settings** icon. Select **Require SSL** and **Ignore**, then click **Apply**.

9.5.2 Enable TLS 1.2 Protocol for HTTPS (on Windows 2008 or 2012)

If you are using HTTPS for secure communication and you wish to enable TLS 1.2, the same protocol must be enabled for the database server, the web server and .NET on the web server. *(Also note that if you are using a digital certificate, it must be SHA-256 or higher.)*

If your web server and database server are both Windows 2016, the TLS 1.2 protocol will be enabled by default. If either server is Windows 2008 or 2012, add the following registry keys:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\SSL 2.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\SSL 2.0\Client]

"DisabledByDefault"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.0]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.0\Client]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.0\Server]

"Enabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.1]
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.1\Client]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.1\Server]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.2]

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.2\Client]

"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvide
rs\SCHANNEL\Protocols\TLS 1.2\Server]

"DisabledByDefault"=dword:00000000
```

9.6 SSO Authentication Blocks Print Preview or Export to XML

XFRACAS's "Print Preview" and "Export to XML" features require DTD files that are installed on the web server. If you have implemented SSO authentication, it may block the website from accessing the DTD files and these features will not respond or will return a blank page.

To address this issue, modify the hosts file on the web server (e.g., C:\windows\system32\drivers\etc\hosts) so the loopback/localhost IP address (127.0.0.1) matches the **XFRACAS Server - IIS Prefix** preference in XFRACAS. For example, if the prefix is "xfracas.servername.com," then you would add the following line in the host file:

```
127.0.0.1 xfracas.servername.com
```

9.7 "ViewState" Errors When XFRACAS is Deployed on Multiple Web Servers

The XFRACAS Configuration File utility enables ViewState encryption and generates a unique machineKey for encryption. If you deploy XFRACAS on multiple web servers that have different machineKeys, it will result in broken images on some chart and dashboard pages, as well as "viewstate" errors in the XFRACAS diagnostic log.

If you are using a load balancer, you may be able to address the issue by setting up *server affinity* at the load balancer such that once a user's web request is tied to a particular server, all requests from that user will continue going to that server.

Alternatively, you can copy/paste the same web.config file onto each of the XFRACAS web servers. You will need to repeat this whenever you change the website configuration.

1. On the primary web server, use the XFRACAS Configuration File utility to set the connection settings and other preferences (as discussed in Section 8 on page 9).

2. After you click **OK** to save the changes, copy the entire file (e.g., C:\inetpub\wwwroot\XFRACAS\web.config) and paste it to replace the file(s) on the other web server(s).

   If you prefer using Notepad (or another application) to manually update the web.config, make sure the machineKey, validationKey and decryptionKey are the same in all files. For example: `<machineKey validationKey="5FC44A043D987BDC849282A0506084F7A3D0952EE5F260D3277F018DFBABD424" decryptionKey="F0522BACBD1E791191F243B08C785B63DBB6E91C5480FE2114793C97BDD8DFA5" validation="AES" decryption="AES" />`

10 Additional IIS Configuration Changes for Enhanced Security

This section provides recommendations to address issues that may be identified if you choose to scan your web server for Open Web Application Security Project (OWASP) security concerns.

For some of the issues listed here, you will need to install the URL Rewrite tool, available at http://www.iis.net/downloads/microsoft/url-rewrite.

10.1 Settings

The tasks performed in the IIS Manager should be done at the default website level (i.e., in the **Connections** pane, open the **Sites** node under the server name and click **Default Web Site**). Alternatively, the model web.config code (see page 19) summarizes the changes made in the IIS Manager.

Note: If you make these changes directly in the web.config file in the root folder for your SEP website, you can skip the steps shown below in italics.

Web Server Default Welcome Page

From the wwwroot directory, remove iisstart.htm, welcome.png and the asp_client folder.

Clickjacking: X-Frame-Options Header Missing

1. *In the IIS Manager Home page, double-click **HTTP Response Headers**.*

2. *In the **Actions** area, click **Add**. Enter **X-Frame-Options** as the name, and **SAMEORIGIN** as the value.*

OPTIONS Method Is Enabled

1. *In the IIS Manager Home page, double-click **Request Filtering**.*
2. *On the **HTTP Verbs** tab, click **Allow Verb** in the **Actions** area and enter **Options** in the Deny Verb window.*

Microsoft IIS Version Disclosure

1. In the following Registry key, create a dWORD entry, DisableServerHeader, and set its value to 1:

   ```
   HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters
   ```

2. In the IIS Manager Home page, double-click **URL Rewrite**.
3. In the **Actions** area, click **View Server Variables**, then click **Add** and enter **RESPONSE_SERVER** in the text box.
4. *Add an outbound rule to rewrite the RESPONSE_SERVER server variable as blank.*
   a. *In the **Actions** area, click **Back to Rules** and then click **Add Rule(s)**.*
   b. *In the Add Rule(s) window, click **Blank rule** in the **Outbound rules** category and click **OK**.*
   c. *Create the outbound rule using the following settings:*
      - *Name: Response Server*
      - *Precondition: None*
      - *Matching scope: Server Variable*
      - *Variable name: RESPONSE_SERVER*
      - *Variable value: Matches the Pattern*
      - *Using: Regular Expressions*
      - *Pattern: .+*
      - *Action type: Rewrite*
      - *Action Properties:*
        - *Value: <leave this field empty>*
        - *Replace existing server variable value: Selected*

ASP .NET Version Disclosure

1. In the IIS Manager Home page, double-click **URL Rewrite**.
2. In the **Actions** area, click **View Server Variables**, then click **Add** and enter **RESPONSE_X-ASPNET-VERSION** in the text box.

3. *Add an outbound rule to rewrite the RESPONSE_X-ASPNET-VERSION server variable as blank.*

   a. *In the **Actions** area, click **Back to Rules** and then click **Add Rule(s)**.*

   b. *In the Add Rule(s) window, click **Blank rule** in the **Outbound rules** category and click **OK**.*

   c. *Create the outbound rule using the following settings:*

      - *Name: x-ASPNet*
      - *Precondition: None*
      - *Matching scope: Server Variable*
      - *Variable name: RESPONSE_X-ASPNET-VERSION*
      - *Variable value: Matches the Pattern*
      - *Using: Regular Expressions*
      - *Pattern: .+*
      - *Action type: Rewrite*
      - *Action Properties:*
        - *Value: <leave this field empty>*
        - *Replace existing server variable value: Selected*

X-Powered-By Header

1. In the IIS Manager Home page, double-click **HTTP Response Headers**.

2. Select the **X-Powered-By** header and click **Remove**.

3. In the IIS Manager Home page, double-click **URL Rewrite**.

4. In the **Actions** area, click **View Server Variables**, then click **Add** and enter **RESPONSE_X-POWERED-BY** in the text box.

5. *Add an outbound rule to rewrite the RESPONSE_X-POWERED-BY server variable as blank.*

   a. *In the **Actions** area, click **Back to Rules** and then click **Add Rule(s)**.*

   b. *In the Add Rule(s) window, click **Blank rule** in the **Outbound rules** category and click **OK**.*

   c. *Create the outbound rule using the following settings:*

      - *Name: X-Powered*
      - *Precondition: None*
      - *Matching scope: Server Variable*
      - *Variable name: RESPONSE_X-POWERED-BY*
      - *Variable value: Matches the Pattern*
      - *Using: Regular Expressions*
      - *Pattern: .+*
      - *Action type: Rewrite*
      - *Action Properties:*

- *Value: <leave this field empty>*
- *Replace existing server variable value: Selected*

Custom Errors

1. In the IIS Manager, open the Configuration Editor.

2. In the **Section** drop-down list, choose **system.web/customErrors**.

3. Set **Mode** to **RemoteOnly**.

10.2 Allowable File Name Extensions

If you have chosen to lock down your IIS by removing the default **Allow unlisted file name extensions** setting, then you must add certain extensions to the allowable list by doing the following:

1. In the **Connections** pane, open the **Sites** node under the server name. Click the **XFRACAS** site.

2. In the Home page, double-click **Request Filtering**.

3. For each of the following extensions, in the **Actions** area, click **Allow File Name Extension** and enter the extension:

.asax	.ashx	.aspx	.axd
.css	.dtd	.gif	.htm
.html	.ico	.js	.png
.xml	.xslt		

10.3 Default web.config Changes

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
        <system.web>
                <customErrors mode="RemoteOnly">
                </customErrors>
        </system.web>
  <system.webServer>
    <httpProtocol>
      <customHeaders>
        <remove name="X-Powered-By" />
                <add name="X-Frame-Options" value="SAMEORIGIN" />
      </customHeaders>
    </httpProtocol>
    <security>
      <requestFiltering>
        <verbs>
          <add verb="OPTIONS" allowed="false" />
        </verbs>
```

```
        </requestFiltering>
      </security>
      <rewrite>
        <outboundRules>
          <rule name="Response Server">
            <match serverVariable="RESPONSE_SERVER" pattern=".+" />
            <action type="Rewrite" />
          </rule>
          <rule name="X-Powered">
            <match serverVariable="RESPONSE_X-POWERED-BY" pattern=".+" />
            <action type="Rewrite" />
          </rule>
          <rule name="x-ASPNet">
            <match serverVariable="RESPONSE_X-ASPNET-VERSION" pattern=".+" />
            <action type="Rewrite" />
          </rule>
        </outboundRules>
      </rewrite>
    </system.webServer>
</configuration>
```

11 Start the DIU Service

The XFRACAS Data Import Utility (DIU) is a service that must run on the web server in order to use any of the following features:

- E-mail notifications that are triggered based on calendar date (e.g., E-mail - Incident Action Due Date, etc.).
- Data imports that have been scheduled to run via the **Data Import** page in the website.

IMPORTANT: If you have a load-balanced environment with multiple web servers, the DIU service should run on only one server.

To start the DIU service:

1. From **Start**, search for “Services” and open the Services window.
2. In the list of local services, right-click **XFRACAS DIU** and select **Properties**.
3. On the **Log On** page, enter the credentials for the account that XFRACAS runs as on the web server (as discussed in Section 5 on page 7).
4. On the **General** page, set the **Startup type** to either “Automatic” or “Automatic (Delayed Start).” Then click **Start** to start the service.

The current status of the DIU service will appear at the top of the Data Import page.

If you need to modify the settings for the DIU service, you can edit Service.xml on the web server. By default, this file is installed in the bin folder for the XFRACAS website (e.g., C:\inetpub\wwwroot\XFRACAS\bin). Typically, this will not be necessary unless you receive specific instructions from ReliaSoft Support.

12 Initial XFRACAS Configuration

After XFRACAS has been installed, you will need to configure it to meet your organization's needs. This section identifies the initial configuration options we recommend to get the site up and running. You can then review the behavior of the system and adjust the settings to achieve the desired behavior for your organization. This may take several iterations to determine the settings that meet your particular needs.

TIP: If you plan to configure XFRACAS with more than one "entity," (where each entity has its own separate user permissions, settings and data), it is important to consider the needs of all entities before you configure the first one. The first entity is typically used as a template for standard operating procedures (SOPs) that need to be the same across all entities.

12.1 Preferences

For the initial configuration, we recommend to set at least the following preferences. For a comprehensive list of all preferences, see "Managing Preferences" in the admin help.

12.1.1 System-Wide Preferences

- **HTTPS for Links**

  SSL Server Mode Required: If True, the website will use https (rather than http) when building links. Before you enable this option, make sure the IIS web server is configured properly for SSL/TLS (as discussed in Section 9 on page 11).

- **SSO Authentication:** XFRACAS uses Windows authentication by default. Alternatively, if your web server is set up to support SSO authentication, XFRACAS will check for the **Auth_User** variable by default. If your SSO method has been configured to use a different variable, set the following preferences:

  - **Single Sign-On (SSO) Authentication Enabled:** If True, your web server is set up for SSO authentication and uses a variable other than **Auth_User**.

  - **Single Sign-On (SSO) Server Variable:** This is the alternative variable that XFRACAS needs to check for SSO authentication.

  The admin/TESTSSO.aspx page on the website provides additional details to help with troubleshooting this configuration.

- **Location of the XFRACAS Website**

  - **XFRACAS Server - Filesystem Prefix:** The absolute path on the web server where the website's IIS folder is installed (e.g., C:\inetpub\wwwroot\XFRACAS\).

- **XFRACAS Server - IIS Prefix:** The path that can be used to build links to pages within the XFRACAS website (e.g., servername/XFRACAS or 10.0.0.2/xfracas).

- **Link to SEP (if Applicable)**
  - **Display SEP Command:** If True, the XFRACAS ribbon will include a link to your organization's SEP web portal.
  - **SEP Server - IIS Prefix**: The path that can be used to build the link to the SEP web portal (e.g., servername/SEP).

- **Upload Files for Attachments**
  - **Attachments - Allow Uploaded Files:** If True, the Attachments window will include the option for users to upload files. The files may be stored in the database or uploaded to a designated folder on the web server, depending on how you configure the related preferences.
  - **Attachments - Store Uploaded Files in Database:** If True, files will be stored in the database. If False, files will be stored in a designated folder on the web server.
  - **Attachments - Uploaded Files Filesystem Prefix:** If applicable, this is the absolute path to the folder on the web server where uploaded attachments will be stored (e.g., C:\inetpub\wwwroot\XFRACAS\uploads\ or D:\storage\xfracas). For requirements and instructions to prepare this folder, see Section 9.4 on page 12.
  - **Attachments - Uploaded Files IIS Prefix:** If applicable, this is the path that will be used to build links to download files that were saved on the web server.
    - If you are using an actual folder within the website, enter a relative path (e.g., XFRACAS/uploads).
    - If you are using a virtual directory created in IIS, enter an absolute path (e.g., http://servername/uploads).

- **SMTP Server for E-mail Notifications**
  - **SMTP Server:** The address of the mail server that will be used for sending e-mails.
  - **SMTP Port:** The port used to connect to the SMTP server.
  - **SMTP Connection Timeout:** The amount of time, in seconds, before the connection to the SMTP server times out when sending e-mails.

12.1.2 String Preferences

Verify that the date formats (**XFRACAS - Date Format - Long** and **XFRACAS - Date Format - Short**) match the culture setting within IIS so dates shown in charts can be displayed correctly.

12.2 Users and Security Groups

You will need to create security group(s) and individual accounts for XFRACAS users.

Remember that the user who created the ReliaSoft database will have a special IT/admin-only account that will have full admin permissions within the website (as discussed in Section 7 on page 8), but you may also choose to provide full permissions for at least one regular website user as well. You cannot assign an admin permission to other user(s) unless you already have that permission yourself.

For more information, see "Managing Users" and "Managing Security Groups" in the admin help.

- Use the **Security Groups** page to create sets of permissions and categories that can be assigned to individual users. A user can be assigned to more than one group if needed. The following groups are created by default in a new database, but you can replace or modify them to meet your particular needs:
  - USER - contains basic permissions to use the site (e.g., create incidents, access reports, etc.).
  - SUPERUSER - contains basic permissions as well as some more advanced functionality (e.g., close problems, make reports public, etc.)
  - ADMIN - contains just the administrative permissions (e.g., add/modify users, work with system configurations, add/remove detail fields, etc.)
- Use any of the following methods to create individual user accounts:
  - Use the **Users** page to create one account at a time. To save time, you may wish to create new accounts by duplicating a similar existing account.
  - Use the **Active Directory** page to import users from Microsoft Active Directory.
  - Use the **Data Import** page to import user account details via XML.
    - Download a sample template: XFRACASXMLTemplate_UserExample.xml
    - Consult the full Document Type Definition (DTD) installed on the web server (e.g., C:\inetpub\wwwroot\XFRACAS\DTD\): User.dtd
- Confirm that users are able to log in to the website (i.e., they can access the main XFRACAS page).

12.3 Systems/Parts

You can use any of the following methods to define the systems/parts that will be used for tracking.

For more information, navigate to "Managing System Templates" and "Managing Serialized Systems" in the admin help.

- Use the **Template** page or the **Serialized** page to create one system or part at a time.
- Use the **Data Import** page to import part details via XML or Excel.
  - Download a sample template/example:
    - XFRACASXMLTemplate_PartsExample.xml
    - XFRACASImportTemplate_Parts.xlsx and XFRACASImportTemplate_Parts_Example.xlsx
  - Consult the full Document Type Definition installed on the web server (e.g., C:\inetpub\wwwroot\XFRACAS\DTD\): **System.dtd**
- Choose **System > Template > XFMEA Import** to import an existing system hierarchy created in ReliaSoft XFMEA, RCM++ or RBI.

  If you want to import failure modes from any existing FMEAs, select **Import failure modes with template**.

12.4 Map Existing Records (if Applicable)

If you need to import records from an existing system, you must first identify how the data will be mapped to available record types in XFRACAS. For example, “trouble tickets” in your previous system might be mapped to “incidents” in XFRACAS.

Note that within XFRACAS:

- Each **Project** can contain multiple Problems.
  - Each **Problem** can contain multiple Incidents.
    - Each Incident can contain multiple Failure Analysis records.

Projects, Problems and Incidents can be created independently of each other and relationships can be created between them afterwards.

A Failure Analysis record can only be created from an existing Incident.

Customer Support records (CSIs) are applicable only if you are tracking serialized systems. Each CSI can have multiple associated Incidents.

12.5 Detail Fields

You can use the **Details** page to manage most of the configurable fields for XFRACAS records. Select which fields you want to capture for each record type (incidents, problems, etc.) and configure them to meet your organization’s needs.

If you will need to import records from an existing system, make sure all relevant fields from your existing records can be mapped to fields in XFRACAS. You can add new details if needed. For example, if the

original “trouble ticket” record captured the number of people affected, you could add a numeric detail called “People Affected” to the XFRACAS Incident page.

For more information, see “Managing Details” in the admin help.

12.6 Criticality Fields

If you want to use calculated criticalities in Incident and/or Problem records, use the **Criticality** page to configure the fields. Then use the **Preferences** page to choose which fields to display and to configure the calculation formulas.

- Boolean Preferences (choose which fields to display)
  - Incident - Display Actual Criticality
  - Incident - Display Potential Criticality
  - Problem - Display Criticality

- String Preferences (define the formulas)
  - Criticality - Incident Actual
  - Criticality - Incident Potential
  - Criticality - Problem Base CIN
  - Criticality - Problem Current CIN

For more information, see “Configuring Criticality Metrics” in the admin help.

12.7 Lists

You can use the following methods to review and populate the “pick lists” that are used throughout the website.

- Use the **Lists** page to manage standard lists, as well as any custom lists that you added via the Details page.

- Use the **Data Import** page to import list data via XML or Excel.

  - Download a sample template: XFRACASImportTemplate_Issues.xlsx and XFRACASImportTemplate_Issues_Example.xlsx

  - Consult the full Document Type Definition installed on the web server (e.g., C:\inetpub\wwwroot\XFRACAS\DTD\): **Issue.dtd**

For more information, see “Managing Lists” in the admin help.

12.8 Action Categories

You can use the **Action Management** page to review and modify the sub-categories that will be available for different kinds of actions throughout the website. For example, when a user creates an action from within the Incident page, the main category is “Incident Action.” If you want to organize those actions into smaller groups, you can define additional subcategories (e.g., “Investigation,” “Repair,” etc.). Sub-categories are optional and can be added at any time.

12.9 Contacts, Companies and Locations

If applicable, you can use either of the following methods to define the contacts, companies and locations that are referenced in Customer Support (CSI) records.

- Use the **Contacts**, **Companies** and **Locations** pages to create one record at a time.
- Use the **Data Import** page to import data via XML. Consult the full Document Type Definitions installed on the web server (e.g., C:\inetpub\wwwroot\XFRACAS\DTD\): **Company.dtd** and **Address.dtd**

For more information, see "Managing Contacts," "Managing Companies," and "Managing Locations," in the admin help.

12.10 Import Records from Existing System (if Applicable)

If you need to import records from an existing system, make sure you have mapped the data to relevant XFRACAS records and data fields (as discussed in Section 12.4 and Section 12.5).

Then you can use the Data Import page to import the records via XML. There are two ways to get an appropriate XML template:

- Go to the page in XFRACAS and export a sample XML file.
- Consult the full DTDs installed on the web server (e.g., C:\inetpub\wwwroot\XFRACAS\DTD): Incident.dtd, Problem.dtd, Project.dtd FailureAnalysis.dtd and UnitCommissioning.dtd.

For more information, see "Data Import Page" in the admin help.

13 Other Configuration Options

- Use the **Resource Editor** page to change any text values in XFRACAS that don't match your organization's needs.
- Customize static pages that need to be edited directly on the web server. These include:
  - **What's New** page (Whatsnew.html) is installed in the website's main folder.
  - **General Error** page (GeneralError.aspx) is installed in the website's main folder.
  - **Terms of Use Agreement pages** (Agreement.aspx and AdminAgreement.aspx) are installed in the website's main folder (displayed when the user visits any of the regular user pages) and in the Admin folder (displayed when the user visits any of the admin pages). To enable this feature, set the **Terms of Use Agreement Page Required** preference to True.
  - **Description Criteria Link** pages are installed in the website's Tips folder (e.g., C:\inetpub\wwwroot\XFRACAS\Tips). If you want to use a file stored in a different location

instead, edit the relevant link on the **Preferences** page under **URL Preferences** (e.g., "Incident - Actual Criticality Tips," etc.).

- **Print Preview XSLT files** are installed in the website's XSLT folder (e.g., C:\inetpub\wwwroot\XFRACAS\XSLT). These configure the "Print Preview" output for an incident, failure analysis, problem, project or CSI. If you want to use a file stored in a different location instead, edit the relevant link on the Preferences page under URL Preferences (e.g., "Incident - Print Preview Style Sheet," etc.).

- Use the **Report Viewer** page to modify the sort orders and hide/display attributes of specialized queries.

- Use the **Report Builder** and **Dashboard Designer** pages to create and deploy to users (i.e., make public) custom queries, custom standard reports, custom charts or custom dashboard layouts, if needed.

- Use the **Create Link** and **Create Announcement** pages to create any public links or system-wide announcements that are needed.

14 Stored Procedures

14.1 Time Metrics

When creating a serialized incident, users can click the **Operational History** link to select from previously entered time metrics (values) for that serial number. By default, this list consists of time values contained within XFRACAS for the serial number. If desired, you can instead pull time value data from another database for use during incident creation. XFRACAS supports this by attempting to call a stored procedure in the XFRACAS database on the fly. *If you want to use this procedure for your XFRACAS implementation, please request assistance from ReliaSoft Support to enable the "XFRACAS - Run Stored Procedure for System Time Metrics" preference.*

The procedure is named **XFRACASGetTimeMetrics** and has four arguments. The first is an incoming argument for the serial number (a string) and the second through fourth are return arguments (numbers) to store the data for the three time metrics. In the default XFRACAS system, the three time metrics are set to 0. Once the stored procedure is modified, the **return_value** variable must be set to 1 in order for the values to be used.

As an example, below is a very simple Oracle stored procedure that returns values from tables named SYSTEM_HOURS, SYSTEM_STARTS and SYSTEM_KWRUNHRS:

```
Create OR Replace PROCEDURE XFRACASGetTimeMetrics
(
SnIN NVARCHAR2;
tm1OUT NUMBER,
tm2OUT NUMBER,
tm3OUT NUMBER
RETURN_VALUE OUT NUMBER)
AS
BEGIN
tm1 := SELECT hours FROM SYSTEM_HOURS WHERE serial_num = SN;
```

```
tm2 := SELECT starts FROM SYSTEM_STARTS WHERE serial_num = SN;
tm3 := SELECT kwrunhrs FROM SYSTEM_KWRUNHRS WHERE serial_num = SN;
RETURN_VALUE := 1;
END;
```

Below is the SQL Server stored procedure that does the same (i.e., returns values from tables named SYSTEM_HOURS, SYSTEM_STARTS, and SYSTEM_KWRUNHRS):

```
CREATE PROC XFRACASGetTimeMetrics
(
@SN NVARCHAR(100),
@TM1 FLOAT OUTPUT,
@TM2 INT OUTPUT,
@TM3 FLOAT OUTPUT,
@RETURN_VALUE INT OUTPUT
)
AS
BEGIN
SET @TM1 = SELECT hours FROM SYSTEM_HOURS WHERE serial_num = @SN;
SET @TM2 = SELECT starts FROM SYSTEM_STARTS WHERE serial_num = @SN;
SET @TM3 = SELECT kwrunhrs FROM SYSTEM_KWRUNHRS WHERE serial_num = @SN;
SET @RETURN_VALUE = 1
END;
```

When using this functionality, if the stored procedure called succeeds and returns data, the user will see rows fetched from XFRACASGetTimeMetrics. This row can be selected like any other to use the listed time values in the incident.

14.2 Importing via External Process

As discussed in Section 12.10 on page 26, importing existing data is typically handled from within the XFRACAS interface by means of XML imports. If, however, you are using an external process to bring data into the system, you will use a stored procedure to increment the unique table ID assigned to each record and the entity display ID for each transactional record. For example, you can use a stored procedure to import data from a Distributed Control System (DCS) or a Supervisory Control and Data Acquisition (SCADA) system.

The procedure is named **RS_GetIDValue** and has three arguments, as follows:

- The first is an incoming argument for the table name. In Oracle, this must be entered in ALL CAPITAL LETTERS.
- The second is an incoming argument for the entity ID. If there is no entity ID, you must enter NULL for this argument.
- The third is a return argument that stores the value to a specified variable.

14.2.1 SQL Server Templates

The following template calls the stored procedure *with* an entity ID. Note that you will replace TABLENAME with the actual table name and XX with the actual entity ID.

```
DECLARE @NextID int
BEGIN
--table_name, entity_id, @NextID OUTPUT is the variable for the id_num
output
EXECUTE RS_GetIDValue 'TABLENAME',XX, @NextID OUTPUT;
PRINT @NextID;
END;
```

The following template calls the stored procedure *without* an entity ID. Note that you will replace TABLENAME with the actual table name.

```
DECLARE @NextID int
BEGIN
--table_name, @NextID OUTPUT is the variable for the id_num output
EXECUTE RS_GetIDValue 'TABLENAME', NULL, @NextID OUTPUT;
PRINT @NextID;
END;
```

14.2.2 Oracle Templates

The following template calls the stored procedure *with* an entity ID. Note that you will replace XXX with the table name in ALL CAPS, and replace x with the entity ID.

```
SET SERVEROUTPUT ON;VARIABLE NEWID NUMBER;
EXEC RS_GetIDValue('XXX',x, :NEWID);
BEGIN
DBMS_OUTPUT.PUT_LINE(:NEWID);
END;
```

The following template calls the stored procedure *without* an entity ID. Note that you will replace XXX with the table name in ALL CAPS.

```
SET SERVEROUTPUT ON;
VARIABLE NEWID NUMBER;
EXEC RS_GetIDValue('XXX',NULL, :NEWID);
BEGIN
DBMS_OUTPUT.PUT_LINE(:NEWID);
END;
```

15 FAQs

Can we implement replication for a ReliaSoft database?

XFRACAS, SEP and the ReliaSoft desktop applications cannot be deployed with bi-directional database replication (*peer-to-peer replication* or *merge replication*). The applications are designed for use with a single back-end database; they do not handle conflict detection and resolution.

It may be possible to use a ReliaSoft database with uni-directional replication (*transactional replication* or *snapshot replication*). However, this is likely to affect the performance of the application(s) and you must test on your own to evaluate the impact in your particular situation. **This type of use is not recommended or supported by ReliaSoft**.

For the purpose of disaster recovery, we recommend to establish a regular schedule for *database backups* and *transaction log backups*. These backups can be stored in a location that is protected from potential failure of the application's database server. If an issue occurs, you can restore the most recent database backup (e.g., nightly) and then restore subsequent transaction logs up to the point right before the failure.