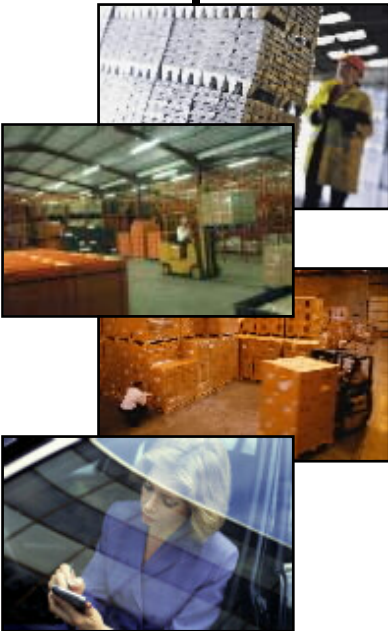




## White Paper

Critical issues to examine when selecting and deploying an RF/Wireless terminal solution.



## ***Situational Overview***

On the surface, the functionality provided by all RF/Wireless terminal solutions currently being offered in the marketplace can appear to be largely similar. Typically, it's only once a solution is deployed and placed into production within your specific environments, with your specific applications, accessed by your specific users, that you discover some of the major challenges. There are many issues that will negatively impact your ability to achieve the 100% productivity gains desired with using RF/Wireless terminals if the chosen solution does not feature the functionality required to properly deal with them.

The goal of this white paper is to call attention to certain critical issues that affect the overall performance and usability of an RF/Wireless terminal solution. Also provided in this white paper are suggested testing methods which can be used to evaluate exactly how a given solution deals with these critical issues, highlighting how it will react in a production mode.

There are several key components of any RF/Wireless terminal solution, including wireless data terminal devices, wireless network topologies and protocols, wireless networking devices (access points, hubs, routers, etc.), wireless terminal emulation software and wireless device management software.

For the purpose of this white paper, we will focus specifically on wireless terminal emulation and device management software, and the critical issues that can have a dramatic overall impact on any solution for utilizing RF/Wireless terminals throughout your enterprise for real-time data capture and queries.

Supply Chain Management (SCM) applications depend heavily on a reliable wireless terminal emulation and device management solution being in place and serving its users without unplanned interruptions and outages in service. Specifically, Warehouse Management Systems (WMS), a critical component of any SCM solution, utilize RF/Wireless barcode scanning devices to capture physical, bar-coded inventory data at various locations within their enterprise, performing real-time updates to databases on their host systems.

Bar-coding inventory items and tracking movement in real-time with RF/Wireless scanning devices provides the enterprise with greatly improved accuracy and timeliness of inventory information contained in their SCM applications that is relied upon for decision support purposes (*e.g. How much of X do I have on hand?, Where is it physically right now?, Do I need to re-order more to have adequate supply to meet demand?, etc.*). Considering the following generally accepted statistics, it is easy to see why companies invest as heavily as they do in bar-coding/real-time data capture:

**Speed of Entry:**

Handwriting (0.7 sec. per char.), Typing (0.6 sec. per char.), Bar Code (0.1 sec. per char.)

**Accuracy:**

Handwriting (1 error per 300 chars.), Typing (1 error per 300 chars.), Bar Code (1 error per 3,000,000 chars.)

The more reliable, available and easy to manage an RF/Wireless terminal solution can be, the greater the gains in productivity and, in turn, the greater the ultimate return on investment in selecting, deploying and maintaining it for the enterprise.

Therefore, it is fair to say that any issues that negatively impact the reliability, availability and ease of management of an RF/Wireless terminal solution are inherently critical and will prevent the maximum return on investment from being realized.

### ***What are the types of issues that will have a negative impact on an RF/Wireless terminal solution?***

There are four main categories of issues that can have a dramatic negative impact on an RF/Wireless terminal solution and, ultimately, on the overall experience of those who will use it and support it.

- 1. Issues related directly to the operation of the wireless device*
- 2. Issues related to wireless access signal strength/coverage*
- 3. Issues related to the wireless network/connectivity to the application host*
- 4. Issues related to effectively managing all the wireless devices and users*

We will now itemize the issues that fall into each of the categories listed above and examine how they negatively affect the user and/or IT staff. Later, we will discuss how to set up easy tests to gauge the ability of an RF/Wireless terminal solution to deal with these issues.

#### **Category 1 - Issues related directly to the operation of the wireless device**

- Turning the device off/losing power to the device for X amount of time
  - *As a result of enabling an "auto shut-off due to inactivity" feature*
  - *To replace a low/dead battery*
  - *At the end of the day, end of a shift, or when taking a break*
- Performing a re-boot of the device
  - *To clear an unplanned "locked up" condition where the device has become non-responsive to user keystrokes or scans*
  - *Intentionally, to have the device retrieve updated software and/or configuration information to use from that point forward*
- Taking advantage of the device's productivity enhancing characteristics
  - *Touch-screens and/or "tap" to select capabilities*
  - *Screen backlighting and display features (color, contrast, brightness, etc.)*
  - *Audible and visual alarming options to alert the user to messages*

## Category 2 - Issues related to wireless access signal strength/coverage

- Attempting a barcode scan/key entry when "out of range" of wireless service
  - *As a result of roaming too far away from a working wireless access point*
  - *As a result of roaming into an area that is blocked from receiving a signal from a working wireless access point (freight container, cold room, etc.)*
  - *As a result of a low battery powering the device negatively impacting wireless signal reception and transmission*
  - *As a result of a weak or disabled wireless access point causing the device to receive and send wireless signals using one that is farther away*

## Category 3 - Issues related to the wireless network/connectivity to the application host

- The device loses contact with the application host for X amount of time
  - *As a result of a working wireless access point not being able to establish IP connectivity with the host due to a network failure*
  - *As a result of a wireless access point becoming completely disabled with no alternate access points available to re-acquire lost wireless services*
- The device experiences delays in host communications due to network load
  - *May cause the application and/or user session to "time out" on the host*
  - *As a result of the amount of data being sent between the device and the host being too "heavy" for the wireless network's available resources*
- The RF/Wireless terminal solution generates a lot of wireless network traffic
  - *As a result of its licensing and/or device configuration methodology*
  - *As a result of its methodology for communicating between the wireless devices and the application host*

## Category 4 - Issues related to effectively managing all the wireless devices and users

- License Management and Enforcement
  - *What happens when new users need to be added?*
  - *How is licensing controlled (e.g. what software and where does it sit?)*
- Software Updates, configuration changes and device replacement
  - *What happens when there is a new version of the solution to deploy? (e.g. new software on the server side?, and on each of the devices?, etc.)*
  - *What happens when a device becomes unusable?*
- Remote Monitoring of the Wireless Devices
  - *Ability for the help desk to see what the users see on their device as they are scanning and accessing applications screens (local LAN connected Administrator, or from a WAN location/Internet location, etc.)*
  - *Ability to see last screen presented prior to disrupted access*

- Diagnostics (Radio, Network, Protocol) and device logging
  - *Ability to enable the collection of statistics and events for a specific device or group of devices*
  - *Ability to determine from the device which access point they are connecting to on the wireless LAN (e.g. client software displaying the IP address of the currently connected to access point, etc.)*
- Determination of cause of loss of wireless service/loss of host access
- Status of all devices
- Sending Messages
- Visibility of sent messages on the devices
- Selective device control (individual devices/groups of devices, etc.)
- Statistics and Logging of events for historical analysis
- System backup and caring for the RF/Wireless terminal solution

***What is the potential severity of the negative impact of these issues?***

When any of the issues listed above occur, the result is the unplanned loss of access to the host application for the wireless user, which in turn usually results in the unplanned need for expensive IT staff to reactively spend time on resolving the problem or figuring out a way to make the necessary changes to the wireless environment. Not all situations will affect both the user and IT staff, but the one thing that is common to all of the issues is that they will negatively impact productivity, unless the RF/Wireless terminal solution being used offers protection from them and has a facility for effectively managing the wireless user environment.

With many of the popular RF/Wireless solutions, even a brief interruption in wireless application access can result in many minutes, or even hours of lost productivity for a wireless user and IT staff to get the user back to where they were before the unplanned disruption:

- User's time to re-logout to the host system they were accessing
- User's time to re-load the application they were using
- User's time to navigate back to the exact screen and cursor location
- IT staff's time to clear hung/orphaned processes on the host
- IT staff's time to reconstruct the details of the last transaction with the user
- IT staff's time to assist the user with re-establishing their session
- IT staff's time to manage each device for software version and configurations
- *And many other non-productive activities related to managing RF/Wireless terminals or solving problems with them due to unplanned outages*

Increased user productivity was the motivation for the selection of which applications you chose to deploy and which computer system platform you chose to host them on. Ease of use and streamlining business processes was no doubt the motivation for which set of applications you chose over another. Reliability and the resulting availability of your applications to their users was no doubt the driving force behind which host computer system platform and run-time environment you chose over another.

Only you know the investment in dollars, time and valuable human resources that you've spent to provide the most reliable and highly available application environment for your users to be the most productive they can be at doing their jobs. In many cases, this investment can be measured in the tens of millions of dollars.

Add to that, the time, effort and dollars invested in providing the wireless infrastructure including the costs associated with the various wireless terminal devices themselves. The reason these very significant investments have been made is all the same...THE PURSUIT OF MAXIMUM PRODUCTIVITY.

The additional investment in an RF/Wireless terminal solution is comparatively small and, as such, its overall significance can appear to be trivial. However, the deployment of the wrong RF/Wireless terminal solution can vary significantly and, in some cases, completely undermine the promise of increased user productivity through the investments made in a highly reliable/highly available application run-time environment and the infrastructure for wireless access to the hosted applications.

***How can you conduct an effective evaluation/test that will demonstrate the ability of an RF/Wireless terminal solution to shield your users and your IT staff from these productivity-robbing issues?***

Setting up for and conducting effective tests of a potential RF/Wireless terminal solution that you are considering for wide-spread deployment is actually quite simple, and does not require a lot of time and effort.

The difficult part of the evaluation process is determining exactly what to test for. The first part of this white paper, listing the critical issues, is intended to provide you with this information. ANY RF/Wireless solution you are considering should be tested for how well it shields you from the associated negative impact on productivity they cause.

That said, we will now explain how to establish a couple of quick and easy test scenarios that can be conducted after installing a fully-functional evaluation copy of an RF/Wireless terminal solution that will cover all of the critical issues raised in this white paper...

**Test Scenario #1, Simulated "Out of Range" Condition**

1. Connect to the host application over a fixed wireless access point.
2. Initiate a session of activity with multiple transactions in the same data entry screen (e.g. scanning a bar-coded item into a field prompting for that value).
3. After performing several transactions in the session, power off the access point you are using to connect to the application host with.

What to look for as a result of this action:

- Does the device indicate that there is a problem with your connection?
  - If so, does it specifically indicate that the problem is due to an “out of range” condition that can be resolved by returning to the coverage area?
  - Is there a facility within the solution to view the status of the disrupted device and what information does it provide you with for diagnosis?
  - Is there a facility within the solution that allows you to view what the user was accessing and what they were doing (screen and cursor location) immediately prior to the unplanned disruption?
4. Restore power to the access point, which will simulate a user returning to adequate wireless coverage.

What to look for as a result of this action:

- Is the user automatically re-connected to the host?
- Does the last screen they were working on re-appear?
- Is their cursor in the same place as they were awaiting the next transactional input value/barcode scan?
- If not, what needs to be done on the user’s side to get back to where they were prior to the “out of range” condition?
- How long did that take?
- How difficult was it?
- What needed to be done on the host computer to allow the user and their device to get back online and back to where they were in the application?
- How long did that take?
- How difficult was it?
- What type of expertise was required to resolve the issue?
- How many people were required to resolve the issue?
- How much productivity was lost?

## **Test Scenario #2, Simulated “Host Access Network Problem” Condition**

1. Connect to the host application over a fixed wireless access point.
2. Initiate a session of activity with multiple transactions in the same data entry screen (e.g. scanning a bar-coded item into a field prompting for that value).
3. After performing several transactions in the session, unplug the Ethernet network cable from the Ethernet port of the access point you are using to connect to the application host with (Access Point is still on, but cannot communicate with the host computer due to the simulated network problem).

What to look for as a result of this action:

- Does the device indicate that there is a problem with your connection?
  - If so, does it specifically indicate that the problem is due to a loss of network access condition?
  - Is there a facility within the solution to view the status of the disrupted device and what information does it provide you with for diagnosis?
  - Is there a facility within the solution that allows you to view what the user was accessing and what they were doing (screen and cursor location) immediately prior to the unplanned disruption?
4. Restore the Ethernet connection to the access point, which will simulate resolution of the network/host connectivity issue.

What to look for as a result of this action:

- Is the user automatically re-connected to the host?
- Does the last screen they were working on re-appear?
- Is their cursor in the same place as they were, awaiting the next transactional input value/barcode scan?
- If not, what needs to be done on the user's side to get back to where they were prior to the "loss of network access to the host" condition?
- How long did that take?
- How difficult was it?
- What needed to be done on the host computer to allow the user and their device to get back online and back to where they were in the application?
- How long did that take?
- How difficult was it?
- What type of expertise was required to resolve the issue?
- How many people were required to resolve the issue?
- How much productivity was lost?

### **Test Scenario #3, Simulated "Loss of Device Power/Power Off" Condition**

1. Connect to the host application over a fixed wireless access point.
2. Initiate a session of activity with multiple transactions in the same data entry screen (e.g. scanning a bar-coded item into a field prompting for that value).
3. After performing several transactions in the session, remove the battery from the device without powering the unit down first. (After going through this test scenario and evaluating the results, perform a similar test by simply powering the unit off, but leaving the battery in the unit)

What to look for as a result of this action:

- Is there a facility within the solution to view the status of the disrupted device and what information does it provide you with for diagnosis?
- Is there a facility within the solution that allows you to view what the user was accessing and what they were doing (screen and cursor location) immediately prior to the unplanned disruption?

4. Restore power to the device and turn it back on.

What to look for as a result of this action:

- Is the user automatically re-connected to the host?
- Does the last screen they were working on re-appear?
- Is their cursor in the same place as they were, awaiting the next transactional input value/barcode scan?
- If not, what needs to be done on the user's side to get back to where they were prior to the "loss of device power" condition?
- How long did that take?
- How difficult was it?
- What needed to be done on the host computer to allow the user and their device to get back online and back to where they were in the application?
- How long did that take?
- How difficult was it?
- What type of expertise was required to resolve the issue?
- How many people were required to resolve the issue?
- How much productivity was lost?

#### **Test Scenario #4, Simulated "Remote Device Re-Configuration" Condition**

1. Connect to the host application over a fixed wireless access point.
2. Initiate a session of activity by running a data entry terminal screen that does a host-side validation of the data being entered by the wireless user.
3. Purposely enter an invalid data value.
4. Note whether or not the device emits an audible tone in conjunction with the message being displayed to the user that the data is invalid or any other message/alert condition you know how to create with the device.

What to look for as a result of this action:

- Where is the message being displayed to the user?
  - Does the solution that you are evaluating provide flexibility as to where and how messages are displayed to the user within the wireless terminal screen?
  - Is there a facility within the solution that allows you to send text messages to the user/users and if so, does it allow you to control how those messages are displayed and how the user is alerted?
5. Locate within the solution where you are able to modify the message alert settings for the device/devices (beep, no beep, double beep, etc.). NOTE: If there is no centralized management facility, you may have to locate this function on the device itself as part of the wireless terminal emulation client software.
  6. Perform the steps necessary to modify the message alert setting to something different than what it was prior to conducting this test and save the change.
  7. Run the same data entry screen that you previously ran prior to the configuration change and check to see if the change has taken effect when a message is displayed and the user is alerted.

What to look for as a result of this action:

- How long did that take?
- How difficult was it?
- Was there a facility within the solution that allowed you to execute the device configuration change remotely from a centralized interface, or did you have to physically make the change on the device itself?
- How long would it take if you had to change many devices to reflect the same configuration change?
- How difficult would that be?
- Does the solution allow for changes to be made to logical groups of devices all at once, versus one by one?
- What is the process for the device to begin using the new configuration?
- Is that process automatic or manual (next time they start a wireless terminal session, physical re-boot of the device, etc.)
- Does any software need to be downloaded to the device for these types of changes to take effect?
- If so, how big is the amount of software that must be "pushed" out to the devices when this happens?
- What effect would that have on your wireless network's performance when that needs to happen to many devices all at once?
- How much productivity was lost making the change?
- What other configuration changes can you see doing on a regular basis?
- What happens when you need to increase the number of licensed users of the RF/Wireless terminal solution or make any changes to the environment?

## ***Summary/Conclusion***

The goal of this document is to provide you with the specific information necessary to determine whether or not the RF/Wireless terminal solution you are considering for a wide-scale production deployment 1.) offers the level of functionality you require, and 2.) provides the right level of protection from issues that will compromise the productivity of the users who will rely on it for mission critical tasks.

Hopefully, we have been able to achieve that goal for you and have assisted you in some way with your evaluation efforts. No matter which solution for deploying RF/Wireless terminals you ultimately select, it is far better to consider all of the critical factors related to this valuable technology prior to introducing it into your daily operations.

eBusiness Solution Pros has been in the business of designing and implementing small, medium and large-scale warehouse, manufacturing and distribution systems that feature reliable wireless access to host applications since 1991. Our Stay-Linked™ reliable RF/Wireless terminal solution benefits from those years of real-world experience and is focused on one critical deliverable: “Preserving Productivity for the Wireless Workforce”.

###

***For more information on Stay-Linked™, or to request a FREE 30-day evaluation copy, please contact your Stay-Linked Certified Partner or contact us at:***

**eBusiness Solution Pros, Inc.  
15991 Redhill Avenue, Suite 210  
Tustin, CA 92780-7320**

**Phone** 714.918.7700

**Web** [www.stay-linked.com](http://www.stay-linked.com)

**e-Mail** [sales@stay-linked.com](mailto:sales@stay-linked.com)