Interference Tests for 900 MHz Frequency-Hopping Public-Safety Wireless Devices

Kate A. Remley [1], Michael R. Souryal [2], William F. Young[1], Daniel G. Kuester [1],

David R. Novotny [1], Jeffrey R. Guerrieri [1]

[1] *NIST Electromagnetics Division*
325 Broadway, Mail Stop 818.02; Boulder, CO, USA, 80305
[1] kate.remley@nist.gov

[2] *NIST Advanced Network Technologies Division*
100 Bureau Drive, Mail Stop 8920; Gaithersburg, MD, USA, 20899
[2] michael.souryal@nist.gov

***Abstract*—We discuss free-field measurement methods designed to quantify interference between wireless devices such as RF identification systems and RF-based emergency beacons used by fire fighters. For public safety applications, standardized testing requires that responder organizations purchase devices that are appropriate for their specific needs. Also, appropriate test methods must be developed because reliability can be life critical.**

I. Introduction

Emergency response organizations count on reliable radio communications between responders, who are often inside a structure, and the incident command station outside. New wireless technology is being developed that can further increase responders' safety and efficiency by remotely monitoring their position, status, and health. The responder community would like to take advantage of this technology. However, even though standards exist for commercial wireless devices such as cell phones, few standards exist for wireless emergency safety equipment. The U.S. Department of Homeland Security (DHS) Office of Standards is working with researchers at the National Institute of Standards and Technology (NIST) to provide technical support for the development of consensus standards for these new products.

One example of DHS/NIST work is to support the National Fire Protection Association (NFPA) in the revision of NFPA 1982: Standard on Personal Alert Safety Systems (PASS), to include RF-based PASS (a PASS is essentially an audible "man-down" alarm). Note that we refer to RF-based PASS as RF PASS in the remainder of the paper. DHS is also supporting NIST in developing measurement methods to quantify the electromagnetic vulnerabilities of radio-frequency identification (RFID) systems in public-safety or other homeland security applications. The RFID work examines vulnerabilities of RFID systems to eavesdropping, jamming [1], unintentional interference [2], and co-channel interference [3]. The work reported here extends prior work to investigate interference between two wireless systems that may be deployed in a firefighter environment: RFID and RF PASS.

The technical strategy for these projects is to first conduct field tests to gather information on key wireless-channel parameters in representative responder locations (high-rise buildings, urban canyons, tunnels, apartment buildings, and other large structures where radio communication problems are typically encountered). Then, researchers replicate these parameters in a controlled, lab-based, free-field test environment. The final step is to compare the performance of a given wireless device in the lab to that measured in the field. This process allows development of general, lab-based test methods that place the device in the same conditions under which it will be used in the field. These standards will help ensure that the response communities' needs are met and will further enhance their safety.

We first report on a reverberation-chamber-based method to measure the radiated power levels from the two types of wireless devices. We describe the uncertainties involved in this method. Knowledge of the radiated power from each device helps in the analysis of the interference between them. We then discuss the test environment for the interference tests and the results of our experiments. Finally, we draw some conclusions and make recommendations for future work.

II. Radiated Output Power Measurement

The RF PASS and RFID systems we considered are both commercially available, frequency-hopping systems that operate in the industrial, scientific, and medical frequency bands between 902 MHz and 928 MHz. The RFID system reader can generate a range of output powers from 15 to 32.5 dBm that is controlled with software.

The RF PASS system consists of a small base-station unit, approximately 22.9 cm by 5.1 cm by 17.2 cm. The unit has one omnidirectional monopole transmit antenna and two identical receive antennas, allowing the use of receive diversity in weak-signal conditions.

We measured the total radiated output power of each in a reverberation chamber with the setup shown in Fig. 1(a). First, we measured a continuous-wave (CW) signal with a known power level to provide a reference for the RFID and RF PASS

Presented at the 2011 IEEE EMC Symposium

device measurements. We then inserted each device, one at a time, into the reverberation chamber.

The transmit antenna used with the RFID system reader was a linearly polarized patch antenna with 8 dBi gain. This antenna was connected to the reader with a coaxial cable connected to a bulkhead in the reverberation chamber. For the RF PASS system, the transmit antenna was integrated into the hand-held unit. The receive antenna for both the RFID and RF PASS measurements was, as above, a linearly polarized patch with a gain of 8 dBi and a return loss of approximately 20 dB across the 900 MHz to 930 MHz frequency range. We aimed this antenna at one of the two mode-stirring paddles in order to minimize the line-of-sight, unstirred signal paths. The receive antenna was connected to a spectrum analyzer (SA) with coaxial cables that were connected to a bulkhead in the reverberation chamber.

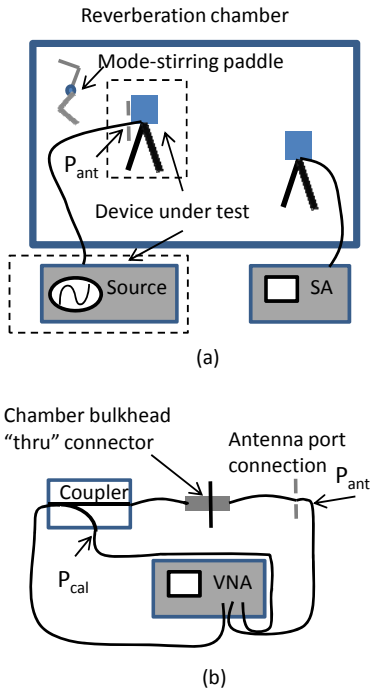

Figure 1: Total radiated power measurement setup; (a) the reverberation chamber setup with a spectrum analyzer to measure total radiated power from the CW, RFID, and RF PASS device sources, and (b) calibration configuration with a CW source stepped from 900 to 930 MHz.

In order to measure the power into the transmit antenna, as required by the FCC, we performed a calibration step. With a VNA, we first measured the loss in the cables, connectors, and RF coupler configuration shown in Fig. 1(b). This allowed us to drive the antenna within the chamber with a known power level at the antenna port, P_{ant}, by monitoring the power at P_{cal}, with a power meter. Then we excited the chamber with the CW source through the 8 dBi patch antenna. The signal was swept in 25 kHz steps from 900 to 930 MHz with a power of 12 dBm at P_{ant}. We measured the maximum received power using the "peak hold" function on the spectrum analyzer (SA) for 21 different paddle positions. We added an additional 18 dB to adjust the results from 12 dBm at P_{ant} to the 30 dBm maximum input allowed by the FCC. The average of the included CW peak-hold measurements, with the 18 dB correction, results in the dashed line shown in Figs. 2 (a) and (b). Note that the maximum received power (rather than the average power) was measured because FCC Part 15, Subpart C (Sec. 15.247(b)(2) & (3)) regulates the maximum transmission power allowed.

To measure the radiated power, with the mode-stirring paddles in a fixed position, we recorded the spectrum of the device, again using the peak hold feature of our analyzer. We acquired the signal over several burst periods to ensure that we recorded the maximum output as a function of frequency for each paddle position. For the RFID device in the example presented here, we captured the signal for 8 s. For the RF PASS device, we captured the signal for 20 s because its bursts occur less frequently, possibly to conserve battery life. We then rotated the mode-stirring paddles and conducted another measurement. We repeated this procedure for a total of 20 and 8 paddle positions for the RFID and RF PASS devices, respectively.

Based on the collected data, we provide an estimate of the random component of uncertainty in the measured peak value. Calculating the standard deviation of the measured maximum for the 8 and 20 paddle positions, the estimated standard deviation $(\hat{\sigma})$ is 1.1 dB and 2.0 dB for the RFID and RF PASS systems, respectively. The random component of uncertainty for these two measurements is then provided by the estimated standard deviation, that is,

$$u_{meas} = \hat{\sigma} \ . \qquad (1)$$

To decrease the uncertainty, we need to increase the number of paddle positions. This procedure can be very time consuming because of the intermittent burst rate on the RF PASS system. Also, in this study, we were interested primarily in the relative power between the various types of devices, that is, comparing the RF devices to the CW source, and comparing the RFID to the RF PASS in measurements made with the same spectrum analyzer and antenna setup. As a result, we expect any systematic uncertainties in the measurements, such as a bias in the spectrum analyzer, to affect all of the measurements in an approximately equal manner. In this case, they become negligible.

The spectra of the bursted signals emanating from the two wireless devices obtained by use of the peak hold feature of the analyzer are shown in Figs. 2(a) and 2(b). We see that the radiated power from the RF PASS device is around 10 dB lower than that of the RFID reader, when the reader is set to the FCC maximum limit of 30 dBm total radiated power. Note that the FCC allows an effective isotropically radiated power (EIRP) up to 36 dBm, and because the antenna we used had an 8 dBi gain, we would expect to reach this limit when the reader output is set to 28 dBm. However, testing in a reverberation chamber effectively eliminates the directivity of the antenna [4] and, thus, the power comparisons for these measurements are evaluated with respect to the FCC 1 watt input threshold (30 dBm). The output power of the RF PASS is not adjustable. The lower radiated power for the RF PASS

device may be due, again, to battery-life conservation, or from the requirement that these devices operate in an "intrinsically safe" mode, minimizing the chance of the device contributing to an explosion in a volatile environment.

Fig. 2 shows that the subcarriers of the RF PASS are somewhat more distorted that those of the RFID reader. From previous tests, we know that this is not due to an insufficient time capture of the peak-hold signal. Thus, these results suggest that the RF PASS device generates a signal with more distortion than the RFID device. Such distortion may make the RF PASS system more susceptible to interference.

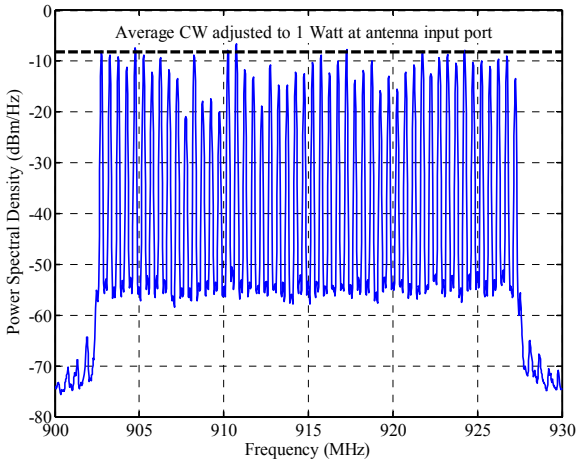

Figure 2: Power spectral density of the signal measured with peak hold from (a) the RFID reader and (b) the portable RF PASS device. Results are taken from 20 and 8 paddle positions, respectively, in the reverberation chamber.

III. Interference Measurements

A. Test Set-up

The real-world scenario we wished to replicate in our laboratory tests assumes that the RFID reader antenna is within close proximity of the portable RF PASS device and that no line-of-sight condition exists between the base station and the RF PASS device. This scenario may be encountered in practice when a fire fighter enters a warehouse or other commercial structure where RFID inventory is conducted or when a fire fighter uses RFID for localization.

To ensure that the coupling between the portable RF PASS unit and the base station is controllable, we isolated the two units from each other by placing them in separate rooms in the NIST near-field antenna metrology laboratory. As shown in Figure 3, the transmit antenna port on the base station was connected with coaxial cables to a variable attenuator (physically, two attenuators in series). The output of the attenuator was connected to a long, shielded 50 Ω coaxial cable. The long cable ran through a wall bulkhead to the semi-anechoic chamber where the portable RF PASS device and the RFID reader tags were located. The RF PASS base-station transmit antenna was connected to the cable and affixed to a metal plate intended to simulate the top surface of the base station. The distance from the transmit antenna to the variable attenuator was approximately 30 meters.

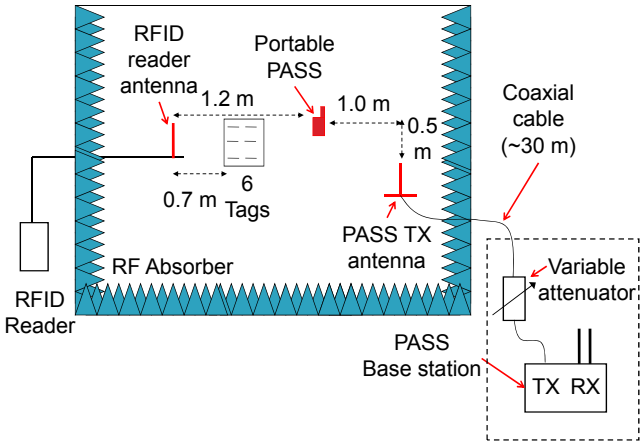

Figure 3: The portable RF-based PASS device was placed 1.2 m from the RFID reader antenna and 1 m from the base-station transmit antenna. The reader continuously queried the six-tag array to generate the interference signal. External attenuation was placed between the PASS base station and the base station's transmit antenna, allowing for study of the effects of both weak-signal reception and interference.

An array of six passive RFID tags was placed with the RF PASS portable unit within a semi-anechoic chamber, as shown in Figure 3. This chamber, shown in the photograph of Figure 4, has interior dimensions (*i.e.*, between tips of the pyramidal absorbers) of approximately 2.4 m by 2.4 m by 2.4 m. The walls (except for the wall directly in the main beam of the pattern of the six-antenna array) and floor were covered with RF absorber consisting of 30.5 cm tall pyramidal blocks designed to attenuate normal reflections in the 1 GHz to 40 GHz range. The wall in the main beam of the antenna array's pattern was covered with 61.0 cm tall pyramidal blocks designed to attenuate normal reflections in the 500 MHz to 40 GHz range The ceiling is open.

The transmitter for the RFID reader was placed immediately outside the semi-anechoic room. A coaxial cable connected the reader with the RFID reader antenna. The RFID tag array was located within the chamber, 0.7 m from the RFID transmit antenna. The portable RF PASS device was

placed behind the RFID tag array, 1.2 m from the RFID reader antenna. The RF PASS transmit antenna was located on the other side of the portable unit, 1.0 m away, as indicated in Figure 3.

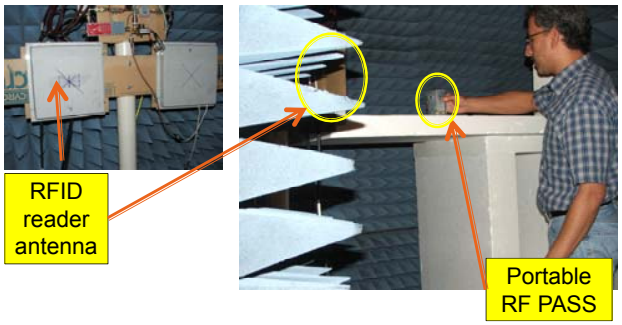

Figure 4: The RFID reader antenna and portable RF PASS device were placed within a semi-anechoic room to study the effects of interference without multipath. An array of six passive RFID tags (not shown) was placed between the reader antenna and the RF PASS unit.

The base station was located in a second room in order to achieve sufficient shielding from the portable unit. For these preliminary tests, we were interested only in the relative ability of one device to interfere with the other during standard operation. Thus, we did not measure the isolation shielding effectiveness between rooms.

During testing, we varied the level of attenuation, increasing it until the communication between the portable unit and the base station was interrupted. The coaxial cable introduced approximately 15 dB of loss; thus, in our graphs, an attenuator setting of zero dB is reported as 15 dB of path loss. The base station and variable attenuator set up are shown in Figure 5.

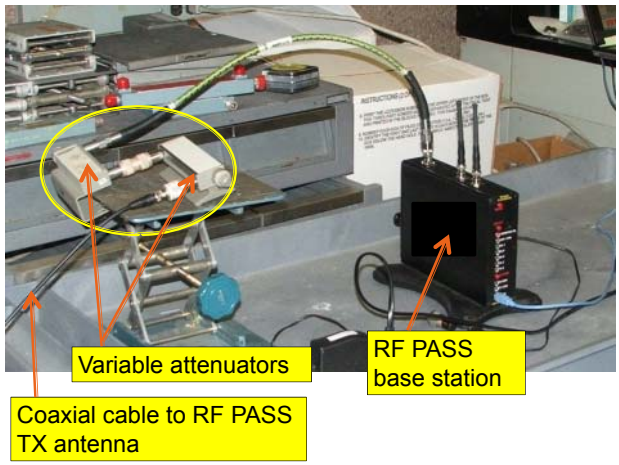

Figure 5: RF PASS base station set-up showing, at left, the coaxial cable coming from the transmit antenna (located in another room). This cable is attached to the base station's transmit antenna port through two variable attenuators (on lab jacks). Also visible are the base station's two receive antennas. The computer that controls the RF PASS system is not shown.

B. Test Results: RFID Interference with RF PASS

The protocols used by many frequency-hopping devices use retransmission algorithms in weak-signal conditions. Consequently, the communication failure between the portable RF PASS device and its base station was typically not a hard failure unless the attenuation and/or level of RFID interference was above a certain threshold. For intermediate values of attenuation (and interference), a delay between sending and receiving the alarm was encountered. As will be shown, the variability in this delay could be quite high.

We first measured the ability of the portable RF PASS device to receive an alarm signal from the base station without any external interference. A delay or failure to receive of the alarm is, therefore, due to weak-signal conditions caused by an increasing level of attenuation introduced into the signal path. We define a failure in the transaction as a delay longer than one minute.

Figure 6(a) shows the results of this test. The mean delay of six repeat tests is shown by the symbols, while the error bars report the standard deviation (+/- one sigma). The portable RF PASS device intermittently received the alarm with a delay between 10 and 30 seconds even for relatively low levels of attenuation. When the external attenuation exceeded a certain threshold (85 dB in this case), the failure rate became significant. Note that these are relative values of attenuation: as discussed earlier, our goal was to examine effectiveness of the test method, so we did not quantify the receiver sensitivity or the effects of inserting a 50 Ω cable between the base station and its transmit antenna.

Figure 6(b) illustrates the effect of interference from the RFID reader on the ability of the portable device to receive an alarm from the base station. As expected, the introduction of interference in the same frequency band as the transmitted signal reduces the success rate of the alarm transmission. Delays are significantly longer and more variable than they were in Figure 6(a), and complete failure occurs at a lower threshold value (around 75 dB in this case).

In Figure 6(c), we increased the output level of the RFID reader to the 30 dBm FCC maximum. In this case, the disruption to the RF PASS reception of the alarm is even more significant. Failures sometimes occurred for the lowest value of attenuation that we inserted, around 15 dB in this case. The complete failure threshold was around 65 dB.

These tests show that, as expected, an interfering signal has the effect of lowering the weak-signal failure threshold of the portable RF PASS device. The frequency-hopping retransmission protocol can introduce long and highly variable delays for levels of interference below that required for a complete failure. Even though our number of repeat measurements (six) was too low to do a full study of the uncertainty in the mean delay, an increased level of variability for interference below the failure threshold was consistently encountered. This indicates that receipt of an alarm may be unpredictable in the presence of this type of interference.

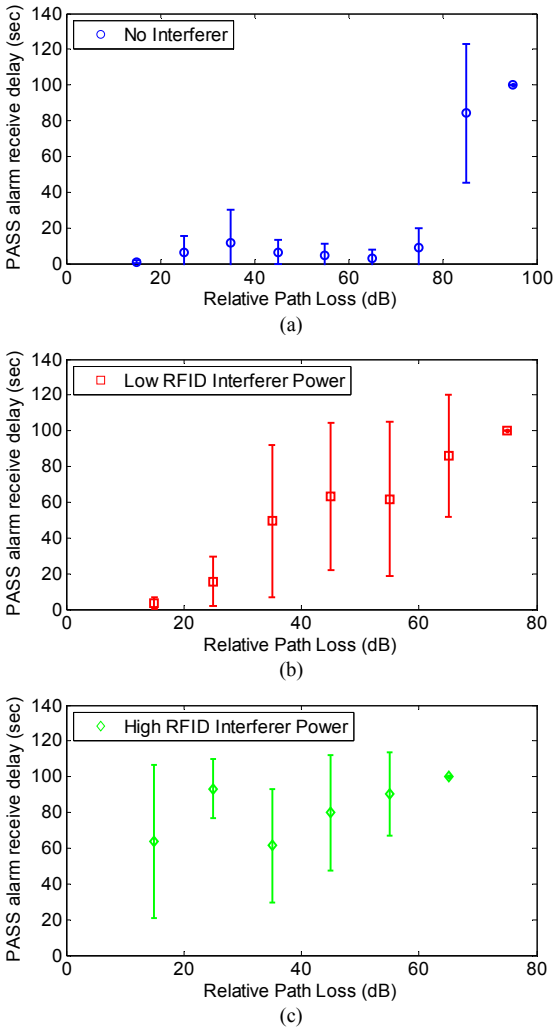

Figure 6: Measured delay for the portable RF PASS device to receive an alarm from the base station with various levels of external attenuation (denoted relative path loss) placed between the two. Six repeat measurements were conducted for each attenuation level. The variability in the delay occurs because of the retransmission period in the frequency-hopping protocol. (a) No external interference; (b) low-level RFID interference; (c) high-level RFID interference.

C. *Test Results: RF PASS Interference with RFID*

In addition to testing the impact of the RFID signal on the RF PASS system, we investigated the effect of the RF PASS signal on RFID performance. For this set of tests, a single cross-dipole tag was placed at a distance of 1 m from the reader antenna along the antenna's boresight. The location of the portable RF PASS unit was varied along a line parallel to the boresight (same height as the tag, but with a 0.15 m horizontal offset). This distance ranged from 0.25 m to 2.25 m from the reader antenna, in 0.25 m increments, as shown in Figure 7. At each distance, the portable RF PASS unit was placed in alarm mode and measurements of RFID performance were made. The RF PASS base station was not used in these experiments.

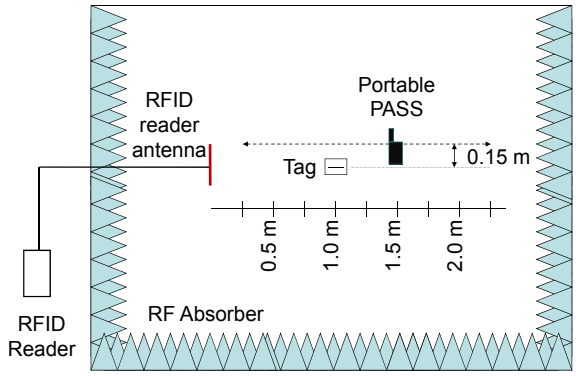

Figure 7: Configuration for testing interference of RF PASS device to RFID. A single tag was fixed at a distance of 1 m from the reader antenna. The position of the RF PASS device was varied along a straight line from 0.25 m to 2.25 m from the reader antenna.

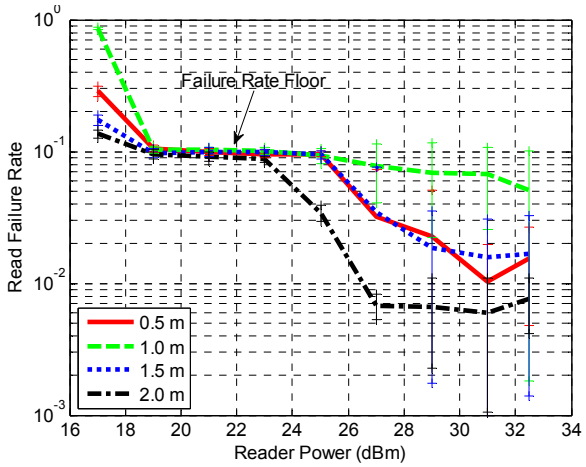

Figure 8: RFID read failure rate vs. nominal reader power setting, for various distances between the portable RF PASS and the reader antenna (see legend).

At each position of the RF PASS unit, six sets of RFID interrogations were conducted, each comprising 1000 interrogation attempts. The number of successful interrogations in each set (N) and the average duration of the set of interrogations $(\overline{D})$ were recorded. RFID performance is reported in terms of the read failure rate (*i.e.*, $1-\overline{N}/N_{\max}$) and the read throughput in reads per second (*i.e.*, $\overline{N}/\overline{D}$), where $\overline{N}$ is the average number of successful interrogations and $N_{\max}$ is the maximum number of response counts.[1] In the absence of an RF PASS signal and at reader power settings of 17 dBm and higher, the RFID read failure rate was less than 1 % and the read throughput was 172 reads/s.

Figure 8 shows the read failure rate as a function of the reader's power setting with the RF PASS unit in alarm mode at four different distances. The error bars correspond to the

[1] $N_{\max}$ exceeds 1000 because the anti-collision protocol reinitiates some inventories. The actual number of inventories is closer to 1030.

standard deviation (+/– one sigma) over the six sets of interrogations. RFID failure rates in the presence of the RF PASS signal are significant, especially at the low end of the reader power range. Increasing the reader power decreases the read failure rate, as expected. However, we also observe a failure rate *floor* of around 10 %. This failure rate floor is analogous to the error floor observed in digital communications in the presence of other sources of interference, such as intersymbol interference [5]. The reader power required to decrease the failure rate below this floor depends on the distance of the RF PASS device from the reader antenna. The closer the RF PASS device is to the 1 m position (i.e., near the tag), the greater the reader power needed to lower the failure rate below the floor.

Figures 9 and 10 illustrate the dependence on the RF PASS unit's distance more clearly. Figure 9 shows read failure rate and Figure 10 shows read throughput, both as a function of distance. At the lower reader powers (i.e., 21 dBm and below), RFID performance suffers the effects of interference at all RF PASS unit distances. At higher reader powers, performance is most affected when the RF PASS unit is close to the tag's position of 1 m from the reader antenna, with failure rates reaching in excess of 5 % even at the reader's maximum power.

In summary, we observe that portable RF PASS devices do have an impact on RFID performance, especially when the RF PASS unit is at a comparable distance from the reader as the tag. The implication for emergency responders carrying both an RFID tag for location-tracking purposes and an RF PASS unit is that location-tracking reliability can be reduced when the RF PASS unit is in alarm mode.

IV. Conclusion

We have described methods for testing and evaluating interference between two frequency-hopping wireless devices that operate in similar frequency bands. Our goal is to develop straightforward yet accurate methods for assessing various types of wireless technology proposed for use by the public safety community. Refinement of these methods is the subject of ongoing research at NIST.

Acknowledgment

The Science and Technology Directorate of the U.S. Department of Homeland Security sponsored the production of this material under Interagency Agreement HSHQDC-10-X-00534 with the National Institute of Standards and Technology (NIST).

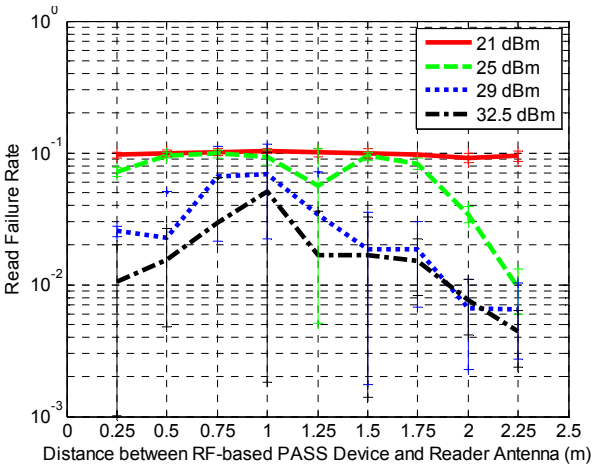

Figure 9: RFID read failure rate vs. distance of RF PASS device from reader antenna for various values of nominal reader power setting (see legend).

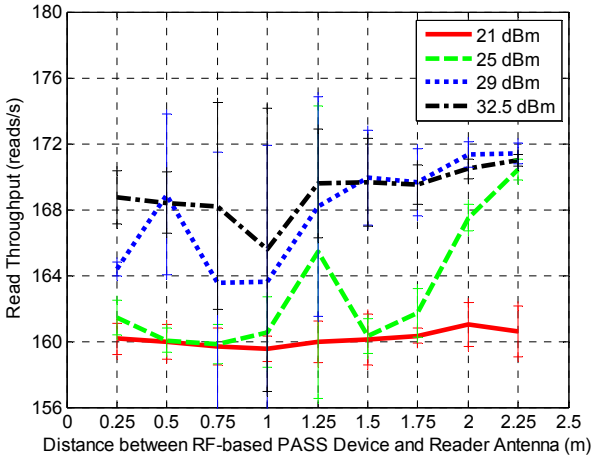

Figure 10: RFID read throughput vs. distance of RF PASS device from reader antenna for various values of nominal reader power setting (see legend).

References

[1] D. R. Novotny, J. R. Guerrieri, M. Francis, and K. A. Remley, "HF RFID Electromagnetic Emissions and Performance," *2008 IEEE EMC Symp. Dig*, Detroit, MI, Aug. 2008, 6 pp.

[2] D. R. Novotny, J. R. Guerrieri, and D. G. Kuester, "Potential interference issues between FCC part 15 compliant UHF ISM emitters and equipment passing standard immunity testing requirements," *2009 IEEE EMC Symp. Dig.*, Austin, TX, Aug. 2009, pp. 161 - 166.

[3] M. R. Souryal, D. R. Novotny, D. G. Kuester, J. R. Guerrieri, and K. A. Remley, "Impact of RF interference between a passive RFID system and a frequency hopping communications system in the 900 MHz ISM band," in *2010 IEEE EMC Symp. Dig.*, Fort Lauderdale, FL, July 2010, pp. 495 - 500.

[4] G. Koepke, and J. Ladbury, "Radiated Power Measurements in Reverberation Chambers," *56th ARFTG Conference Digest*, 7 pp., Nov. 2000.

[5] A. Goldsmith, *Wireless Communications.* New York: Cambridge University Press, 2005.