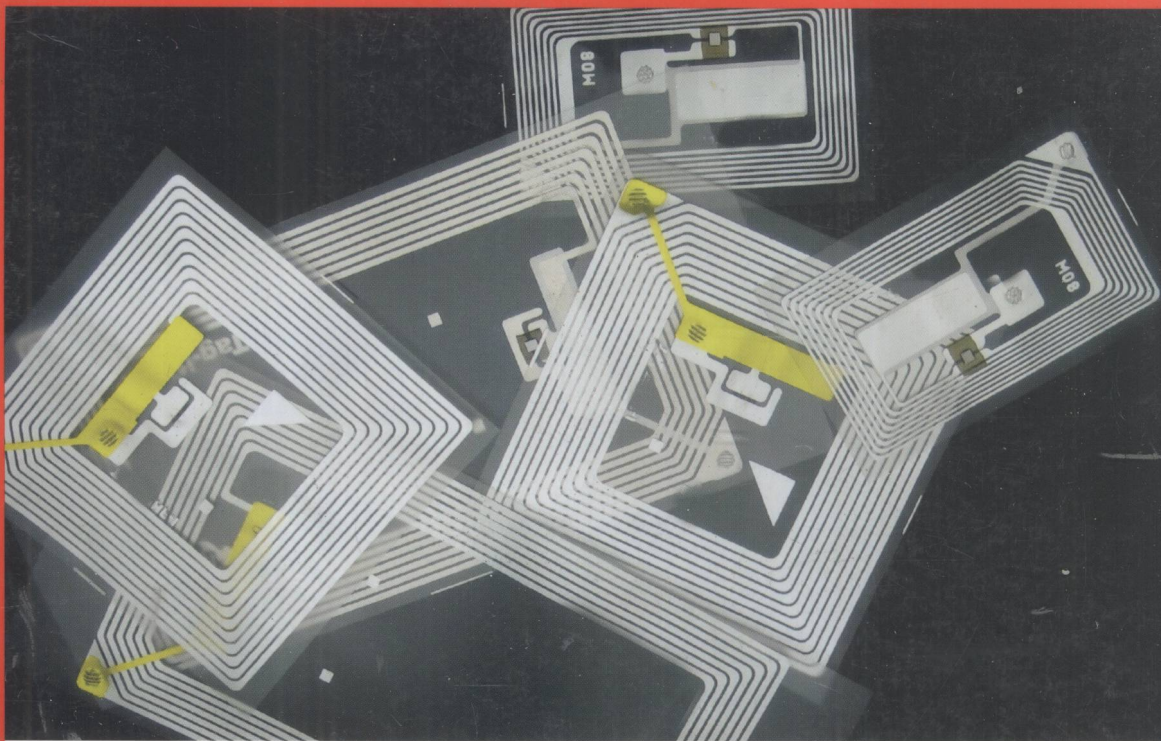


COMMUNICATIONS ENGINEERING SERIES



The RF in RFID

Passive UHF RFID in Practice

Daniel M. Dobkin



CD-ROM
INCLUDED

TN92
D633-2

The RF in RFID

Passive UHF RFID in Practice

Daniel M. Dobkin



E2008000269



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Newnes is an imprint of Elsevier



Newnes


附光盤壹張

Newnes is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Copyright © 2008, Elsevier Inc. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone: (+44) 1865 843830, fax: (+44) 1865 853333, E-mail: permissions@elsevier.com. You may also complete your request online via the Elsevier homepage (<http://elsevier.com>), by selecting "Support & Contact" then "Copyright and Permission" and then "Obtaining Permissions."

 Recognizing the importance of preserving what has been written, Elsevier prints its books on acid-free paper whenever possible.

Library of Congress Cataloging-in-Publication Data

Dobkin, Daniel Mark.

The RF in RFID : passive UHF RFID in practice / Daniel M. Dobkin.
p. cm.

Includes index.

ISBN 978-0-7506-8209-1

1. Radio frequency identification systems. 2. Radio frequency—Identification. 3. Wireless communication systems. I. Title.

TK6553.D59 2007

621.384—dc22

2007027647

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

ISBN: 978-0-7506-8209-1

For information on all Newnes publications
visit our website at www.books.elsevier.com

08 09 10 11 10 9 8 7 6 5 4 3 2 1

Printed in the United States of America

Working together to grow
libraries in developing countries

www.elsevier.com | www.bookaid.org | www.sabre.org

ELSEVIER

BOOK AID
International

Sabre Foundation

The RF in RFID

Contents

Chapter 1: Introduction	1
1.1 What, When, and Where, Wirelessly	1
1.2 Why Would You Read This Book?	2
1.3 What Comes Next?	3
1.4 Acknowledgments	4
1.5 Further Reading	4
Chapter 2: History and Practice of RFID	7
2.1 It All Started with IFF	7
2.2 Making it Cheap	9
2.3 Making and Selling: Tracking Big Stuff	15
2.4 Tracking Small Stuff: AutoID and The Web of Things	19
2.5 RFID Systems and Terminology	22
2.6 Types of RFID	24
2.6.1 Frequency Bands for RFID	24
2.6.2 Passive, Semipassive, and Active Tags	34
2.6.3 Communications Protocols	42
2.7 The Internet of Things and UHF RFID	46
2.8 Further Reading	48
2.8.1 History	48
2.9 Exercises	49
Chapter 3: Radio Basics For UHF RFID	51
3.1 Electromagnetic Waves	51
3.2 Describing Signal Voltage and Power	55
3.3 Information, Modulation, and Multiplexing	58
3.4 Backscatter Radio Links	68
3.5 Link Budgets	73
3.5.1 Reader Transmit Power	75
3.5.2 Path Loss	75
3.5.3 Tag Power Requirement	77
3.6 Effect of Antenna Gain and Polarization on Range	80
3.7 Propagation in the Real World	93

3.8	Capsule Summary: Chapter 3	99
3.9	Further Reading	100
3.9.1	Signal and Signal Processing	100
3.9.2	Backscatter Links	100
3.9.3	Antennas	100
3.9.4	Reflection from Dielectric Surfaces	101
3.10	Exercises	101

Chapter 4: UHF RFID Readers **103**

4.1	A Radio's Days (and nights)	103
4.2	Radio Architectures	107
4.3	Radio Components	110
4.3.1	Amplifiers	112
4.3.2	Mixers	126
4.3.3	Oscillators and Synthesizers	133
4.3.4	Filters	144
4.3.5	Digital-Analog Conversion	151
4.3.6	Circulators and Directional Couplers	155
4.4	RFID Transmitters	159
4.4.1	Transmitter Architectures	160
4.4.2	Transmit Power Efficiency	168
4.4.3	Phase and Amplitude Noise	171
4.5	RFID Receivers	175
4.5.1	Receiver Architectures	176
4.5.2	DC Offsets and Recovery	179
4.5.3	Phase and Amplitude Noise and Sensitivity	180
4.5.4	Example Design Calculations	181
4.6	Digital-Analog Conversion and Signal Processing	184
4.7	Packaging and Power	187
4.8	Capsule Summary	187
4.9	Further Reading	189
4.9.1	RFIC Design	189
4.9.2	Analog-digital conversion	189
4.9.3	Amplifiers	190
4.9.4	Mixers	190
4.9.5	Reader Architecture and Signal Processing	190
4.10	Exercises	191

Chapter 5: UHF RFID Tags **195**

5.1	Power and Powerlessness	195
5.2	RF to DC	197
5.3	Getting Started, Getting Data	207
5.4	Talking Back	210

5.5	Tag IC Overall Design Challenges	220
5.6	Packaging: No Small Matter	222
5.7	Other Ways	230
5.8	Capsule Summary	234
5.9	Further Reading	235
5.9.1	Tag IC Design	235
5.9.2	Chip Assembly Techniques	236
5.9.3	Conductive Inks	236
5.9.4	SAW tags	237
5.9.5	organic ICs	237
5.10	Exercises	237
 Chapter 6: Reader Antennas		241
6.1	Not Just for Insects Anymore	241
6.2	Current Events: Fundamentals of Antenna Operation	242
6.2.1	Got Gain?	243
6.2.2	Polarization	249
6.2.3	Impedance and Bandwidth	254
6.2.4	The Patch Antenna	260
6.2.5	It's All On the Datasheet (Except the Price!)	267
6.3	Antennas for Fixed Readers	268
6.3.1	Doors and Portals	268
6.3.2	Interference and Collocation	271
6.3.3	Conveyor Antenna Configuration	274
6.4	Antennas for Handheld or Portable Readers	278
6.5	Near-field Antennas	284
6.6	Cables and Connectors	287
6.7	Capsule Summary	295
6.8	Afterword: An Electron's Eyelash	296
6.9	Further Reading	297
6.9.1	General Antenna Theory and Practice	297
6.9.2	Exotic Reader Antenna Configurations	297
6.10	Exercises	298
 Chapter 7: Tag Antennas		305
7.1	World to Tag, Tag to World	305
7.2	Impedance Matching and Power Transfer	306
7.3	Dipoles and Derivatives	314
7.3.1	Wiggling Wires	315
7.3.2	Match L with L of L	319
7.3.3	Getting Loaded	321
7.3.4	Fat and Thin	323

- 7.3.5 Folding Up 327
- 7.3.6 Polarization 330
- 7.3.7 Radar Scattering Cross-Section 332
- 7.4 Tags and the (local) Environment 336
 - 7.4.1 Nearby Objects 336
 - 7.4.2 Nearby Tags 345
- 7.5 Near-field and Hybrid Tag Antennas 352
- 7.6 Capsule Summary 354
- 7.7 Further Reading 355
- 7.8 Exercises 357

Chapter 8: UHF RFID Protocols 361

- 8.1 What a Protocol Droid Should Know 361
- 8.2 Days of Yore 370
- 8.3 EPCglobal Generation 1 374
 - 8.3.1 EPCglobal Class 0 375
 - 8.3.2 EPCglobal Class 1 Generation 1 385
- 8.4 ISO 18000-6B (Intellitag) 393
- 8.5 ISO 18000-6C (EPCglobal Class 1 Generation 2) 398
 - 8.5.1 Overview and Tag Memory Organization 400
 - 8.5.2 Reader and Tag Symbols and Coding 402
 - 8.5.3 Packet Structure 413
 - 8.5.4 Medium Access Control 416
 - 8.5.5 States and Commands 423
 - 8.5.6 Normal Operation and Key User Parameters 427
 - 8.5.7 Protocol Performance and Link Timing 433
 - 8.5.8 Concluding Remarks 436
- 8.6 Capsule Summary 437
- 8.7 Further Reading 438
 - 8.7.1 General Communications Protocols 438
 - 8.7.2 RFID Protocols: The Source Docs 439
 - 8.7.3 RFID Protocols: More Information 439
 - 8.7.4 RFID Protocols: Security and Privacy 440
- 8.8 Exercises 440

Afterword 445

Appendix 1: Radio Regulations 447

- A1.1 Couldn't Wait for Global Warming 447
- A1.2 FCC PART 15 449
- A1.3 European Standards 453
- A1.4 Those Other Few Billion Folks 456

Appendix 2: Harmonic Functions	459
A2.1 Sines and Cosines	459
A2.2 Complex Numbers and Complex Exponentials.....	460
Appendix 3: Resistance, Impedance and Switching	467
A3.1 Electric Company Detective Sherlock Ohms	467
A3.2 Resistance is Useless?.....	470
A3.3 Switching.....	475
Appendix 4: Reflection and Matching	477
A4.1 Reflection Coefficients	477
A4.2 A Simple (But Relevant) Matching Example	480
Index	485

Introduction

1.1 What, When, and Where, Wirelessly

To a quantum mechanic, the whole universe is one god-awful big interacting wavefunction—but to the rest of us, it's a world full of separate and distinguishable objects that hurt us when we kick them. At a few months of age, human children recognize objects, expect them to be permanent and move continuously, and display surprise when they aren't or don't. We associate visual, tactile, and in some cases audible, and olfactory sensations with identifiable physical things. We're hardwired to understand our environment as being composed of separable things with specific properties and locations. We understand the world in terms of what was where and when. So, one can forgive us for being disappointed that the computers and networks that form so large a part of our lives and often seem so intelligent in other respects (at least on a good day) are clueless when it comes to perceiving and recognizing all these discrete physical objects that we so easily detect and categorize. Why do we have to laboriously inform a computer database, by typing or mousing or tapping a screen, that a perfectly recognizable object has arrived at our doorstep? Why is so much human intervention needed for such a simple task?

It is to correct this deficiency of networked sensibilities that the field of automated identification (auto-ID) has arisen. Auto-ID includes any means of automating the task of identifying a physical object. To date, by far the most common means of doing so is to print a special machine-decipherable *bar code* on an object, and then image or scan the code using an optical transducer to extract an identifying number. One-dimensional bar codes (so named because information is obtained in traversing the pattern in a single direction, not because such patterns are in fact absent depth and height) are easily deciphered and, in the form of the universal product code (UPC) and its more modern descendents, nearly ubiquitous in the commercial world. Two-dimensional bar codes are also available and pack more information into the same space. Optical character recognition (OCR) can be used to acquire information from conventional human-readable text, at the cost of an increase in computing requirements and decreased reliability. However, all optical methods of identifying an object have some deficiencies. Most fundamentally, the sensing device must be able to see the identifying mark: optical techniques require a clear *line of sight*. Not only objects but dirt, paint, ink, and other

objectionably opaque but relentlessly commonplace substances can distort or deface bar codes and other optical marks, obscuring the information that optical auto-ID techniques require. Mechanical damage to the marks or labels degrades their readability. To store more data requires more space, or the use of finer markings visible from a shorter distance. Finally, data stored in printed marks on a surface is not readily modified or extended, save perhaps by wholesale replacement. While optical techniques for object identification are versatile and inexpensive, it is clear that in many cases another approach may be helpful.

To remedy some of the deficiencies of optical ID, we can turn to an alternative technique, radio-frequency identification (RFID). RFID is the use of radio communications to identify a physical object. RFID is really not one but a suite of identification technologies because of the differing characteristics of the radio waves of varying frequency used, and because of the differing approaches to operating the sensors that serve to identify individual objects. RFID has existed for more than half a century, but its widespread application has had to wait for inexpensive integrated circuits to enable small, low-cost *transponders* (the parts of the system that get attached to an object to be identified, more commonly known as RFID *tags*) to be fabricated. Over the last three decades, as the capability of integrated circuits has doubled and the cost per function halved about every 2 years, religiously attending to Gordon Moore's famous law, new RFID applications have become economically feasible. In particular, since the mid-90s, a great deal of effort has been focused on the application of RFID in the manufacture and distribution of goods: *supply chain* management, where until recently the bar code reigned supreme. To serve the needs of manufacturing, distribution, and shipment functions, RFID tags must be very inexpensive, compact, mechanically robust, and readable from at least a meter or two away. As we will examine in more detail in Chapter 2, this combination of requirements has led to the choice of ultra-high-frequency (UHF) radio waves and *passive* RFID tags as the approach of choice for many supply chain applications, and it is UHF RFID technology that is the main topic of this book.

1.2 Why Would You Read This Book?

The purpose of *The RF in RFID* is to provide users of UHF RFID with an understanding of how identification information gets from a tag to a reader and in some cases back to the tag. We will use that understanding to see how the system of tags, readers, and antennas goes together, and analyze the capabilities and limitations resulting from the choices of tag, reader, antenna, and protocol. This book is for people who want to know why things RFID are the way they are and what (if anything) can be done about it, and perhaps be entertained upon occasion along the way.

As we will see as we proceed, the replacement or supplement of bar codes with RFID tags may give rise to a substantial increase in the amount of information available about objects

being made, shipped, or sold, and thus create a need for improved software solutions to enable useful integration of this new knowledge into the existing infrastructure for managing such transactions. The reader must, alas, turn elsewhere for advice and insight on software integration issues: this book is focused on tags, readers, and their interactions. For folks familiar with the OSI reference model for communications systems, *The RF in RFID* is a book about the *physical layer* of a UHF RFID system, with some digressions into the *data link layer*, but no higher.

You don't need a prior acquaintance with radio technology to read the book (although it doesn't hurt), but familiarity with basic electrical engineering concepts of current, voltage, power, frequency, capacitance, and inductance is very helpful. A general familiarity with algebraic manipulation, and the concepts of an integral and derivative, will be needed to follow the derivations of key formulas; a brief review of a few more specialized mathematical tools that are widely used in electrical engineering is provided within the Appendices in the interests of completeness.

1.3 What Comes Next?

The structure of the remainder of this book is depicted in Figure 1.1.

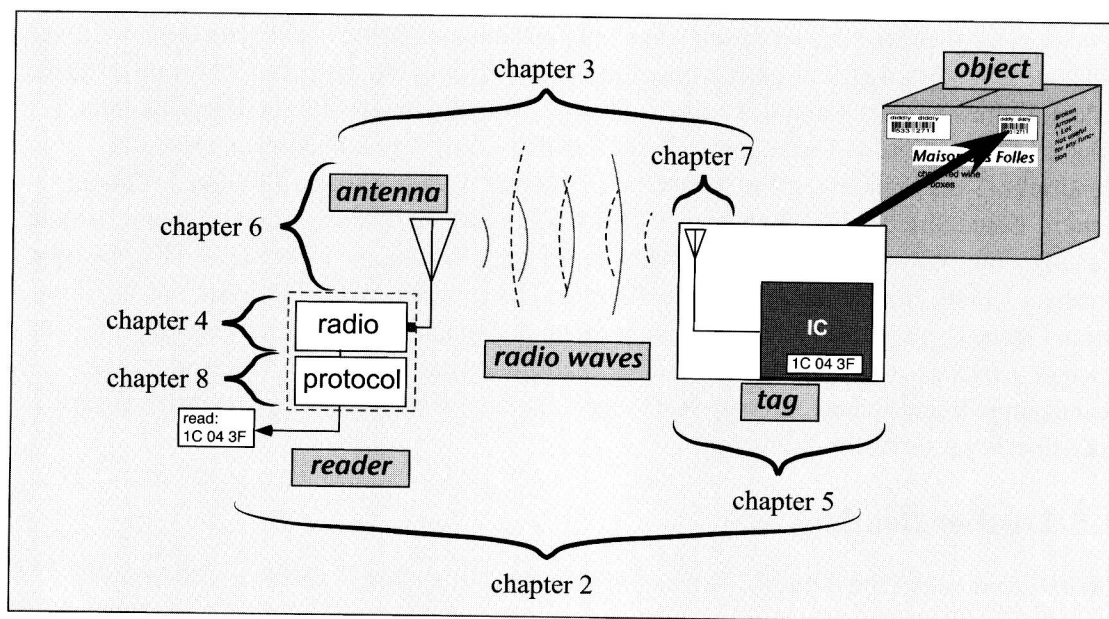


Figure 1.1: Overview of this Book.

Chapter 2 is a general introduction to RFID, including a bit of history, some terminologies, and an examination of the various flavors of RFID and their characteristics and uses. Chapter 3 introduces the reader to the basics of radio technology: transmission, modulation, bandwidth, signal voltage, and power. Chapter 4 describes how the specific radios used in UHF RFID readers work. Chapter 5 delves into the operation of passive UHF RFID tags. Chapter 6 examines reader antennas: how they work and how they are characterized and described. Chapter 7 extends this discussion to the peculiar requirements of passive tag antennas. Chapter 8 reviews the tag-reader protocols used in UHF RFID. A brief Afterword rounds out the main text of the book. Appendices cover some supplemental information, including the radio regulatory world in which manufacturers and users of RFID systems must operate, and some electrical engineering background useful for those from other fields.

In the interests of clarity, detailed citations are not provided within the text. However, each chapter contains a Further Reading section directing the still-curious reader to additional materials related to the topics covered therein. Each chapter (except this one) also contains exercises to provide an opportunity to exercise concepts introduced in the text; answers may be found at the author's web site, www.enigmatic-consulting.com. The book is accompanied by a CD containing hopefully useful and perhaps also entertaining supplementary materials; we shall occasionally draw the reader's attention to those relevant to particular sections of the text.

1.4 Acknowledgments

A book is a collective endeavor even when only one author's name appears on the front cover. This one is no different. The author gratefully acknowledges the assistance of (in no particular order) Andrew Crook, Richard Woodburn, Roger Stewart, Douglas Litten, Barry Benight, Michael Leahy, Gordon Hurst, John Myers, Stephen Colby, Chris Parkinson, Dewayne Hendricks, Titus Wandinger, Jim Mravca, Peter Mares, Dan Deavours, Tali Freed, Gabriel Rebeiz, Louis Sirico, Lilian Koh, Egbert Kong, Michael Lim, Leslie Downey, Craig Harmon, Gene Donlan, William Schaffer, Kathy Radke, Kendall Kelsen, Nick McCurdy, Greg Durgin, Prashant Upreti, Jim Buckner, Bertrand Teplitxky, Kuan Sung, Wong Tak Wai, Tan Jin Soon, Brian Ogata, Sanjiv Dua, and Hank Tomarelli, with apologies to those inadvertently omitted. Special thanks go to my colleagues Dan Kurtz, Nathan Iyer, and Steven Weigand for consistent support and shared curiosity and to John Bellantoni for sharing his extensive experience in every aspect of radio design.

1.5 Further Reading

"RFID Handbook (2nd edition)", Klaus Finkenzeller, Wiley 2004. *This is a wide-ranging introduction to RFID technology and applications, focusing on inductively-coupled systems but with a discussion of UHF RFID. The technical material is challenging for someone*

unfamiliar with the field (though perhaps it will be more accessible after you finish The RF in RFID).

RFID Field Guide, Manish Bhuptani and Shahram Moradpour, Sun Microsystems Press 2005. Marketing- and ROI-focused; a useful complement to the current volume and Finkenzeller's book.

RFID Sourcebook, Sandib Lahiri, IBM Press, 2006. A nice guide for folks who need to implement supply-chain RFID systems, with guidelines, rules of thumb, and checklists for the various aspects of the project.

A great number of diverse web sites touch upon RFID-related matters. Some useful ones are:

RFID Journal, www.rfidjournal.com

Association for Automatic Identification and Mobility (AIM Global), www.aimglobal.org

EPCglobal Inc., www.epcglobalinc.org

RFID Wizards, www.rfidwizards.com

RFID Online Solutions, www.rfidonlinesolutions.com

RFID Tribe, www.rfidtribe.org

RFID Revolution, www.rfidrevolution.com

RFID Switchboard, www.rfidsb.com

History and Practice of RFID

2.1 It All Started with IFF

By the 1930s, the primitive biplanes of fabric and wood that had populated the skies above the battlefields of World War I had become all-metal monoplanes capable of carrying thousands of kilograms of explosives and traveling at hundreds of kilometers per hour: by the time observers could visually identify an incoming flight, it was too late to respond. Detection of airplanes beyond visual range was the task of microwave radar, also under rapid development in the 30s, but mere detection of the presence of aircraft begged the key question: whose side were they on? It was exactly this inability to identify aircraft that enabled the mistaken assignment of incoming Japanese aircraft to an unrelated United States bomber flight and so ensured surprise at Pearl Harbor in 1941. The problem of identifying as well as detecting potentially hostile aircraft challenged all combatants during World War II.

The Luftwaffe, the German air force, solved this problem initially using an ingeniously simple maneuver¹. During engagements with German pilots at the beginning of the war, the British noted that squadrons of fighters would suddenly and simultaneously execute a roll for no apparent reason. This curious behavior was eventually correlated with the interception of radio signals from the ground. It became apparent that the Luftwaffe pilots, when they received indication that they were being illuminated by their radar, would roll in order to change the backscattered signal reflected from their airplanes (Figure 2.1). The consequent modulation of the blips on the radar screen allowed the German radar operators to identify these blips as friendly targets. This is the first known example (at least to the author) of the use of a *passive backscatter* radio link for identification, a major topic of the remainder of this book. *Passive* refers to the lack of a radio transmitter on the object being identified; the signal used to communicate is a radio signal transmitted by the radar station and *scattered* back to it by the object to be identified (in this case an airplane).

¹ Unfortunately, at the moment this is an unverified Internet report, for which I have been unable to find an archival source—but it is such a fun story I had to include it anyway! An authoritative citation for (or debunking of) the story would be appreciated. –DMD

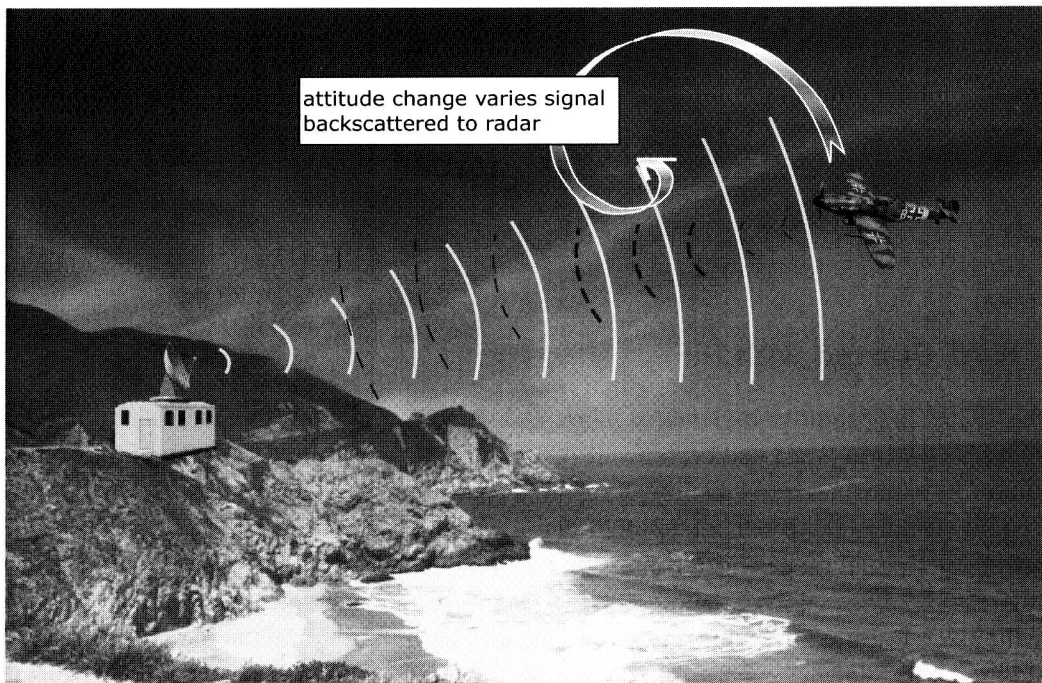


Figure 2.1: The Use of Backscattered Radiation to Communicate With a Radar Operator (not to scale!).

As a means of separating friend from foe, rolling an airplane was of limited utility: any aircraft can be rolled and no specific identifying information is provided. That is, the system has problems with *security* and the size of the *ID space* (1 bit in this case). More capable means of establishing the identity of radar targets were the subject of active investigation during the 1930s. The United States and Britain tested simple IFF systems using an active beacon on the airplane (the XAE and Mark I, respectively) in 1937/1938. The Mark III system, widely used by the Britain, the United States, and the Soviet Union during the war, used a mechanically tunable receiver and transmitter with six possible identifying codes (i.e., the ID space had grown to 2.5 bits). By the mid-1950s, the radar transponder still in general use in aviation today had arisen. Modern transponders are *interrogated* by a pair of pulses at 1030 MHz, in the ultra-high frequency (UHF) band about which we will have a lot more to say shortly. The transponder replies at 1090 MHz with 12 pulses each containing 1 bit of information, providing an ID space of 4096 possible codes. A mode C transponder is connected to the aircraft altimeter and also returns the current altitude of the aircraft. A mode-S transponder also allows messages to be sent to the transponder and displayed for the pilot. Finally, the typical distance between the aircraft and the radar is on the order of one to a few kilometers. Since it takes light about $3 \mu\text{s}$ to travel 1 km, the radar reflection from