


Microwaves Are Everywhere: RFID-Do You Know Where Your Pet Is?

PETER H. SIEGEL ^{1,2,3} (Life Fellow, IEEE)

(Special Series Paper)

¹THz Global, La Canada, CA 91011 USA

²Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125 USA

³NASA Jet Propulsion Laboratory, Pasadena, CA 91109 USA (e-mail: phs@caltech.edu).

ABSTRACT This is the third article in our continuing series of general interest tutorial papers on the applications of microwaves in areas of science and technology that might not be appreciated by every engineer. The tagging of people, animals, and all manner of things for individual identification purposes has been an obsession of humanity since the earliest days of community existence and personal property. Doing so permanently, discretely, and without the possibility of removal or alteration was the realm of science fiction and spy novels until very recently. In this article we examine, from a microwave perspective, the techniques, devices, development and basic operation of the now ubiquitous RFID industry which, in my humble opinion, and like so many technological and science innovations, takes on the mantra of the Roman deity, Janus: *transitioning from a past seeking change for the better, to a future which promises both benefits and dangers in the embrace of new technology*. The author hopes you will enjoy this month's "Microwaves are Everywhere."

INDEX TERMS Microwave tags, RFID, interrogator, backscatter communications, commercial applications of microwaves.

I. INTRODUCTION

The concept of using radio frequency energy to autonomously interrogate and confirm the identity of an object has its roots both in the development of radar and less widely known, in the history of power beaming and listening devices. A series of widely distributed news stories in 2016, about a mysterious illness affecting US and Canadian diplomats in Havana, Cuba, had several experts suggesting that microwave exposure was a likely cause [1]. The supporting results of a comprehensive and very recent (2020) National Academies report [2], page 2 wherein, "*The committee found the unusual presentation of acute, directional or location-specific early phase signs, symptoms and observations reported by DOS (Department of State) employees to be consistent with the effects of directed, pulsed radio frequency (RF) energy*" invokes the notable story of Leon Theremin's "Great Seal bug" well described in [3]–[4], and is an appropriate lead-in to the vast field of radio frequency identification (RFID).

II. HISTORICAL BACKGROUND

Theremin's (Lev Termen¹) ingenious – and completely passive listening device was secretly installed inside a wooden replica of the Great Seal of the United States, which after being presented to the US Embassy in Moscow in 1945, was hung on a wall and remotely activated by a strong CW (continuous wave) microwave beam broadcast from an outside van or nearby building. The "Thing" as it was later called, was

¹Theremin (born in Russia as Lev Sergeyevich Termen, 1896-1993) is a fascinating historic figure spanning the Russian revolution, World War II, Stalin and finally the Cold War era. From his 1928 invention of the capacitively coupled (touch free) musical instrument - the thereminovox (darling of the science-fiction genre and still very much in vogue for its unique design and sounds), to his rise to prominence in Lenin's time, and his subsequent fall and banishment to the Gulag labor camps under Stalin, are the stuff of spy novels. Theremin's inspired invention of the sound-to-RF modulated listening device – a precursor of the RFID tag - while still a prisoner in the war years, spurred his reconciliation and recognition under Khrushchev. However, he ended his remarkable career with a second fall-from-grace under Brezhnev, when he was labelled as a western sympathizer. His, is a thrilling story [5].

a combination RF-and-acoustic device, wherein a vibrating metallic membrane sealing off a highly resonant RF cavity, picked up sound waves in the room and modulated the cavity volume, and hence the resonant frequency. The true genius of the invention was the addition of an antenna to the cavity whose load (and hence reflection coefficient) varied with the cavity dimensions. When illuminated with a strong microwave source (at first thought to be in the 300 MHz range, but later analyzed and determined to have most likely functioned between 1.3 and 1.8 GHz [3], [6]), the reflected power was modulated in sync with the membrane volume changes and the sounds in the room could be recovered with an appropriate backscatter RF receiver. The “Thing” remained in the US Embassy from 1945 until its accidental discovery by British intelligence in 1951 [4]. In 1960, the US Ambassador, Henry Cabot Lodge, revealed the device to the world at a United Nations Security Council meeting directly after the downing of a US U-2 spy plane over the Urals and the capture of pilot, Francis Gary Powers, to show that the Soviet Union also spied on the US [7].

In a prescient paper in 1948, Harry Stockman of Air Materiel Command, Cambridge, Massachusetts, reported on the concept and early experiments in interrogating and remotely reading the broadcasted ID of targets utilizing a highly directive RF transmitter [8]. Stockman correctly pointed out that using frequencies much smaller than the target diameter d ($\lambda \ll d$), yielded a signal-to-noise closer to $1/r^2$, r being the target distance - much higher than what could be achieved from the usual $1/r^4$ radar backscatter signal between two isotropic radiators. He experimented with specific target coded identification using both physically moving (rotating), and audio modulating (sonically exciting one or more reflecting walls which were made of flexible metallic membranes), a directive corner reflector. The reflected microwave power (S and X bands were used) modulated the phase, and less dramatically, the amplitude of the received RF signal, and encoded the particular source modulation. Coded target ID variations were also read out by changing modulation frequencies, and Stockman even suggested covert operation using frequency hopping or embedding coherent signals in noise, which could be separated out through a heterodyne receiver process [8], page 1204. Although Stockman’s targets were not completely passive like Theremin’s “Thing” (the targets contained an audio source and amplifier to modulate the corner reflector membrane, rather than picking up a naturally generated sound wave in the vicinity), the similarity is clear. However, it would take almost a dozen more years before this idea of modulated backscatter communications began to get some serious attention.

The concept of using directed RF beams to transfer power, and then using that power to operate a remote electronic device, is a key component of modern RFID. A passive diode mounted across a dipole antenna and powered through the induced voltage at the dipole terminals could be used to vary the antenna load. A separate modulator, coupled to the diode,

could be employed to send a more noise-immune and easily decoded backscatter signal to the transmitter or reader [9]. By the 1960s high power RF beaming was already being proposed by tube pioneers such as Raytheon’s W.C. Brown [10], [11]. Moreover, operating mW level remote devices using RF energy harvesting via a rectifier circuit, rather than an on-site power source, was also the subject of several patents, notably Robert Richardson’s [12], as early as 1963. Roger Harrington, at Syracuse University [13], and Joseph Ryerson, at Rome Air Development Center [14], both in New York, worked on generating enhanced radar backscatter signals from load modulated targets containing directional antennas (dipoles). Joseph Vogelmann at Chromalloy American Corp., in NY [15], enhanced the concept with an actively modulated ferrite antenna load, and added a demodulation circuit in the receiver that greatly improved signal-to-noise. However, it was Donald B. Harris, who in 1952, first proposed [16], and then eight years later in 1960 [17], extended a patent that combined both the ideas of powering a “batteryless” voice-over-radio transponder from a directed RF beam, and modulating the weakly retransmitted signals back to the localized power source, for demodulating and repeat broadcasting.

Simple inductively coupled systems (two electric coils spaced close enough together to achieve magnetic field overlap) were used in the early 1960s to track train movement past an interrogator, which also supplied power to a passive transponder (via the coupled coil) to activate an oscillator [18]. Less error prone harmonic circuits –frequency f_0 broadcast from the interrogator into a varactor diode on the transponder with nf_0 , n being the higher harmonic number reflected back out to the receiver – were already in operation by the late 1960s for trains [19]. By the early 1970s, variants of both the inductive and fully RF antenna-coupled backscatter transponders with triggered oscillator return or swept frequency resonators, had made their way into the commercial market of 1-bit (“present” or “not present”) Electronic Article Surveillance (EAS) sensing for mitigating theft of merchandise in stores. John Walsh at Sensormatic [20], [21], George Lichtblau [22] at Checkpoint Systems, and Arthur Minasy at Knogo Corporation [23] (swept resonant absorption), were early innovators, and all the associated companies are now multibillion-dollar international entities.

A technology explosion was brewing, as many non-contact coupling ideas, more compact and complex integrated circuit implementations, lower power consumption through CMOS-based IC’s, and new transponder packages with more robust and error free reader communications algorithms, began to be developed for what was shaping up to be an enormous and varied worldwide applications market. Transportation and animal tracking stimulated early prototypes. A short, but very influential PROCEEDINGS OF THE IEEE letter in 1973, by Alfred Koelle et al. [24], at Los Alamos Science Labs, New Mexico, outlined one of the first uses of an RF homodyne radar system to remotely power an oscillator and code generator (12 bit) and process backscatter signals from a transponder

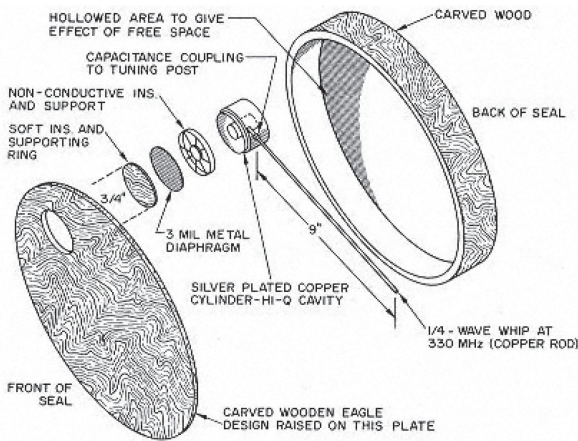


FIGURE 1. Above: Structure of the Theremin "Great Seal Bug". Left: Photo of the wooden wall hanging. From [4], Figs. 2(c). and 2(d). ©IEEE, w/perm.

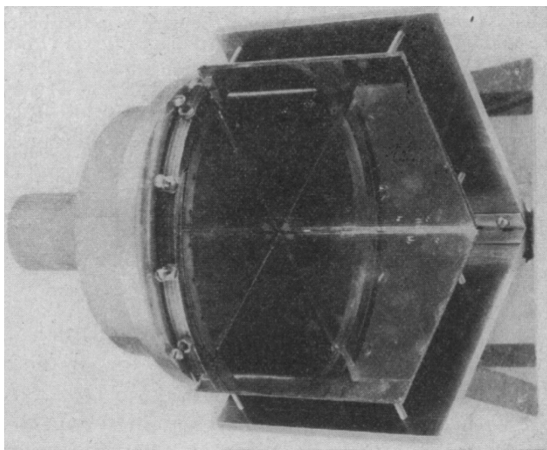


FIGURE 2. Stockman corner-cube with one mirror (left) replaced by a metallic membrane and vibrated through a sonic amplifier. From [8], Fig. 10. ©IEEE, w/perm.

antenna operating in the 915 MHz ISM band (see footnotes 7 and 8 in [25]) with a 20 kHz load modulation. The system was intended for monitoring the temperature and identity of cattle through an applied tag, and the range (limited by the transmitter power) was a few meters. The circuit block diagram is reproduced in Fig. 3. Similar inductively coupled RF backscatter circuits were also being developed for the EAS and direct ID markets at this time [26].

In the transportation sector, a very forward looking and sophisticated prototype automatic highway toll booth-to-vehicle

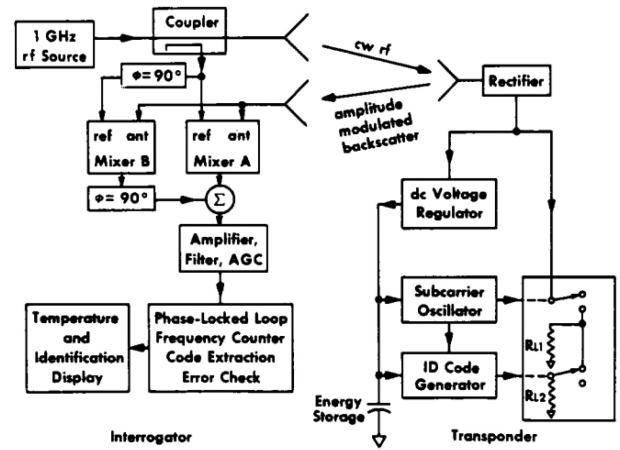


FIGURE 3. Circuit diagram for Los Alamos animal identification and temperature tracking RFID system at 915 MHz. From [24]. ©IEEE, w/perm.

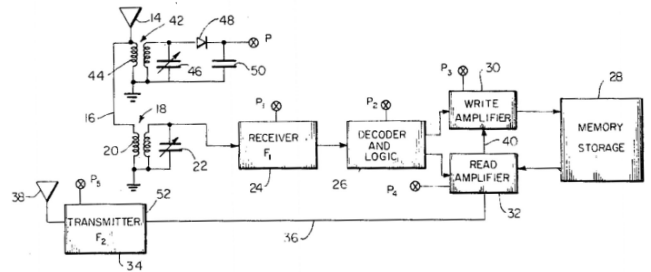


FIGURE 4. Circuit diagram from Cardullo patent [27] showing first use of read/write memory for use in a toll collection system. Fig. 1 from US Patent 3713148. US Patent and Trademark Office.

interrogation system with a read-write memory chip and the capability of storing and deducting multiple payments, was developed, and marketed to the New York Port Authority by Mario Cardullo and William Parks in 1973 [27]. It was partially based on earlier concepts for vehicular tracking [28] that had been gaining steam since the railroad car tracking systems of late 1960s. The growing requirements for very high interrogation speeds (msec), and the ability to operate without direct visual line of sight at meter distances, was well satisfied by the backscatter RF technique. The circuit from Cardullo's patent is shown in Fig. 4.

Except for the EAS market, the RFID field advanced at a snail's pace through the 1970s and 80s. A quick search of US patents post 1975, has the first use of the term "RF identification" in William Bell III's 1976 write up, "Object identification system using an RF roll-call technique" [29]. The patent is for a transponder that receives a carrier modulated with a coded binary sequence that is processed and matched to a predetermined identification sequence on the receiver, and then broadcasts back a frequency shifted carrier signal to acknowledge being "polled" by the reader [29]. Wikipedia credits Proximity Devices, Sunnyvale California founder, Charles

Walton, with the first use of the term “RFID” [30] in his 1983 US patent on “Portable radio frequency emitting identifier” [31], however the author could not find the acronym, or even the fully written out term, in the patent. It definitely shows up by 1990, in Fujitsu’s description of a “radio-frequency identification system” that is based on RF transmission, detection, and retransmission of alternating circularly polarized signals [32]. It also occurs, almost as an afterthought, in David Teller’s et al. 1990 patent granted five months later, on an inventory control system for stacked beverage bottles [33].

In the engineering literature, “RF identification” first appears as a searched block term on IEEE Xplore in 1989, in Peter Hewkin’s of Scientific Generics, U.K., overview of smart tags [34], and as an acronym “RF I.D.” in his conference paper of the same year on automotive applications [35]. The term was just becoming popular in the academic community at this stage, and shows up in a Nanyang Tech. Inst., Singapore, paper by Ooi, Lim, and Lau in Nov. 1989 [36]. Finally, “RFID” appears as a standalone in two papers on vehicular applications in 1991 [37], [38]. Some additional historic details can be found in an often-referenced historical overview on RFID by Jeremy Landt [39].

As the unique capabilities, and the great variety of major tracking and identification problems that could be addressed by radio frequency circuits became clearer, and the costs of chips and circuitry dropped, the field moved heavily into the commercial world, and the number of patents in the US exploded. Between 1975 and 1990 there were only about 100 US patents involving RFID components, systems, or applications. By 2000 this had jumped to 3000. In January 2010 it was 20000 and at the end of 2020, it was over 145000! Similarly, the IEEE Xplore journal and conference papers on RFID topics (metadata) went from just a handful in 1975, to 25 or so in 1990, reached 300 by the year 2000, jumped to 8000 in 2010, and now totals well over 22000, including 170 books and at least one fully devoted topical journal which started in 2017: IEEE JOURNAL OF RADIO FREQUENCY IDENTIFICATION. The monetary worth of the field is estimated to be around 12 billion US dollars today, and to grow to over 26 billion within the next 5 years [40].

III. HOW THEY WORK

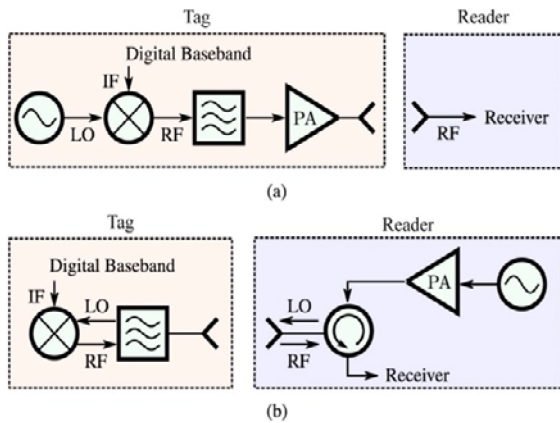
An RFID system in its simplest form, consists of an interrogator (transmitter/reader) and a transponder (receiver/transmitter) or tag, sending or reflecting back a signal that differs in some desirable way from that of the interrogator. Although the interrogator is generally active, as it is supplying a signal for the transponder, the transponder functionality can be broken out into a wide range of operational categories, some of which can be combined or overlapped: analog or digital; passive or active (powered); magnetic or electric field coupled; contacting or contactless; near or remote; smart (contains a CPU) or dumb (preset); static (Read Only) or modifiable (Read/Write); duplex or sequential communications; and other broad preferences.

For purposes of our microwave-centric viewpoint, we consider only RFID systems which are contactless, electric field coupled, and generally separated by distances of many wavelengths. Frequently, this mode of RFID operation is referred to as “backscatter communications.” These systems most often operate in the assigned industrial, scientific, and medical (ISM) bands at 860–960 MHz (UHF), 2.4–2.48 GHz, 5.7–5.9 GHz, and 24–24.3 GHz (microwave). Higher frequency operational bands under restrictive power radiating constraints are currently: 61–61.5, 122–123 and 244–246 GHz [41], Table 5.3. The choice of frequency is based on many considerations, but very broadly (for transponders that are small), the coupling efficiency to the transponder, the operating distance, and the data transfer rates, all increase with higher frequencies, while the line-of-sight tolerance, immunity from interfering objects, and penetration into materials (especially tissue), all decrease as the carrier frequency goes up. At the end of the article we will cover one example of a magnetically coupled interrogator and transponder in the kHz range (HF), as an illustration of where microwaves might play a larger role in the future. HF tags generally use close in inductive coupling circuits (coils) and operate in the 125 and 134 kHz range. An excellent non-technical overview of RFID functions and applications can be found in [42].

Perhaps the most important operational distinction between different backscatter RFID systems is the use of a portion of the incoming RF field to power some functional element on the transponder via energy harvesting with an antenna and rectifier. Without this feature it is hard, although not impossible², to do more than produce a 1-bit ID signal – either “present” or “not present” – as in EAS systems. The RFID can operate in an analog mode with amplitude, phase or frequency modulation – as in the Theremin device [4], or as in early EAS systems that simply altered an antenna load impedance or reflected back harmonics of the carrier generated by a passive nonlinear device on the tag [20]–[23]. Alternatively, a much more flexible and operationally complex digital mode can be realized when sufficient interrogator power is available to energize microchips on the tag. If space, cost, and operational lifetimes are not serious issues, than a tag or transponder can carry a small battery to directly power a strong active response in the presence of an interrogating signal (as in Fig. 5(a)), or to simply power circuitry that is used to perform on-board IC functions and/or modulation of the backscatter signals. In this mode the transponder chip is sometimes referred to as full active.

EPROMS have been the most widely utilized re-programmable storage media on RFID transponders, and advances in CMOS during the 1990’s allowed the implementation of extremely efficient and fast Schottky diode rectifiers (for energy harvesting), and a wide range of digital operations that could be encoded onto a single microchip. These

²For example, one could use an interrogator with a swept frequency signal and a transponder with multiple resonances, or the interrogator signal could induce changes in the transponder that are separately modulated by internal or external processes.



Comparison between simple (a) active (transmitting; ASK) against (b) passive (backscattering; load-modulated) communication topologies.

FIGURE 5. Passive or semiactive (below) and active (above) RFID circuit block diagrams. From [44]. ©IEEE, w/perm.

circuit advances meant that entire RFID transponders could be shrunk to the scale of a few millimeters, with the limiting size component often the RF antenna. At this scale RFID transponders could be integrated into paper, plastic tags, cards, pills, and even cloth or textile yarn [43], costing only a few cents. A typical digital active and passive (semi-active) RFID component structure is reproduced from [44] in Fig. 5.

In a digital circuit and communications protocol, the RFID interrogator and tag function as a MODEM (modulator-demodulator), and signal modulation can take on any of the three broad standards: amplitude, frequency, or phase shift keying – ASK, FSK or PSK, as illustrated in Fig. 6, which is reproduced from [41]. Typically, the communications follow a half-duplex timing sequence which allows the interrogator power to be harvested and stored in capacitors on board the tag during the listening phase, and then converted and used in the talking sequence for power-on modulation and other IC functions. A typical front-end circuit configuration is reproduced from [45] in Fig. 7.

The interrogator usually operates in an environment wherein many potential transponders reside within the polling range, and therefore communications have to implement one or more of the common multiplexing schemes graphically illustrated in Fig. 8 .

In addition, collision – the simultaneous receipt of data response sequences from multiple tags – has to be dealt with using fairly sophisticated digital polling or binary search protocols that can be interrogator initiated (synchronous) or transponder initiated (asynchronous). These have a wide range of clever implementations – often proprietary – and can make or break a particular application by greatly improving tag throughput or reducing data errors [41]. As RFID backscatter applications – especially longer-range systems, but also short range secure card transfers - began to proliferate, protection against hacking and data theft through unwarranted eavesdropping moved to center stage. An enormous and growing

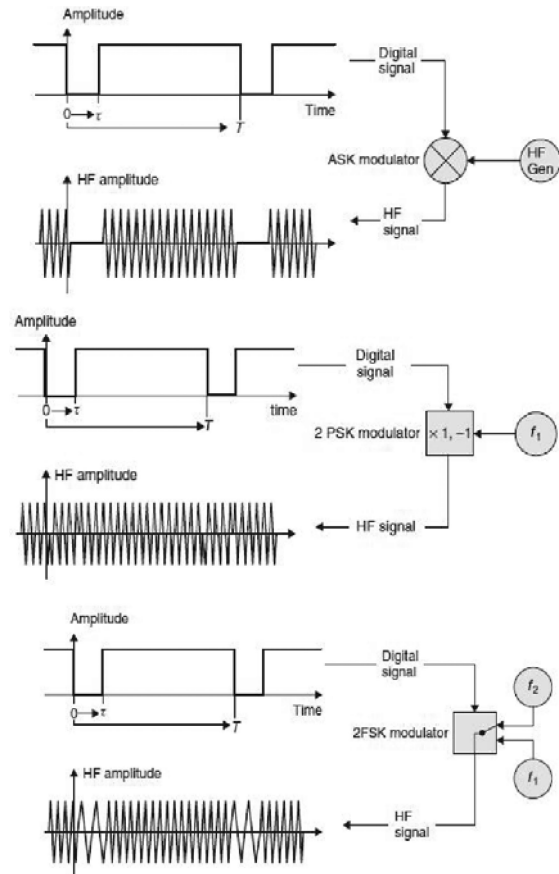


FIGURE 6. Amplitude, Phase and Frequency Shift Keying. From [41]. Figs. 6.7, 6.9 and 6.11 combined. ©John Wiley & Sons, w/perm.

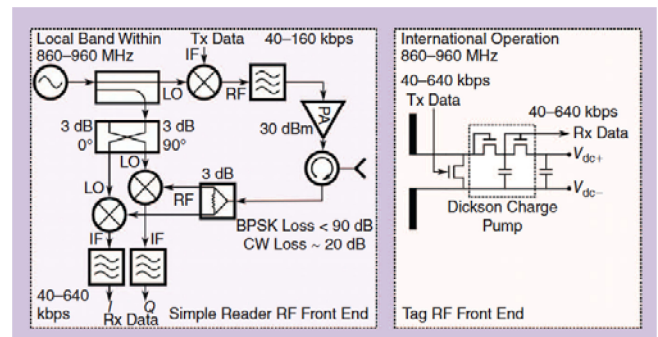


FIGURE 7. Typical front end circuitry for a digital ASK RFID system at UHF frequencies. From [45], Fig. 3. ©IEEE, w/perm.

effort is now being placed on both authentication and encrypted keying for interrogators and transponders [46], [47].

Given the proclivity by industry and governments to utilize RFID technology for everything from inventory control, to package tracking, to secure transactions, to automotive and transportation systems, to monitoring animals and people, and now present in every corner of the industrialized world for the Internet of Things, one would hope that a variety of safety and security controls and standards were in place. This is

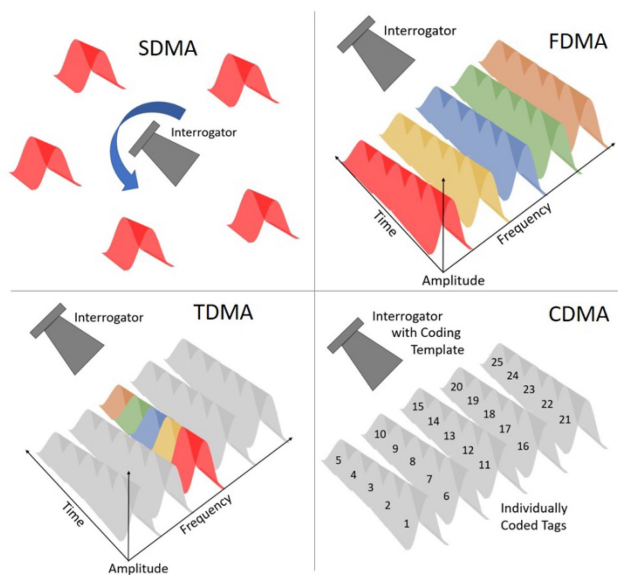


FIGURE 8. Graphic depictions of the four major interrogator modes: Spatial division multiple access (SDMA) – tags polled in different directions, Frequency division multiple access (FDMA) – each tag uses a different frequency, Time division multiple access (TDMA) – tags polled sequentially, and Code division multiple access (CDMA) – tags respond with specific assigned IDs. All modes require anti-collision mitigations.

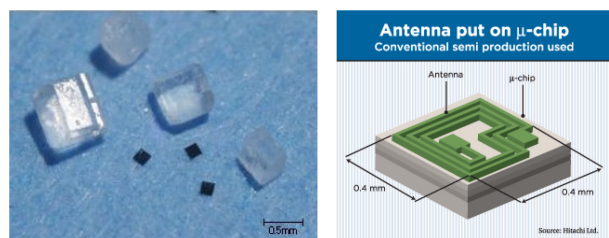


FIGURE 9. Left: Hitachi 2.45 GHz RFID 0.16 mm² chips next to salt grains [52]. Right: integrated antenna/capacitor schematic [51]. Interrogator-transponder distance is ~50 cm [53]. Images Hitachi, Ltd. Press releases from 2003 and 2006 [51], [52].

partially true, as many ISO and ANSI standards have been developed and widely deployed to help standardize readers and transponders across industries, applications and countries, but also for regulating RF frequency usage, exposure and interference [48], [49], but there is still a long way to go. Universal interrogators and transponders for every available frequency band, communications protocol, and RFID form factor are not yet available, and the variety and expansion of the technology and applications seems to be growing much faster than most standards.

The race to create ever smaller digital RFID microchips has already surpassed the realm of science fiction. In 2001, Hitachi Corp. released a 0.4 × 0.4 mm silicon-on-insulator CMOS microchip with an integrated 2.45 GHz antenna/rectifier, and e-beam written 128-bit ROM ID [50], [51]. In 2006, the chip was reduced to 0.15 × 0.15 mm × 7.5 microns thick, boasted antenna coupling pads on both surfaces,

and had a backscatter range of almost 50 cm using a 300 mW interrogator [52], [53]! These chips are commonly referred to now as “smart dust.”

IV. USE IN ANIMALS: DO YOU KNOW WHERE YOUR PET IS?

Animal identification was one of the driving applications for compact RFID tags and there was strong early interest in completely passive tags that were small enough to be non-surgically implanted (injected) and carried subcutaneously. A very complete and well-written history of animal RFID systems and functionality can be found in [54], and the following draws heavily on this reference.

Around the same time as the Los Alamos backscatter homodyne system [24] was being publicized, several very complete and all passive (energy harvesting) inductively coupled interrogator-transponder circuits were already in the patent queue. Jorgen Vinding’s 1967 “Interrogator-responder identification system,” [55] and Thomas Kriofsky and Leon Kaplan’s 1975 patent on, “Inductively coupled transmitter-responder arrangement,” [56] were particularly groundbreaking and influential. One of the earliest RFID patents to emphasize small size and the possibility of animal implantation was granted to Michael Beigel of International Identification Corporation, Rosemount, NJ, in 1982 [57]. The tag operated passively through inductive coupling and on-board capacitors, and contained a fixed identification sequence generated by an analog counter and a one bit PROM. The patent describes the fully implantable capsule size as approximately 6 × 6 × 1.5 mm. A single chip version of a similar circuit with frequency shift keying and full memory storage capability was patented by Thomas Milheiser of Identification Devices, Inc., Boulder Colorado, in 1988 [58], and according to [59], this device was specifically intended for injection into animals. However, these devices still had separate antenna/coils, rectifier, and digital signaling components. A complete single chip structure, with all components integrated onto the silicon (as in [50]) was proposed in 1989 [59], but not realizable at the time.

In addition to the small scale of the transponder, there was also a biomaterials compatibility issue to overcome, as well as a means of stabilizing the position of the device within the tissue of the host animal over an extended time period. A series of patent applications from Vern Taylor et al. of Destron/IDI Inc. (formerly Identification Devices, Inc.) and Hughes Aircraft in Boulder, Colorado [60], culminated in the precursor of the modern injectable animal RFID tag in 1993. The final patent [60], describes a completely glass sealed, needle injected, passive transponder with a small diameter inductive coil of 1200 turns of 1 mil aluminum wire around a ferrite core (6500 microhenry), and a single chip FSK modulated coding element with on board rectifier, and without the need for capacitive storage (the response was sent while the interrogator signal was present). The RFID capsule was intended for monitoring fish that passed by a dam on the Colorado river, and was only 2.1 mm diameter and 10.2 mm long!

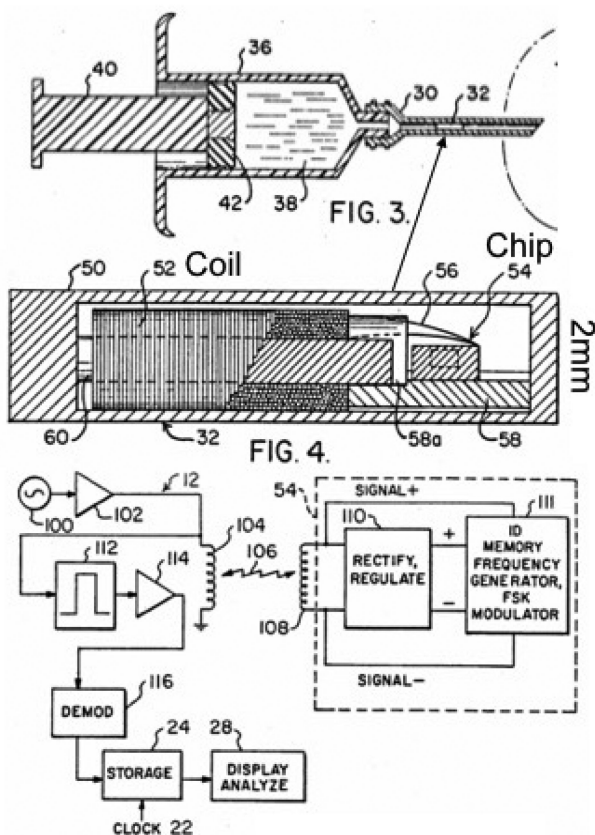


FIGURE 10. Taylor et al. encapsulated, injectable RFID tag and circuit. From [60], US Patent and Trademark Office.

The transponder functioned at around 400 kHz and operated up to a distance of approximately 5 cm. It was produced commercially by Destron and Hughes in the late 1980's. Drawings from the Taylor patent are reproduced in Fig. 10, and show the hypodermic, encased capsule with interior coil and chip, and interrogator-transponder circuitry.

The Destron system inspired a plethora of improvements and innovations including working at lower frequencies (125 and 134 kHz) to take advantage of regulated bands and communications protocols in the US and Europe [61], increasing the transponder read distance with more sensitive interrogator circuitry [62], new modulator protocols to increase the telemetry speed [63], and even the inclusion of continuous temperature monitoring in the transponder [64]. The non-reactive, biocompatible glass package and its placement in the fatty tissue just below the skin, has proven to be an outstanding success for long term tracking and identification of animals from livestock, to pets of all sizes and types. The encapsulated transponders do not migrate from their injected locations if the placement is done properly. Trovan Ltd., U.K., started in 1988, was an early commercial innovator, and is now a multinational company with 360 million transponders in animals worldwide. One of the largest current suppliers of injectable microchips for pets, Datamars, Inc., Lugano

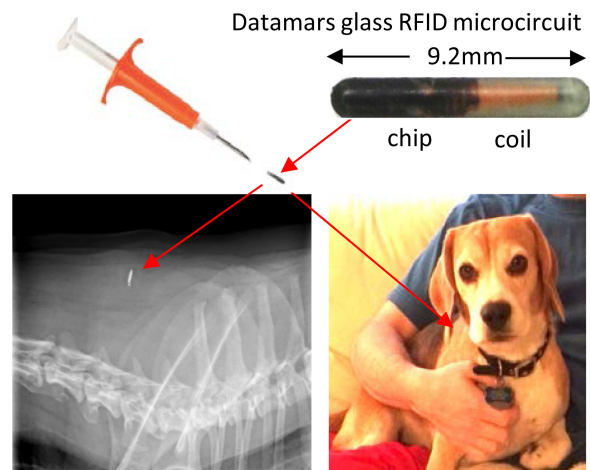


FIGURE 11. Datamars 135 kHz glass RFID microcircuit 981013B (upper right) with injection needle (upper left) for pets (lower right) and X-Ray of inserted chip 12 years after injection (lower left) into Maxwell! X-Ray courtesy Kym Mitchell, DVM, Montrose Pet Hospital, Montrose, CA, USA, April 11, 2021. Datamars microchip and needle images with permission from Petlink.

Switzerland, operating internationally under Petlink, Inc., maintains a complete worldwide “lost and found” pet database repository. Datamars has about 40% of the RFID pet market and boasts a biocompatible polymer-based 11mm long \times 1.6 mm diameter transponder casing with 64-bit memory, a read distance of 24 cm, and operates at 134 kHz under ISO 11784 and 11785. My own canine companion, Maxwell, has had one of the earlier glass versions of the Datamars transponders between his shoulder blades since 2009 (Fig. 11).

In case you were wondering, the 2020 Covid pandemic year was the best in Datamars 30-year history, with 11 million newly adopted and tagged pets in the US alone! This is one application where higher frequency tags (UHF and even microwave) could play a major role as they develop more fully, adding useful monitoring and tracking capabilities that can only work effectively at the greater interrogator-transponder distances enabled by the higher frequencies and more efficient power coupled backscatter techniques.

V. USE IN PEOPLE: WE KNOW WHO & WHERE YOU ARE

The RFID industry has exploded with the rise of the Internet of Things. Everything valuable we own (including ourselves) may soon be connected and trackable. In 1998, Kevin Warwick, a cybernetics professor at the University of Reading, U.K. was the first reported person to have an RFID chip implanted into his body [65]. The procedure was surgically performed – since the capsule was 23×3 mm – and the insert was removed after 9 days. The US Food and Drug Administration approved the use of an implantable microchip – the Verichip - for identification purposes in humans in 2004, at the request of a Florida company [66], Applied Digital Solutions. In 2009, British scientist Mark Gasson had an RFID device

implanted in his hand and then he introduced a computer virus into the implant – becoming the first computer virus infected human [67]!

The rapid improvement of microwave backscatter systems, aided by higher frequency operation, more directional and highly coupled antennas [68], smaller and much more functionalized and complex CMOS chips, and faster and less error prone communications protocols, may soon replace the close-in-only inductively coupled reader and transponder RFID systems in common use. Along with the preponderance of sophisticated and flexible transceiver-based devices already carried by nearly every person in the form of their cell phone, that are constantly linked to networks in every corner of the globe, the addition of embedded microscopic, attached or printed-on tags, and even tissue implanted RFID transponders, is already having a revolutionary impact on society. The upcoming controversies over individual privacy with the ability to absolutely identify and/or track both goods and individuals – wherever they might be – and the fears that society could be reduced to a panopticon – where a central authority can monitor every individual, should not be taken lightly. If you have any doubts about the timeliness of this revolution, be sure to check out Apple’s new Air Tags – a blue tooth network that can access any iPhone in the world to locate your tagged device – with permission, of course! On the flip-side, RFID will unify and simplify our lives in so many ways. As mentioned in the abstract, this is definitely a *Janus technology*!

VI. SUMMARY & CONCLUDING REMARKS

In a short summary of this sort, it is impossible to cover a field now as vast as the RFID industry. The field is so large, so well capitalized, and changing and evolving so rapidly, that any overview is out of date between the original drafting and publication! The worldwide standards in the UHF bands in particular, are still rolling out, and updates are being implemented even before the standards have been fully adopted [69]. In addition, RFID technology, and the transponder tags in particular, are continuously evolving – like sentient lifeforms – as they add new functionality, information gathering capabilities, and embed themselves in more and more processes that interact with, and sometimes dictate our own behaviors!

The author can only hope he has given the reader a bit of the history and a few of the most common operational parameters that are encompassed in the components and implementation. Perhaps the most appropriate summary of the RFID field comes from previously mentioned RFID pioneer, Jeremy Landt, who wrote in his popular historical account of the field [39], “*At first glance, the concept of RFID and its application seems simple and straightforward. But in reality, the contrary is true. RFID is a technology that spans systems engineering, software development, circuit theory, antenna theory, radio propagation, microwave techniques, receiver*

design, integrated circuit design, encryption, materials technology, mechanical design, and network engineering, to mention a few. Increasing numbers of engineers are involved in the development and application of RFID, and this trend will likely continue.”

ACKNOWLEDGMENT

The author would like to thank Steve Wilcox of Petlink (a division of Datamars SA, Switzerland) for an interesting conversation on the Datamars RFID system for pets and permission to use the images at the top of Figure 11. Thanks are also extended to Dr. Kym Mitchell of Montrose Pet Hospital for the X-Ray image of Maxwell in Fig 11, and for many years of quality care. The author also thanks Dr. Alex Siegel for reference [41] and Dr. Heather Lee for help with some of the images in Fig. 8. Finally, the author is grateful for many useful comments and corrections from one of the reviewers, who also very appropriately reminded the author that Janus, or a counterpart, does not exist in the Greek mythological cosmos (originally attributed in the Abstract), but rather is strongly anchored in the more pragmatic Roman pantheon of deities. This reviewer also pointed out the similarity between the ever evolving and improving RFID chips, and the continual change and adaptation of organic lifeforms. He/she may not be too far off the mark!

REFERENCES

- [1] B. A. Golomb, “Diplomat’s mystery illness and pulsed radiofrequency/microwave radiation,” *Neural Comput.*, vol. 30, pp. 2882–2985, 2018.
- [2] The National Academies of Sciences, Engineering, and Medicine, “An assessment of illness in U.S. government employees and their families at overseas embassies,” D. A. Relman, and J. A. Pavlin, Eds., Washington, DC, USA: The National Academies Press, Study Report, 2020, 76 pages. [Online]. Available: <https://doi:10.17226/25889>.
- [3] Crypto Museum, “The thing, great seal bug.” Created Sep. 18, 2015. Accessed: Apr. 13, 2021. [Online]. Available: <https://www.cryptomuseum.com/cover/bugs/thing/index.htm>
- [4] P. Nikitin, “Leon Theremin (Lev Termen),” *IEEE Antennas Propag. Mag.*, vol. 54, no. 5, pp. 252–257, Oct. 2012.
- [5] A. Glinsky, *Theremin: Ether Music and Espionage*. Urbana, IL, USA: Univ. Illinois Press, Sep. 14, 2000, 480 pages, ISBN-10 0252025822.
- [6] G. Brooker and J. Gomez, “Lev Termen’s great seal bug analyzed,” *IEEE Aerosp. Electr. Syst. Mag.*, vol. 28, no. 11, pp. 4–11, Nov. 2013.
- [7] Conseil de Sécurité, “Security Council official records, 15th year, 860th meeting,” S/PV860, paragraph 85, 16 pp., 1960. Accessed: Mar. 29, 2021. [Online]. Available: https://www.un.org/ga/search/view_doc.asp?symbol=S/PV.860
- [8] H. Stockman, “Communication by means of reflected power,” *Proc. IRE*, vol. 36, no. 10, pp. 1196–1204, 1948.
- [9] J. H. Richmond, “A modulated scattering technique for measurement of field distributions,” *IRE Trans. Microw. Theory Techn.*, vol. 3, no. 4, pp. 13–15, 1955.
- [10] W. C. Brown, “Experiments in the transportation of energy by microwave beam,” *1958 IRE Int. Conv. Rec.*, vol. 12, no. 2, pp. 8–17, 1964.
- [11] W. C. Brown, “The technology and application of free-space power transmission by microwave beam,” *Proc. IEEE*, vol. 63, no. 1, pp. 11–25, Jan. 1973.
- [12] R. M. Richardson, “Remotely actuated radio frequency powered devices,” U.S. Patent 3,098,971, Jul. 23, 1963.
- [13] R. L. Harrington, “Field measurements using active scatterers,” *IEEE Trans. Microw. Theory Techn.*, vol. 11, no. 5, pp. 454–455, Sep. 1963.
- [14] J. L. Ryerson, “Scatter echo area enhancement,” *Proc. IRE*, vol. 50, no. 9, pp. 1979–1980, Sep. 1962.

- [15] J. Vogelman, "Passive data transmission technique utilizing radar echoes," U.S. Patent 3,391,404, Jul. 2, 1968.
- [16] D. B. Harris, "Radio transmission system," U.S. Patent 2,607,004, Aug. 12, 1952.
- [17] D. B. Harris, "Radio transmission systems with modulatable passive responder," U.S. Patent 2,927,321, Mar. 1, 1960.
- [18] R. A. Kleist and C. S. Jones, "Responder device," U.S. Patent 3,018,475, Jan. 23, 1962.
- [19] M. H. Postman, "Interrogator-responder signaling system," U.S. Patent 3,384,892, May 21, 1968.
- [20] J. Welsh, R. Vaughan, and L. L. Gordon, "Article surveillance method and system," Canadian Patent CA947398A, granted May 1974 with U.S. application US63925067A, Mar. 30, 1967.
- [21] J. Welsh and R. Vaughan, "Article surveillance," U.S. Patent 4,063,229, Dec. 13, 1977.
- [22] G. Lichtblau, "Electronic security systems," U.S. Patent 3,810,147, May 5, 1971.
- [23] A. Minasy, "Apparatus for article theft detection," U.S. Patent 3,696,379, Oct. 3, 1972.
- [24] A. Koelle, S. Depp, and R. Freyman, "Short-range radio-telemetry for electronic identification, using modulated RF backscatter," *Proc. IEEE*, vol. 63, no. 8, pp. 1260–1261, Aug. 1975.
- [25] P. H. Siegel, "Microwaves are everywhere: Ovens - from magnetrons to metamaterials," *IEEE J. Microwaves*, vol. 1, no. 2, pp. 523–531, Apr. 2021.
- [26] J. P. Vinding and A. R. Koelle, "Comments on 'Short-range radio-telemetry for electronic identification, using modulated RF backscatter,'" *Proc. IEEE*, vol. 64, no. 8, p. 1255, Aug. 1976.
- [27] M. Cardullo and W. L. Parks III, "Transponder apparatus and system," U.S. Patent 3,713,148, Jan. 23, 1973.
- [28] A. S. Palatnick and H. R. Inhelder, "Automatic vehicle identification systems—Methods of approach," *IEEE Trans. Veh. Technol.*, vol. 19, no. 1, pp. 128–136, Feb. 1970.
- [29] W. Bell, "Object identification system using an RF roll-call technique," U.S. Patent 3,981,011, pp. 8, col. 1, line 44, Sep. 14, 1976.
- [30] Wikipedia, "Charles Walton (inventor)," Accessed: Apr. 14, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Charles_Walton_inventor
- [31] C. Walton, "Portable radio frequency emitting identifier," U.S. Patent 4,384,288, May 17, 1983.
- [32] H. Sugawara and H. Ashida, "Radio-frequency identification system," U.S. Patent 4,926,187, May 15, 1990.
- [33] D. M. Teller, R. Sheryll, and L. Ong, "Inventory control system," U.S. Patent 4,961,533, pp. 15, col. 16, line 35, Oct. 9, 1990.
- [34] P. Hewkin, "Smart tags—the distributed-memory revolution," *IEE Rev.*, vol. 35, no. 6, pp. 203–206, Jun. 22, 1989.
- [35] P. F. Hewkin, "Future automatic identification technologies," in *IEE Colloq. Use Electron. Transponders Automat.*, London, U.K., 1989, pp. 6/1–6/10, Feb. 15, 1989.
- [36] T. H. Ooi, C. H. Lim, and K. T. Lau, "Low cost RF identification and locating system," *IEEE Trans. Consum. Electron.*, vol. 35, no. 4, pp. 831–839, Nov. 1989.
- [37] P. Davies, C. Hill, and J. Siviter, "AVI research for commercial vehicle operations," in *Proc. Veh. Navigation Inf. Syst. Conf.*, Troy, MI, USA, 1991, pp. 97–102.
- [38] R. F. Peelen, "Problems and opportunities of nonstop vehicle recognition," in *IEE Colloq. Technol. Road Pricing Route Guid.*, London, U.K., 1991, pp. 3/1–3/8.
- [39] J. Landt, "The history of RFID," *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, Oct./Nov. 2005.
- [40] IDTechEx, "RFID forecasts, players and opportunities 2019–2029," Accessed Apr. 25, 2021. [Online]. Available: <https://www.idtechex.com/en/research-report/rfid-forecasts-players-and-opportunities-2019-2029/700>
- [41] K. Finkenzerler, *RFID Handbook*, 2nd ed. (translated by R. Waddington, Ed.) West Sussex, U.K.: Wiley, 2003.
- [42] V. D. Hunt, A. Puglia, and M. Puglia, *RFID-A Guide to Radio Frequency Identification*. Hoboken, NJ, USA: Wiley-Interscience, 2007.
- [43] G. Andia, "Slenderly and conformable passive UHF RFID yarn," in *Proc. IEEE Int. Conf. RFID*, 2017, pp. 130–136.
- [44] D. G. Kuester, D. R. Novotny, and J. R. Guerrieri, "Baseband signals and power in load-modulated digital backscatter," *IEEE Antennas Wirel. Propag. Lett.*, vol. 11, no. 11, pp. 1374–1377, Nov. 16, 2012.
- [45] D. Kuester and Z. Popovic, "How good is your tag?: RFID backscatter metrics and measurements," *IEEE Microw. Mag.*, vol. 14, no. 5, pp. 47–55, Jul./Aug. 2013.
- [46] A. Kumar, A. Jain, and M. Dua, "A comprehensive taxonomy of security and privacy issues in RFID," *Complex Intell. Syst.*, vol. 7, pp. 1327–1347, 2021, doi: [10.1007/s40747-021-00280-6](https://doi.org/10.1007/s40747-021-00280-6).
- [47] T. Nandy *et al.*, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151054–151089, 2019.
- [48] IEEE, "Information technology—Smart transducer interface for sensors and actuators—Part 7: Transducers to radio frequency identification (RFID) systems communication protocols and transducer electronic data sheet (TEDS) formats," *ISO/IEC/IEEE 21451-7:2011(E) (Revision of 1451.7-2010)*, pp. 1–92, Feb. 10, 2012.
- [49] IEEE, "IEEE health informatics—PoC medical device communication part 00101: Guide—guidelines for the use of RF wireless technology," *IEEE Standard 11073-00101-2008*, pp. 1–125, 2008.
- [50] M. Usami, "The world's smallest RFID chip technology," H. Casier, M. Steyaert, A. van Roermund Eds., in *Analog Circuit Design*. Dordrecht, Netherlands: Springer, Part III, pp. 277–288, 2011.
- [51] Y. Hara, "Hitachi process embeds antenna on RF identification chip," EDN, Sep. 15, 2003. Accessed May 6, 2021. [Online]. Available: <https://www.edn.com/hitachi-process-embeds-antenna-on-rf-identification-chip/>
- [52] Hitachi Ltd., "World's smallest and thinnest 0.15 x 0.15 mm, 7.5µm thick RFID IC chip," News Release, Feb. 6, 2006. Accessed May 6, 2021. [Online]. Available: <https://www.hitachi.com/New/cnews/060206.html>
- [53] M. Usami *et al.*, "An SOI-based 7.5µm-thick 0.15x0.25mm² RFID chip," ISSCC 2006, session 17, paper 17.1, 10 pages, Feb. 7, 2006.
- [54] P. R. Troyk, "Injectable electronic identification, monitoring, and stimulation systems," *Annu. Rev. Biomed. Eng.*, vol. 1, pp. 177–209, 1999.
- [55] J. P. Vinding, "Interrogator-responder identification system," U.S. Patent 3,299,424, Jan 17, 1967.
- [56] T. A. Kriofsky, and L. M. Kaplan, "Inductively coupled transmitter-responder arrangement," U.S. Patent 3,859,624, Jan. 7, 1975.
- [57] M. Beigel, "Identification device," U.S. Patent 4,333,072, Jun. 1, 1982.
- [58] T. A. Milheiser, "Identification system," U.S. Patent 4,730,188, Mar. 8, 1988.
- [59] G. T. Carroll, "Single chip transponder device," U.S. Patent 4,857,893, Aug. 15, 1989.
- [60] V. Taylor, D. Koturov, J. Bradin, and G. E. Loeb, "Syringe-implantable identification transponder," U.S. Patent 5,211,129, May 18, 1993.
- [61] G. A. DeMichele, "Impedance matching coil assembly for an inductively coupled transponder," U.S. Patent 5,084,699, Jan. 28, 1992.
- [62] M. A. K. Schwan and P. R. Troyk, "High efficiency driver for transcutaneously coupled coils," *Proc. Annu. Int. Eng. Med. Biol. Soc.*, vol. 5, pp. 1403–1404, 1989.
- [63] P. R. Troyk and G. A. DeMichele, "Method and apparatus for producing a subcarrier signal for transmission by an inductively coupled transponder," U.S. Patent 5,198,807, Mar. 30, 1993.
- [64] D. J. Urbas and D. Ellwood, "System monit. programmable implantable transponder," U.S. Patent 5,252,962, Oct. 12, 1993.
- [65] K. Warwick, "Questions for Kevin Warwick," *New York Times Mag.*, section 6, p. 27, Sunday, Oct. 4, 1998. [Online]. Available: <https://www.nytimes.com/1998/10/04/magazine/sunday-october-4-1998-questions-for-kevin-warwick.html>
- [66] J. H. Tanne, "FDA approves implantable chip to access medical records," *BMJ*, vol. 329, Nov. 6, 2004, Art. no. 1064.
- [67] M. N. Gasson, "Human enhancement: Could you become infected with a computer virus?," in *Proc. IEEE Int. Symp. Technol. Soc.*, 2010, pp. 61–68.
- [68] K. V. S. Rao, P. V. Nikitin, and S. F. Lam, "Antenna design for UHF RFID tags: A review and a practical application," *IEEE Trans. Antennas Propag.*, vol. 53, no. 12, pp. 3870–3876, Dec. 2005.
- [69] The Global Language of Business, "Regulatory status for using RFID in the EPC gen2 (860 to 960 MHz) band of the UHF spectrum," GS1, 21 pp. Accessed: May 10, 2021. [Online]. Available: https://www.gs1.org/sites/default/files/docs/epc/uhf_regulations.pdf



PETER H. SIEGEL (Life Fellow, IEEE) received the B.A. degree in astronomy from Colgate University, in 1976, the M.S. degree in physics from Columbia University, in 1978, and the Ph.D. degree in electrical engineering (EE) from Columbia University, in 1983. He has held appointments as a Research Fellow and Engineering Staff with the NASA Goddard Institute for Space Studies, New York City, NY, USA, from 1975 to 1983, a Staff Scientist with the National Radio Astronomy Observatory, Central Development Labs,

Charlottesville, VA, USA, from 1984 to 1986, a Technical Group Supervisor and Senior Research Scientist at the Jet Propulsion Laboratory (JPL), National Aeronautics and Space Administration (NASA), Pasadena, CA, USA, from 1987 to 2014, and a Faculty Associate in electrical engineering and Senior Scientist in biology at the California Institute of Technology (Caltech), Pasadena, CA, USA, from 2002 to 2014. At JPL, he founded and led for 25 years, the Submillimeter Wave Advanced Technology (SWAT) Team, a group of over 20 scientists and engineers developing THz technology for NASA's near and long-term space missions. This included delivering key components for four major satellite missions and leading more than 75 smaller research and development programs for NASA and the U.S. Department of Defense. At Caltech, he was involved in new biological and medical applications of

THz, especially low-power effects on neurons and most recently millimeter-wave monitoring of blood chemistry. He was an IEEE Distinguished Lecturer and the Vice-Chair and Chair of the IEEE MTTT THz Technology Committee. He is currently an elected member of the MTTT AdCom. He has more than 300 articles on THz components and technology and has given more than 250 invited talks on this subject throughout his career of 45 years in THz. His current appointments include the CEO of THz Global, a small research and development company specializing in RF bio-applications, a Senior Scientist Emeritus of biology and electrical engineering with Caltech, and a Senior Research Scientist Emeritus and a Principal Engineer with the NASA Jet Propulsion Laboratory. Dr. Siegel has been recognized with 75 NASA technology awards, ten NASA team awards, the NASA Space Act Award, three individual JPL awards for technical excellence, four JPL team awards, and the IEEE MTTT Applications Award in 2018. He is honored to take up the responsibility as the Founding Editor-in-Chief of IEEE JOURNAL OF MICROWAVES, which he hopes will invigorate the microwave field. Among many other functions, he served as the Founding Editor-in-Chief for IEEE TRANSACTIONS ON TERAHERTZ SCIENCE AND TECHNOLOGY, from 2010 to 2015, and the Founder, in 2009, Chair through 2011, and elected General Secretary since 2012, of the International Society of Infrared, Millimeter, and Terahertz Waves (IRMMW-THz), the world's largest society devoted exclusively to THz science and technology.