Don Lancaster's

Tech Musings

January, 1996

Several helpline callers have asked me what I thought of certain invention marketing firms. Well, I firmly believe that *if you have to ask, your product is doomed to failure!*

Asking this question proves to me that you remain an industry outsider. Almost always, industry outsiders are fruitlessly laboring on non-solutions to non-problems.

Industry outsiders *always* commit one or more of what those French Veterinarians call a *four paw*. One or more laughingly absurd assumptions about marketing, demand, patents, competition, sales channels, or the value of any totally undeveloped and unproven concept.

Even if we ignore that sad history of invention marketing scams and the 100 percent complaint rate that I've gotten over these outfits on our help line, it all boils down to this:

An invention marketing firm is extremely unlikely to ever generate a worthwhile long term net positive cash flow for you.

But it does turn out that there are useful alternates known as *Product Development Assistance Providers*.

Here's how you tell the two apart: A product assistance provider should *always* (A) Be hard to find because they will never have to advertise; (B) *never* use *any* sales techniques, let alone those high pressure ones; (C) repeatedly and pointedly tell you up front that your concept has major flaws and monumental risk factors; (D) offer you low cost services on an exactly stated cash-and-carry basis; and, of course, (E) gladly provide a satisfied client list.

I've posted a long list of product development assistance providers as INVENORG.PDF on *www.tinaja.com* Another good source for this type of info are those superb annual freebie directories published by *Batelle*.

Check these out.

The really sad thing is that you can easily become an industry insider. You accomplish this by aggressively subscribing to the free industry trade journals, sending for all the available tech lit, attending shows or seminars, and making full use of *Dialog* and the other online resources. Becoming an industry insider should *immensely* improve your chances of success.

Above all, *never* call yourself an inventor or behave like one! To do so sets you up for every ripoff and scam in the book. Plus bunches that have not yet made print.

Instead, you position yourself as a *purveyor of risk reduction*. In which you do many of the same things as an inventor. But in workable and proven ways that dramatically improve your final results. More details on this in Your best source for ongoing info on effective product development is *Midnight Engineering* magazine. And much more on your own small scale tech venture appears in my *Incredible Secret Money Machine II* .

Reverse Engineering

Reverse Engineering is the process of taking apart some existing device to see how it works. You might want to do this as an intellectual challenge; to restore missing documentation; to make improvements or mods; or to repair a broken unit.

Reverse engineering is totally and completely legal. So long as it is not used *in any manner* for the theft of any services or intellectual property. Most reverse engineering is also a lot of fun and a great learning tool.

For this month's sidebar, I have gathered together a few of the more important reverse engineering tools that I've found handy along the way. I've also shown a few major reverse engineering steps in figure one. At least the ones that work for me.

Let us go step by step through a

0. Your best information *always* comes from *outside* the device itself.

1. Seek out all available documentation. Thoroughly study it.

2. Try to contact the original manufacturer. Use the *Electronic Industry Telephone Directory*, The *EEM Master* or CD ROM phone disks.

3. Try to get in touch with user groups, known users, or known buyers and sellers for more information. Check surplus listings. Also subscribe to relevant trade journals. Place classified ads. *Rochester Electronics* and similar obsolete semiconductor houses can also be of help.

4. Make aggressive use of the online resources. Such as GEnie's RADIO RoundTable or the Internet.

5. Do a thorough visual inspection.

6. Use dental X-rays to view through sealed epoxy or to second guess mystery integrated circuit chips.

7. Try to identify chip part numbers by using the *I.C. Master*. Other useful resources here are the *ECG*, *NTE*, and the *Radio-Shack* directories. Be sure to get data sheets and ap notes for all chips.

8. Trace out the schematic by doing a resistive matrix. Do *not* use an ordinary ohmmeter on its X1 range. Generate a complete schematic.

9. Avoid any and all preconceived notions of how something "has" to work. Wait on the hard parts and let your subconcious work for you.

10. Fill it with water and see where it leaks. Do this by applying reasonable and *current limited* voltages to supply pins, and reasonable test signals to inputs. Then observe the output behavior.

11. If software is involved, excercise it. Two extremely useful software debugging tools are a print-to-disk routine and an I/O comm recorder.

12. Carefully document and record your results.

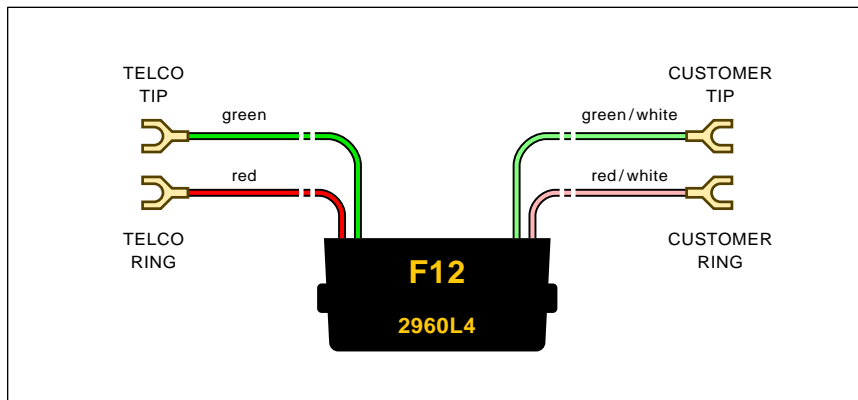Fig. 1 – WORKING GUIDELINES for your own reverse engineering.

Fig. 2 – THE NORTHERN TELECOM 2960 NETWORK INTERFACE goes between your phone and the telco lines.

recent example. I've just acquired a large pile of the *Northern Telecomm #2960* network interface devices. Or, more formally, the *Remote isolation device/maintenence termination unit.*

Or RID/MTU for short.

I had hopes of these being a part 68 interface. Or at least a DAA. It turns out they are neither, but still do appear to be a highly useful and valuable component. One with a lot of non-telecom uses.

Out of the bag, we have a small epoxy block with four wires coming out of it. Green, red, green/white, and red/white. A large "F12" on the side. The outside shipping cases seemed pretty badly flood damaged, but I did manage to salvage a bill of lading

that – wonder of wonders – included the barely legible device installation data sheet. And a 1988 release date.

But no schematic.

Their telephone number was no good, so the next step was to look in the *Electronic Industry Telephone Directory* to find the current supplier. Those CD ROM phone disks are also super handy here. *Select Phone* is one of many. Sadly, the supplier is still being chased at column deadline.

Next, you disassemble the part. If you have lots of them, be willing to sacrifice one or two.

Sealed units are rare, but the usual method to attack them is with dental X-rays. These can even be free if you have a curious dentist. Besides their

obvious use of seeing through potting compound, dental X-rays can tell you the chip size and complexity.

Even if you are not an ic expert, it is fairly easy to spot the difference between optocoupler and opamp. Or tell CPU from ROM.

In this case, the X-ray revealed a small circuit board, an 8-pin minidip, a fuse, two diodes, five resistors, and four tantalum capacitors.

You can also find epoxy dissolving chemicals. From *Master Bond*.

It was fairly easy to carve up the potting compound. But, in hindsight, I should have let the dentist do it. At any rate, the ic was identified as part number "1060". Now, most functions of most integrated circuits should be easy to sort out. But in a telecomm part, it could be anything. I next went to the *IC Master*. There were a dozen different ic's with 1060 in their name, but the LB1060AB *Loop Termination Switch* from *AT&T* leaped out as the most obvious choice.

Well, calling the local distributor revealed that this chip was stock at $4.40 each. But both the local rep and AT&T themselves insisted the chip was obsolete. With the specs no longer available. In other words, they would still sell you the part, but not tell you what it is or how to use it.

Fortune 500 strikes again.

I then checked the surplus route. *The Mart* is the leading magazine of used telecomm stuff in the country. It gave me the list of Northern Telecom buyers which I am currently mining. Even better, Marvin Birnbom from *Surplus Traders* maintains a hot buy and sell surplus phone fax list. By the most amazing of coincidences, there were 300,000 of the LB1060AB chips offered for immediate sale!

With full specs available.

Next in line is a circuit trace. This is *infinitely* easier if you have the full specs for all the involved parts. Your optimum starting point is a *continuity matrix*. Where you check connections between *every* point in the circuit.

Your best possible checker would apply no more than 0.1 volt and a mil or so maximum. And respond *only* to 0.1 Ohm or less. Or, better yet, offer a changing tone with resistance. This prevents you from forward biasing semiconductor P-N junctions and giving you misleading results.
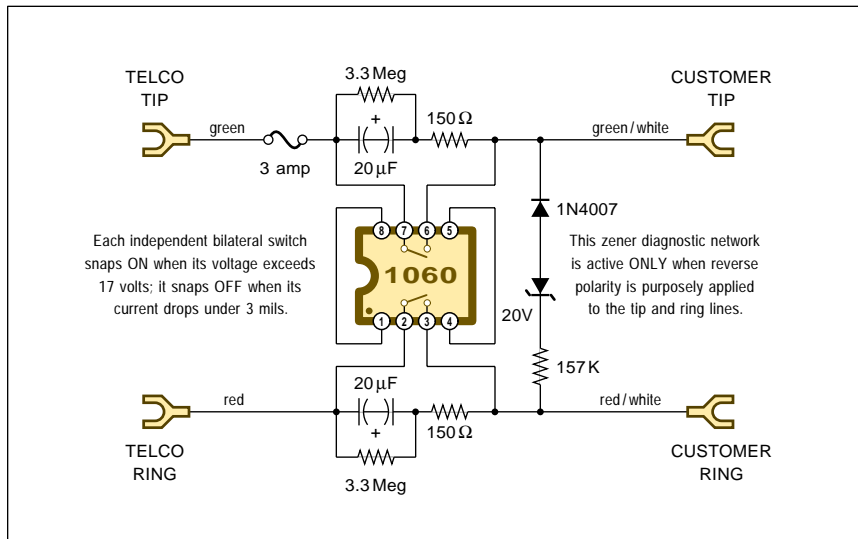

Fig. 3 – SCHEMATIC FOR THE 2960 INTERFACE. In normal use, both bilateral switches turn on when the usual telco line voltage is present. They stay on so long as something is off hook. For a diagnostic test, the line voltage is dropped to zero, turning both switches off. Special test signals then decide if it is a telco or customer problem.

If you must use an old fashoned ohmmeter instead, *never* use the 1X range, as it applies dangerously high currents. *Always* be certain to check continuity in *both* directions. Any difference tells you a PN junction is involved in the path.

Do remember that ic chip pins go *counterclockwise* from the top. And that all pins *reverse* when you flip the board over. A strong light source and a good magnifier are essential.

A "fill it with water and see where it leaks" step came next. I chose a *current limited* power supply to fake the phone line and see when and how the device opens and closes. Doing so reveals the 2960 turns on when the supply voltage exceeds plus or minus 34 volts. The 2960 stays on so long as there's three mils of load current.

Much more on nailing down any unusual supply sources (and similar reverse engineering tools) are found in my *Resource Bin* reprints as well as on *www.tinaja.com*.

A Closer Look

A circuit for the 2960 appears in figure three. The 1060 data magically showed up just as I finished up the preliminary trace.

Here is what the device does: This is a solid state relay that gets placed between the telco tip (green) and ring (red) and your tip (green-white) and ring (red-white) lines.

Should a problem occur with your phone, the telco can use the 2960 to make a simple test to find out if it is your problem or theirs. And be able to do so from their front office.

No field service call is needed!

The 1060 chip contains two totally separate bilateral switches. Without any supply voltage, each switch will normally remain *off*. If the voltage across *either* switch exceeds 17 volts, the switch will turn on and conduct heavily. Steady state currents of one amp can be handled, with pulses to ten amps. Forward drop is around a volt. Your switch stays on so long as current remains above three mils.

Normally, there are 48 volts of dc on the phone line with everything on hook. Since this is above the 34 volts of both bilateral switches in series, *both* switches are normally *on*. This connects telco to customer. As soon as you go off-hook, you provide the

(A) Pulse and sawtooth test generator

(B) Low power LED flasher

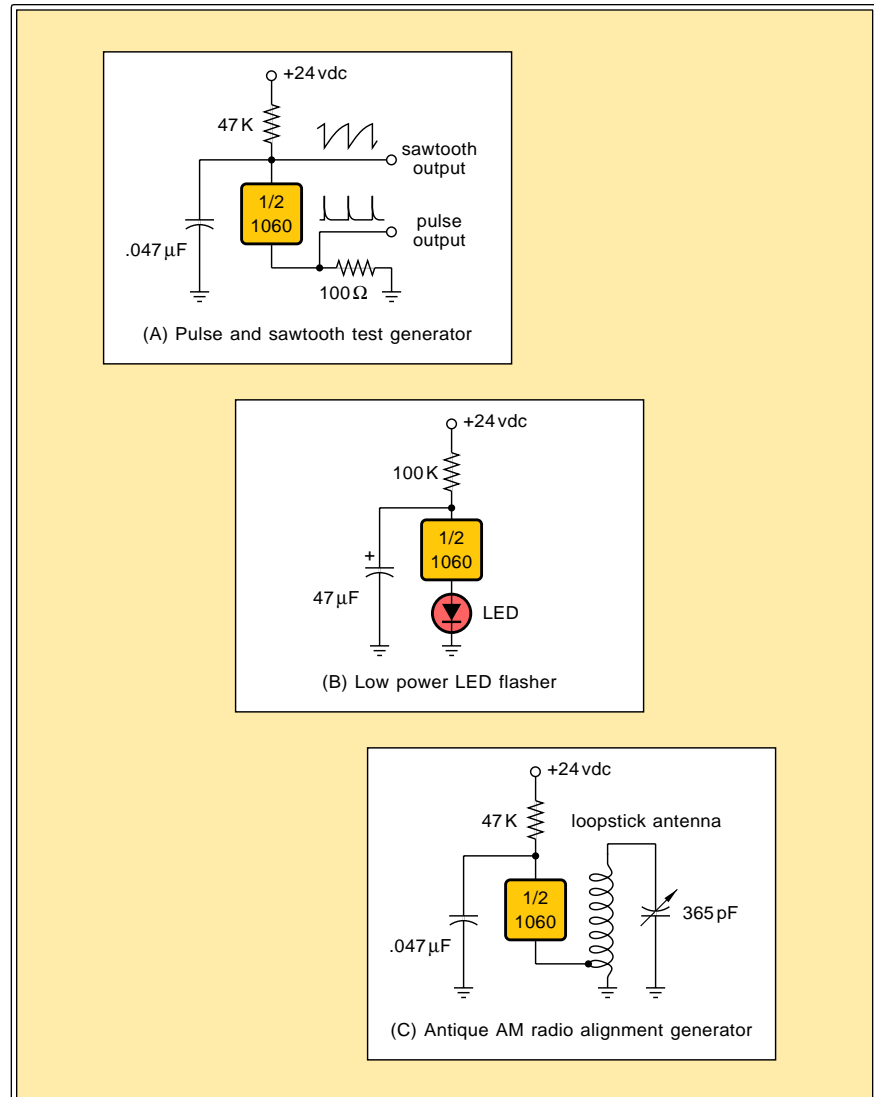(C) Antique AM radio alignment generator

Fig. 4 – BILATERAL ANALOG SWITCHES have lots of non-telco uses. Here are three ideas to get you started using the 2960 or 1060.

holding current to *keep* the switches turned on. So far, so good.

Now, suppose you have a phone problem. You notify the telco. They temporarily drop their line voltage to zero. The bilateral switches snap off, disconnecting anything of yours from the phone line.

Between those coupling capacitors and that diagnostic zener network on the output, various tests can quickly be run for opens, for shorts, or line degradation. In most cases, the telco can immediately determine whether the problem is yours or theirs.

Note that the zener only conducts with high *reverse* line polarity. This diagnostic network effectively stays out of the circuit during normal use.

The 2960 also includes an internal fuse to block you from sending nasty currents into their phone line. This fuse also gives lightning protection.

Other Uses

Just what good are these beasties? What can we do with them that does *not* involve the telephone company? Basically, you have a pair of rather decent bilateral switches. They can get used together or separately.

The unneeded diagnostic parts can get removed and used elsewhere. Or you can disable them by clipping the 150 Ohm and 157K resistors. These could also be drilled out.

Use the red wires for one switch and the green ones for the other.

REVERSE ENGINEERING RESOURCES

Bomarc Services
Box 1113
Casper WY 82602
(307) 237-3361

Dialog Info Services
3460 Hillview Ave
Palo Alto CA 94304
(415) 858-2700

ECG/Phillips
PO Box 3277
Williamsport PA 17701
(717) 323-4691

EEM
645 Stewart Ave
Garden City NY 11530
(516) 227-1300

EITD
2057-2 Aurora Rd
Twinsburg OH 44087
(216) 425-9000

Encyclopedia Associations
835 Penobscot Bldg
Detroit MI 48226
(313) 961-2242

IC Master
645 Stewart Ave
Garden City NY 11530
(516) 227-1300

The Mart
899 Presidential Ste 110
Richardson TX 75081
(800) 864-1155

Master Bond
154 Hobart St
Hackensack NJ 07601
(201) 343-8983

NTE Electronics
44 Farrand St
Bloomfield NJ 07003
(201) 748-5089

Pro CD Inc
222 Rosewood Drive
Danvers MA 01923
(800) 237-8931

Rochester Electronics
10 Malcolm Hoyt Dr
Newburyport MA 01950
(508) 462-9332

Surplus Traders
PO Box 276
Alburg VT 05440
(514) 739-9328

Synergetics
Box 809
Thatcher AZ 85552
(520) 428-4073

Once again, the rules are: Switch goes *on* above 17 volts. Switch stays on with 3 mils or more of current. Your switch works equally well with *either* current polarity.

Obviously, we have a crowbar for a power supply or an overvoltage detector. We can build a set-reset flip flop memory or latch. All sorts of ac phase control possibilities come to mind. A doorbell, HVAC, or alarm voltage easily power your circuits. And there's also a bunch of possible home automation uses.

Figure four does show us several variations on the classic *relaxation oscillator*. In 4-A, we have a simple sawtooth frequency generator. In 4-B, we add a LED in the loop to make a low power flasher. Average current goes down by the selected duty cycle of the lamp flashing.

In 4-C, we add a loopstick antenna and a tuning capacitor. Making up a shorter range AM radio transmitter. One that is also handy for test and alignment of antique radios.

Let me know if you want some of these 2960 units to play with. There's all sorts of possibilities here.

This Month's Contest

Better yet, let's make a contest out of it. Dream up some new use for a remotely contollable and snap action analog switch. Or else find me some market for a few of these beasties.

As usual, there'll be a dozen or so *Incredible Secret Money Machine II* books going to the dozen or so best entries. Along with an all expense paid (FOB Thatcher, AZ) *tinaja quest* for two going to the very best.

Be sure to send all your *written* entries to me here at *Synergetics* and not to **Electronics Now** editorial.

For my insider secrets on winning industrial conests in general, check CONTEST.PDF on *www.tinaja.com*.

More Good Reads

Be sure to read *The H-P Way* by David Packard. Subtitled "How Bill Hewlett and I Built our Company".

Yeah, this is a tad dull and overly yea-team boom-rah. And his claim that a LED taillight can improve gas mileage by one mile per gallon is a tad hard to swallow. Uh, beyond that, though, this is a must read if you are developing a small tech business. 200 pages from *Harper Business Press*. $17 list in hardback.

Wings of Giants appears to have badly missed a key point: That first man-powered flight happened in New Zealand. And did so years ahead of the Wright Brothers.

More on sunflowers and Fibonacci sequences in *Nature's Numbers* by Ian Stewart. Subtitled *The Unreal Reality of Mathematics*. See pages 127-144 for additional info.

And for a hilarious alternate take on Microsoft, try out *Microserfs* by Douglas Coupland. And published by *Regan Books*.

A Great Solar CD

Karen Perez of *Home Power* just sent me her latest *Solar II Renewable Energy CD ROM*. A labor-of-love project that offers "the best info available in the fields of renewable energy, home scale energy systems, sustainable technologies, resources, and communications." $29.50.

This is greatly improved over the older Solar I. The primarily new material now includes color pictures, better navigation, and total Acrobat .PDF support. 350 Megs worth of text and GIF files. For Mac and PC.

More on alternate energy resources in HACK28.PDF. More on Acrobat in ACROBLAT.PDF and hundreds of other files in *www.tinaja.com*.

New Tech Lit

A well done tutorial on Quantum Computing appears in *Science* for October 13, 1995. On pages 255-260. With a good bibliography. Quantum computing offers the potential of a *billion* to one speedup over today's PC's. Also in the same issue, some new magnetoresistive materials and a

NAMES AND NUMBERS

Assn Energy Engineers
4025 Pleasantdale Rd #410
Alanta GA 30340
(404) 447-5083

BasicBooks
10 E 53rd Street
New York NY 10022
(212) 207-7057

Batelle Pacific Northwest
Box 999 K6-54-Watts
Richland WA 99352
(509) 372-4274

BKL
421 Feheley Dr
King of Prussia PA 19406
(610) 277-2910

Flesher
2460 N Powers Blvd Ste K
Colorado Springs CO 80915
(719) 570-7833

Fluid Power Bookstore
1100 Superior Avenue
Cleveland OH 44114
(800) 321-7003

GEnie
401 N Washington St
Rockville MD 20850
(800) 638-9636

Harper Business Press
10 E 53rd Street
New York NY 10022
(800) 242-7737

Home Power
PO Box 520
Ashland OR 97520
(916) 475-3179

Luke Systems International
27827 Via Amistosa Ste 101
Agoura Hills CA 91301
(818) 991-9373

Midnight Engineering
1700 Washington Ave
Rocky Ford CO 81067
(719) 254-4558

MX-Com Inc
4800 Bethania Station Rd
Winston-Salem NC 27105
(800) 638-5577

PC Card Products
7447 W Wilson Avenue
Chicago IL 60656
(800) 323-6858

Regan Books
10 E 53rd Street
New York NY 10022
(212) 556-2599

Science
1333 H St NW
Washington DC 20005
(202) 326-6400

Snaptron
2468 E 9th Street
Loveland CO 80537
(303) 663-2820

speech recognition breakthrough.

A 64 page catalog listing hundreds of energy books is now offered by the *Association of Energy Engineers*.

Books on hydraulics are stocked by the *Fluid Power Bookstore*.

Freebie samples of keyboard snap disks are offered by *Snaptron*. *Luke Systems International* is yet another obsolete semiconductor source.

PCMCIA card and frame kits are sold by *PC Card Products*.

A new *MX-COM* product guide on all their highly unusual comm, caller id, and security chips.

More info on electroluminescent panels: *BKL* has lots of data and kits available. Despite EL being a "cold light", the efficiency of today's best panels is only around *one-third* that of a plain old light bulb. Around six Lumens per Watt or so. While the brightness increases with frequency and voltage, the efficiency does *not*. Best overall efficiency takes place at low voltage and frequency. Both the

brightness and efficiency will drop substantially over time.

One fresh approach to on-demand *hardback* book binding has been released by *Flesher*. Around $3 and 3 minutes per book. For your custom hardbound covers, a peel-and-stick technique gets used. A taped spline and no provision for trimming the actual pages. Way overpriced, but still a partial BOD solution.

Much more on tested and proven small scale desktop home publishing opportunities in my *Book-on-demand Publishing Kit* from *Synergetics*. Full details in our nearby ad.

As usual, additional tech support can be found on my new web site at *www.tinaja.com*

I've just bought an *entire* college electronics department at an auction. There are some outstanding buys in everything from logic analyzers to printed circuit etchers to mint Tek manuals to fine test and breadboard bargains. Write or call for a list. ❖