Hacking With GnuRadio

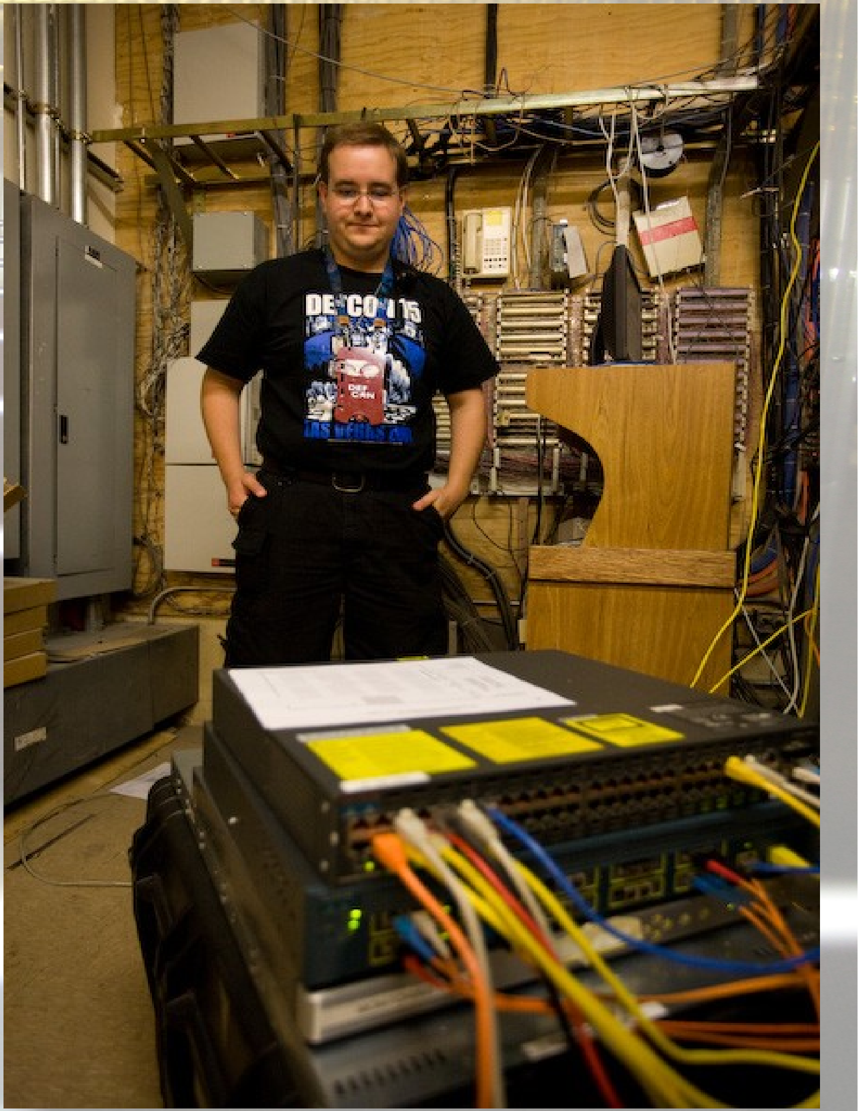
How to have fun with wireless transmissions!

netSPI

RISK COMPLIANCE SECURITY

David M. N. Bryan

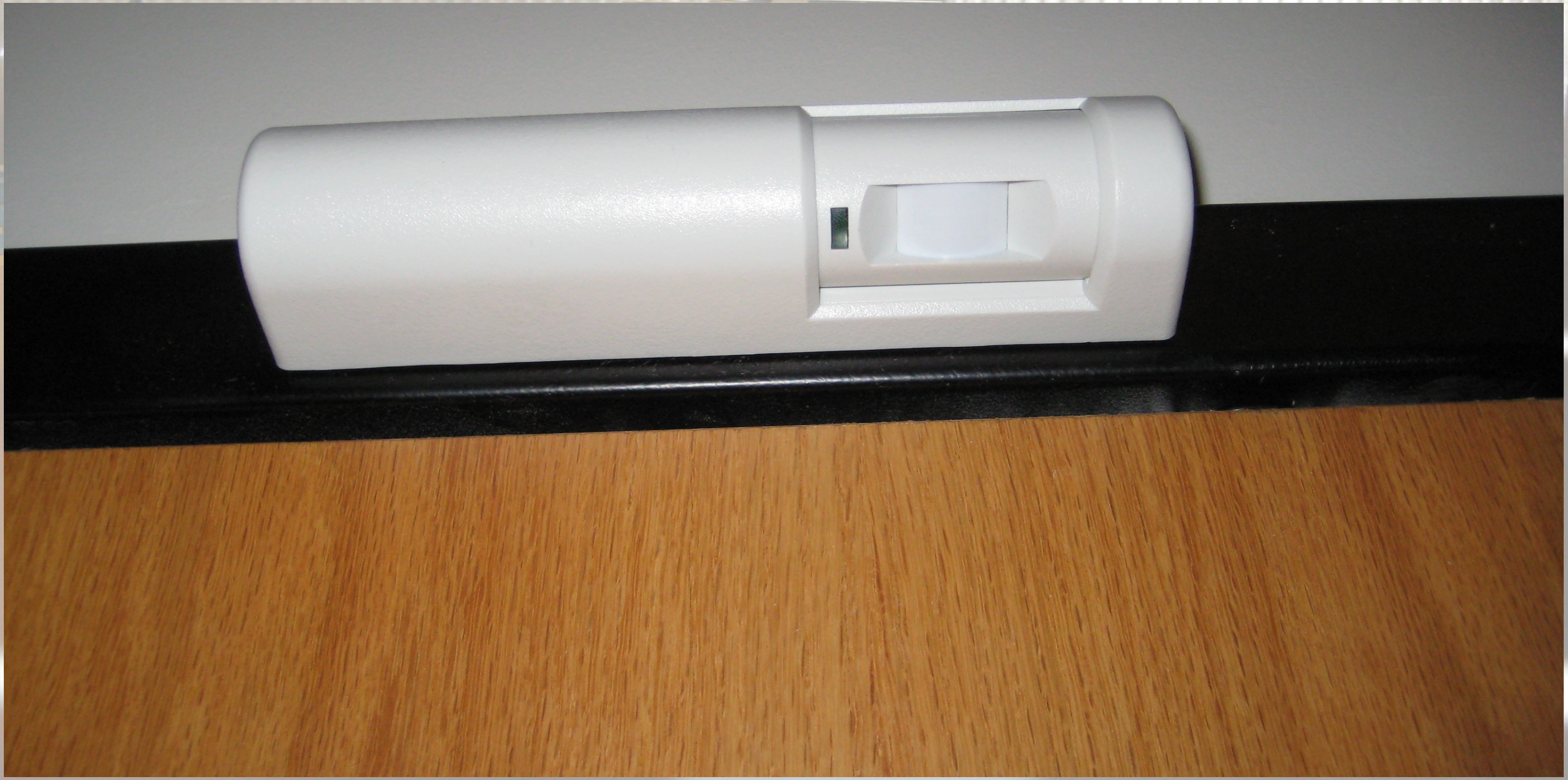
- Info Security Consultant
- CISSP
- HAM
- Hacker
- DEFCON



netSPI
RISK COMPLIANCE SECURITY

Hacker Spaces!!!

What is this?



Is that a hot pack in your pocket?

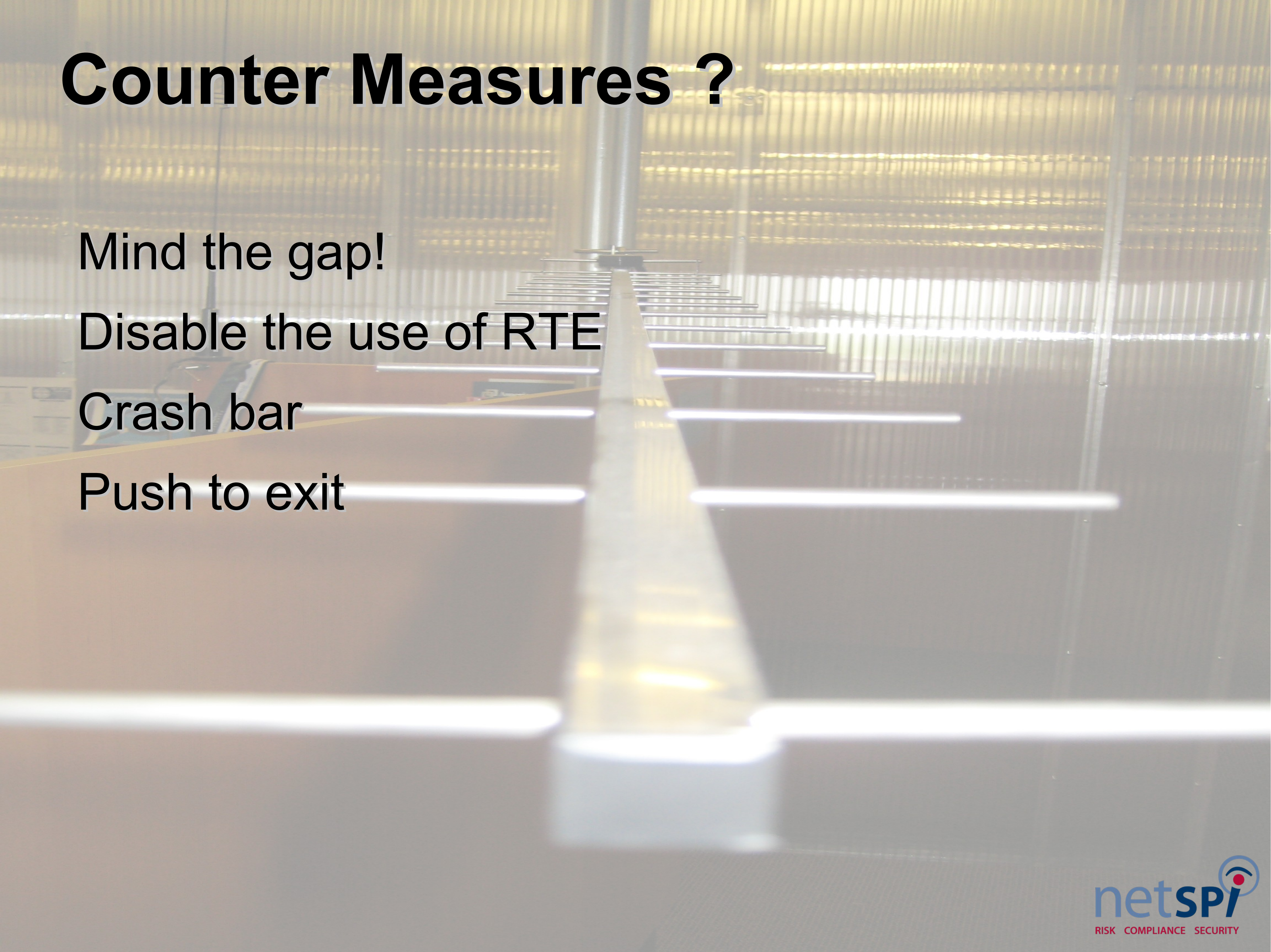
netSPI
RISK COMPLIANCE SECURITY

netspi
RISK COMPLIANCE SECURITY

netspi

RISK COMPLIANCE SECURITY

Counter Measures ?



Mind the gap!

Disable the use of RTE

Crash bar

Push to exit

Hacking With GnuRadio

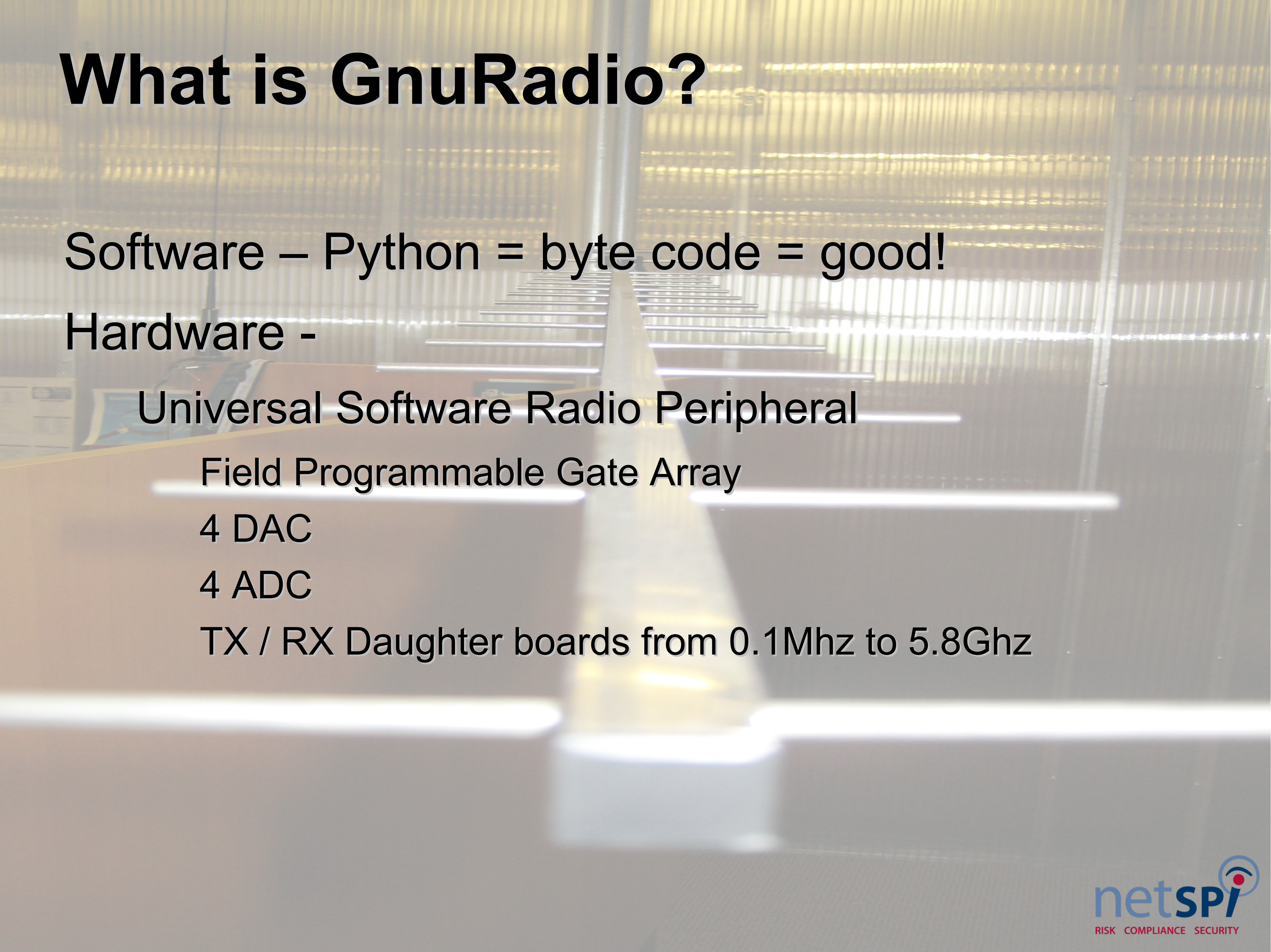
What is GnuRadio?

What you need

Requirements

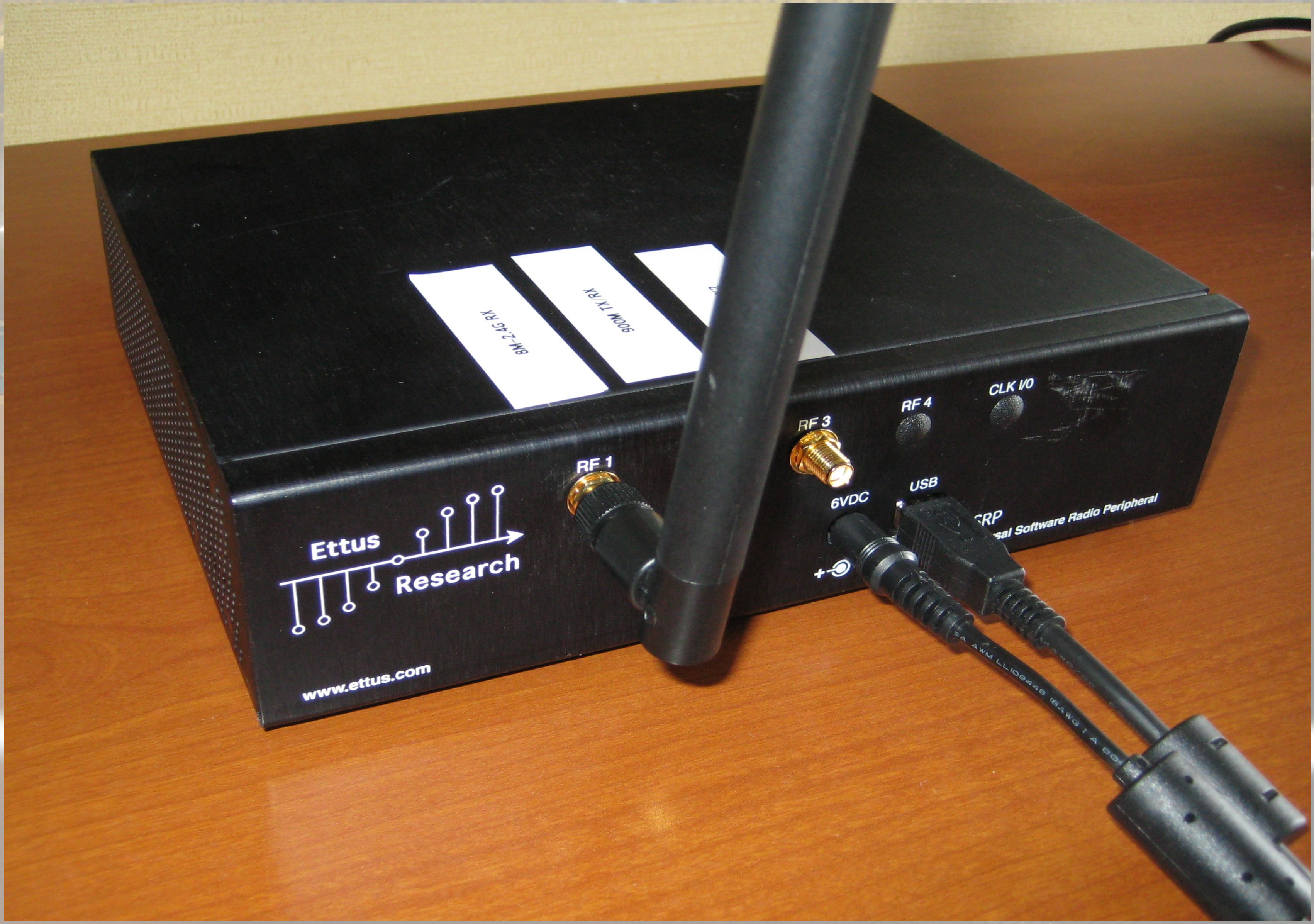
Costs

What is GnuRadio?

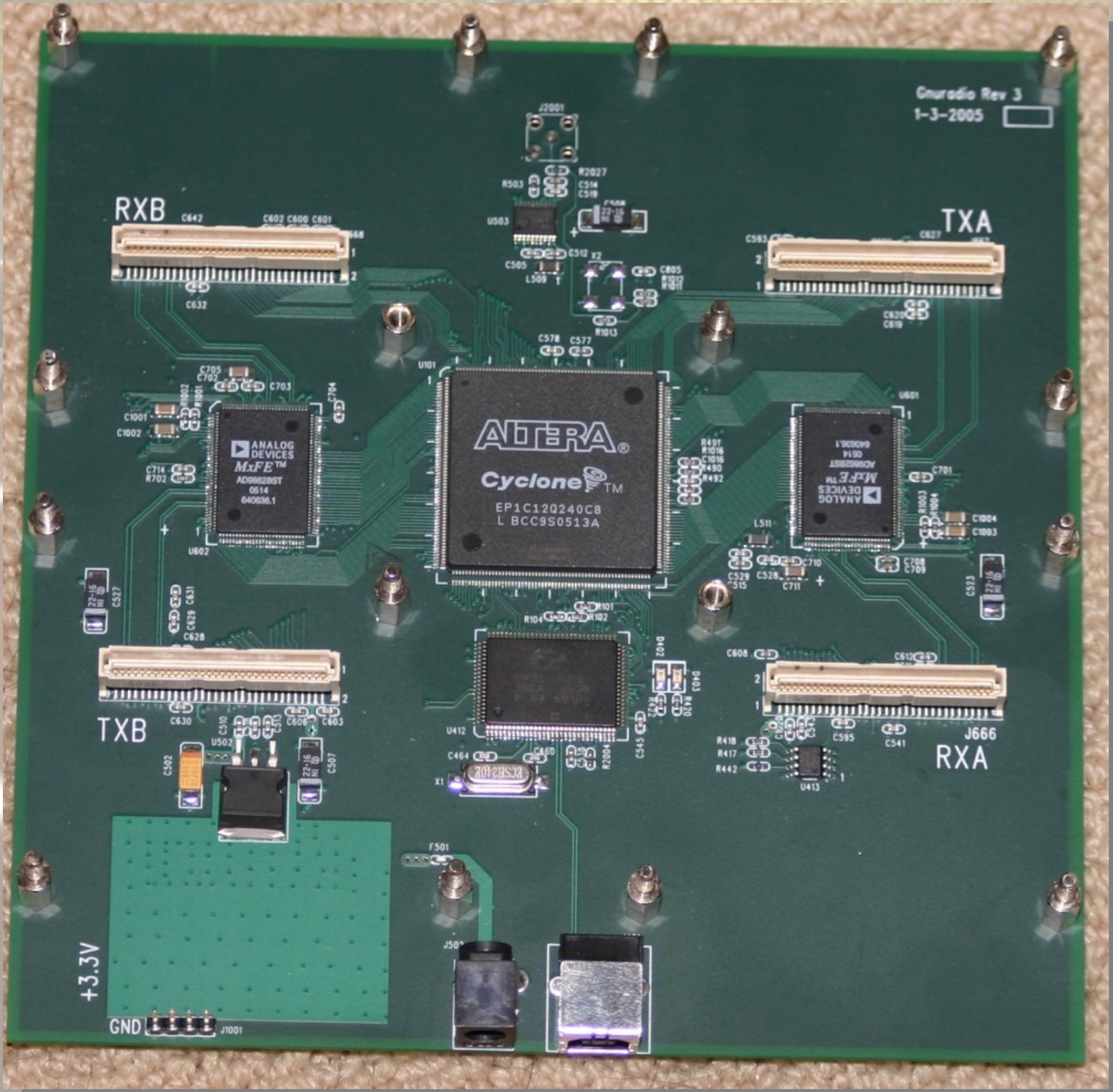


- Software – Python = byte code = good!
- Hardware -
  - Universal Software Radio Peripheral
    - Field Programmable Gate Array
    - 4 DAC
    - 4 ADC
    - TX / RX Daughter boards from 0.1Mhz to 5.8Ghz

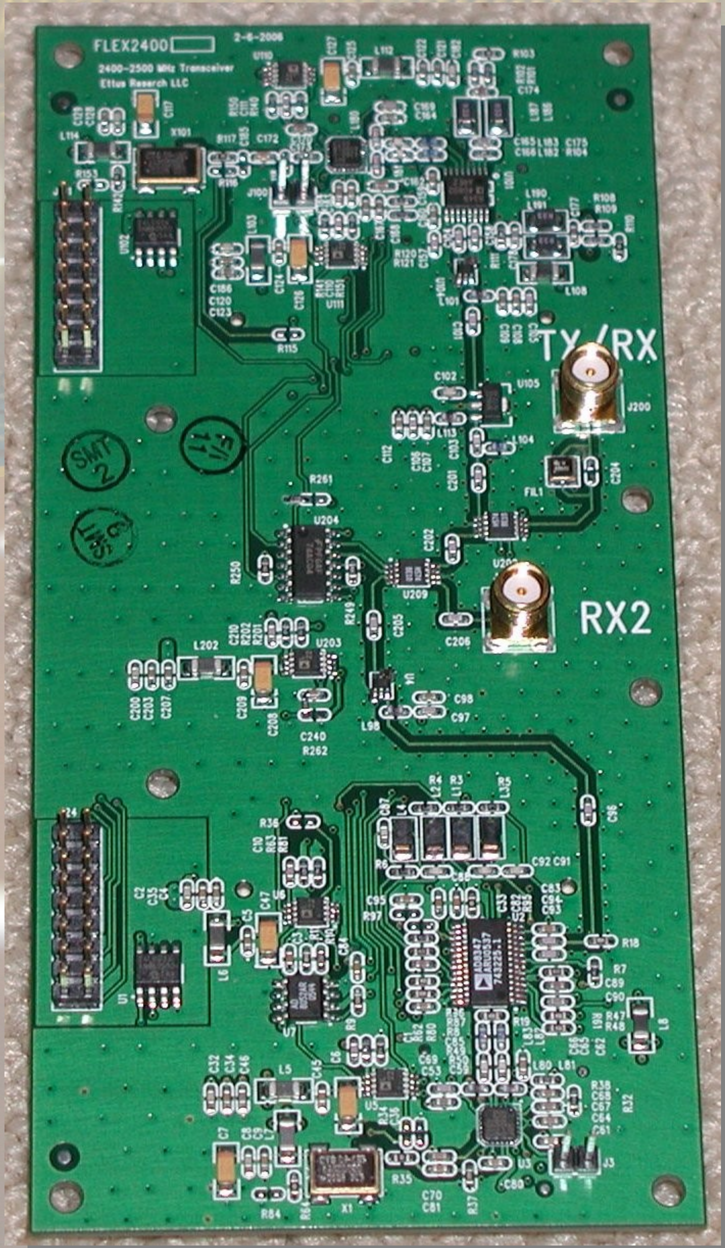
USRP v1.0

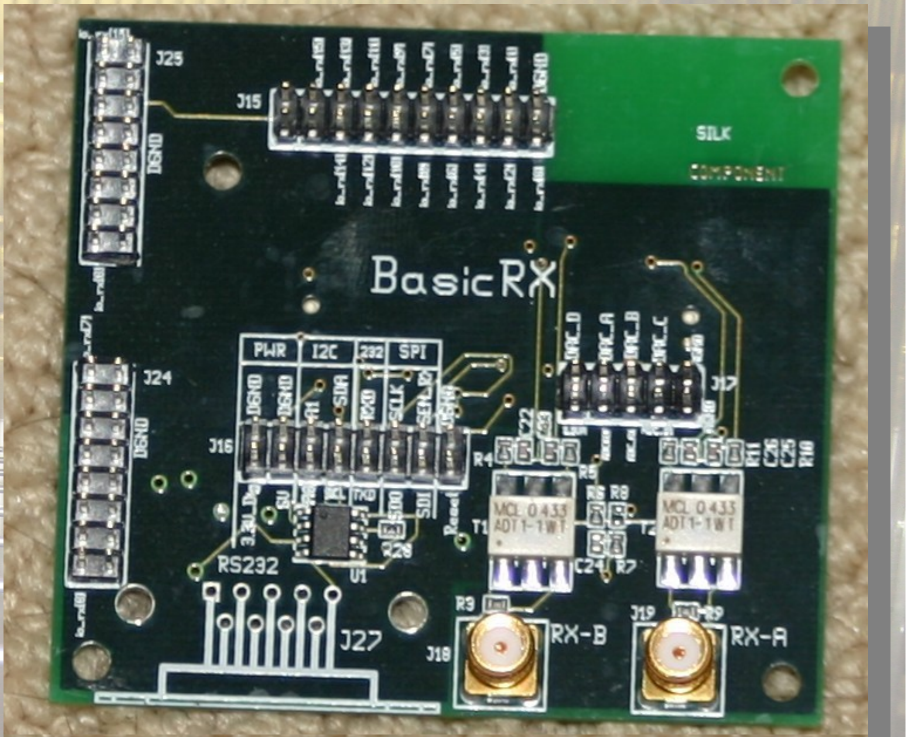

8M 2.4G RX
900M TX RX
RF 1
RF 3
RF 4
CLK I/O
6VDC
USB
SRP
sal Software Radio Peripheral
Ettus
Research
www.ettus.com

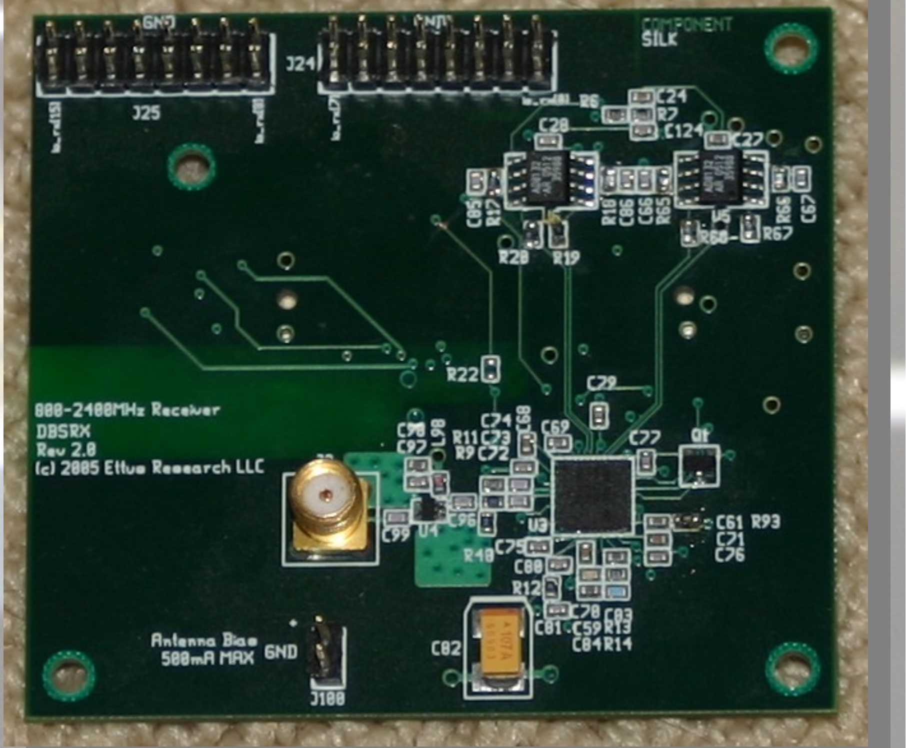
USRP Board


Gnuradio Rev 3
1-3-2005
RXB
TXA
TXB
RXA
J666
ALTERA
Cyclone
EP1C12Q240C8
ANALOG DEVICES
MxFE
AD9862BST
+3.3V
GND
J1001

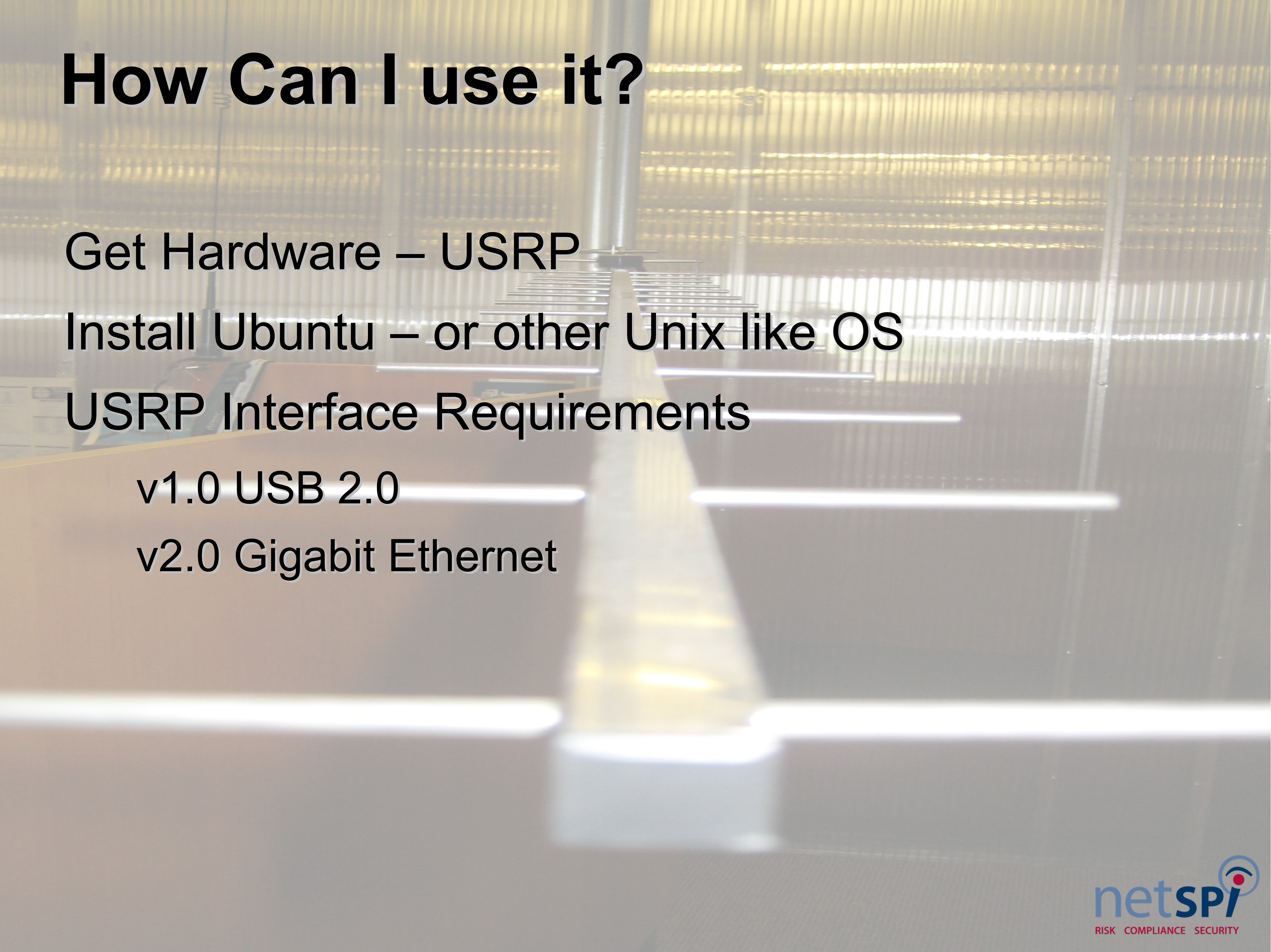
Daughter Boards





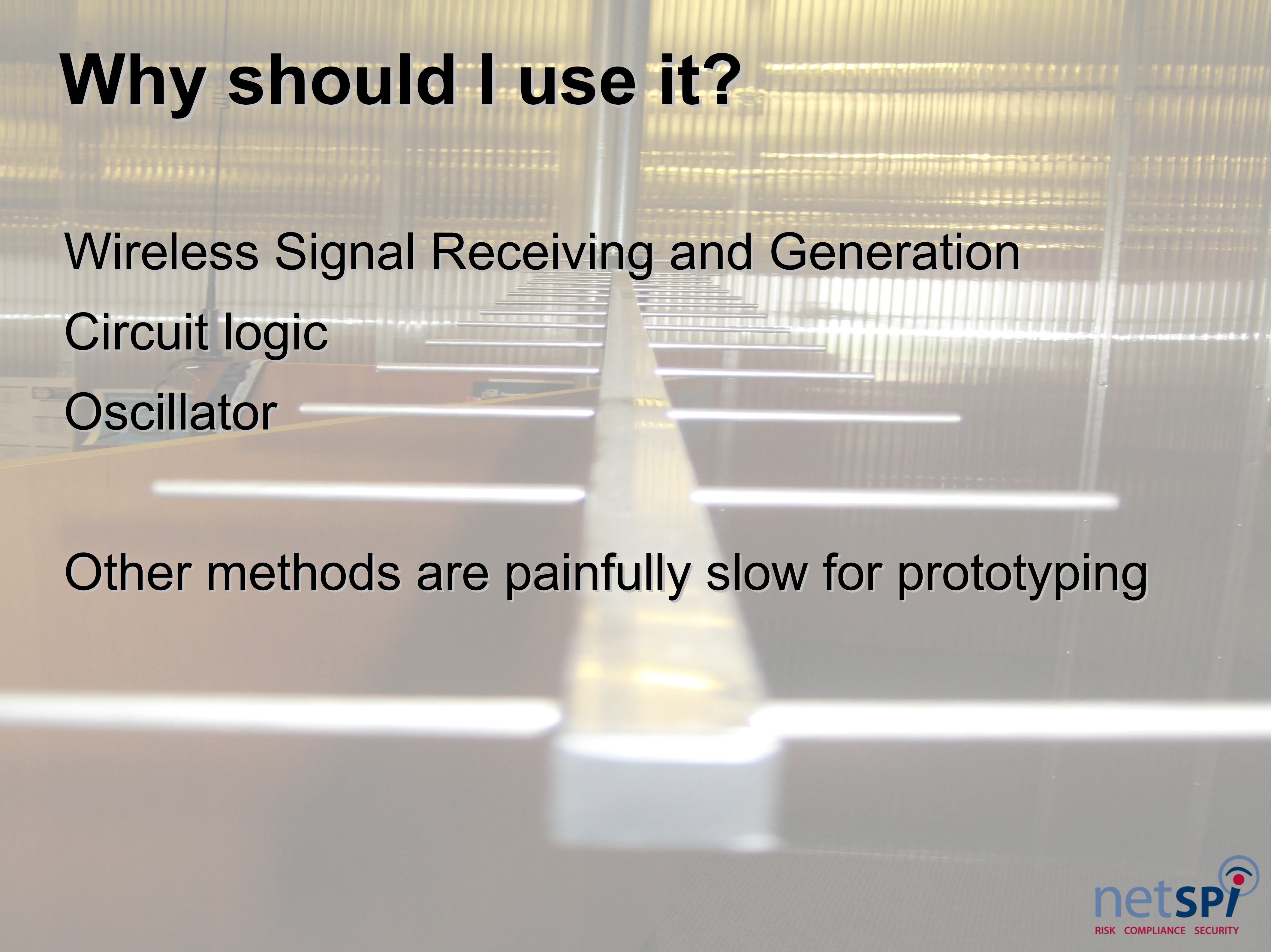


How Can I use it?



- Get Hardware – USRP
- Install Ubuntu – or other Unix like OS
- USRP Interface Requirements
    - v1.0 USB 2.0
    - v2.0 Gigabit Ethernet

Why should I use it?



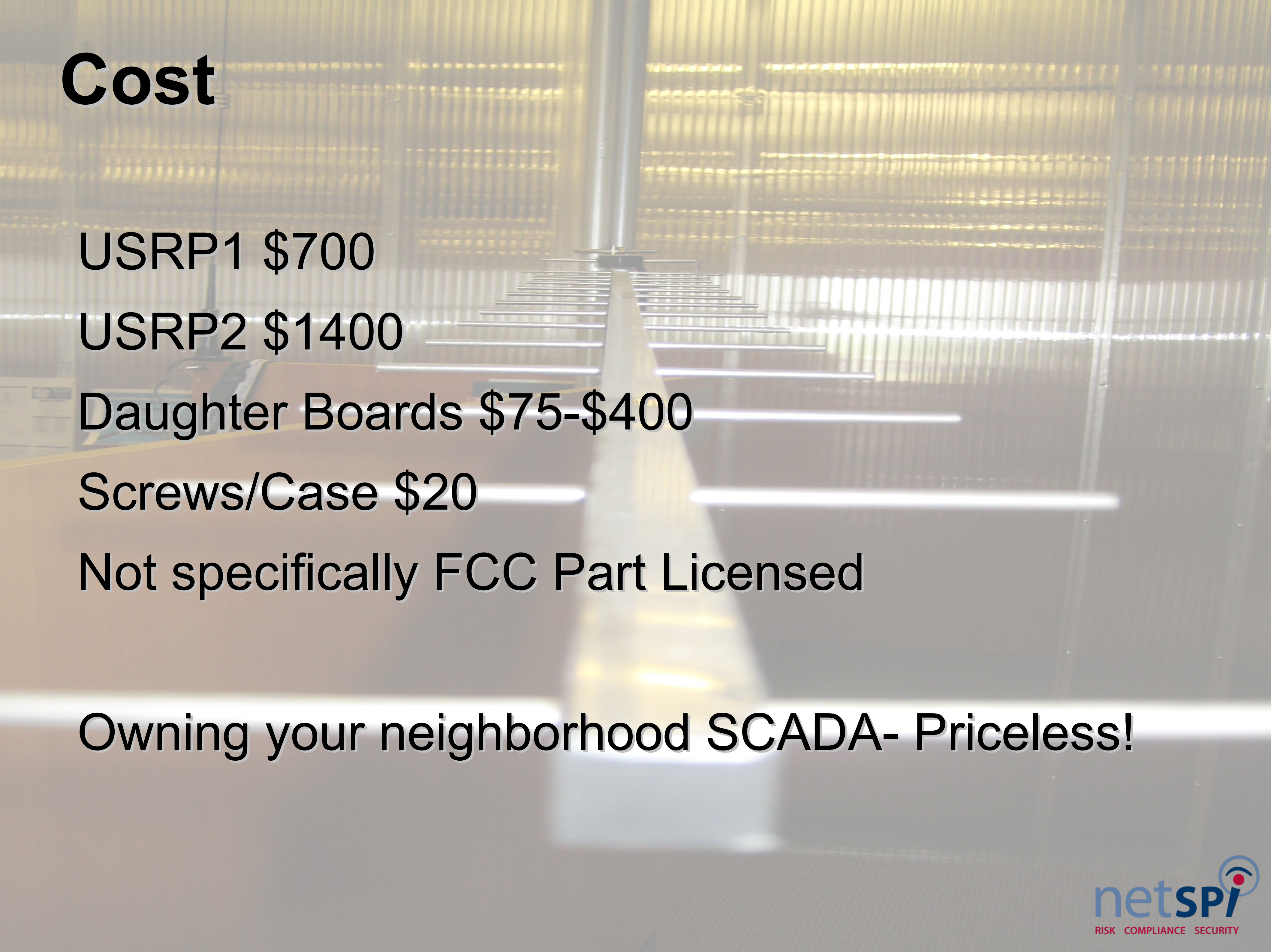
Wireless Signal Receiving and Generation

Circuit logic

Oscillator

Other methods are painfully slow for prototyping

Cost



USRP1 $700

USRP2 $1400

Daughter Boards $75-$400

Screws/Case $20

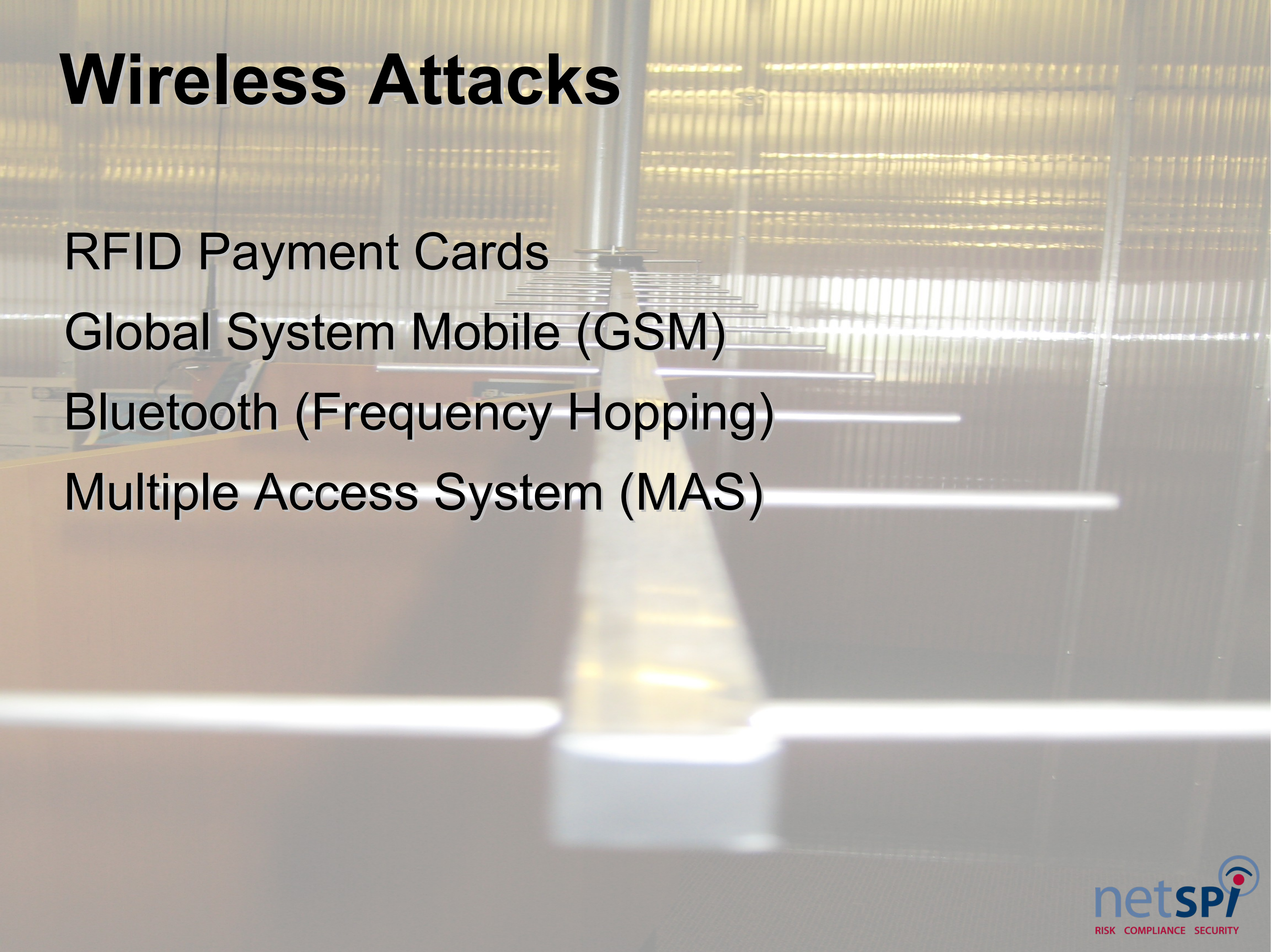
Not specifically FCC Part Licensed

Owning your neighborhood SCADA- Priceless!

netSPI
RISK COMPLIANCE SECURITY

So what can we do with it?

Wireless Attacks



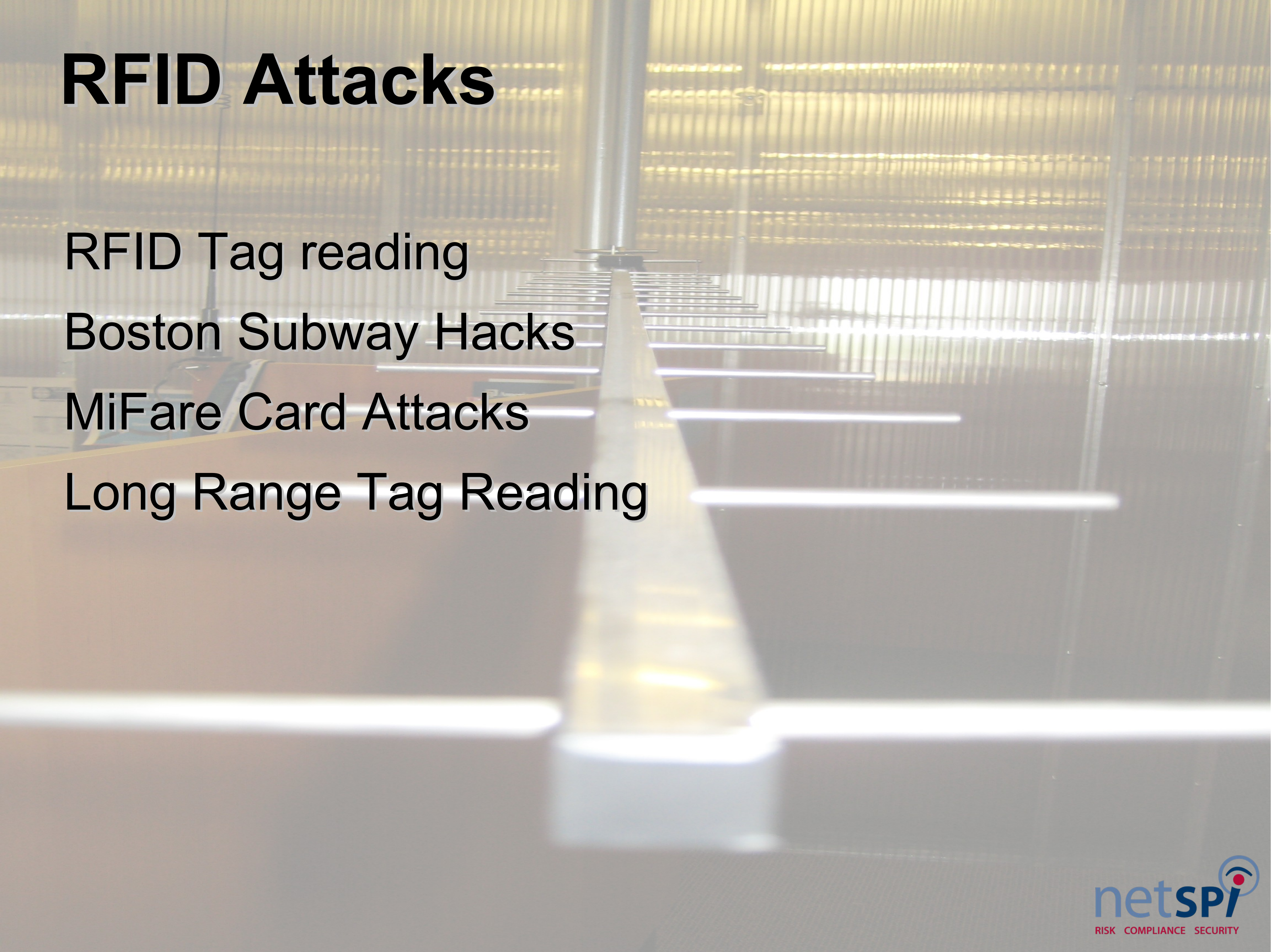
RFID Payment Cards

Global System Mobile (GSM)

Bluetooth (Frequency Hopping)

Multiple Access System (MAS)

RFID Attacks



RFID Tag reading

Boston Subway Hacks

MiFare Card Attacks

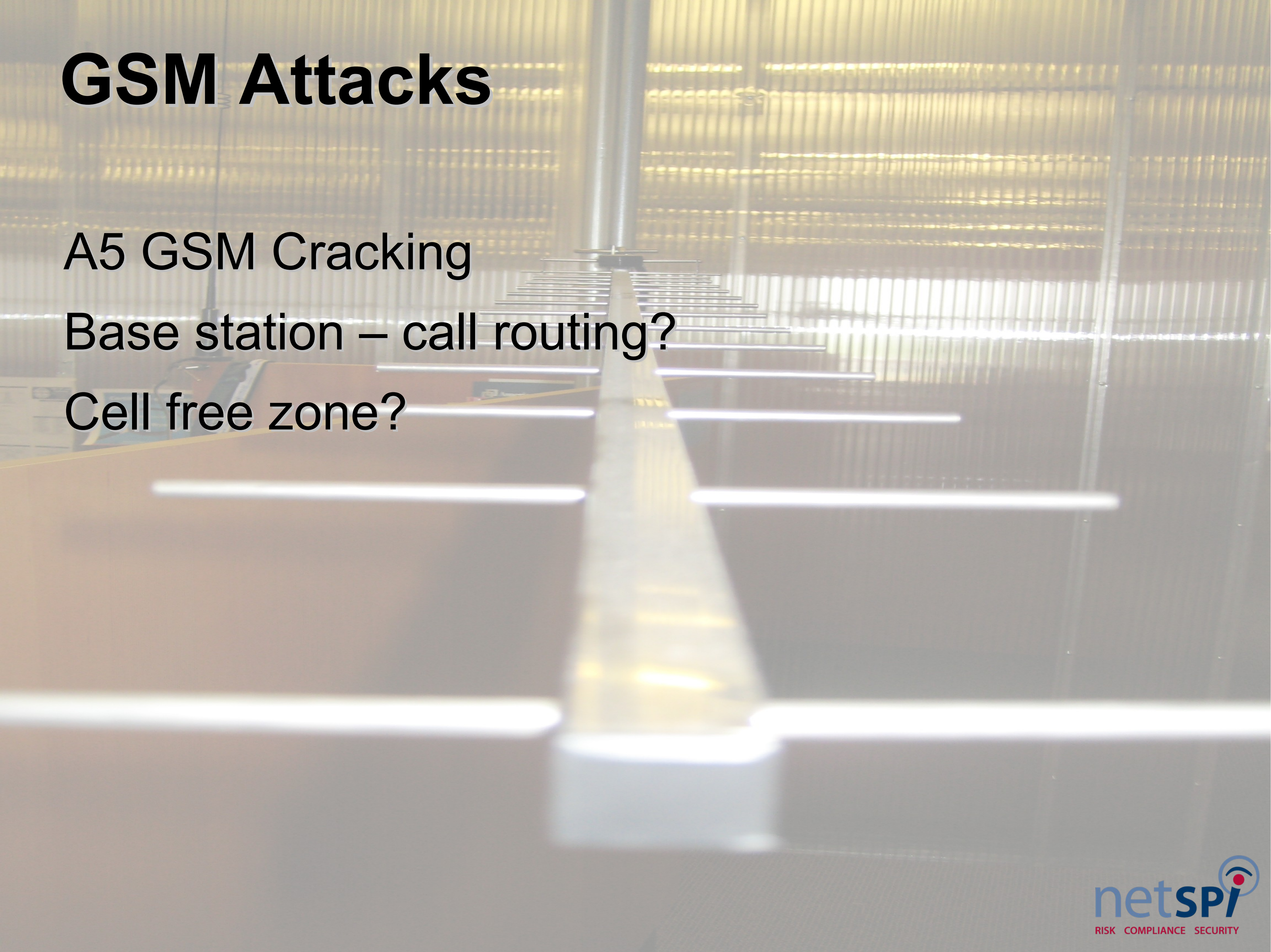
Long Range Tag Reading

GSM Attacks

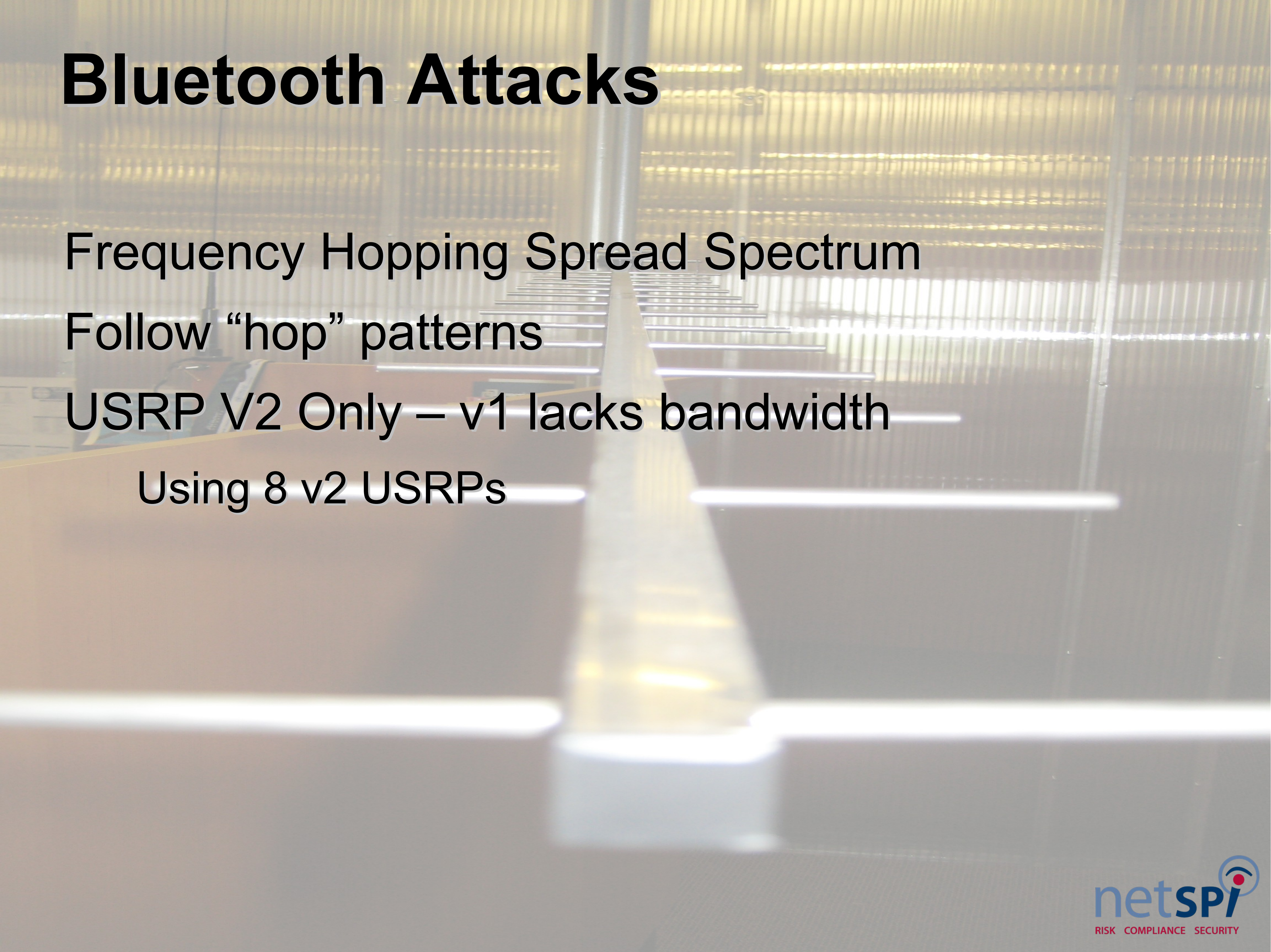
A5 GSM Cracking

Base station – call routing?

Cell free zone?



Bluetooth Attacks



- Frequency Hopping Spread Spectrum
- Follow “hop” patterns
- USRP V2 Only – v1 lacks bandwidth
  - Using 8 v2 USRPs

MAS System

Multiple Access System

Computer Applications in Power, IEEE

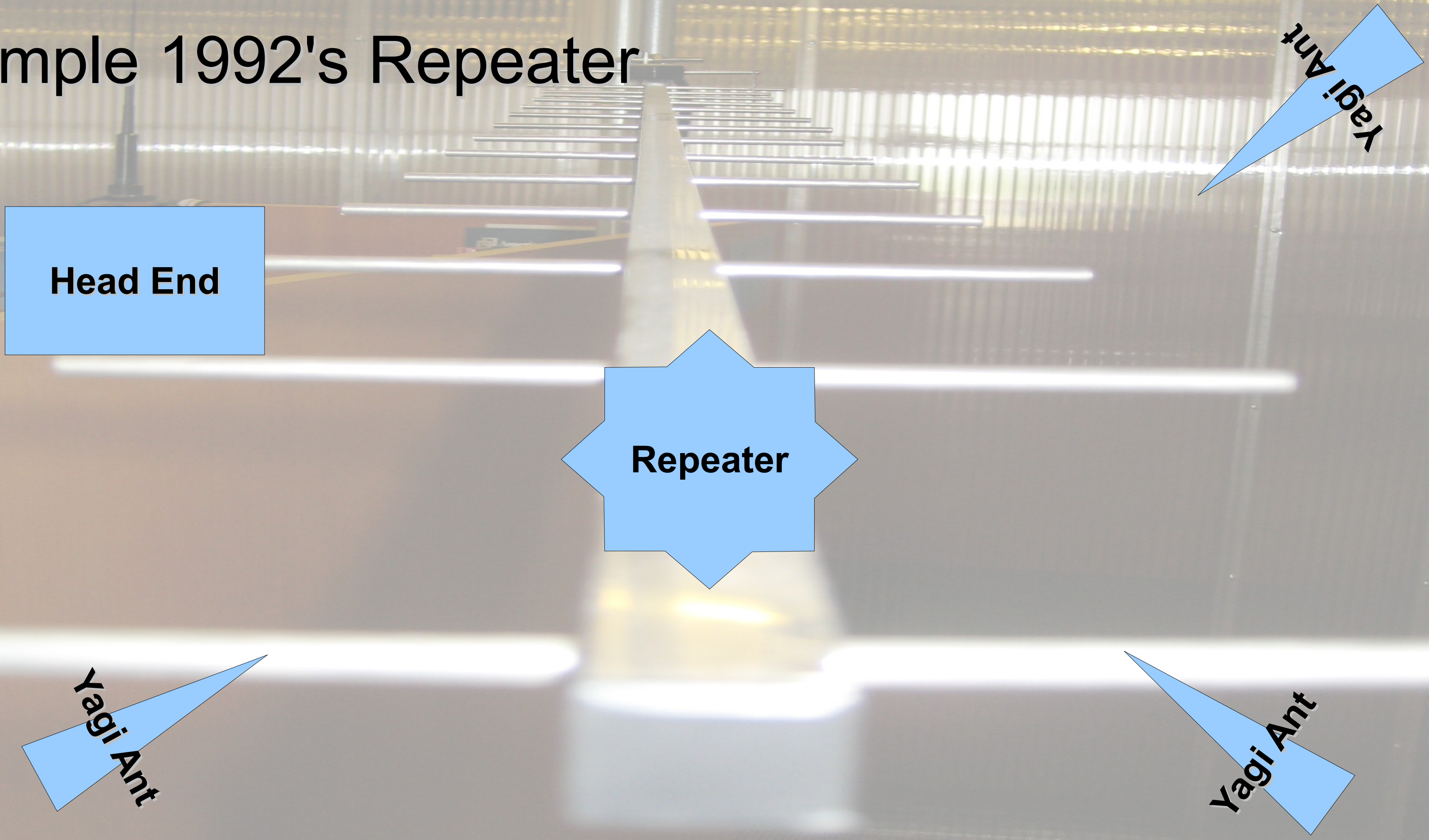
Volume 5, Issue 4, Oct 1992 Page(s):29 - 32

Digital Object Identifier 10.1109/67.160043

Summary:The use of 900 MHz radio for supervisory control and data acquisition applications was investigated by the Houston Lighting and Power Company (HL&P). Multiple address system applications in the 928/952 MHz band were evaluated. (etc....)

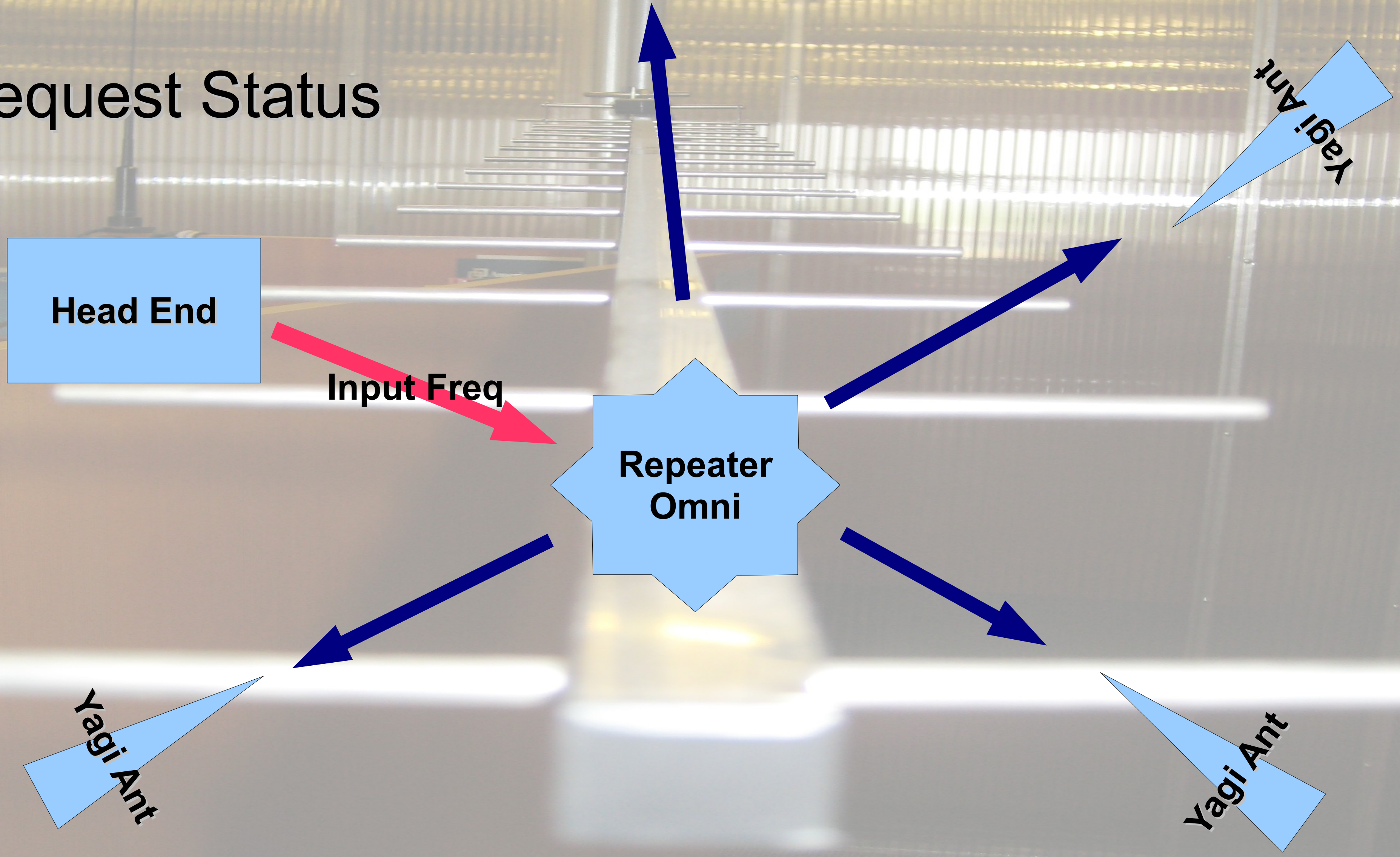
MAS System Attacks

Simple 1992's Repeater



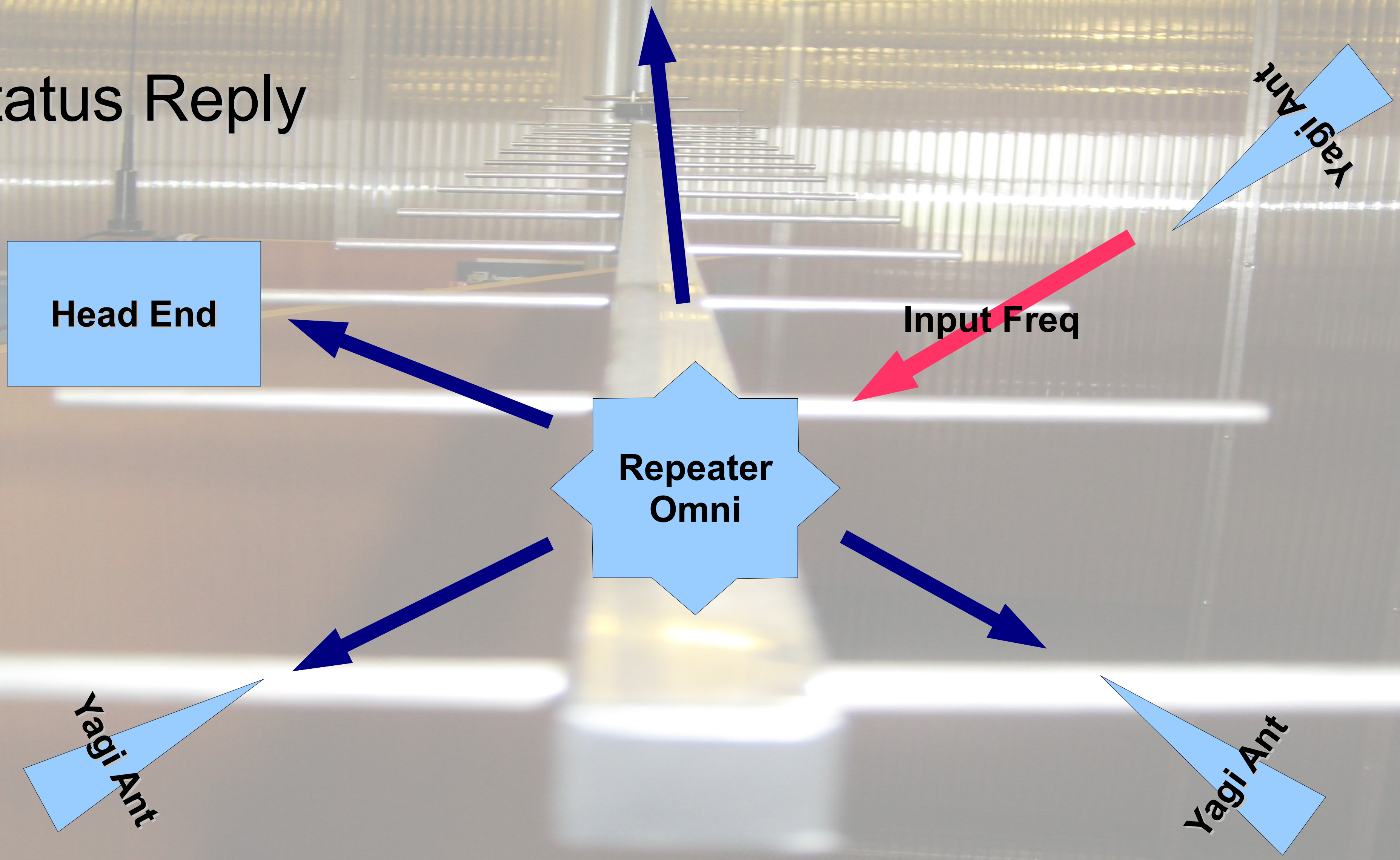
MAS System Attacks

Request Status



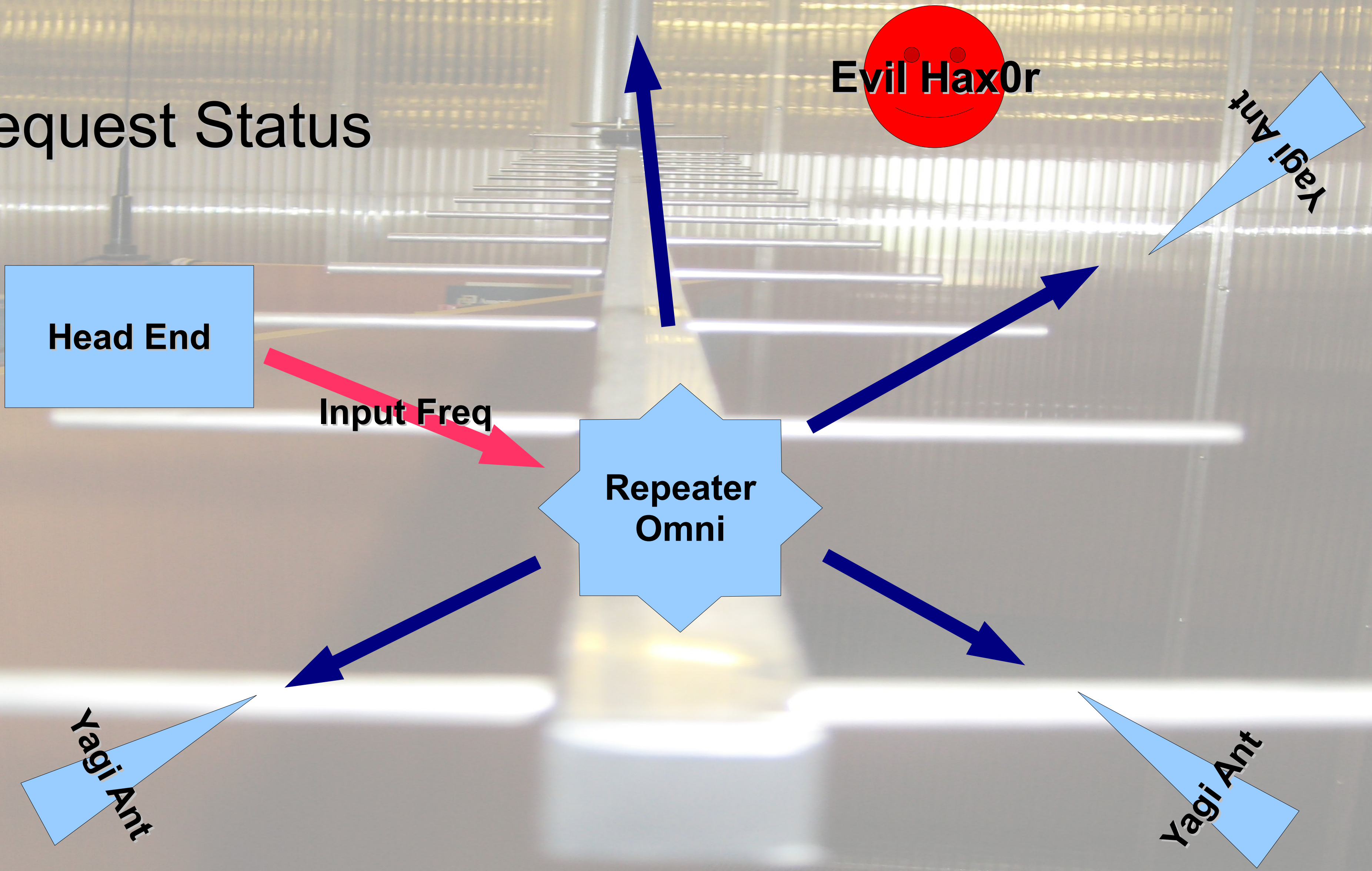
MAS System Attacks

Status Reply



MAS System Attacks

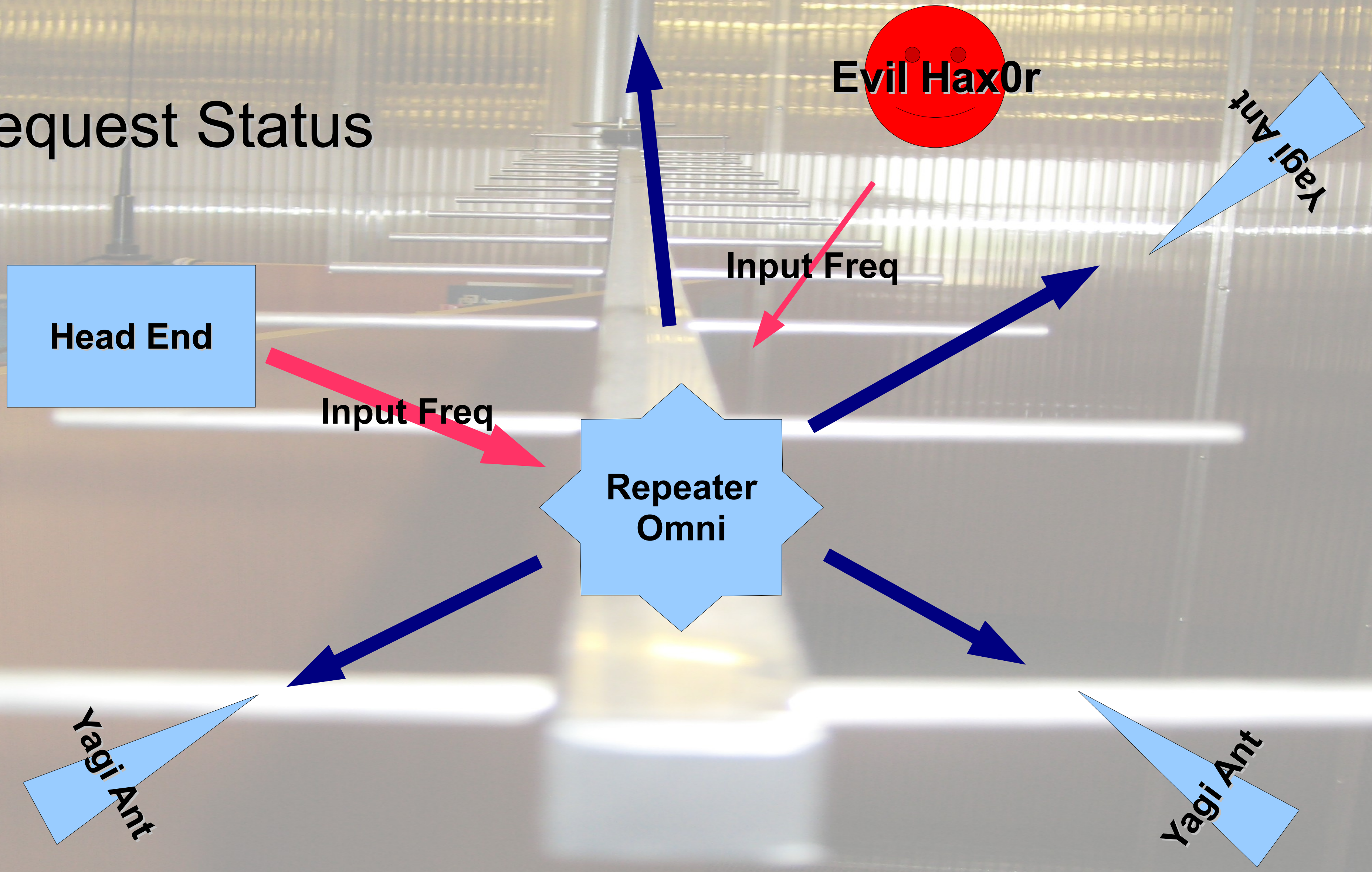
Request Status



netSPI
RISK COMPLIANCE SECURITY

MAS System Attacks

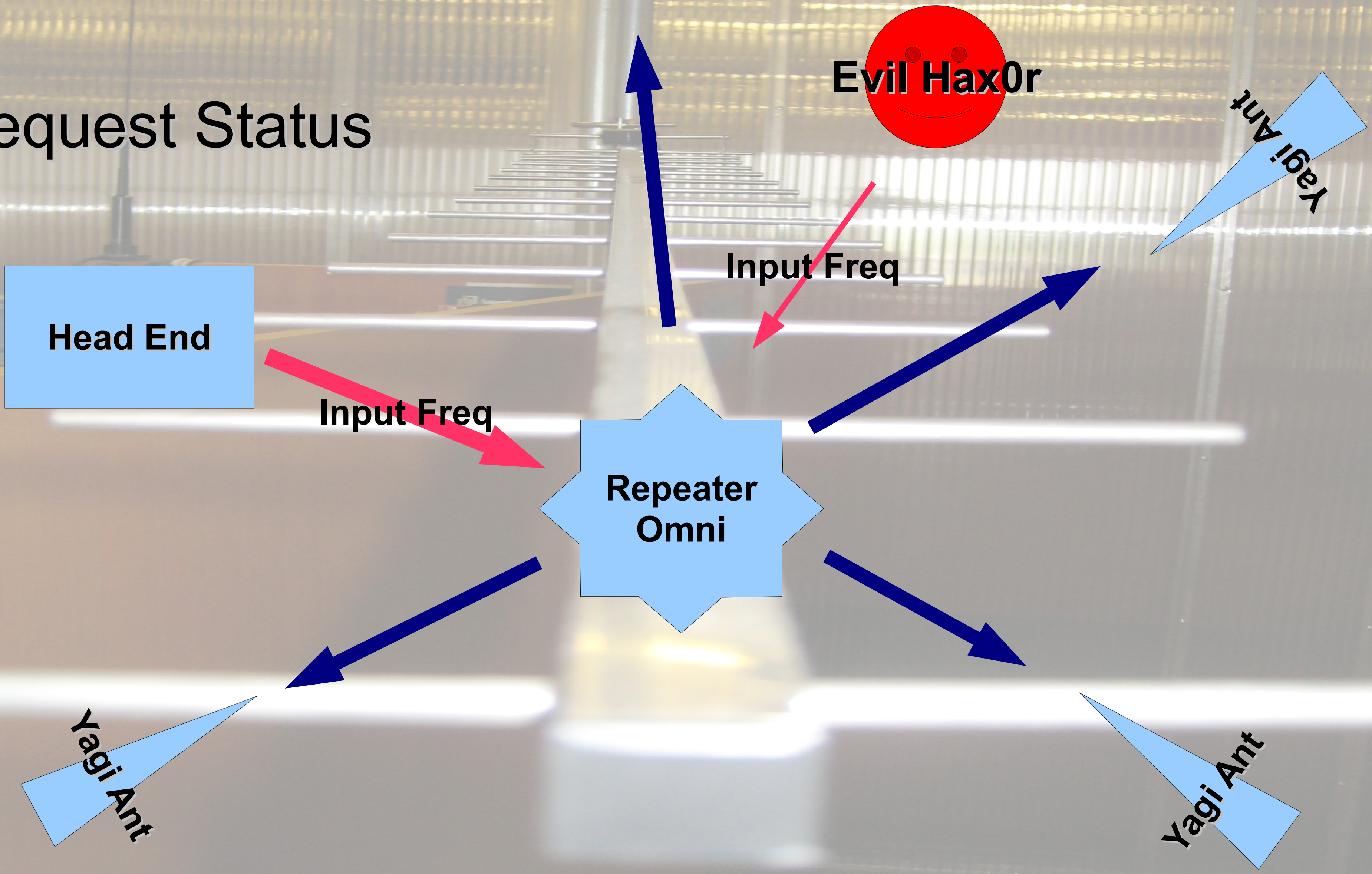
Request Status



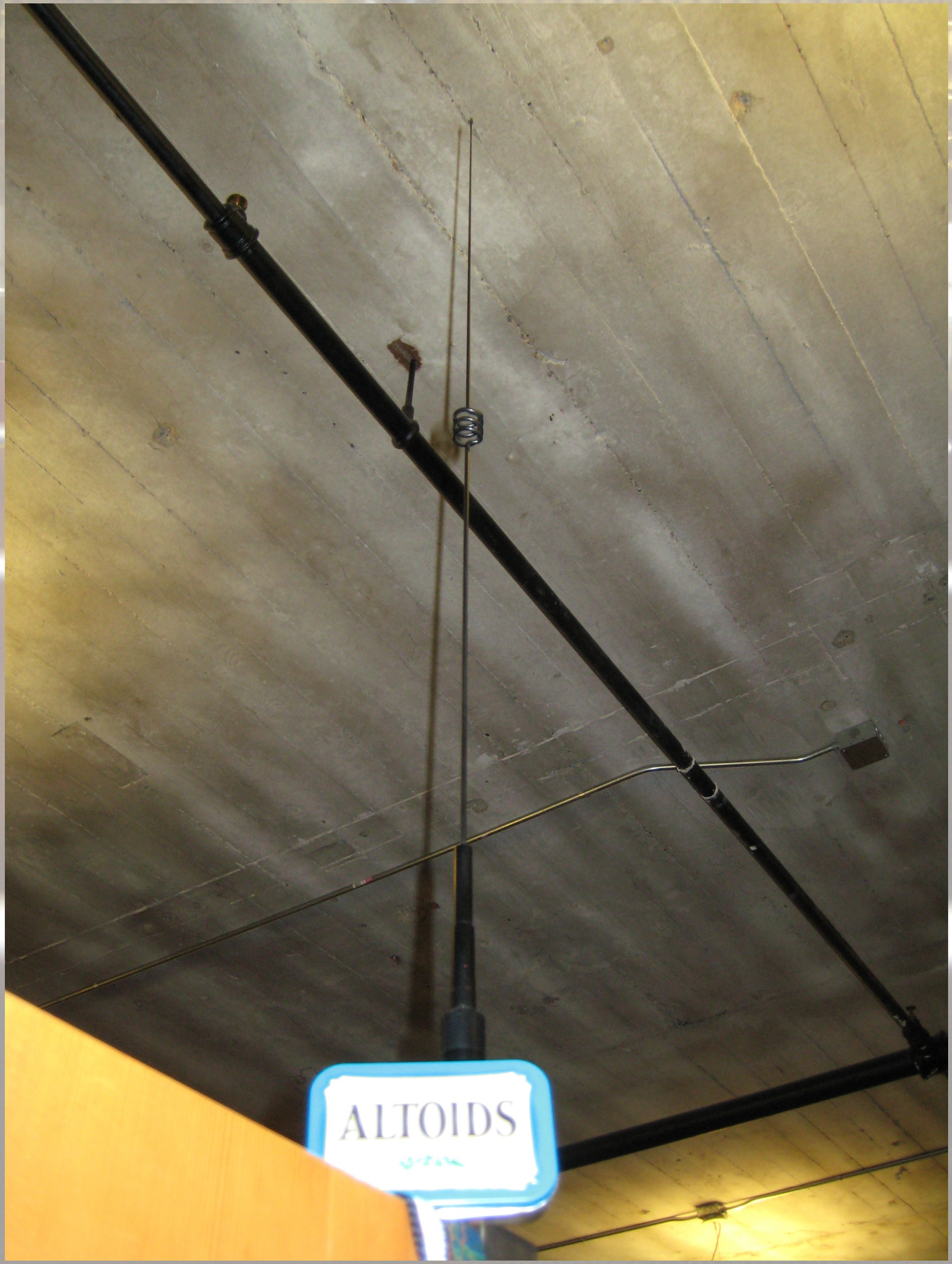
USRP - First Attempt

MAS System Attacks

Request Status

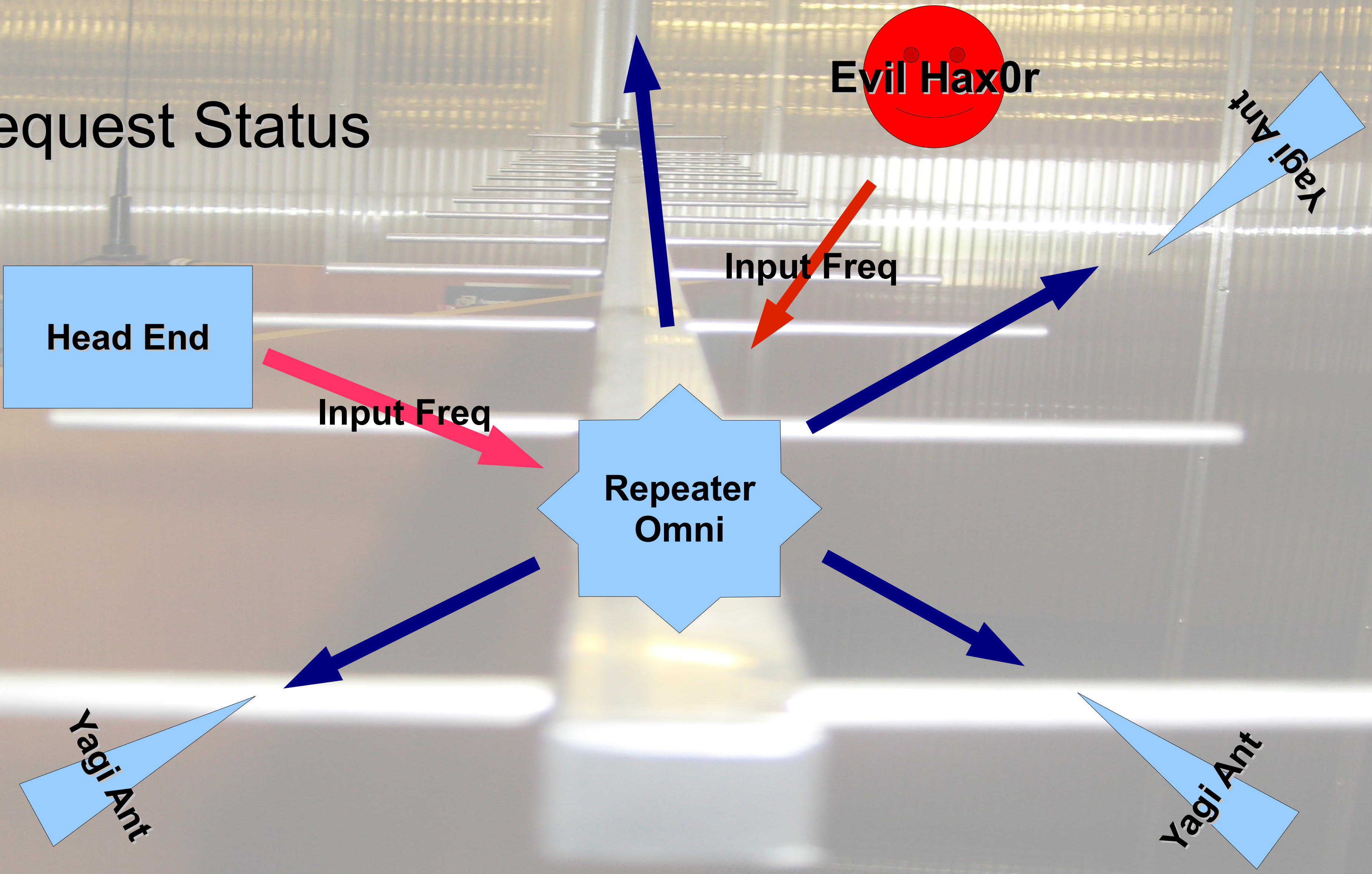


USRP - Second Attempt

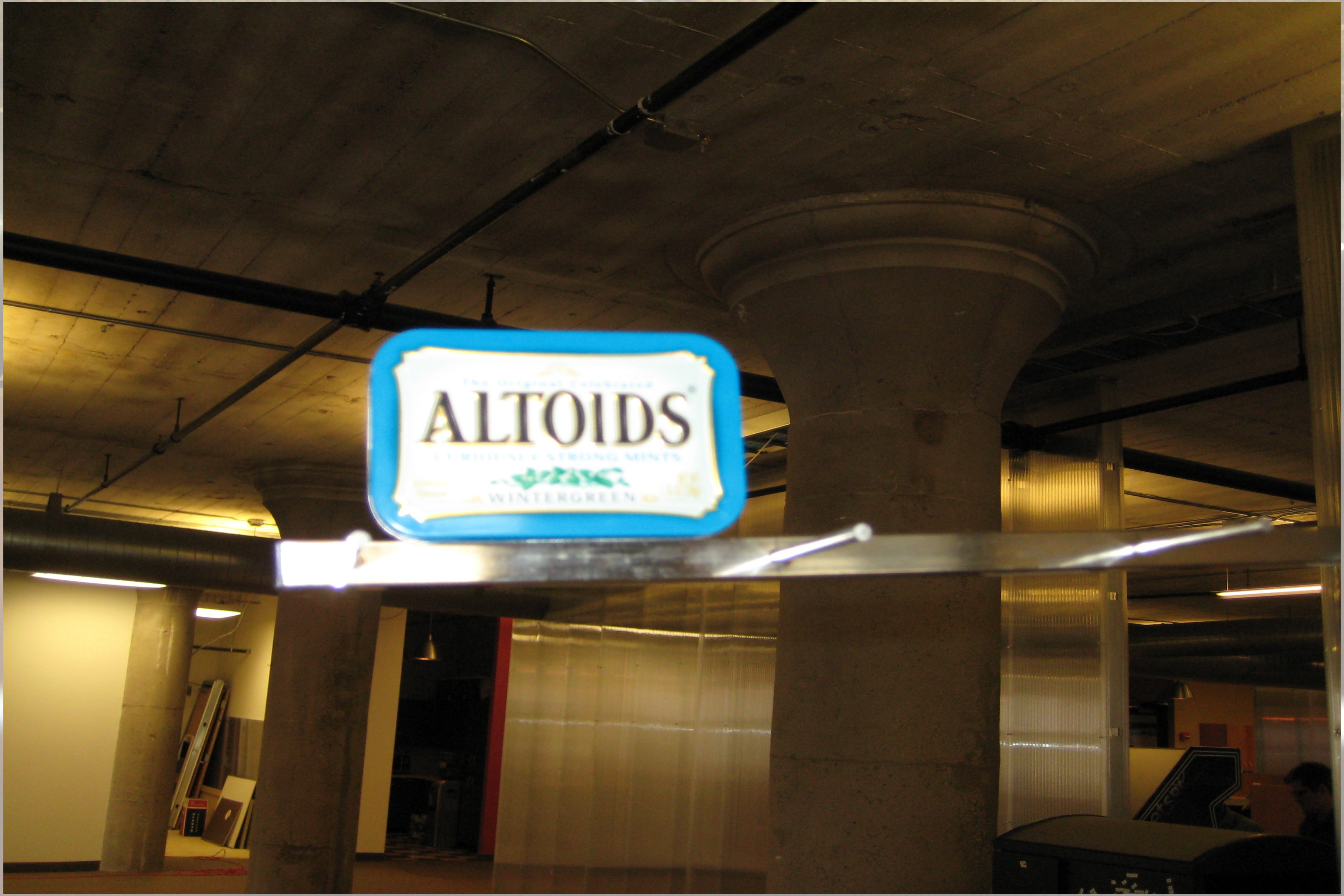


MAS System Attacks

Request Status

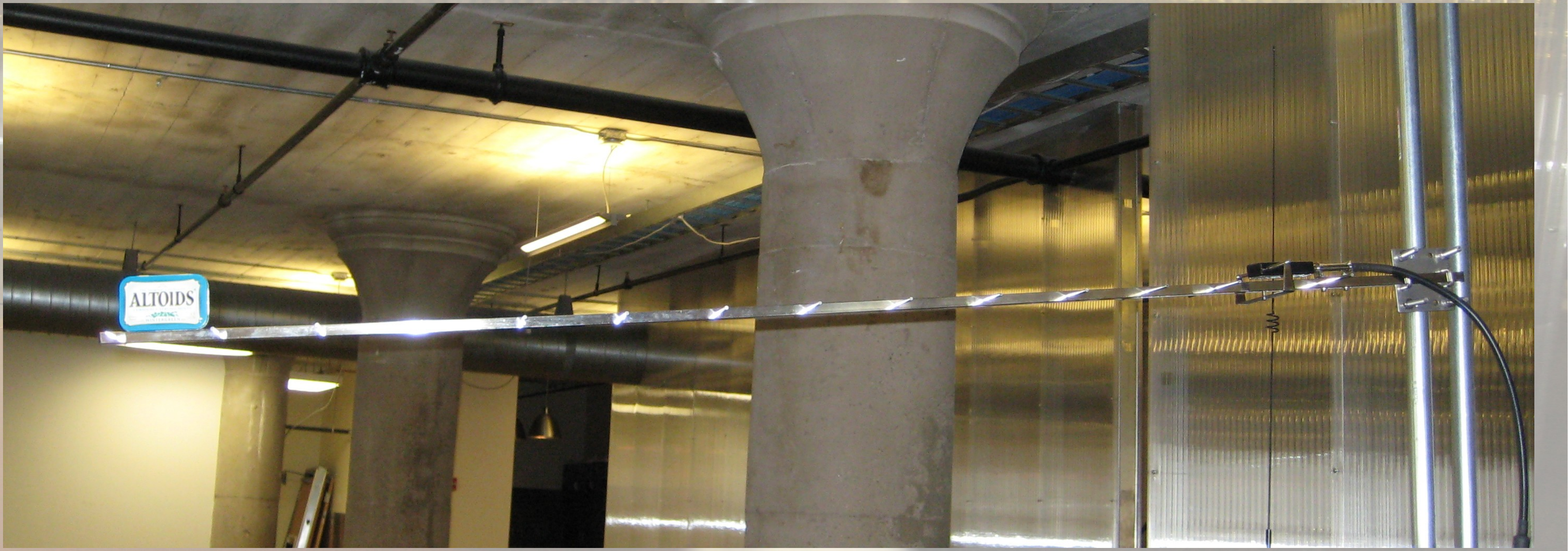


USRP - Third Attempt

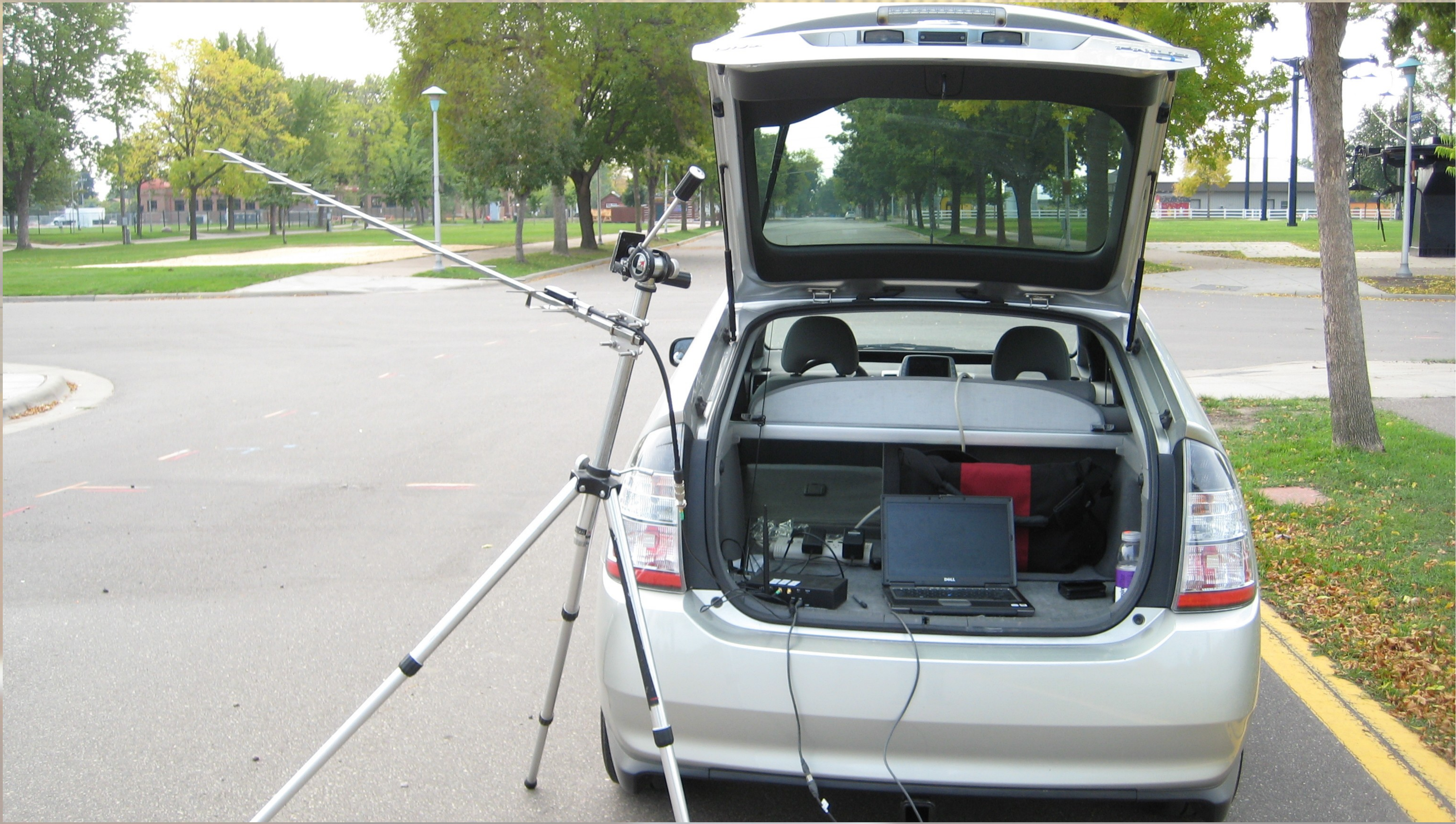


USRP - Third Attempt

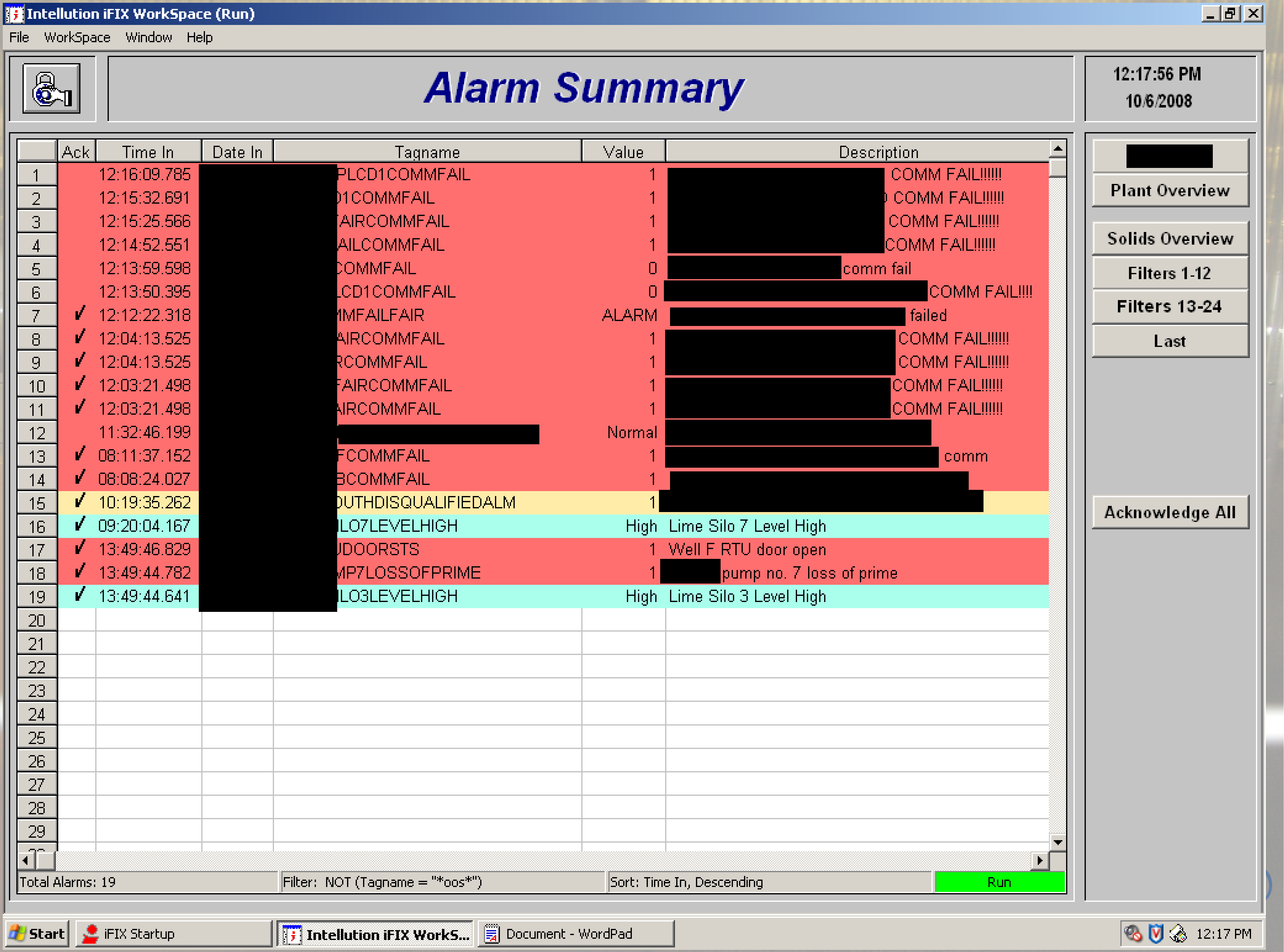
USRP - Third Attempt



USRP - Third Attempt



USRP - Third Attempt



Alarm Summary

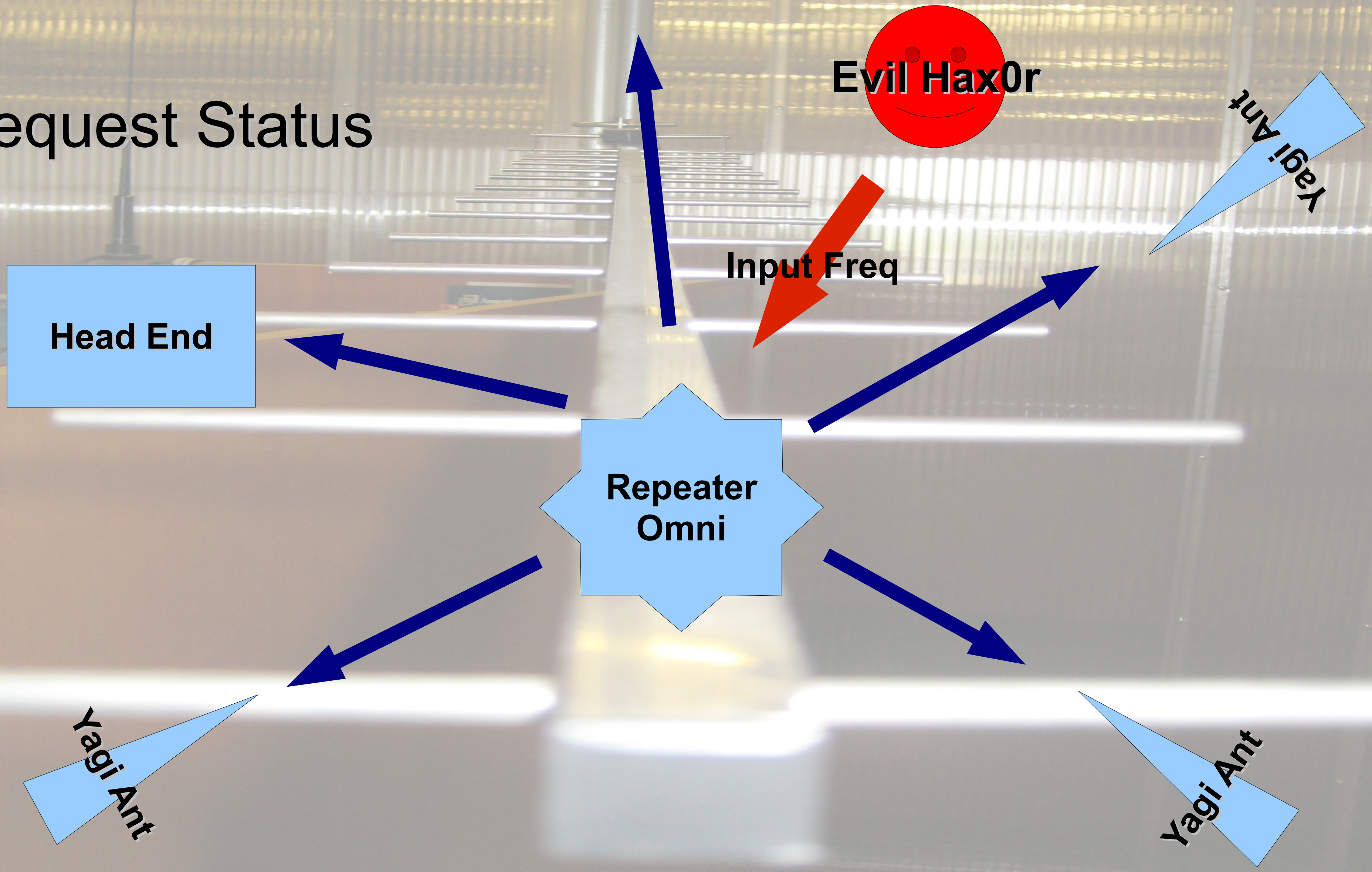
12:17:56 PM
10/6/2008

	Ack	Time In	Date In	Tagname	Value	Description
1		12:16:09.785	[redacted]	[redacted]PLCD1COMMFAIL	1	[redacted] COMM FAIL!!!!!
2		12:15:32.691	[redacted]	[redacted]01COMMFAIL	1	[redacted] COMM FAIL!!!!!
3		12:15:25.566	[redacted]	[redacted]AIRCOMMFAIL	1	[redacted] COMM FAIL!!!!!
4		12:14:52.551	[redacted]	[redacted]AILCOMMFAIL	1	[redacted]COMM FAIL!!!!!
5		12:13:59.598	[redacted]	[redacted]COMMFAIL	0	[redacted]comm fail
6		12:13:50.395	[redacted]	[redacted]LCD1COMMFAIL	0	[redacted]COMM FAIL!!!!
7	✓	12:12:22.318	[redacted]	[redacted]MMFAILFAIR	ALARM	[redacted] failed
8	✓	12:04:13.525	[redacted]	[redacted]AIRCOMMFAIL	1	[redacted] COMM FAIL!!!!!
9	✓	12:04:13.525	[redacted]	[redacted]RCOMMFAIL	1	[redacted] COMM FAIL!!!!!
10	✓	12:03:21.498	[redacted]	[redacted]FAIRCOMMFAIL	1	[redacted]COMM FAIL!!!!!
11	✓	12:03:21.498	[redacted]	[redacted]AIRCOMMFAIL	1	[redacted]COMM FAIL!!!!!
12		11:32:46.199	[redacted]	[redacted]	Normal	[redacted]
13	✓	08:11:37.152	[redacted]	[redacted]FCOMMFAIL	1	[redacted] comm
14	✓	08:08:24.027	[redacted]	[redacted]BCOMMFAIL	1	[redacted]
15	✓	10:19:35.262	[redacted]	[redacted]OUTHDISQUALIFIEDALM	1	[redacted]
16	✓	09:20:04.167	[redacted]	[redacted]LO7LEVELHIGH	High	Lime Silo 7 Level High
17	✓	13:49:46.829	[redacted]	[redacted]UDOORSTS	1	Well F RTU door open
18	✓	13:49:44.782	[redacted]	[redacted]MP7LOSSOFPRIME	1	[redacted]pump no. 7 loss of prime
19	✓	13:49:44.641	[redacted]	[redacted]LO3LEVELHIGH	High	Lime Silo 3 Level High
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						

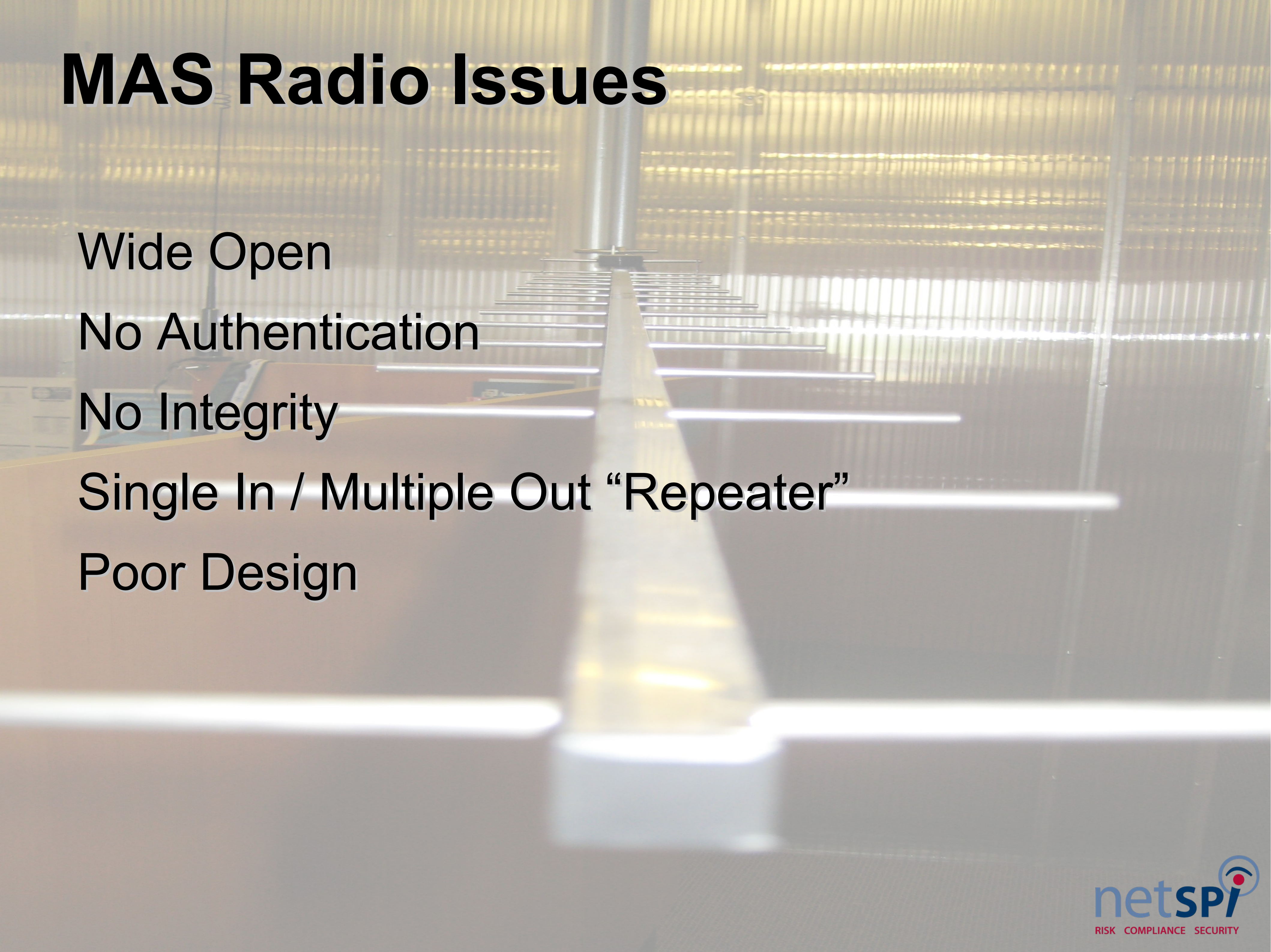
Total Alarms: 19 | Filter: NOT (Tagname = "*oos*") | Sort: Time In, Descending | Run

MAS System Attacks

Request Status

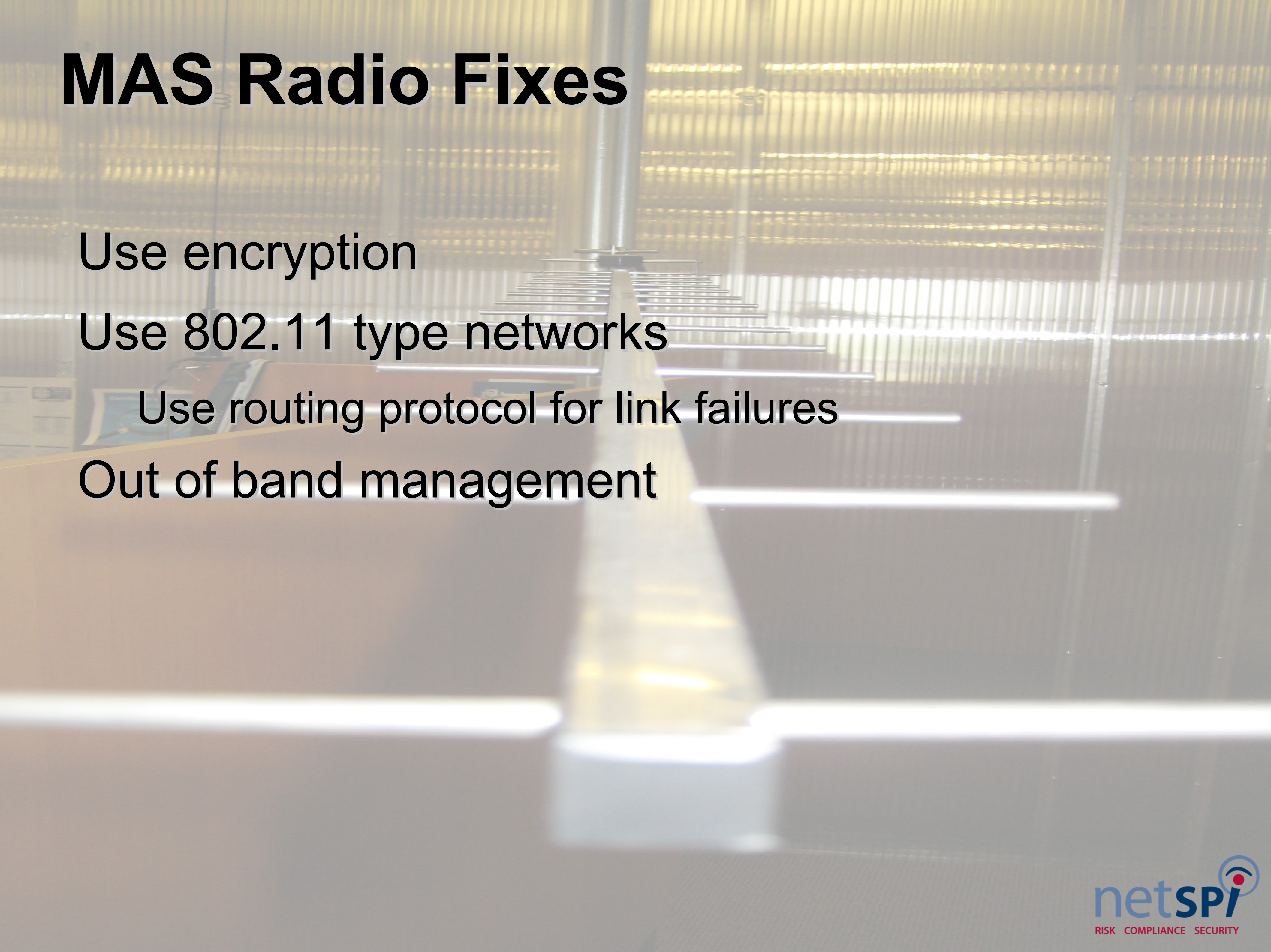


MAS Radio Issues



- Wide Open
- No Authentication
- No Integrity
- Single In / Multiple Out “Repeater”
- Poor Design

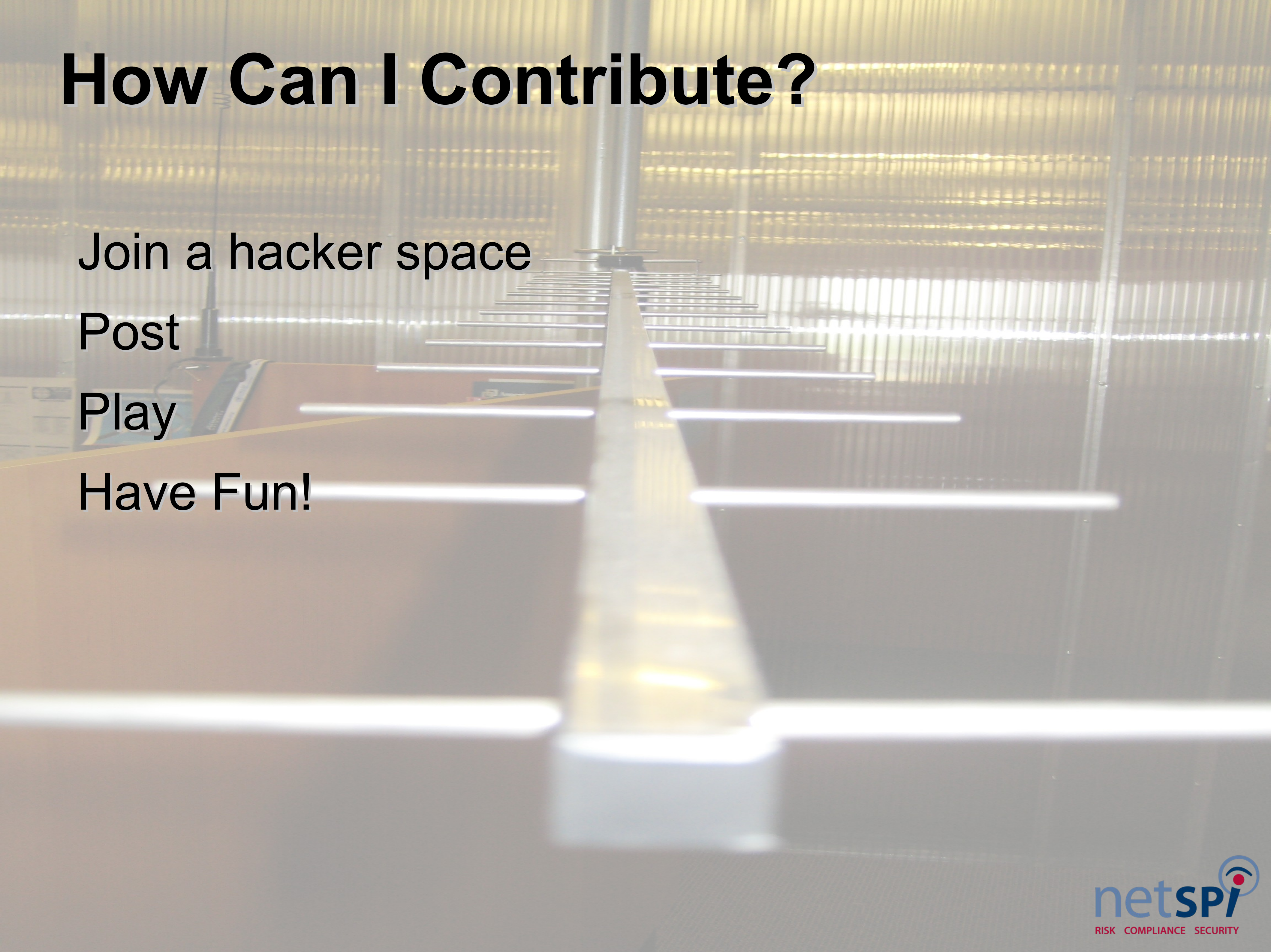
MAS Radio Fixes



- Use encryption
- Use 802.11 type networks
  - Use routing protocol for link failures
- Out of band management

Demo ?

How Can I Contribute?



- Join a hacker space
- Post
- Play
- Have Fun!

Thank you!

My wife, Heather

netSPI

RISK COMPLIANCE SECURITY

References

- dc612.org
- tcmaker.org
- www.gnuradio.org
- http://www.ettus.com/
- www.ece.vt.edu/swe/chamrad/crdocs/CRTM09_060727_USRP.pdf
- http://www.gnu.org/software/gnuradio/doc/exploring-gnuradio.html
- http://www.blackhat.com/presentations/bh-europe-08/Steve-DHulton/Whitepaper/bh-eu-08-stev
- http://dc4420.org/files/dominicgs/bluesniff_slides.pdf
- http://www.rfidhackers.com/
- http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral
- http://www.flickr.com/groups/1043068@N22/