MITIGATION OF GPS VULNERABILITY

USING TIME TRANSFER OVER MICROWAVE SYSTEMS

APRIL 2013

Anurag Gupta
Aviat Networks, Inc.

Abstract

This presentation enumerates the critical infrastructure sectors that use GPS for Frequency or Time and are connected over one or more microwave links.

It touches up on how each of the sectors are likely to use the time/frequency

The mechanisms of transferring frequency and time over microwave links are covered and possible methods of backing up GPS are suggested

The level of accuracy in frequency/time transfer required for the backup mechanisms for some of the CIS sectors is also proposed.

Critical Infrastructure Sectors

List of the Critical Infrastructure sectors from about 2 years ago.

Recent visit to the DHS web site shows two sectors removed from the list

- Postal and Shipping
- National Monuments & Icons

http://www.dhs.gov/files/programs/gc_1189168948944.shtm

Critical Infrastructure Sectors

Critical Infrastructure Sector	GPS for frequency/ time	Microwave Connectivity
Banking & Finance	Time	yes
Chemical	Time	yes
Commercial Facilities	?	?
Communications	Time/ frequency	Mostly Yes
Critical Manufacturing	Time	yes
Dams	Time/ frequency	yes
Defense Industrial Base	Time	? (yes)
Emergency Services	Time	Yes
Energy	Time/ frequency	Yes
Food & Agriculture	x	x
Government Facilities	Time (?)	Yes/ May be
Healthcare & Public Health	x	Yes
Information Technology	Time/ Frequency	Yes
Nuclear Reactors, Materials & Waste	Time	Yes
Transportation	Time/ Geospatial apps	?
Water	(?)	Yes

Critical Infrastructure Sectors- Coverage

Number of CIS that depend on GPS for Time or frequency 10

Number of CIS that have microwave connectivity 12

Overlap 100%

Microwave can effectively provide coverage for

Back up to GPS for time/ frequency

Typical Uses of Time/ Frequency

Communications

Applicable Sectors: Telecom, IT, Emergency Services

- Synchronization of Networks- TOD, Phase, frequency
- Handing over of calls between adjacent communicating entities

SCADA- Supervisory, Control & Data Acquisition

Applicable Sectors: Chemical, Critical Manufacturing, Dams ,Defense Industrial Base, Energy, Nuclear Reactors.

- Providing common time base for supervisory, control & alarm events
- Support for event logging

PMU synchronization

Applicable Sectors: Energy, Nuclear (power generation)

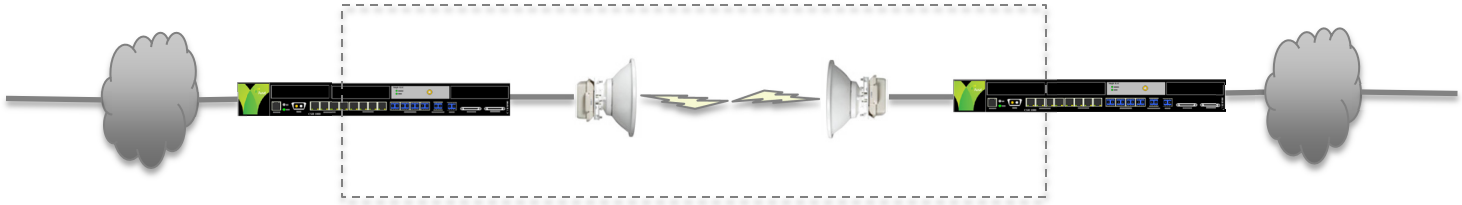
Regulatory Compliance, Transactional Forensics

Applicable Sectors: Finance, Banking

- Transaction logging

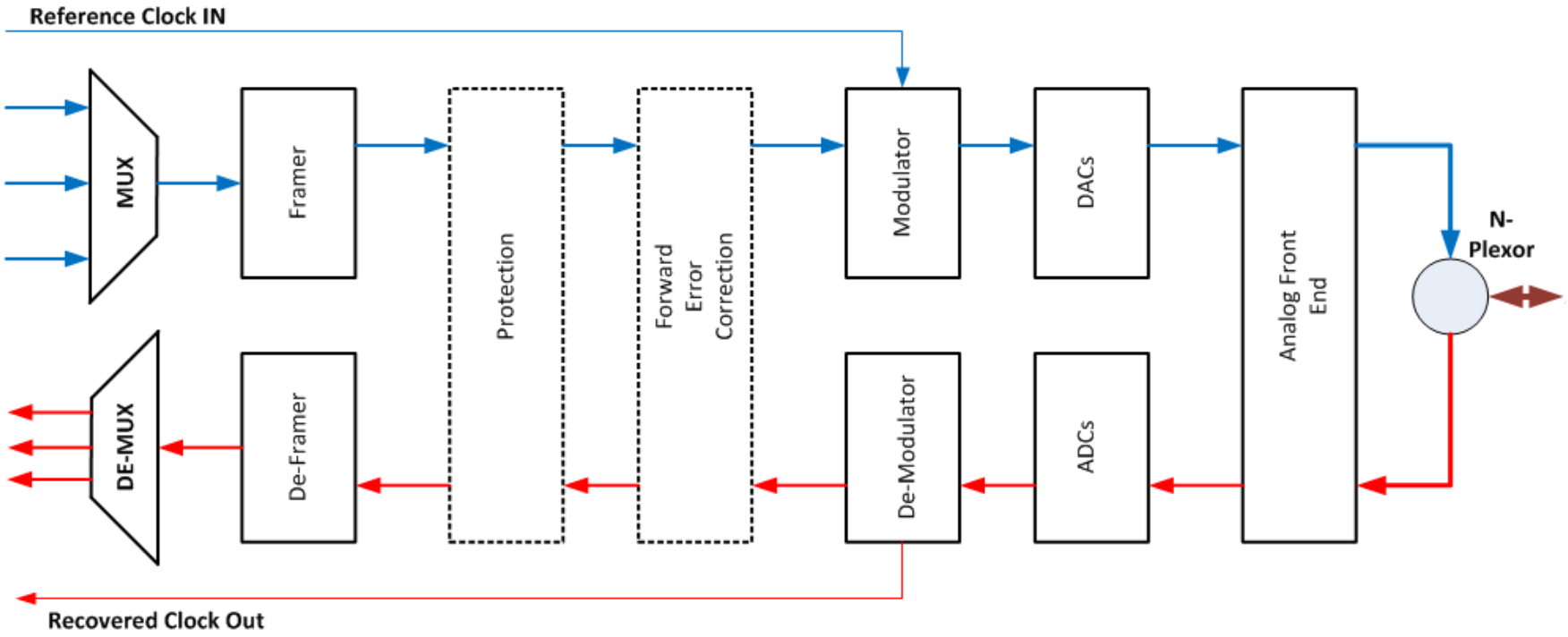
These are some conditions unique to µWave deployments

1. Links are essentially line of sight (LOS)
2. Due to varying environmental conditions the adaptive modulation techniques are used
3. Irrespective of modulation used the framing used by each manufacturer's equipment is unique
4. This implies that the µWave link is book-ended by equipment from same manufacturer.



Microwave Modem

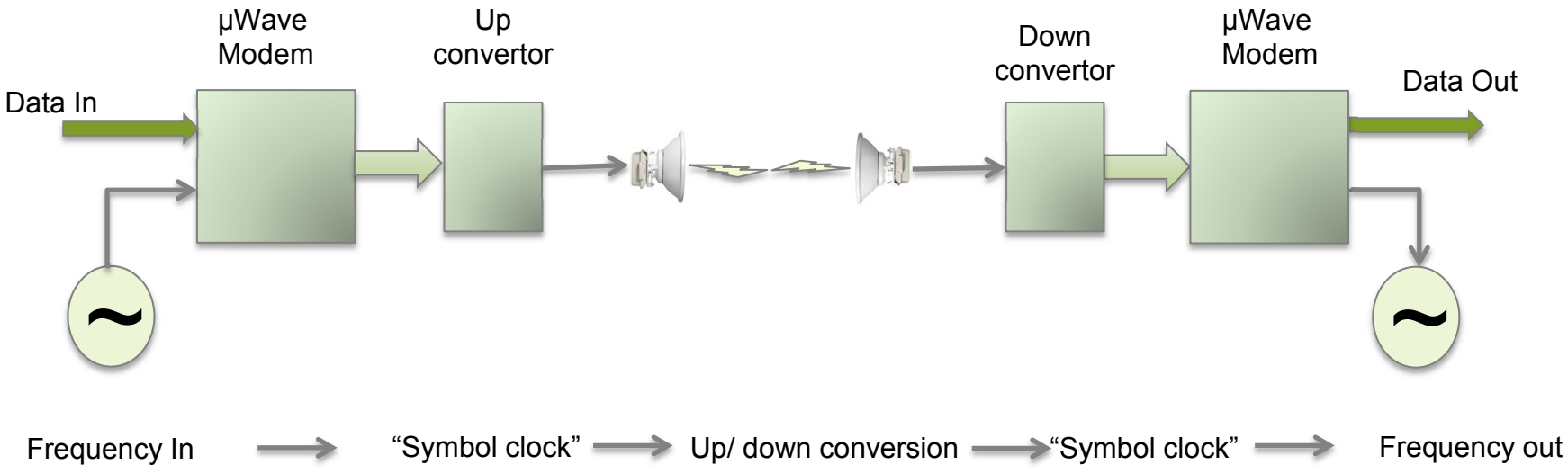
Simplified block diagram



- Data passes through a Framer, Protection mechanisms, FEC , Digital modems & AFE
- Reverse on the way back

Time transfer over microwave links

Step 1- Transferring frequency

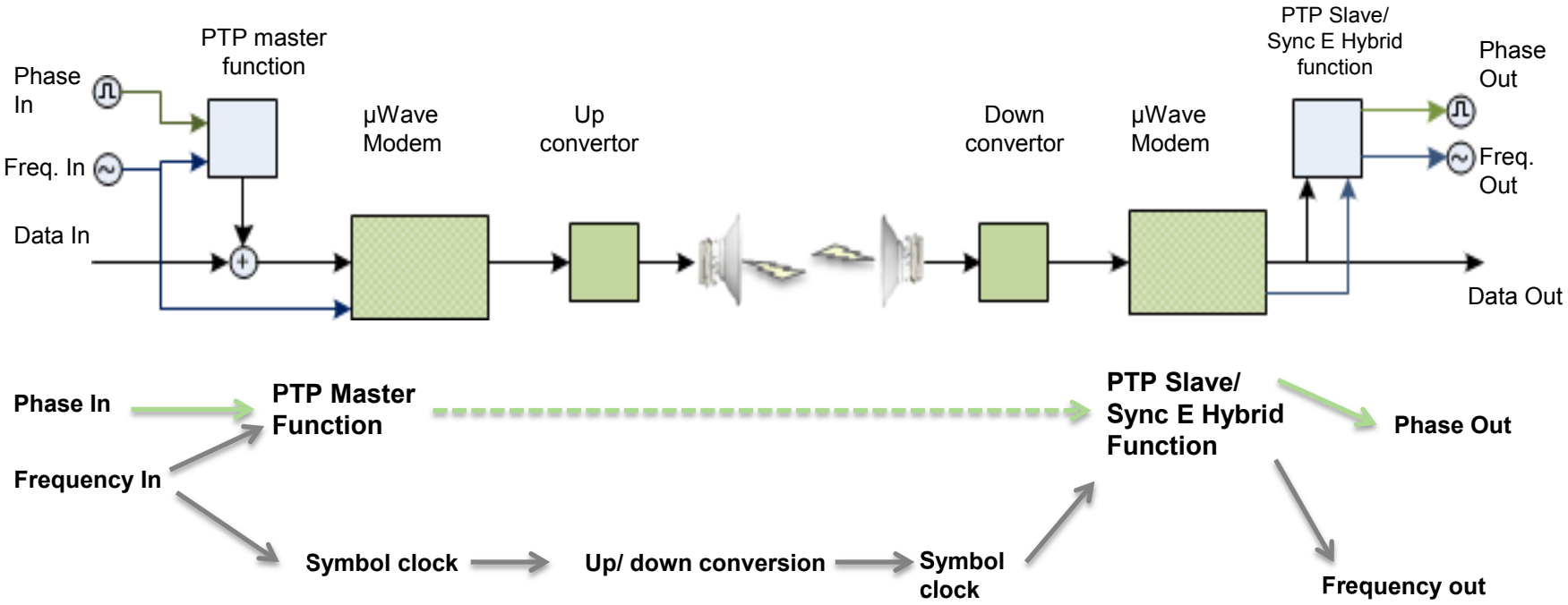


- The Frequency Out is physically traceable to Frequency In
  - F_{in} is used to generate the “symbol” at the transmit end.
  - Symbol clock is recovered by the modem at the receive end
  - F_{out} is regenerated from the symbol clock
- This scenario is reminiscent of the Sync-E operation

Time transfer over microwave links

Step 2 option A - Transferring Phase "A relatively simplistic way"

Run PTP/ IEEE 1588 over the microwave link

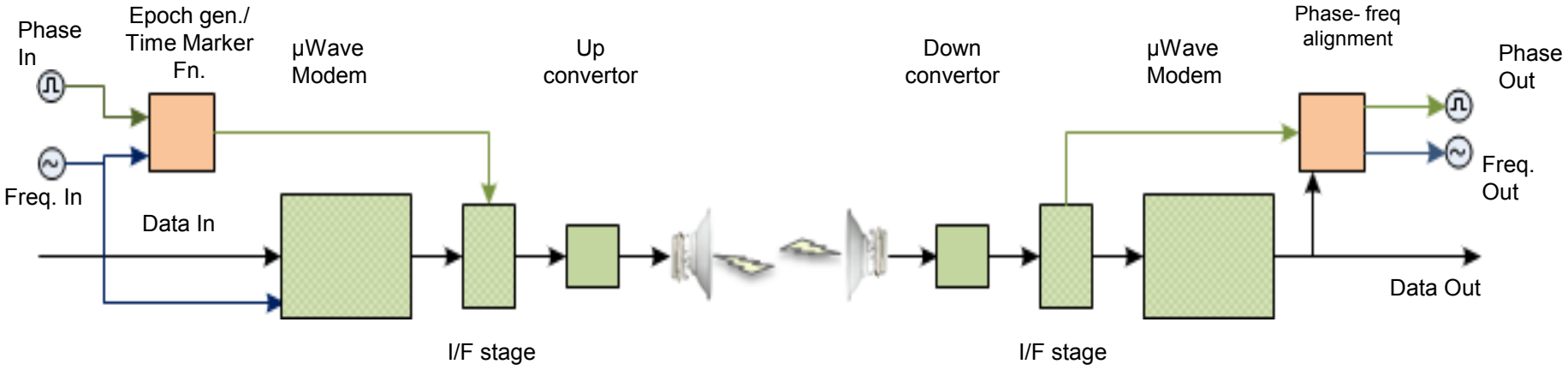


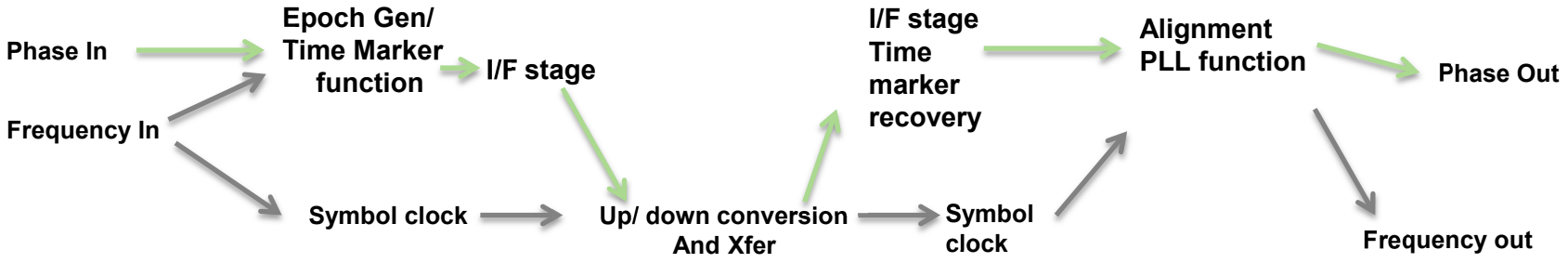
Step 2 option A - Transferring Phase "A relatively simplistic way"

- On the upstream node common frequency (F_{in}) is fed to the Physical layer and PTP function.
- The "$Phase_{in}$"
  - Is fed to the PTP master function
  - Is transferred in-band over the packet data path
  - Recovered at the remote end by PTP "slave" function
- The output phase and frequency are aligned using techniques similar to those used in PTP- Sync-E Hybrid modes

Pro(s)	Con(s)
Needs no special support from modem, IF or RF functions	Requires relatively complex hardware and software implementations
	To achieve accurate phase recovery the PTP servo function would need to be ACM state aware
	Cost

Step 2 option B- Transferring Phase- I/F stage support



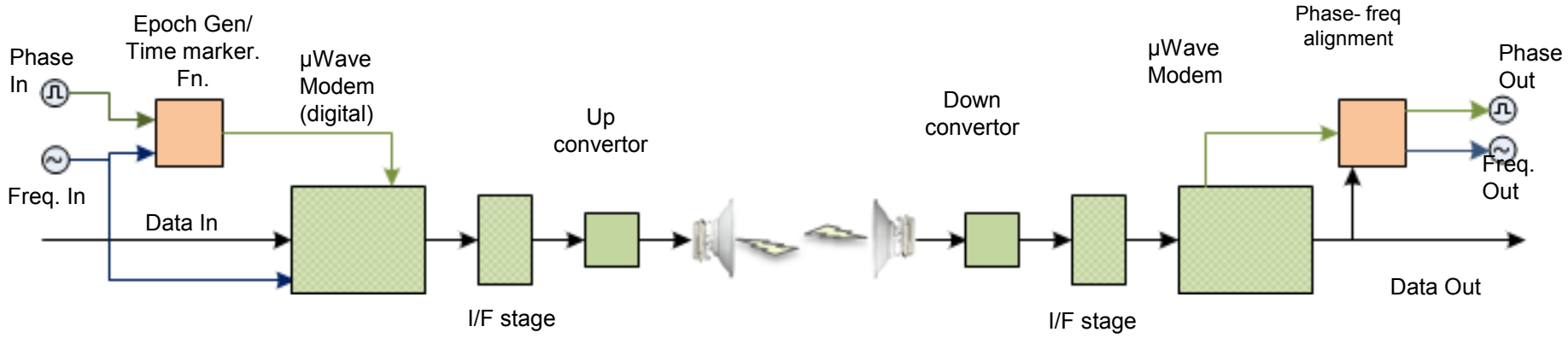


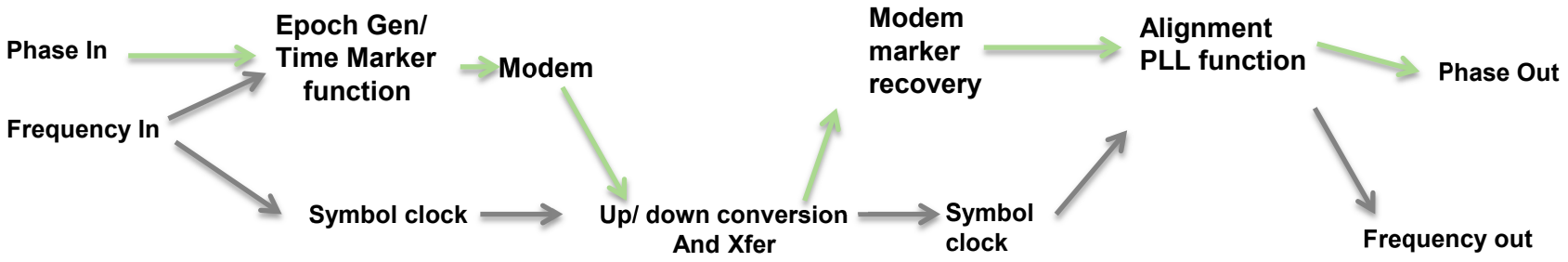
Step 2 option B- Transferring Phase- I/F stage support

- On the upstream node common frequency (F_{in}) is fed to the Physical layer and Time marker/ epoch generation function.
- The $Phase_{in}$
  - is fed to the (above) time marker function
  - The time marker is used to generate “time marker” event at the I/F stage
  - The event is Recovered at the remote I/F stage
- The output phase and frequency are aligned using standard DPLL techniques.

Pro(s)	Con(s)
Cost would be lower than option A	Requires Time marker event generation and recovery support at the I/F stage in microwave modems
Relatively straight forward logic implementable in simple CPLD/ FPGA	

Step 2 option C- Transferring Phase- modem support





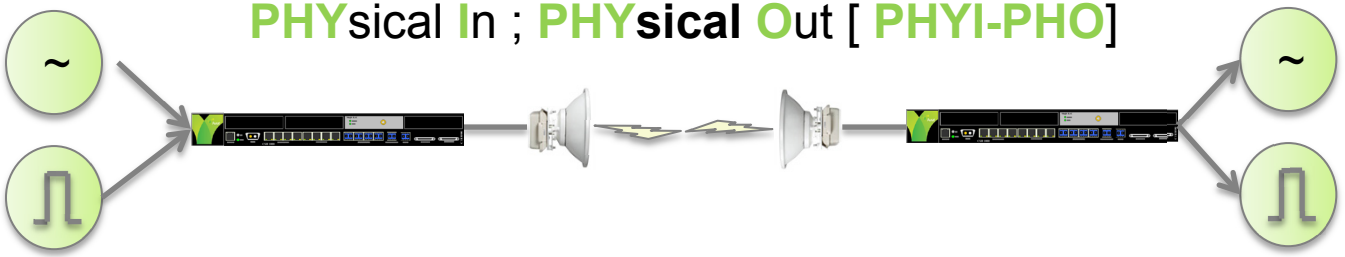
Step 2 option C- Transferring Phase- modem support

- On the upstream node common frequency (F_{in}) is fed to the Physical layer and Time marker/ epoch generation function.
- The $Phase_{in}$
  - Is fed to the (above) time marker function
  - This is used to generate “time marker” event at the “Modem” stage on the Tx side
  - The event is recovered at the remote modem
- The output phase and frequency are aligned using standard DPLL techniques.

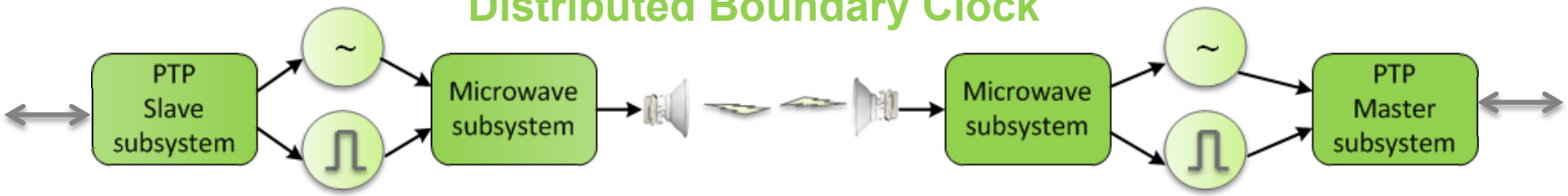
Pro(s)	Con(s)
Cost would be lower than option B	Requires Time marker event generation and recovery support at the stage in microwave modems
Relatively straight forward logic implementable in simple CPLD/ FPGA	

Time transfer over microwave links

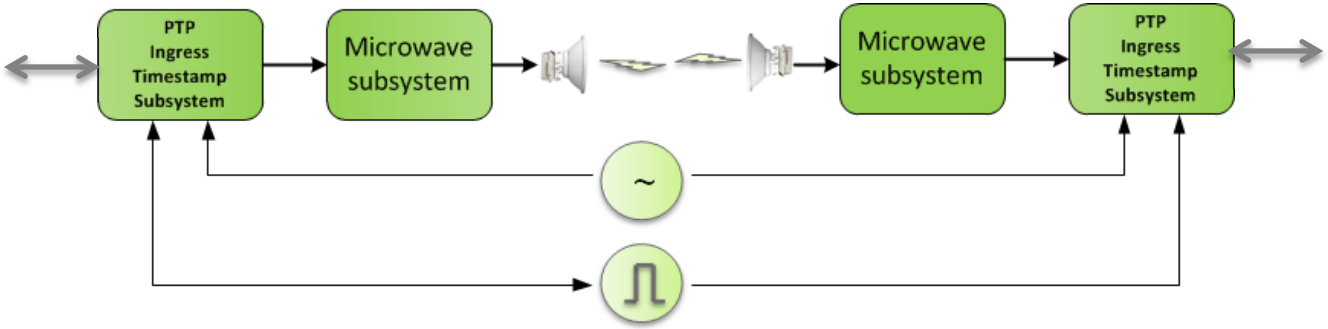
PHYsical In ; PHYsical Out [PHYI-PHO]



Distributed Boundary Clock

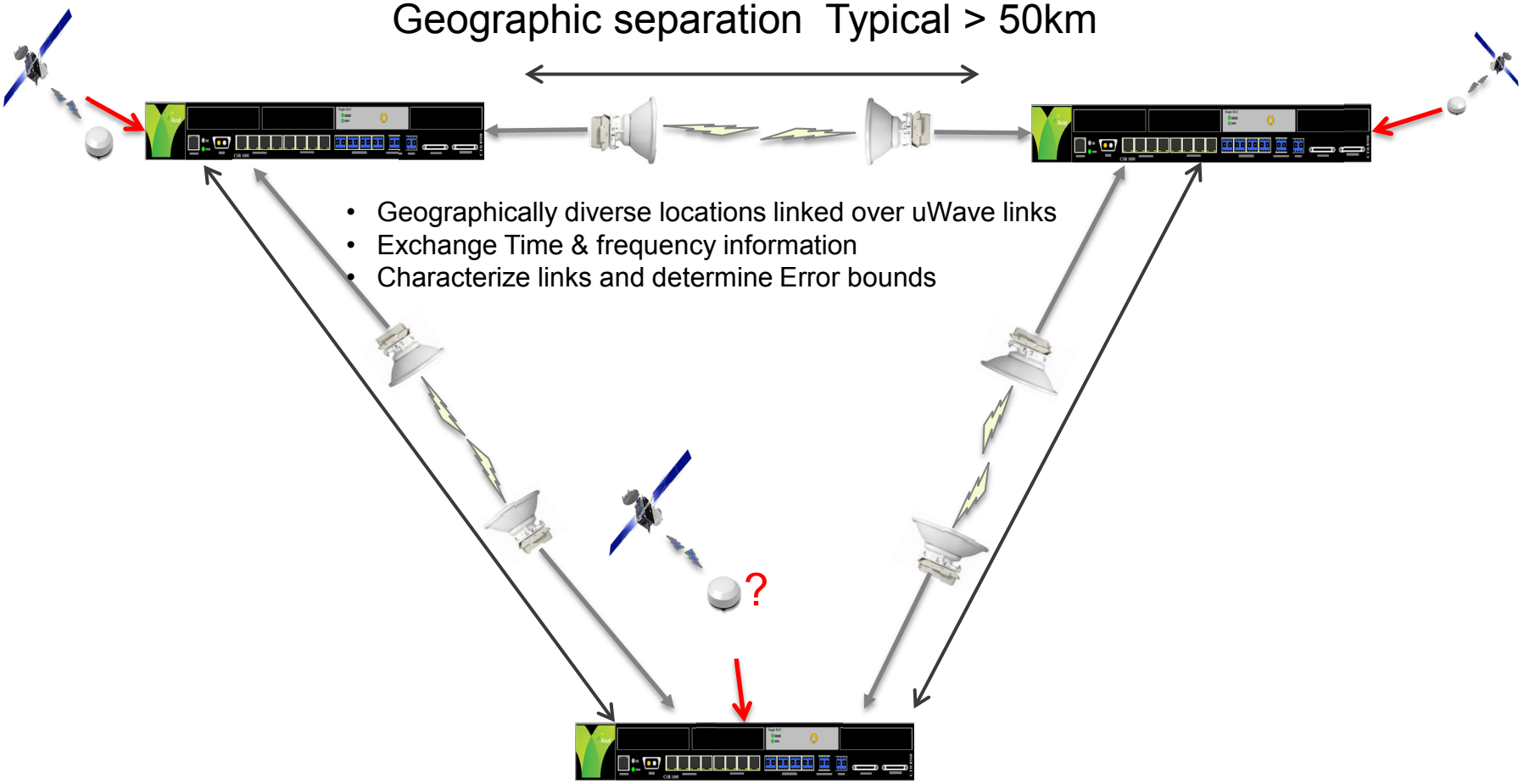


Distributed Transparent Clock



Mitigation

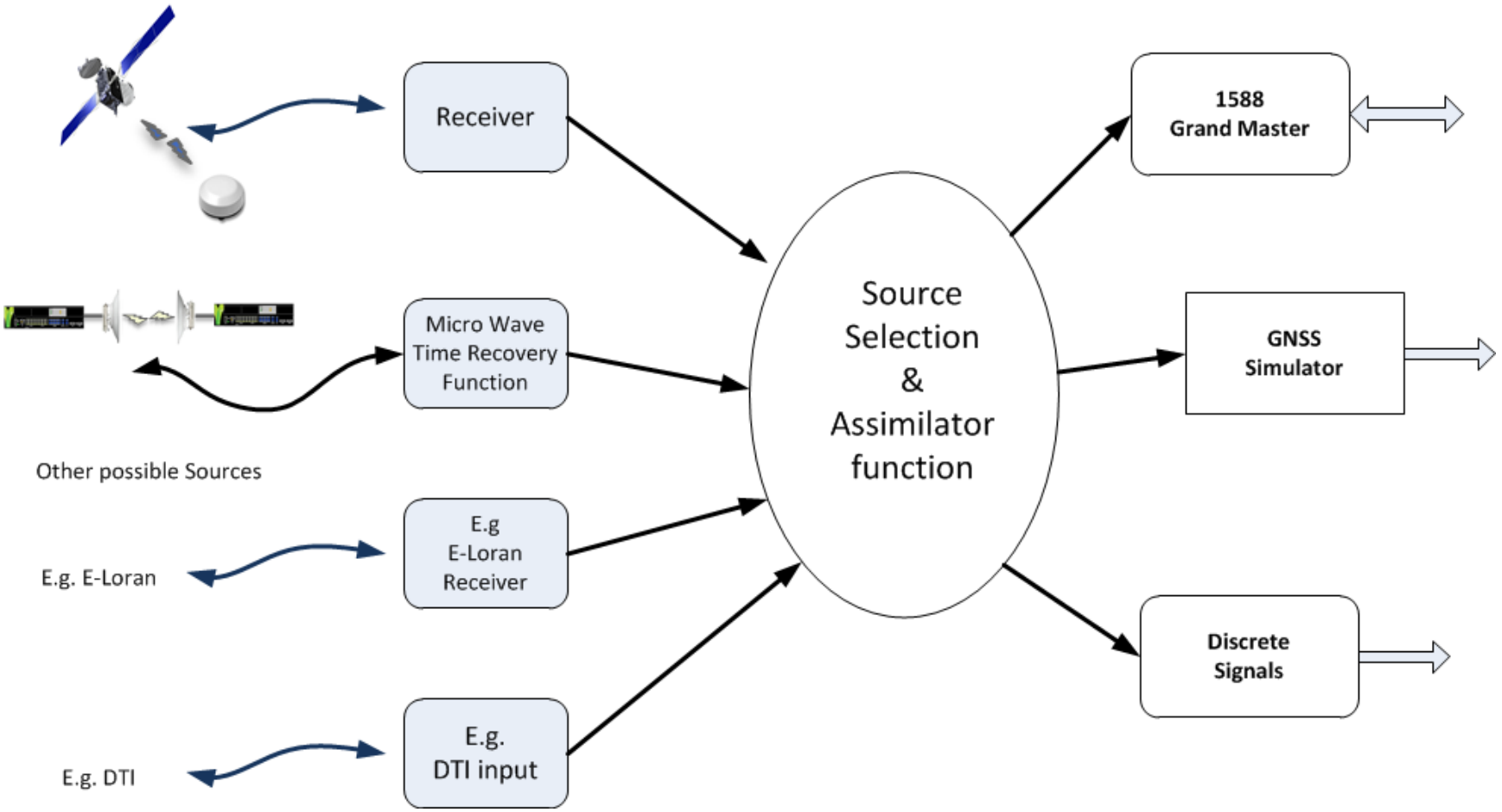
Geographic Diversity & Redundancy



If GPS is compromised, the system could switch over to the uWave Backup

Mitigation

Ensemble of clock sources



Aviat NETWORKS

Targeted Accuracy By Application

This table proposes targets for time/ frequency accuracy by applications

CIS/ Application	End application accuracy target	Clock accuracy (lines in the sand ☺)
Telecom (aggregation)	500ns to 1.5uS	~50 nS
Telecom (leaf nodes)	> 1 uS	~50 nS
Energy / Power PMU	1uS to 10uS	50nS
Multiple / fault logging	10uS to 5mS	100 -500 nS
Multiple / SCADA	<1ms to 100mS	100 -500 nS
HTF/ Latency Measurements	500uS to 10mS	100 -500 nS
Finance/ Transactional TS	10 to 100mS	100 -500 nS

Open invitation to audience to augment the table….

Summary & Conclusion

- Most entities in CIS use GNSS for synchronization
  ……use Microwave for communication

- Microwave links with timing enhancements
  …….can provide reliable back up to GPS for synchronization applications

THANK YOU FOR YOUR ATTENTION.....

QUESTIONS?

Anurag Gupta
+1-408-567-7286
Email: anurag.gupta@aviatnet.com