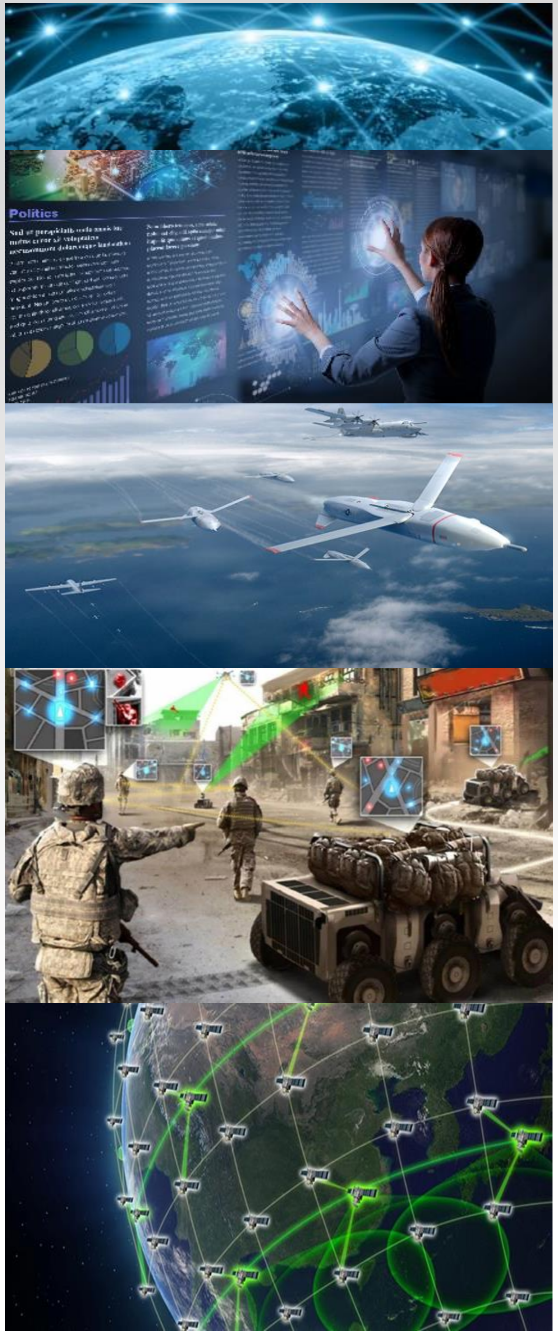
In-Situ Monitoring/Lifetime Prognostication of Critical System Components Utilizing Unintended Emission Analysis Techniques

Dr. Nick Martin
Defense Microelectronics Activity
Office of the Under Secretary of Defense (Research & Engineering)

22nd Annual NDIA Systems and Mission Engineering Conference
Tampa, FL | October 23, 2019



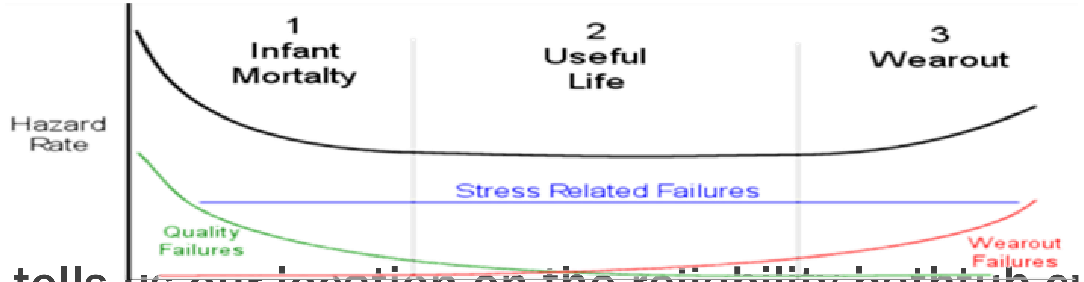
Traditional Reliability/Lifetime Prognostication

$$AF = \left(\frac{V_A}{V_R}\right)^n EXP\left(-\left(\frac{E_A}{k_B}\right)\left(\frac{1}{T_F} - \frac{1}{T_I}\right)\right)$$

- **Issue 1: The above equation is applied indiscriminately to virtually every active and passive device to quantify reliability**
  - Discrete components to integrated circuits: no distinction is made for device architectures or even the materials used in device fabrication
- **Issue 2: Extremely tenuous link to physical reality (E_A and n)**
  - E_A is formally defined as the minimum kinetic energy required for molecular collisions to result in a chemical reaction
  - For reliability calculations E_A is redefined as the energy required to activate latent defects in the material-are these concepts equivalent??
  - For reliability calculations E_A is treated as a constant. Yet, in chemical reactions, there is a much greater probability that molecules will collide and initiate a reaction due to thermal agitation at higher temperatures. This implies E_A has some degree of temperature dependence
  - Values for E_A used in reliability calculations are subjective estimates
    - Usually, E_A is given as a range of values…and the above equation is sensitive to both E_A and n (often not defined at all and typically taken to be unity)
  - Manufacturers acknowledge these issues by de-rating calculated lifetimes using these methods, often by an order of magnitude

Unintended Emission Analysis

- **Main Idea: All active electronics generate unintended emissions**
  - Examples: power fluctuations, electromagnetic fields, thermal profiles
  - Passive electronics can also be induced to yield emission data
  - Very strong physical basis: emissions are characteristic of device architecture and fabrication materials
- **Emission Data can be leveraged to quantify degradation**
  - Causal relationship between component condition emission spectra
  - Devices in various stages of degradation have unique emission spectra
- **Comparative analysis of known good to degraded components**
- **Analysis of emission data and associated distributions can be used to prognosticate Remaining Useful Life (RUL)**



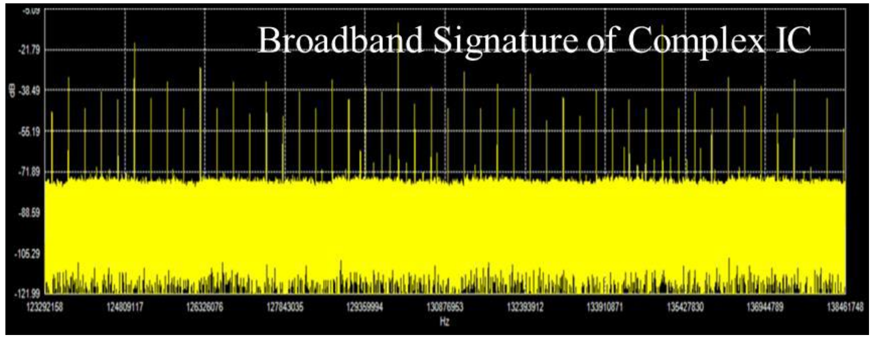
- **Emission analysis tells us our location on the reliability bathtub curve-Traditional reliability approach does not provide this information**

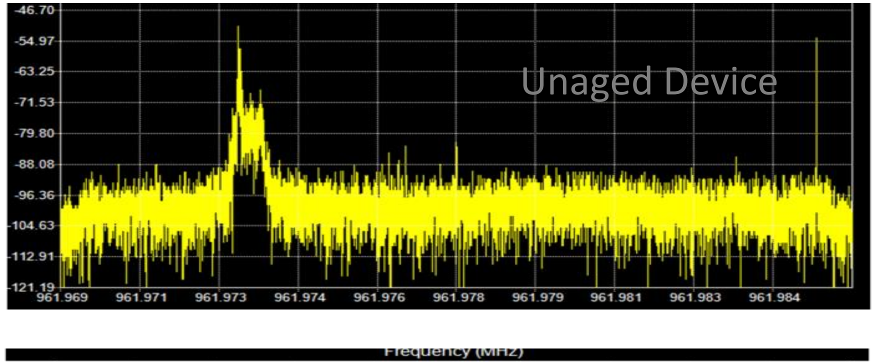
Analytic Signals & Transforms

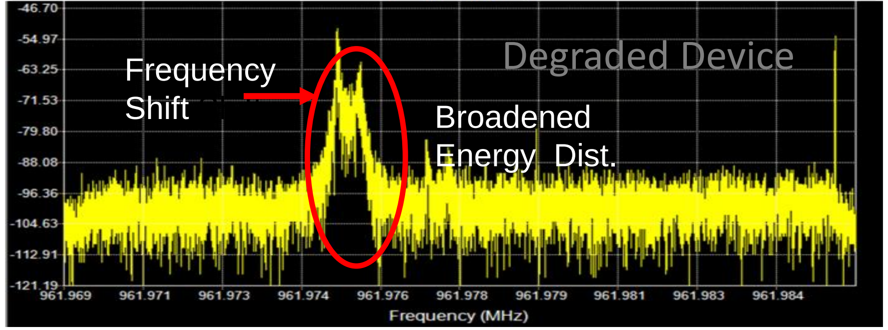
- **Analytic Signal: A complex-valued function with no negative frequency component**
  - Created from emission data- retains strong link to physical device
- **General form:**
  - $Y(t) = y(t) + ih(t)$
- **Analytic signals are created by application of mathematical transforms to the sampled data**
  - Common transforms include the Fast Fourier Transform (FFT) and the Hilbert Transform
- **Why transform the sampled data?**
  - Very subtle changes in the real-valued signal are easily identified in the transform domain
  - Transformed signal contains more dynamic information than original measured signal
    - Amplitude
    - Phase
    - Instantaneous frequency….many others
- **Analytic signals form the basis of an algorithmic approach to monitoring device degradation and lifetime prognostication**

EM Signature Analysis Data Acquisition

- **Emission data detection with high acuity RF sensor**
  - Collection of broadband data
- **Extended Frequency range**
  - Billions of data points per part
  - ~ 1 hour to collect data
- **Target parameters of interest:**
  - Frequency shifts of specific peaks
  - Harmonic content
  - Energy distribution
  - Time varying shifts in data
- **Extremely sensitive technique**
  - Extremely close to theoretical limit of -173 dBm
  - Can detect process variation, code changes, packaging stress…and aging



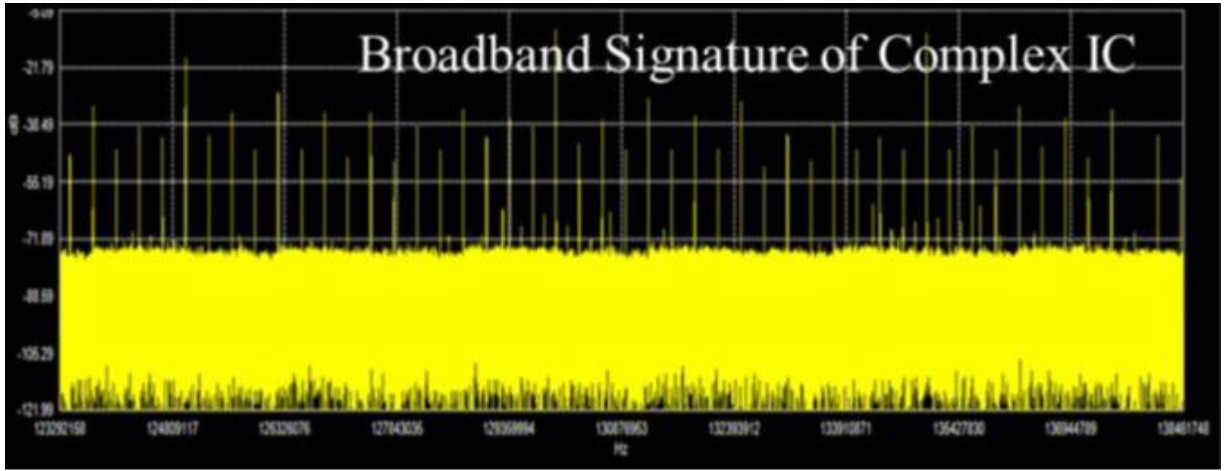


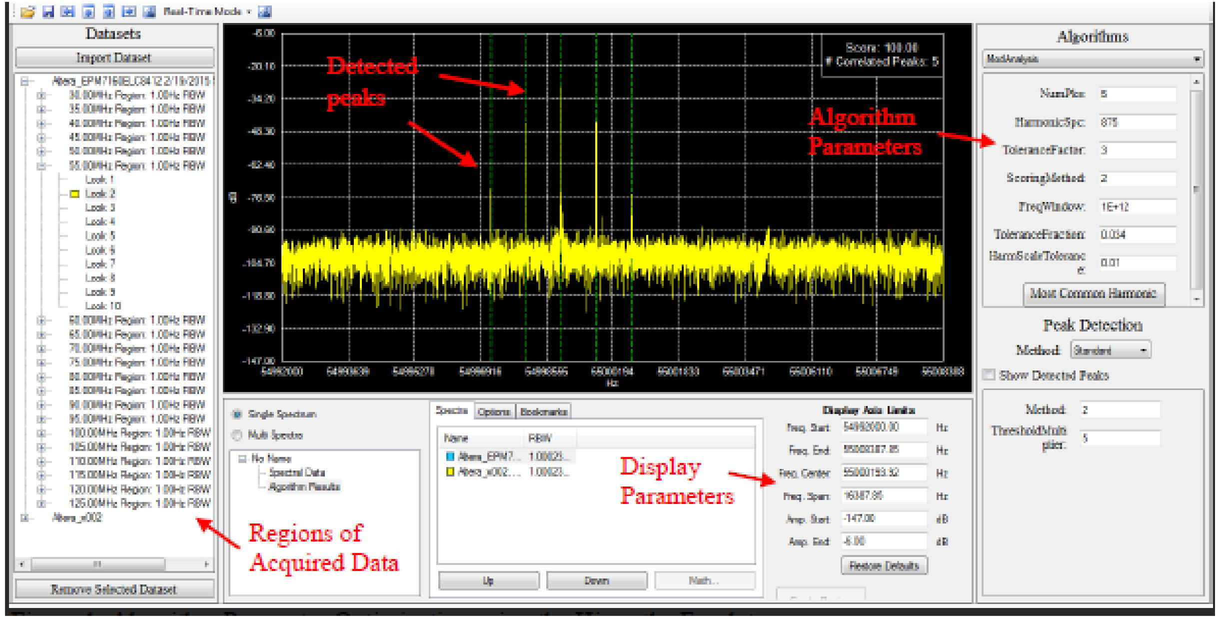


Slide content courtesy of Dr. Andrew Portune, Nokomis, Inc.

EM Signature Analysis Emulation Software

- **Emulation software used to capture time-varying content**
  - Certain broadband signature metrics are time dependent
  - Provides a platform for detailed signature assessment
- **Can also be utilized for comparative assessments of multiple data sets**





Score: 100.00
Correlated Peaks: 5

Algorithms: ModAnalysis

NumPks: 5
HarmonicSpc: 875
ToleranceFactor: 3
ScoringMethod: 2
FreqWindow: 1E+12
ToleranceFraction: 0.034
HarmScaleTolerance: 0.01

Peak Detection
Method: Standard
☐ Show Detected Peaks
Method: 2
ThresholdMultiplier: 5

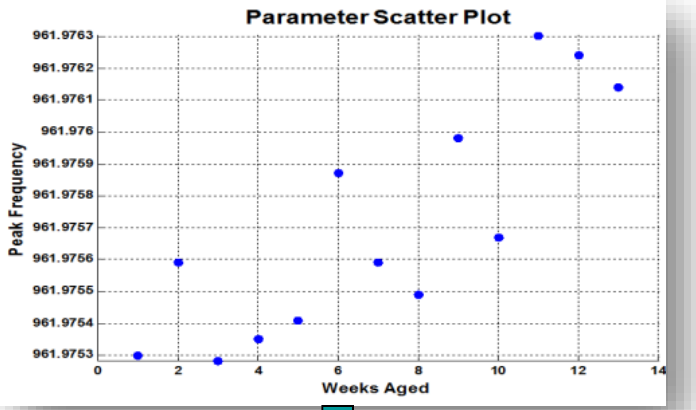
Display Axis Limits
Freq. Start: 54992000.00 Hz
Freq. End: 55008387.85 Hz
Freq. Center: 55000193.92 Hz
Freq. Span: 16387.85 Hz
Amp. Start: -147.00 dB
Amp. End: -6.00 dB

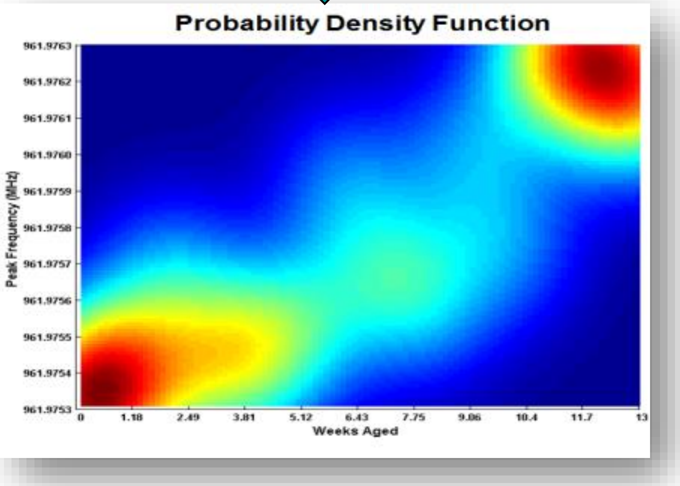
Slide content courtesy of Dr. Andrew Portune, Nokomis, Inc.

Distribution Statement A: Approved for public release. Distribution is unlimited.

Remaining Useful Life (RUL) Prognostication

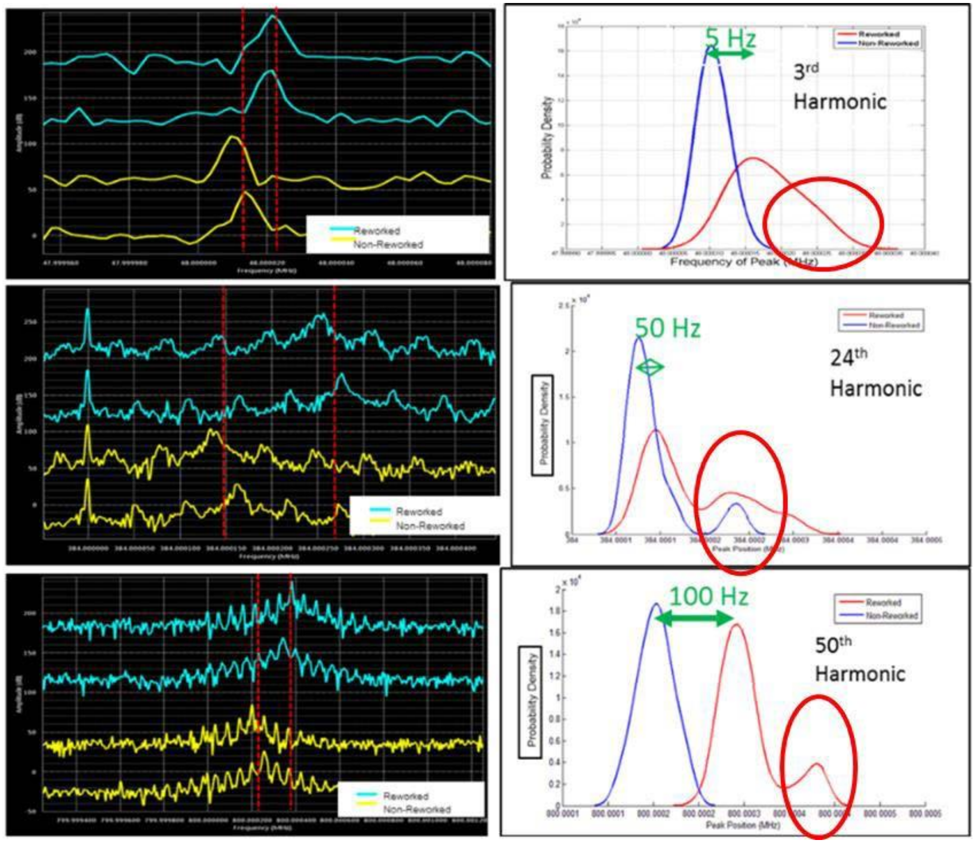
- **RUL prognostication performed using Bayesian statistics**
- **Utilized functional relationships between signature metric values and device age**
  - Function parameter sets each have a calculated likelihood based on how well they fit measured data
  - RUL predicted by each parameter set is weighted by its likelihood
  - Combination of weighted RULs for all parameter sets provides a RUL predicted by each metric
  - Combination of RUL predictions for all metrics increases accuracy and lowers uncertainty
- **Bayesian approach leverages previous measurement history on the DUT and other similar devices to increase accuracy**





Probability Distribution Analysis for Health/Lifetime Monitoring

- **Probability distribution functions (PDF) created for each signature metric**
- **Multiple metrics utilized to determine lifetime/quantify degradation**
- **Comparative analysis with known good sample generally correlates changes to circuit condition**
  - Shift in mean value
  - Broadening of distribution
  - Bimodal behavior
- **Algorithmic methodology and high degree of integration allows real time monitoring of PDFs associated with component-of-interest**



Prognostication Mathematics

Number of signature metrics measured

Likelihood of the specific RUL calculated for that signature metric

$$P(RUL_i)=\prod_{i=1}^{n} L_{Si}RUL_{Si}$$

Probability of specific RUL

Likelihood that a specific function parameter set for a signature metric function accurately describes measured data

Number of measurements made over time

Measured metric value

Calculated metric value

$$L_{S_i}(\{p\}) = \prod_{j=1}^{m} e^{-\frac{\left(y_{measured,j}-f\left(x_j,\{p\}\right)\right)^2}{2\sigma_j{}^2}}$$

Expected metric value variance

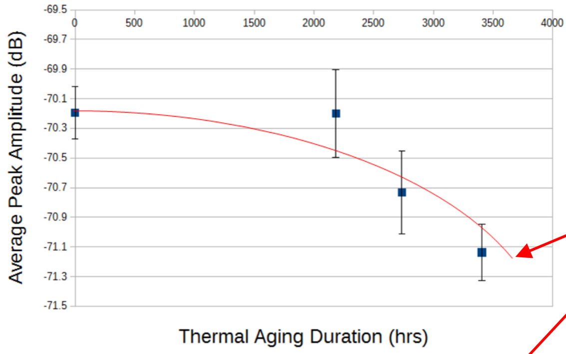
Probability of an RUL value determined by multiplying PDFs for each signature metric, where each PDF is calculated based upon measured signature metric values

$$\boxed{P(RUL_i|\{S\})=\frac{\prod_{j=1}^{m} P\left(S_j|RUL_i\right)}{\sum_{i=i}^{n}\left\langle\prod_{j=1}^{m} P\left(S_j|RUL_i\right)\right\rangle}}$$

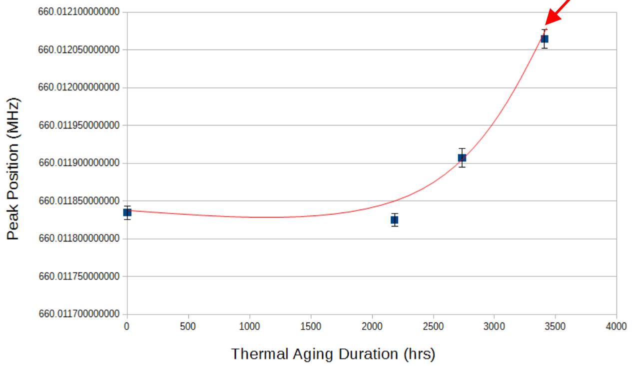
Slide Content Courtesy of Dr. Andrew Portune, Nokomis Inc.

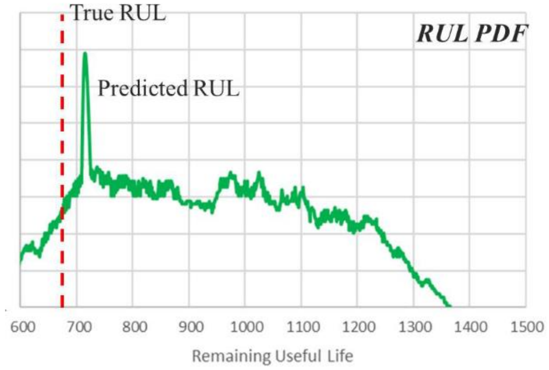
Sample RUL of MSP 430 Embedded Flash

- **One thermally aged devices at 150℃ for 2736 hrs**
- **Two metrics utilized in sample calculation (Shown at Right)**
  - – Average peak amplitude (dB)
  - – Peak Position (MHz)
  - – Error bars represent one stddev
- **End of life taken to be device with 3408 hrs at 150℃**
  - – Enabled comparison of predicted result to known sample
- **Result: Predicted RUL deviation from known RUL by 49 hrs (7.2%)**
  - – Prediction would be more precise and accurate if more metrics were utilized (in practice multiple metrics are utilized)



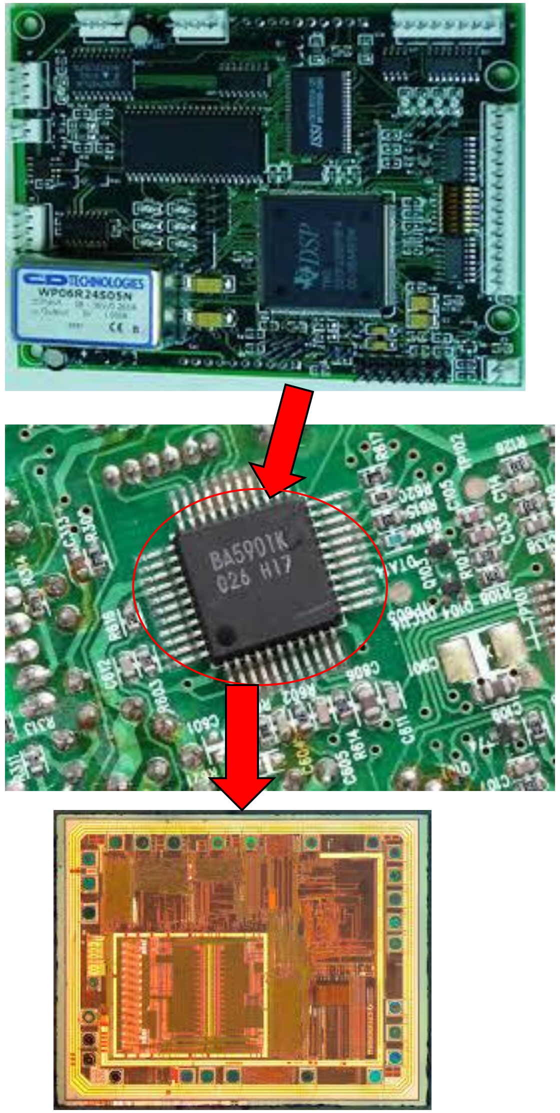
3408 hrs





In-Situ Monitoring: Scalability

- **Techniques discussed have a broad application space:**
  - Circuit Card Assembly (CCA) level: multiple components
  - Passive and active component level
  - Design IP level: specific embedded, on-die components
- **Techniques described are technology agnostic:**
  - More complex devices yield more emission data
  - Localization of component on CCA possible due to unique emission spectra occurring in different bandwidths for each device
  - Simple devices such as passives are more difficult, due to less emission data
- **Capable of detecting change in single transistors**
  - Degradation or change of state induced by software (bit change from zero to one)



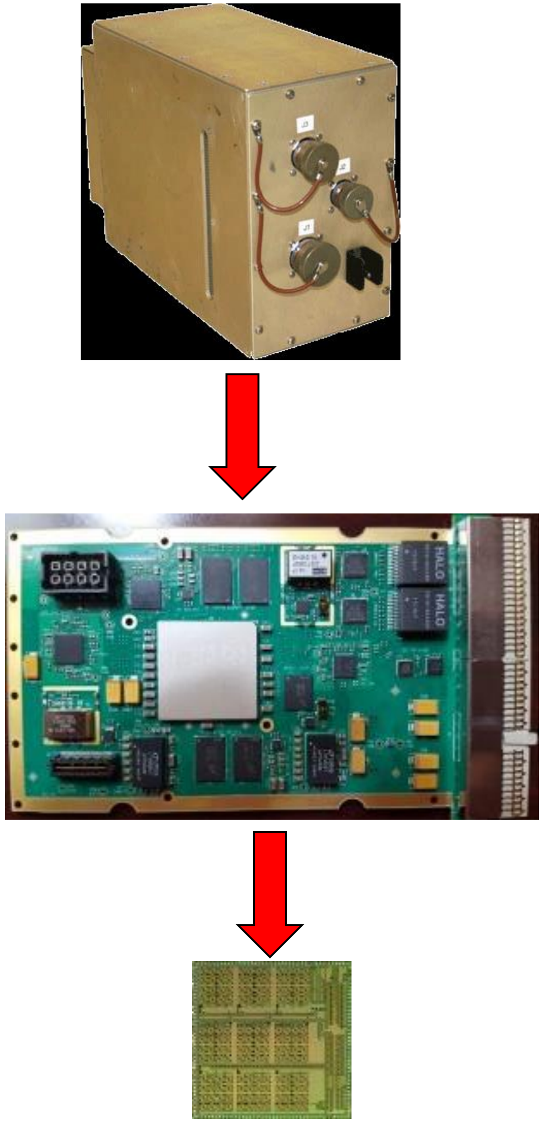
In-Situ Monitoring: Integration

- **In-situ monitoring possible due to miniaturization of multi channel, high acuity RF sensor**

- **Integration steps shown at right**
  - 5’’X9’’X14’’ 20 lb box (1st generation)
  - 3’’X9’’ Circuit Card Assembly (2nd generation)
  - 8mmX8mm Semiconductor die

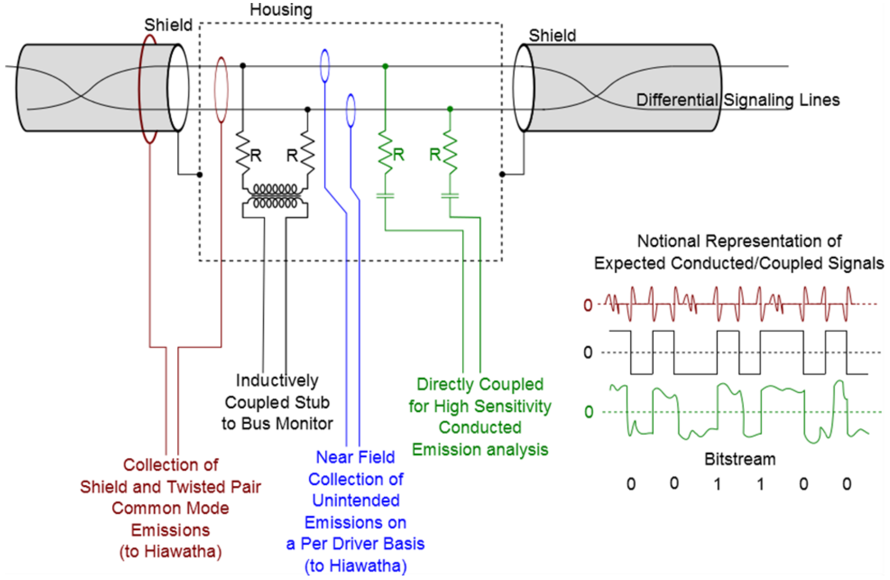
- **More capability added at each level of integration**

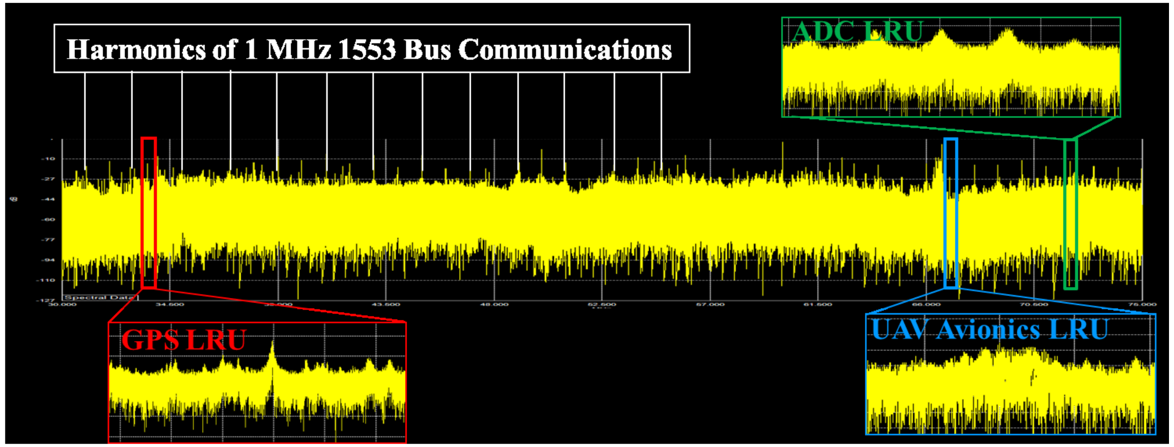
- **Sensor can be added to system at multiple levels:**
  - As a discrete component on CCA to monitor system “health”
  - As embedded IP on a semiconductor die, to monitor other embedded IP (e.g. the Flash Memory on a microcontroller chip



Additional Application: Cyber Threat Detection

- Monitoring capability can be extended beyond quantification of degradative effects
- Custom hardware built for high acuity acquisition of conducted RF emissions on data bus
- Successfully utilized to detect signature changes caused by the execution of cyber attacks on hardware connected to data bus





Slide content courtesy of Dr. Andrew Portune, Nokomis, Inc.

Conclusions

- **Traditional reliability estimations are imprecise and error-prone**
  - Arrhenius terms (E_A and n) are not well defined…can cause gross over estimation of component lifetime
  - The link between the equations and physically meaningful or measurable device parameters is weak.
  - May be acceptable for portions the commercial sector
  - Not acceptable for mission or safety-critical applications
  - Not easy to assess remaining component lifetime or actual state of degradation using these methods

- **EM Signature Analysis Methodology is Highly scalable and easily integrated**
  - Ideal for in-situ, real-time monitoring of passive and active electronics at a variety of levels (CCA, Individual component, on-die IP
  - Allow for more precise reliability/degradative state estimates, even when used with a few metrics
  - Monitoring can be extended to include real-time threat detection

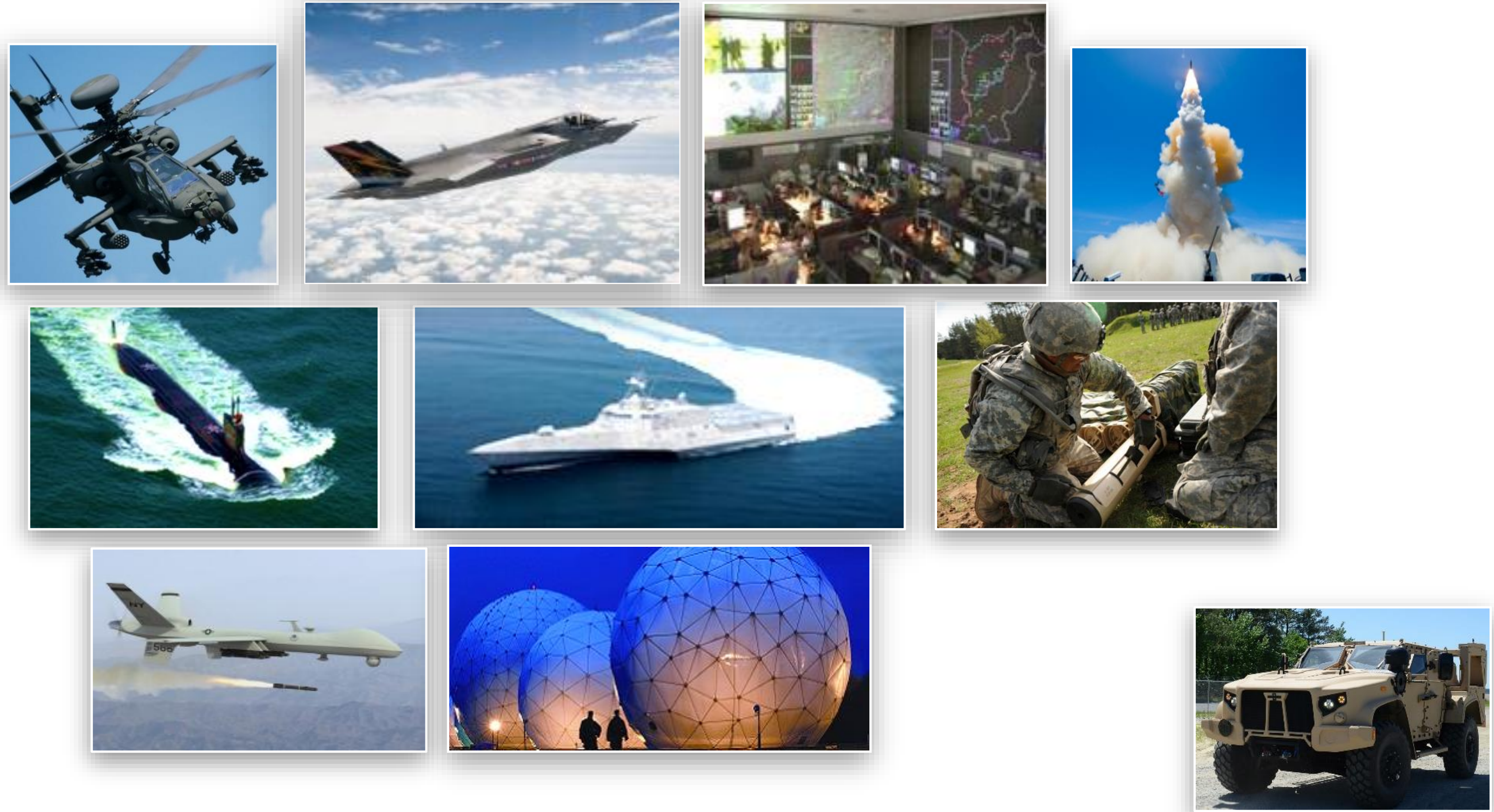
For Additional Information

Nick Martin, Ph.D.
Technical Lead, Warfighter Solutions Division
Defense Microelectronics Activity (DMEA)
Office of the Under Secretary of Defense
for Research and Engineering

(916) 231-1669 | nick.martin@dmea.osd.mil

DoD Research and Engineering Enterprise

Solving Problems Today – Designing Solutions for Tomorrow



DoD Research and Engineering Enterprise
https://www.CTO.mil/

Defense Innovation Marketplace
https://defenseinnovationmarketplace.dtic.mil

Twitter
@DoDCTO