Hardening the Internet of Things

Requirements for Commercial Technology Implementation

William Tonti *FIEEE*

Institute of Electronic and Electrical Engineers,

445Hoes Lane, Piscataway NJ 08854

w.r.tonti@ieee.org

Abstract:

The Internet of Things (IOT) is poised to revolutionize the computing platform placing a new computing engine at both physical and virtual edges. This is in stark contrast to a current centralized cloud or decentralized server platform. The robust end to end computing model used by cloud or server models has to be made available in IOT based edge computing. One must develop a trusted computing methodology for mission critical IOT (MCIOT). MCIOT decision making and hardening from a computing perspective are the subject of this paper.

MCIOT computing decisions affecting transactions are the area to be explored. MCIOT transactions are defined as an action that creates a response and offers a new decision matrix. This matrix is developed at the computing physical or virtual edges. An MCIOT transaction may be viewed as a simple linear expansion where $f(mciot) = m(mciot) + B$. The “output” $f(mciot)$ represents a transactional decision based on an MCIOT system, or edge result. Examples of MCIOT transactions are real time traffic, finance movement or triggers, HVAC changes, and object identification. These are a few of the infinite array of MCIOT decisions having real consequences, both virtually and physically. Decisions, or transactions made will affect the next computing cycle. These may result in negative consequences should the decisions be false, or compromised.

Voas in [1] describes an IOT system and a network of things (NOT) having the structure of sensors, aggregators, actors, and output channels. (SAAC) A mission critical decision surrounding MCIOT in a SAAC platform contains a fundamental set of requirements which when implemented will harden a SAAC composition. Fulfilling the requirements is a first step towards an Industrial IOT.

If one decomposes an MCIOT implementation into the SAAC piece-parts we may envision the following subsystem requirements which require specification:

Primitive Sensors: Their calibration, identity, use model and tracking require a specification and use model.

Aggregators: Built in Self Test (BIST) [2], new and existing primitive sensor validation are requirements and advanced specifications to continuously validate the MCIOT SAAC system.

Actors: High level control of the clusters that are self aware of their physical and virtual environments.

Channels: These are a trusted communication fabric that ties the MCIOT system together. This fabric has similar requirements as the primitive sensors.

In this treatments on an MCIOT SAAC system we assume the underlying technologies across the platform are silicon based or silicon like. Using the above assumption allows us to provide an MCIOT solution using many well know practices. The calibration identity and use models may be encoded by using the novel electronic embedded fuse (e-fuse). [3,4,5,6]. Figure 1 shows a typical silicon based e-fuse.

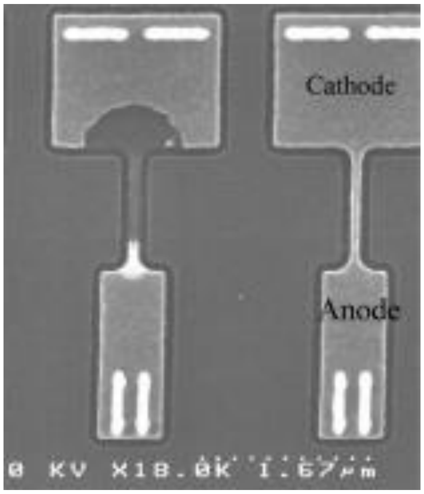

Figure 1: *Electronic Fuse (e-fuse) shown in the 90nm Silicon node. Programmed mode (left) and un-programmed mode (right). One time programming is accomplished through controlled high currents that create electromigration in the e-Fuse. This alters the e-fuse impedance from a low state to a high state when programmed.*

Programming is accomplished within a silicon die and can dynamically personalize its identity and or calibrate and validate SACC elements. e-fuse does not add additional costs in the manufacture of a die element. The e-fuse devices themselves are standard across many design systems and are represented as library elements having two distinct states alterable one time through on die programming. Programming may be implemented at any time including field or use programming.

US Patent 7,966,537 [7] teaches autonomic computing through the use of a novel method where real time field condition environmental parameters (e.g. time, temperature, voltage, duty cycle) are coordinated with a known reliability model that can trigger a pre wear-out condition and subsequent action to repair. Tracking and repair of a die subsystem is made possible using e-fuse or a comparable technology. This is an important feature for SAAC elements to consider in their design. The capability to self-diagnose, repair, or enable dynamic system calibration is made possible.. e-fuse becomes an integral enabler of autonomic computing in an MCIOT SAAC system. Figure 2 shows a block diagram system level overview. In this implementation a die, or in our case a SAAC element is repaired based on a predetermined use model that is tracked by a cycle timer, and recorded in a memory element. When the timer reaches a pre-determined state a repair processor is requested to replace a sub element in the die. This continues until the sub elements are exhausted.

BIST [2] is an internal die self test system. When deployed it diagnoses and validates SAAC components real-time, typically by executing a mission critical test and comparing against an expected result. BIST engines by design execute at clock speed and have no additional latency or external stimulus that may compromise the result. BIST engines remain in a quiescent state when not used, and as such they are "trustworthy". A SAAC component self awareness results by combining the results of BIST and autonomic repair [7]. BIST provides real time measurements, and autonomic repair allows decisions on functionality to be made based on modelled expectations such as those taught in [8]. These modelled expectations are the translations of physically measured die wearout (e.g. oxide, wiring, ionics, transport) into an empirical use model. The overall SAAC system reliability must be considered when deploying a distributed and decentralized MCIOT system. Figure 3 depicts the overall system reliability measurements using an industry standard model in [8] to predict failures. In figure 3 a system level accelerated burn in model is used to improve a systems lifetime compared to components that are not pre accelerated to uncover early lifetime failures. Using the "Burn-In" process is an excellent method to harden an MCIOT SAAC system.

It is a simple modification in Figure 2 to combine both BIST and autonomic predicted results. In this new implementation BIST and autonomic repair may be used to validate known good MCIOT over time, feeding the BIST and-or autonomic model results into the repair processor, and then post validating the repair using BIST for measurement and the creation of a new starting timestamp that will restart the subsystem.

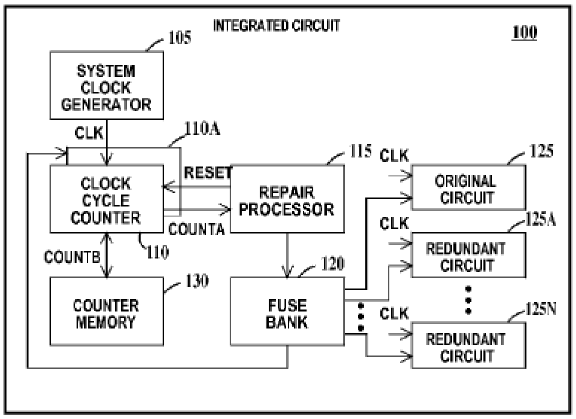

Figure 2: *USP7,966,537 Autonomic computing solution for use in an MCIOT implementation. In this example circuit repair is autonomically enabled based on a use model that tracks active cycles. e-Fuse technology is used to implement the repair by replacing internal elements at their end of life.*

Blockchain technology [9,10] in the MCIOT SAAC implementation in a NOT environment may be used to control the SAAC trusted network and cluster exchanges. The movement of $f(mciot)$ to the actuator or decision implementing environment is then through a trusted process. By it's very nature blockchain affords downstream network transaction validation which is one way to verify the NOT in an MCIOT SAAC system.

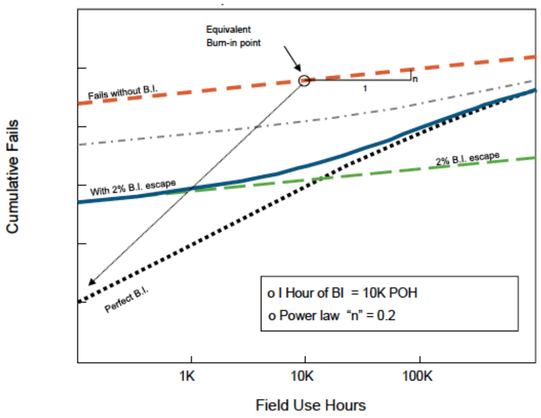

Figure 3: *Effect of System level failures over lifetime hours for various forms of Burn-In accelerated stress from 100% coverage to 0% component coverage. There is a noticeable increase in failures during a systems early life)less than 1000 use hours) for parts having no accelerated stress, or parts having an escape portion of stress. This of course is dependent on the defect density of the system prior to stress and must be measured or sampled to set the expectation.*

Conclusion:

Hardening MCIOT design and implementation may be accomplished through the use of existing technologies deployed in an NOT environment. The set of SAAC distributed elements, sensors, aggregators, actors, and output channels) coupled with on board BIST engines capable of autonomic calibration and repair have the potential to provide a robust and trusted $f(mciot)$ result.

References:

[1] J. Voas, “Network of Things” NIST Special Publication 800-183, pp 1-18 (2016).
[2] R.D.Adams, “An integrated memory self test and EDA solution”, IEEE International Workshop on Memory, Technology, Design and Testing, (2004)
[3] W. Tonti, “MOS Technology Drivers” IEEE Transactions on Device and materials Reliability”, V8, N2, pp406-415 (2010).
[4] W. Tonti, J. Fifield, J. Higgins, W. Guthrie, W. Berry, S. Narayan “Reliability and Design Qualification of a Sub-Micron Tungsten Silicide e-Fuse” 42’nd annual International Reliability Physics Symposium” pp161-165 (2004).
[5] C. Kothandaraman; S. K. Iyer; S. S. Iyer,” Electrically programmable fuse (eFuse) using electromigration in silicides”, IEEE Electron Device Letters, V23I9, pp523-525 (2002).
[6] Electrical fuse lets chips heal themselves, IEEE Spectrum, V41I10, pp16-20, (2004)
[7] A. Bonaccio, M. LeStrange, W. Tonti, S. Ventrone, “Digital reliability monitor having autonomic repair and notification capability”, US Patent 7,966,537, (2011)
[8] W. Tonti, B. Kareh “Chip Reliability” IRPS Tutorial Proceedings, (1997).
[9] S.Fujimura, H.Watanabe, A.Nakadaira, T.Yamada, A.Akutsu, “BRIGHT: A Concept for sa Decentralized Rights Management System Based on Blockchain”, IEEE ICCE-Berlin, pp345-346, (2015)
[10] X.Xu, C.Pautasso, L.Zhu, V. Gramoli, A. Ponomare, S.Chen, “The Blockchain as a Software Connector” IEEE/IFIP 13’th Working Conference on Software Architecture, pp182-191, (2016)

William R. Tonti

Dr. Tonti holds a BSEE from Northeastern University, an MSEE and a P.h.D from the University of Vermont, and an MBA from St. Michael’s College. He retired from IBM in 2009 after 30+ years of service, working as the lead semiconductor technologist for a large part of his career. Dr. Tonti holds in excess of 290 issued patents, and has been recognized as an IBM Master Inventor. He was honored by having his 250’th patent issue transcribed into the U.S. Congressional Record. Dr. Tonti is a Fellow of the IEEE a past IEEE Reliability Society President, a recipient of the IEEE Reliability Engineer of the Year award, and the IEEE 3’rd Millennium medal. Dr. Tonti joined IEEE in 2009 as the Director of IEEE Future Directions where he works alongside staff and volunteers to incubate new technologies within the IEEE.