Input to the Commission on Enhancing National Cybersecurity

Date:	September 8, 2016	
Joint submission made by:	**Brian Snow** Security and Ethics Specialist briansnow@comcast.net +1-301-854-3255 Formerly United States National Security Agency for 30+ years, designing secure products and systems, including 12 years as Technical Director	**Synaptic Laboratories Ltd.** www.synaptic-labs.com Designers of safe and secure computing and communication architectures. Developers of general-purpose soft IP for FPGA devices, to increase security and performance, and to reduce circuit area. **Benjamin Gittins, CTO** b.gittins@synaptic-labs.com +356 9944 9390
Topic of this submission:	**Security can and must be improved in and around programmable (FPGA) computing devices: a) A Base-line of Security Is Needed in Commercial FPGA Products and Systems, and b) Security Risk Assessments And Audits Must Be Expanded To Include Field Programmable (FPGA) Computing Devices That Are Very Widely Deployed In Commercial and Industrial Systems. Both Can Be Readily Achieved at Low Cost.**	
RFI topic areas this submission relates to:	• Cybersecurity Insurance • Cybersecurity Research and Development • Public Awareness and Education • Critical Infrastructure Cybersecurity • Federal Governance • State and Local Government Cybersecurity • Internet of Things	
Input submission contents:	(1) A 1 page executive summary for this comment, in the format requested by the RFI, which "identifies the topic addressed, the challenges, and the proposed solution, recommendation, and/or finding." We have inserted headings that match these points in the executive summary. (2) A supporting 16 page White Paper with approximately the same title as this RFI submission, on the same subject. That white paper was drafted by Synaptic Laboratories Ltd., with independent external technical support and document review provided by Brian Snow. This White Paper is supported and championed by Brian Snow as a sound approach offering a way ahead to increase SIGNIFICANTLY security in future products, at REASONABLE cost. (3) A supporting 5 page document titled: "A preliminary scoping of the (low cost) effort for auditors to prepare an introductory level of FPGA device security risk assessment" written by Synaptic Labs.	

Security can and must be improved in and around programmable (FPGA) computing devices: a) A Base-line of Security Is Needed in Commercial FPGA Products and Systems, and b) Security Risk Assessments And Audits Must Be Expanded To Include Field Programmable (FPGA) Computing Devices That Are Very Widely Deployed In Commercial and Industrial Systems. Both Can Be Readily Achieved at Low Cost.

1 Page Executive Summary

RFI Topics: Cybersecurity Insurance, Cybersecurity Research and Development, Public Awareness and Education, Critical Infrastructure Cybersecurity, Federal Governance, State and Local Government Cybersecurity, Internet of Things

The Challenges: Field programmable computing devices are already widely deployed at the heart of many systems across blue chip industries, and their industrial use is constantly expanding with a forecast compound annual growth rate of the market segment being estimated by Intel at 7% up until 2023. They are a natural vector for malicious hacking, including theft of valuable proprietary IP, customer data, monitoring of programs and activities, and re-programming for unauthorised purposes. This is because they are, by their very design, meant to be (re-)programmed and monitored **in the field**. Furthermore, FPGA devices **are routinely outside the scope of security risk audits**, making them a weak link in many companies security chains. These issues, combined with the increasing public awareness of the LOW COST attack vectors against FPGA devices and the increasing incidence and risks of insider attacks, means these devices are well positioned to become the **preferred path** to covertly enter and subvert, or take unauthorized control of, products or systems. A concerted effort must be made today to ensure that at least a base-line level of FPGA security is achieved for all FPGA devices deployed in all markets, in keeping with the accepted objective of ensuring an adequate level and chain of safety and security across all devices and inter-connected systems and processes that business, industry, government and society depend upon. This effort can be very low cost, with very broad benefits, for reasons detailed in the attached White Papers.

The Recommendation: We respectfully propose that the Commission's detailed recommendations to strengthen cybersecurity should include the following points (that are argued in greater detail in the White Papers attached to this submission):

1. Developers of all FPGA based products, in all market segments, can and must ensure their products employ a base-line of security (that is already readily available to them for free in the devices, or at very low cost to licence, and requiring low effort), to mitigate unauthorised reverse engineering, tampering, and malware injection of both (a) the configuration of the FPGA device itself; and (b) the software that is run by (soft or hard) processor core(s) operating within the FPGA. The contents of highly vulnerable flash memory should be protected using security controls. Secure authenticated communication of all wide-area communications of FPGA devices should also be maintained. Additional controls may be required based on a security risk analysis.
2. Similar to the controls used to demonstrate Year 2000 readiness, FPGA designers and companies that buy or use their products, need to be ready to show that their FPGA's are employing at least a base-line level of security. To do that, enterprises need to regularly audit all systems they are dependent on, to identify where FPGA devices are used, and to assess their safety and security capabilities and risks together. Staff education and FPGA monitoring strategies must be put in place to ensure security functionality is enabled and not disabled, along with plans to monitor and respond to evolving threats. Additional security controls should be implemented in devices whose critical functionality (or interconnectivity to more critical systems) is identified by the security risk audit to demand a higher level of assurance in that device. Risk auditors must be ready to explain how the high risk FPGA attack vectors are managed, including for the wider commercial and industrial systems that these devices are part of, and/or interact with.
3. Professional audit firms must begin to offer FPGA assessments in their safety and security risk assessments for customers. This is easily possible because of (a) the low number of device manufacturers, device families and known risk vectors, and (b) the fact that the known risks and the range of security controls available for FPGA devices are well documented. Therefore audit firms should begin to systematically develop the ability to perform security aware failure mode and effects analysis (FMEA) for all systems that use FPGA devices. Audit firms should also be able to perform Security Fault Analysis as required. FMEA analysis on FPGA devices should be routinely used during all company security risk audits, to identify the appropriate level of security for each FPGA device, including identifying when more advanced FPGA security controls and/or higher levels of security assurance are necessary. The reasons why it is 'low effort' for audit firms to implement this recommendation are also outlined in the two attached White Papers.

Sincerely,

Brian Snow and Benjamin Gittins (CTO, for Synaptic Laboratories Ltd.)

A Base-line of Security Is Needed in Commercial FPGA Products and Systems, and Security Risk Assessments And Audits Must Be Expanded To Include Field Programmable (FPGA) Computing Devices That Are Very Widely Deployed In Commercial and Industrial Systems. Both Can Be Readily Achieved at Low Cost

A WHITE PAPER

by

Synaptic Laboratories Ltd
www.synaptic-labs.com

Designers, in collaboration with Intel PSG, of soft IP solutions for FPGA devices:
General purpose IP *for enhanced security, software acceleration (system caches), superior on-chip communication (bus/interconnect), etc.*
Breakthrough architectures
for safety and mixed-criticality applications

and

Brian Snow

Security and Ethics Specialist
Formerly United States National Security Agency
for 30+ years, designing secure products and systems,
including 12 years as Technical Director

Monday, 5 September 2016 - Version 1.3a

This document was drafted by Synaptic Laboratories Ltd., with independent external technical support and document review provided by Brian Snow. No party or author was paid for contributing to this White Paper.

Table of contents

Abstract

Deloitte warns: *"Theft of IP is now placing the future of companies at risk" [10].* KPMG warns: *"Collectively, we sleepwalked into a position of vulnerability and failed to learn lessons of embedding security into products right out of the gate….The bottom line: Every company is now a cyber security company and every company needs to keep an eye on security." [21]*

Field programmable computing devices (FPGA's) are widely deployed in many blue chip industries. They are a natural vector for malicious hacking, including theft of valuable proprietary IP, customer data, monitoring of programs and activities, and re-programming for unauthorised purposes. This is because they are, by their very design, meant to be (re-)programmed and monitored in the field. Furthermore, FPGA devices are routinely outside the scope of security risk audits, making them a weak link in many companies security chains.

Attacks against FPGA devices can come from both trusted insiders and untrusted outsiders. KPMG reports that 65 percent of fraudsters are employed by the victim organization and a further 21 percent are former employees. In

particular, KMPG reports that "Weak internal controls are a contributor in 61% of cases." and that "[T]he biggest frauds over-ride or circumvent controls". Therefore risk audits against FPGA devices must also explicitly consider insiders working alone or together with outsiders [23].

All these issues, combined with the increasing public awareness of the LOW COST attack vectors against FPGA devices, means these devices are well positioned to become the preferred path to covertly enter and subvert, or take unauthorized control of, products or systems. FPGA designers must ensure their products employ a base-line of security. Security risk assessors must ensure that the security is present, enabled, and maintained during the deployed life of the product, and that it is not deliberately or inadvertently turned 'off' without an appropriate risk assessment and management approval.

FPGA manufacturers are aware of the broad security risks, and have steadily introduced some key security measures. It is important to be aware that inbuilt security features of modern FPGA devices must be explicitly ENABLED by the designers during production, and/or by the technical staff during deployment of a finished product. Furthermore, highly affordable commercial grade protection has also now become available for another major attack vector. This is to protect software (including the boot loader and application) running on a core in the FPGA that is accessing code and data stored on highly vulnerable flash. This type of flash protection needs to be employed by the designers.

FPGA designers, and companies that buy their products, need to be ready to show that their FPGA's are employing *at least* a base-line level of security. When challenged, when a hack or problem occurs, there can be no excuse for companies that have failed to include a base-line level of security in FPGA devices, when solutions are readily available at very low cost, including some that are made freely available in the device by the manufacturer. **Risk auditors** must be ready to explain how the high risk FPGA attack vectors are managed, including for the wider commercial and industrial systems that these devices are part of, and/or interact with. To assist commercial product designers and risk assessment auditors, in this presentation we explore key attack vectors that must be protected to provide a *base-line* level of security in commercial FPGA projects. We point to some examples of readily available security solutions that can be employed in FPGA devices today. We discuss the role of risk assessment auditors, and list some issues to consider when exploring the necessary introduction of FPGA security risk assessments.

Author Biographies

Benjamin Gittins is the lead author of this White Paper. Based in Europe, he designs soft IP for FPGA devices, is a security architect, and is CTO of Synaptic Laboratories Ltd. He was the only expert from outside North America and not from a major defence company that was invited to participate at President Barack Obama's *'closed, by invitation only'* US National Cybersecurity Summit, and the only cyber security advisor invited to the *'closed, by invitation only'* NATO co-sponsored Dubrovnik Conference on Nuclear Safety and Security. In the past he has co-authored security publications with iconic industry figures, such as Prof. Martin Hellman and Brian Snow, and 6 of his proposals to the US National Cybersecurity Summit were accepted for publication in the Summit proceedings. As chief architect for Synaptic Laboratories Ltd., he designs general purpose soft IP solutions for FPGA devices: for security, software acceleration (system caches), superior on-chip communication (bus/interconnect), and in collaboration with Intel PSG is creating high performance breakthrough Safe and Secure Real-Time (SSRT) architectures for safety and mixed-criticality applications [22] (tinyurl.com/MCF-SSRT).
Synaptic Labs' Company website: www.synaptic-labs.com
Benjamin Gittins' contact details: b.gittins@synaptic-labs.com +356-9944-9390

Brian Snow is considered to be a 'grandfather' of the security industry. According to Prof. Richard Ford, Director of the Harris Institute, *"Brian Snow has done a tremendous amount of good in the world as an advocate for security"*. Brian has very unique and deep experience that spans almost the entire evolution of today's technological and security landscape. This includes more than 30 years distinguished service in the US National Security Agency (NSA). For more than 20 years he performed and directed R&D of cryptographic components and secure systems in the US NSA. He created and managed the US NSA's Secure Systems Design division. His career culminated with 12 years as Technical Director over the three major divisions of the NSA: Research Directorate, Information Assurance Directorate, and Directorate for Education and Training. He was a senior technical security advisor to US government agencies, organisations, and to corporations, both large and small. Brian was active in several of the most prominent security initiatives that created security standards and solutions that are employed globally today. He has many patents, awards, and honours attesting to his creativity. Many cryptographic systems serving the U.S. government and military use his algorithms. He has been inducted into the NSA's own Cryptomathematic Institute as a Distinguished Member. He was appointed an Advisory Board Member of the US National Cybersecurity Hall of Fame. *{This Board is comprised of iconic security leaders that have had a significant impact in the building of the cyber security community (globally).}* He was also appointed to the cross-agencies US National Academy of Sciences Committee that advised the White House on Future Research Goals and Directions for Foundational Science in Cybersecurity. *You can read more about Brian Snow and access some of his other publications on this* link. (http://tinyurl.com/z3wl5tv).
Brian Snow's contact details: briansnow@comcast.net +1-301-854-3255

Introduction

Field programmable computing devices are already widely deployed at the heart of many systems across blue chip industries, and their industrial use is constantly expanding with a forecast compound annual growth rate of the market segment being estimated by Intel at 7% up until 2023 [1]. Like general purpose computers, by their very design these devices are highly vulnerable to malicious attacks. Attacks against FPGA devices can compromise internal operations, expose personally identifiable information and can result in serious intellectual property breaches. However these devices usually fall outside the scope of most commercial and industrial ICT security risk assessment audits. This is a serious problem that today can and should be addressed at the corporate board and security practitioner levels.

In this White Paper, the authors provide guidance on how risk auditors can assist. They list some of the minimum base-line security requirements that a broader risk assessment process must address, and they identify practical solutions that are readily available, at low cost, that FPGA designers can employ to satisfy these base-line requirements in most FPGA products.

Naturally, higher criticality applications will require additional security measures as identified in an audit by safety and security experts.

Security is Essential for Safety

Products and systems have safety standards (such as IEC 61508 and IEC 60335) to provide assurances against primarily benign, passive and non-adaptive risks, such as manufacturer faults, human errors, or natural occurrences such as earthquakes and power outages. Security standards are increasingly being deployed because products must also operate in the adaptive, hostile environment of escalating security threats from human attackers.

Without adequate security, malicious attacks can compromise and undermine safety controls. Also, increased network interconnectivity means attackers can compromise lower-assurance devices and mount attacks against products and systems (in the production or supply chains) with higher levels of safety and security requirements.

This has led to the understanding that it is necessary to provide an appropriate and adequate level of both safety AND security for every interconnected and

interdependent device that we depend upon. Security risk assessments and audits are key tools to inform this strategy.

Programmable FPGA devices should be included in Security Risk Assessments

To protect against adaptive, insider and outsider human attackers, business and enterprise security risk analysis has evolved over time to include a range of inter-related and inter-connected domains, for example: application security; operating system security; network security, and physical building security. The next domain that must be included is programmable computing devices. This domain currently fall outside the scope of most audit processes.

Similar to desktop and server computers, these devices are very vulnerable to security risks because they are manufactured to be programmed and re-programmed 'in the field', wherever they are deployed. These programmable computer chips are called Field Programmable Gate Array (FPGA) devices [2]. This White Paper focuses on the unaddressed risks associated with this specific class of devices.

These risks fall within the responsibility of companies to manage. Thankfully FPGA chip manufacturers such as Altera (now part of Intel) have already started to provide inbuilt security [3], [4], [5], such as (a) cryptographic primitives embedded in the silicon to provision a range of hardware root of trust capabilities; (b) IP protection of the programmable hardware logic, and (c) means to control external access to the internal monitoring and diagnostic capabilities of the FPGA chip that could be used to attack the device. Furthermore there are commercially viable solutions readily available to counter other threats such as, but not limited to, (a) the unauthorised monitoring and tampering of external FPGA communications, (b) means to detect and respond to various fault injections attacks [6], [7] against the correct operation of the FPGA device and (c) means to protect against the unauthorised monitoring of unintended emanations [8] of the FPGA device to extract secrets. Therefore auditors can readily identify risk vectors and solutions, and companies can rapidly achieve the necessary initial base-line of security, without which they remain seriously exposed.

What are FPGA devices?

FPGA devices are electronic chips in products and systems that allow their digital (and analog) hardware circuitry to be reprogrammed with NEW or modified functionality, in the field [2]. Many FPGA devices also include

general purpose processor cores (e.g. 1 GHz ARM Cortex-A9 cores) that are capable of running software that can also be reprogrammed in the field.

Where can FPGA's be found?

FPGA devices are already found performing important, and even essential, functionality in a vast array of products and systems, including industrial control systems and communications, across the globe in many blue chip industries. Since their introduction in 1984, FPGAs have grown in capacity by more than a factor of 10 thousand and in performance by a factor of 100 [9]. Cost and energy per operation have both decreased by more than a factor of 1000 [9]. Their relative cost continues to decrease with improved manufacturing and higher levels of system-on-chip integration which combines high performance general purpose processor cores, dedicated communication peripherals and reprogrammable logic [1]. This has led to a significant and continued increase in the use of FPGA devices in a very wide range of application domains and markets. For example, Intel estimates [1] up to 30% of cloud service providers nodes will use FPGA by 2020 for a broad range of applications such as image identification, artificial intelligence (convolutional neural networks), security, big-data and encryption. Intel also estimates [1] a ~$11B incremental serviceable available market (SAM) by 2020 as integrated FPGAs become cost competitive with application specific integrated circuits (ASICs) and application specific standard products (ASSPs).

Intel recently declared [1] that FPGA devices are and will continue to grow as a major platform in their global business, and to strengthen this opportunity they purchased FPGA company Altera for more than US$16 Billion in 2015. Most industries will continue to increase their dependence upon these devices. With the growing use of FPGA's in industry, increasing amounts of intellectual property is contained within and flows across these devices. Attacks against FPGA devices can compromise internal operations, expose personally identifiable information and can result in serious intellectual property breaches. The hidden costs of an IP breach is explored in depth by Deloitte in their recent article [10].

Why are FPGAs vulnerable?

The very fact that they are DESIGNED to be monitored and re-programmed IN THE FIELD makes FPGA devices a natural target for attackers. Also, the configuration of the hardware circuitry and the software that run on these FPGA devices is often stored in external flash memory that is connected directly to that FPGA device. Unprotected code and data stored in external

flash memories are well known to be highly vulnerable to hacking [11], [12], [13], [14].

Given the wide range of known vulnerabilities of FPGA devices and the escalation of all types of security threats generally means it is critical for businesses / enterprises to have assurances about both the safety AND security of the hardware and software aspects of all commercially deployed FPGA devices. This is currently a black hole in most ICT security risk assessment audits.

FPGA attacks can come from inside and outside an organisation

Risk assessments are equally necessary for FPGA devices deployed in unsecured and in more secure environments. Most organisations will accept that FPGA's deployed outside secure premises are exposed to high levels of risk, and would agree that these should be managed in the usual manner, such as security risk assessments, audit and an appropriate level of risk management and monitoring. However, some organisations are not aware of their risks in relation to FPGA devices that are deployed within secured premises. Hacking, fraud and corruption go hand in hand. The problem of the high and increasing level of insider risks posed by trusted employees, working alone or in partnership with outsiders, is reported widely in the media. The problem is highlighted yet again in the 2016 KPMG White Paper titled: "Global profiles of the fraudster: Technology enables and weak controls fuel the fraud" [23]. In this analysis of their clients, KPMG reports that 65 percent of fraudsters are employed by the victim organization, and a further 21 percent are former employees. Among employees, 38 percent worked at the organization for more than six years. 42% of fraud over $1 million were perpetrated purely by internal fraudsters, **32% by internal and external parties working together**, and 25% purely by external fraudsters.

Many hacks are specifically related to frauding the organisation out of funds, or proprietary IP, or customer data. Some are specifically aimed at causing costs for the organisation e.g. from disgruntled ex-employees, and others are aimed at subverting systems for other unauthorised purposes.

KPMG identifies that "**Weak internal controls are a contributor in 61% of cases**." Furthermore "the biggest frauds over-ride or circumvent controls".

For all these reasons security risk assessments are necessary for FPGA devices deployed in unsecured and in more secure environments. Companies and risk

auditors must explicitly consider the risk of insiders working alone or colluding together with technically advanced outsiders.

Awareness of low-cost FPGA vulnerability is increasing, making attacks more likely

The vulnerability of FPGA devices is publicly known and reported online [15], advertising the fact that many types of attack against FPGA's are very low cost. Step by step hacking guides are in fact already freely available on the Internet. Therefore it is becoming increasingly impossible to plead ignorance of FPGA vulnerabilities and the risk of targeted attacks, or to continue without a basic level of FPGA device security that is based on an appropriate risk assessment and that is subject to periodic audit to confirm the required level of security is present and has been maintained.

More attacks against FPGA devices can be expected because:

(a) They are already present inside many critical and high value systems, from industrial control to stock exchanges, and their use is ever expanding;
(b) They are subject to low cost attacks; and
(c) FPGA security is often completely overlooked in security risk audits.

Attacks against FPGA devices are well positioned to become the preferred path to covertly enter and take unauthorized control of a product or system.

The role of external audit firms

At a minimum, auditors and corporate managers must begin to be seen to be assessing and embracing the minimum level of security that is required by FPGA devices.

Such an audit will first identify where FPGA devices are serving in a client's products and production systems, which models are being employed, and their security capabilities. This is a very low cost step that can be easily executed. An audit will also determine the required level of security that is appropriate in each case, will identify if and when additional hardware security controls should be deployed in higher criticality systems, and make recommendations for ongoing monitoring and enhancing security over time in the context of interconnected systems and other related key factors, such as system performance. That audit can be done in two iterations. In the first iteration, a very low cost audit will focus on addressing the obvious risks that can be identified and addressed rapidly at low cost. The second iteration will then

focus on identifying other risks that may be more subtle or potentially harder to address. As an example, the second iteration of an audit may identify that adding anti-tamper capabilities (such as sensors that monitor the internal health of the FPGA) along with their remote monitoring may significantly increase the safety and security of a higher criticality system. See [24] for an evaluation of the low cost for an audit firm to prepare for the first iteration of an FPGA audit.

Five elements to consider in exploring an FPGA risk assessment audit

1. It is often of concern to management that a security audit may identify weaknesses that are extremely difficult or very costly to manage, even at a basic level. This is typically not the case with FPGA devices in low to medium criticality systems, for two reasons:
   - Many modern FPGA's include some essential security features, and an audit will identify those and ensure that they are being employed;
   - FPGA's are designed to be reprogrammed after deployment. This is good news in as far as it implies that new security solutions can also be retro-fitted.

2. Management is aware that sometimes staff will be unaware of available security features, or may disable them through ignorance, error, or simply to make their own work easier. It is important to be aware that the inbuilt security features of modern FPGA devices must be explicitly ENABLED by the designers during production and/or by the technical staff during deployment of a finished product. Enabling and maintaining ENABLED status of these security features is typically not complex or costly.

   A broader security risk assessment and audit that includes FPGA risk assessment will determine what security functionality and controls are currently available in the company's deployed FPGA devices, that they are being correctly employed, that all relevant staff are aware of the security features, and that the security is not being switched off or by-passed without an appropriate level of risk assessment and management approval.

3. Management is aware that encryption is a basic fundamental requirement when data and code can be readily monitored, copied or modified. Today, encryption is often automatically provided by companies for all Internet communications, for example even to protect

a $1 online eCommerce transaction and to protect instant messaging.

However, encryption is not widely employed to protect the code and data in FPGA devices, even though these devices are at high risk because they are specifically designed to be monitored and reprogrammed in the field. Therefore, a minimum base-line level of FPGA security must include the use of encryption. For example, authenticated encryption should be used for all wide-area network communications to and from FPGA devices.

In addition, as stated in the "Why are FPGAs vulnerable?" section above, particular attention MUST be made to protect all the contents of the external flash memories connected to the majority of FPGA devices. This is due to the relative ease and high impact of low-costs attacks against external flash memory.

4. Management understands that adding security has a cost. In the case of FPGA devices, it is reasonable to expect that the cost may be shared with the supplier of the FPGA based product or system. This is because the device provider shares a vested interested in the continued correct operation of their product, and also in maintaining a customer's confidence and loyalty, as well as in protecting their valuable proprietary IP that is deployed in the device.

5. Concerning the cost of adding security, this is often very low cost with modern FPGA devices because certain security functionality is provided freely in the device by the manufacturer. Some devices, such as Intel's Altera MAX 10 range includes on-chip flash that is intrinsically faster and more secure than using off-chip flash. The security audit must establish that these mechanisms are being enabled and maintained correctly. Furthermore, Synaptic Laboratories inline AES hardware encryption solution for protecting software access to highly vulnerable off-chip flash can be employed with options that can INCREASE software performance WITHOUT increasing total circuit area overheads. In such cases the performance and circuit area costs of inline memory encryption have been entirely removed and replaced with advances over what was achievable previously.

The security measures outlined in this white paper assist to protect on all those levels, rewarding companies that adopt the available security controls, and can benefit from cost sharing when required.

A base-line level of FPGA security can be readily achieved today at low cost

Today, there is no excuse for any FPGA product in any market to be deployed without the following base-line level of security controls:

- Encrypting the bitstream used to program the hardware logic of the FPGA device – to protect against reverse engineering of the programmable logic;
- Securely configuring the FPGA to ensure only authorised encrypted bitstreams are loaded into the FPGA device – to protect against tampering and malware injection into the hardware.

NB: the above 2 critically important security functions are already freely available in many FPGA devices, such as the Altera devices from Intel. When present, these controls must be ENABLED in every FPGA deployed in the field. A very low cost audit can rapidly identify if these security features are present in a FPGA device and if they are enabled [24].

- Encrypting the executable code and data that is stored and accessed at run-time from highly vulnerable external flash memory – this code and data must be encrypted when at rest in the flash memory, and when in flight between the flash memory and the soft or hard core processors residing within the FPGA device.

  Encryption of this code and data can provide controls against unauthorised monitoring, reverse engineering, pirating and tampering, including modifications that can result in the device performing illicit tasks or in not performing authorised tasks.

  In addition to the risk to proprietary IP and to the safe and correct operation of the device, customer data may also be stored or processed in those memories. In such cases the stakeholders must be ready to demonstrate that they have in place at least a minimum of audited security, or risk government penalties and consumer loss of confidence.

  A very low cost audit can rapidly identify if security controls are in place to address these class of risks [24].

What organizations must do today

Enterprises need to undertake an audit of all systems they are dependent on, to identify where FPGA devices are used, and to assess their safety and security risks together. Then, immediate steps can be viably taken to ensure that a minimum base-line level of security is present for all FPGA devices. This audit can be done in two iterations, in which the first iteration focuses on the risks that are easy to identify and easy to remedy at very low cost [24].

This first iteration will at the very minimum achieve a stronger overall, systemic chain of security. Education and monitoring strategies can be put in place, along with plans to monitor and respond to evolving threats, and implement additional security controls in those devices whose critical functionality (or interconnectivity to more critical systems) demands a higher level of assurance in that device.

The goal, over time, is to ensure that the company achieves and continually maintains a broader base line level of security that will ensure a stronger overall chain of security, with higher security in those vectors that require it, to protect against the full spectrum of evolving attack vectors that are relevant to that specific enterprise and its stakeholders.

What audit firms should do today

Today, external audit firms must combine FPGA safety and security analysis [16] to ensure that (a) they have become aware of the known risks and (b) that they have an understanding of (or access to information on) the full range of security controls available for FPGA devices. In particular, external audit firms must prepare the ability to perform the first iteration of a safety and security audit that focusses on the risks that are easy to identify and easy to remedy at very low cost. This preparation can be done at very low cost [24]

They should begin to systematically develop the ability to perform security aware failure mode and effects analysis (FMEA) [17], [18] for all systems that use FPGA devices. This must include the ability for audit firms to assess the risk of network based attacks and physical attacks against the FPGA device, and through each device to interconnected systems. In very high criticality systems, a Security Fault Analysis [19], [20] should also be performed on the FPGA to determine the security properties of the device when a hardware fault is encountered.

FMEA analysis on FPGA devices should be routinely used during all customer audits, to identify the appropriate level of security for each FPGA device, including identifying when more advanced FPGA security controls and/or higher levels of security assurance are necessary to protect the operation of higher criticality systems.

A concerted effort must be made today to ensure that an adequate base-line level of FPGA security is achieved for all FPGA devices deployed in all markets, in keeping with the accepted objective of ensuring an adequate level and chain of safety and security across all devices, systems and processes that business and industry depend upon. The first steps to achieve this can be done at low cost [24].

Conclusion

In today's interconnected and interdependent world, our collective economic and physical security is dependent on achieving better security processes and control across all the devices, systems and processes we depend on. The number of systems employing FPGA devices continues to increase steadily [1] as does public awareness of FPGA vulnerabilities and their low cost attack vectors.

Today, it is possible to significantly increase the level of both safety and security assurances around the use of field programmable computing devices (FPGA) at very low cost. Commercial grade security solutions are readily available to protect modern FPGA devices, including key solutions that are either already provided in the device by the manufacturer, or that are readily obtainable at negligible cost. Many of these solutions do NOT slow down performance or consume a lot of circuit area in the programmable device. Given these facts, there is little reason why auditing and implementing security controls for FPGA devices shouldn't take place right now, in any market.

New security solutions continue to become available. Organizations that undertake this necessary work can be rewarded with practical real-world gains that are more than just 'added burden, better security'. For example, solutions such as the AES inline encryption for off-chip flash (from Synaptic Labs www.synaptic-labs.com) can be employed with options that can actually INCREASE system performance WITHOUT increasing total circuit area overheads (by replacing the use of inefficient technologies found in most off-chip flash projects). Identifying such positive developments are already part of an ICT auditor's mandate.

It will not be difficult for security risk assessors to begin to offer FPGA security risk assessments [24]. In our data hungry and dependent systems, and in our information rich world, risk assessment audit firms need to begin to make available to customers preliminary FPGA safety and security risk assessments as a minimum standard component of all ICT security audits. This will close a current gap in ICT security assessment, and result in improved security controls in these programmable computing devices that are at the heart of a multitude of products and systems, across many blue chip industries. This will begin to prepare organisations for future hardware related risk assessments. These will be especially necessary as the Internet of Things grows.

Improving security in these vulnerable FPGA devices will also contribute to improving the overall safety and security of the devices and systems they are connected to, ensuring a stronger overall chain of protection. The end result can only be a win/win for all stakeholders… and an investment in a safer and more secure future.

Contact

Benjamin Gittins
Chief Technical Officer
Synaptic Laboratories Ltd.
Website: www.synaptic-labs.com
Email: b.gittins@synaptic-labs.com
Mobile: +356-9944-9390

References

[1] Intel. Acquisition of Altera. Investor slideshow, Intel, June 2015.

[2] A. Moore. FPGA for Dummies. John Wile & Sons, Inc., 2014. https://www.altera.com/en_US/pdfs/literature/misc/FPGAs_For_Dummies_eBook.pdf

[3] Altera. Using the Design Security Features in Altera FPGAs. Application Note 556, Altera Corporation, 2016.

[4] Altera. Arria 10 SoC Secure Boot User Guide. Application Note 759, Altera Corporation, March 2016.

[5] T. Lu, R. Kenny, and S. Atsatt. Stratix 10 Secure Device Manager Provides Best-in-Class FPGA and SoC Security. White paper 01252-1.0, Altera Corporation, June 2015.

[6] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache. Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures. Proceedings of the IEEE, 100(11):3056–3076, Nov 2012.

[7] D. Karaklajić, J. M. Schmidt, and I. Verbauwhede. Hardware designer's guide to fault attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 21(12):2295–2306, Dec 2013.

[8] NSA. Tempest fundamentals. Standard NSA-82-89, NACSIM 5000, U.S. National Security Agency, Fort George G Meade, Maryland, USA, Feb. 1982. A redacted version is available online.

[9] S. M. Trimberger. Three Ages of FPGAs: A Retrospective on the First Thirty Years of FPGA Technology. Proceedings of the IEEE, 103(3):318–331, March 2015.

[10] J. Gelinne, J. D. Fancher, and E. Mossburg. The hidden costs of an IP breach: Cyber theft and the loss of intellectual property. Deloitte Review issue 19, July 2016.

[11] Jeong Wook (Matt) Oh. Reverse Engineering Flash Memory for Fun and Benefit. HP. Black Hat USA 2014.

[12] M. Gorobets, O. Bazhaniuk, A. Matrosov, A. Furtak, and Y. Bulygin. Attacking Hypervisors via Firmware and Hardware. Slideshow, Intel Security - Black Hat USA, 2015.

[13] Bunnie & xobs. The Exploration and Exploitation of an SD Memory Card. 30C3: 30th Chaos Communication Congress. December 2013.

[14] A. Greenberg. Why the security of USB is fundamentally broken. July, Wired Magazine, 2014.

[15] T. Wollinger, J. Guajardo, and C. Paar. Security on FPGAs: State-of-the-art Implementations and Attacks. ACM Trans. Embed. Comput. Syst., 3(3):534–574, Aug. 2004.

[16] A. Avižienis, J.-C. Laprie, and B. Randell. Dependability and its threats: A Taxonomy. In Topical Days: Fault Tolerance for Trustworthy and Dependable Information Infrastructures, IFIP World Computer Congress. Kluwer Academic Publishers., Aug. 2004.

[17] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security Application of Failure Mode and Effect Analysis (FMEA), pages 310–325. Springer International Publishing, Cham, 2014.

[18] A. J. Kornecki and M. Liu. Fault Tree Analysis for Safety/Security Verification in Aviation Software. In Electronics, number 2, pages 41–56, 2013.

[19] Unknown. Fault Simulation Requirements for Security Fault Analysis. US National Security Agency. DOCID: 3928948. A declassified version is available on the www.nsa.gov website. https://www.nsa.gov/news-features/declassified-documents/cryptologic-quarterly/assets/files/fault_simulation.pdf

[20] Lieutenant J.M. Coppens. Logical Fault Analysis of Fault Secure Systems Using VHDL. Thesis, Royal Military College of Canada, May 1997.

[21] KPMG. Cyber security a failure of imagination by CEOs. White paper. Publication number: 132969-G. KPMG International Cooperative, December 2015

[22] Mixed Criticality Forum. Safe and Secure Real-Time (SSRT) Project. Project website page. http://tinyurl.com/MCF-SSRT

[23] KPMG. Global profiles of the fraudster: Technology enables and weak controls fuel the fraud. Technical Report 133426-G, KPMG International, May 2016.

[24] Synaptic Laboratories. "A preliminary scoping of the (low cost) effort to prepare an introductory level of FPGA device security risk assessment", 23 August 2016.

A preliminary scoping of the (low cost) effort to prepare an introductory level of FPGA device security risk assessment

By Synaptic Laboratories Limited

Table of contents

1. Begin with an introductory level of FPGA risk assessment

The cost and effort required to prepare auditors to undertake introductory FPGA risk assessment audits is limited in scope and requires primarily information gathering and compilation from readily available FREE sources.

We recommend that risk auditors begin by offering an introductory level of field programmable gate array (FPGA) device security risk assessment to customers and clients. **This level of risk assessment has very limited costs (on all vectors) to the auditor and to the customer / client.**

The introductory level will also inform and orientate auditors, customers and clients to the wider need and process for hardware security risk assessments. This will be very helpful as we move increasingly towards an IoT world.

2. An introductory level of FPGA risk assessment delivers primarily information and increased awareness that contributes towards certain action that reduces current and future risks

Through the introductory audit process, informed and aware auditors and customers / clients will:

1. **compile a list of / know the brand and model number of the FPGA devices that run in their products and systems**
   (the audit process would collect data on that)

2. **identify the functions performed on those FPGA devices and the level of criticality of those functions**
   (the audit process would collect data on that)

3. **determine any relevant mandatory requirements related to the function performed by those FPGA devices**
   (e.g. protection of confidential customer data)

4. **evaluate the common attack vectors to their FPGA devices, to identify the level of risk those attacks pose to the programs and systems that run on, or rely on, their FPGA devices**
   (the number of attack vectors that can be managed directly by commercial enterprises is quite low and is easily encompassed within the scope of an introductory audit. Source material on relevant attack vectors and their level of difficulty to implement is readily available online and in publications. Military / defense and similar high assurance organisations are subject to high cost e.g. state sponsored attack vectors that are outside the scope of the proposed introductory audit. However, the press is constantly reporting on instances that show that organisations that could be expected to maintain very high levels of security fail to provide even low-levels of security. Therefore it would be reasonable to expect that even high assurance customers would be willing participate in introductory FPGA risk assessment audits.)

5. **increase awareness within the audited company that FPGA devices can be a very weak link, to attack other products and systems**
   (The concept of security chains, and the interconnectivity of devices and systems, and the importance of managing 'weak links', are all well understood issues today. One simple example of an interconnected 'weak link' would be an insecure FPGA device deployed in the field that acts as a sensor for a much wider system. Reprogramming the sensor / FPGA can impact the entire system and its safe operation)

6. **identify the (intrinsic and added) security capabilities currently present and ensure they are ENABLED in their FPGA devices**

7. **identify the range of other relevant security options that are currently available, and that can be implemented inside or alongside their FPGA devices, with estimates of associated costs to deploy and maintain in the**

short, medium and longer term.

This includes identification of related advances that can permit added security while simultaneously INCREASING software performance and REDUCING total circuit area in the product. Consequently, the FPGA risk assessment process can contribute to and add value to the wider ICT assessment process, where auditors are already mandated to identify performance improving and other technologies that can deliver a positive benefit to the customer.

8. **determine any extra security they can request to be implemented by their suppliers**
   (also to ensure they have ENABLED the readily available security - designers and suppliers are known to simply not install or activate security, even if it is freely available in the device)

9. **establish whether or not the customers staff are maintaining the security, or disabling it**
   (studies reveal that staff disable security functions in computing devices. Senior management may think their device/s have security but in fact it may not be operational - the absence of FPGA security risk assessments, spot audits and education, means disabled security usually goes undetected).

10. **Risk assessments will inform the customer about the educational needs and spot checking that may be necessary to ensure that the customer / clients own staff are not disabling the security**
    (studies have shown that disabling occurs out of ignorance and/or deliberately)

This introductory level of FPGA risk assessment contributes to reduce current and future risks.

It also prepares the customer for any further round of FPGA auditing and risk management that may be identified as necessary. It also prepares auditors and customers for future hardware risk assessment activities, especially as the Internet of Things progresses. (Intel reports that it plans to manufacture 50 billion IoT devices by 2020)

3. The cost and effort to prepare audit firms for an introductory level of FPGA security risk assessments can be easily defined and scoped

FPGA's are a well established product globally, used in most blue chip industries for more than 30 years. Information about the devices, and their security risks, and the available security solutions are all readily available online and in published material, especially from the main FPGA manufacturers.

Two large FPGA manufacturers (Intel and Xilinx) dominate ~90% of the entire world markets. They both offer a very limited number of FPGA device families. Those devices employ very similar security controls. The FPGA manufactures (and their partners) advertise commercially available security solutions for their FPGA devices. Both

companies have extensive websites and publications that provide information and guidance, plus teams of sales support and technical experts deployed globally. Auditors can tap this expertise online and in person, in their own home countries.

For these reasons **the cost and effort required to prepare auditors to undertake introductory FPGA risk assessment audits is limited in scope and requires primarily information gathering and compilation from readily available FREE sources.**

4. The cost and effort by the customer to perform for an introductory level of FPGA security risk assessments can be easily defined and scoped

Similarly, the effort required by the customer is limited in scope:

1. compiling a register of their FPGA devices, the functions allocated to those devices and levels of criticality of those functions

2. identifying any statutory obligation that might apply to those functions (e.g. protection of customer data)

3. identifying and obtaining written assurances from their suppliers that they are enabling all freely-available security controls within the FPGA devices used in the products provided by that supplier to the customer

4. identifying a list of the the security controls that are implemented in their devices, based on information sourced from their supplier or their own internal documentation/project requirements/specifications

5. checking to ensure that their staff, and their suppliers staff, are aware of the importance of that security, and that it is never disabled without appropriate risk assessment and management approval.

5. What items would assessors need to prepare for the customer as part of an introductory level of FPGA security risk assessment?

1. A short written guide to the common FPGA risk vectors.

2. A short list of the major FPGA device manufacturers and their device families *(This is very simple to compile as two manufacturers - Intel and Xilinx - dominate approx 90% of the entire world markets for these devices. Their device families are few in number and are all listed with extensive information online)*

3. The list of security options and solutions made available by the two (or three) top manufacturers, including basic information on how to check if the security has been installed and is being maintained correctly.

Those security solutions will fall into one of 3 groups:

a. hardware solutions that are built into the device/s at point of manufacture and that basically every product and system can use if the product designer activates them;

b. hardware solutions that can be implemented by product and system designers *(in to the programmable logic of the devices)* after manufacture; and

c. software solutions that can be run on processor cores implemented in the FPGA devices.
(There are only a very limited number of security solutions available to protect the actual FPGA devices. Therefore compiling a list is not a time consuming, large scale effort. The major manufacturers have product information readily available online and in publications, plus engineers and security experts available to assist)