Office for
Nuclear Regulation

Cyber security considerations in Field Programmable Gate Array based system design

Dr Andrew White

Principal Nuclear Safety Inspector,

Office for Nuclear Regulation, UK

Content

- Purpose and activities of the Office for Nuclear Regulation (ONR), and the UK approach to nuclear safety regulation - context

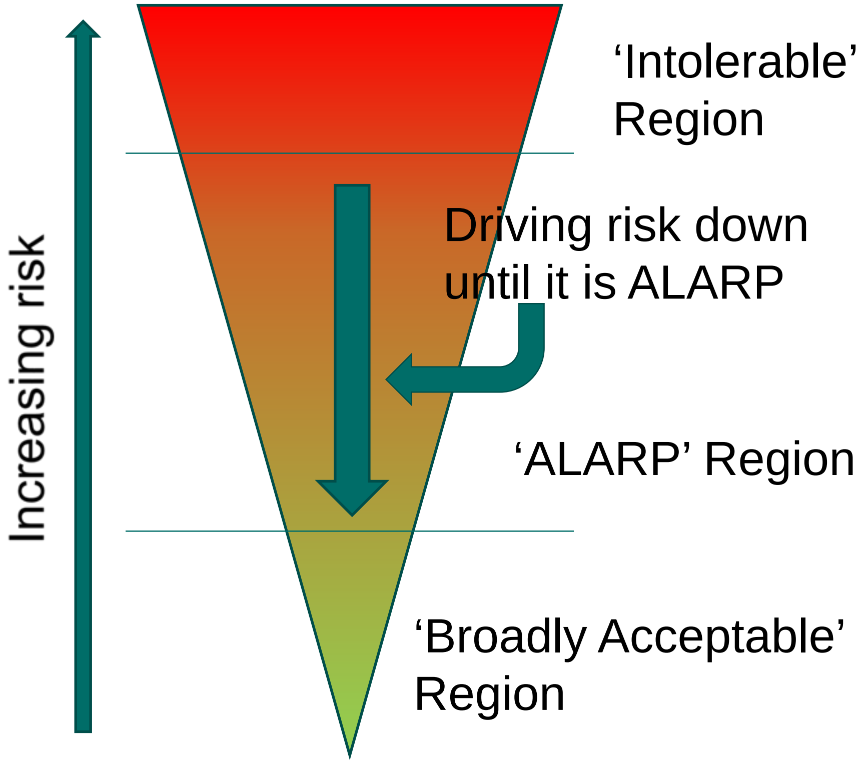
- The challenges in ensuring FPGA based systems are adequately secure against cyber threats

- Measures that contribute to managing the safety consequences of cyber security threats

The Office for Nuclear Regulation

- ONR regulates the nuclear industry on behalf of the public to ensure that the risks arising from activities in the nuclear industry remain adequately low.
- There is a legal requirement to reduce risk 'So Far As Is Reasonably Practicable (SFAIRP)'.
- In the UK nuclear industry, we use the term 'ALARP' to describe reducing risks to 'As Low As Reasonably Practicable'.
- SFAIRP and ALARP are used interchangeably

As Low As Reasonably Practicable


Increasing risk
'Intolerable' Region
Driving risk down until it is ALARP
'ALARP' Region
'Broadly Acceptable' Region

- If the 'cost' of a risk reduction measure is grossly disproportionate to the reduction in risk, the risk is considered 'ALARP'

- Practically this is not done through an explicit comparison of cost and benefits, but generally by applying established relevant good practice (RGP) and standards, and arguing this is adequate.

Nuclear regulation in the UK is goal setting

- Licensee’s have to demonstrate they have applied relevant good practice and that risks cannot be further reduced
- There are 36 license conditions that the licensees must adhere to
- Breach of a license condition will result in regulatory action
- The license conditions require that a safety case must be maintained and be a continuous demonstration that activities are being managed so they remain adequately safe

UK regulation – the safety case

- The safety case should argue why the risks associated with the activity are ALARP and is often of a Claims, Arguments, Evidence structure
- For this to be successfully argued the potential options for how the activity can be carried out should be described, so that the most appropriate can be selected, and it must be demonstrated that nothing further can be done to reduce risk
- Any modifications to systems or the environment will require the safety case to be updated
- ONR assesses safety cases and requires improvements to engineered systems where the licensee cannot demonstrate that risks are ALARP

What cyber threats do we face?

- Malware
  - Specifically designed to perform an unwanted function or to prevent a wanted function completing
- Hijack of legitimate functions
  - Use of legitimate functions to perform unwanted actions
- Denial of service
  - Prevention of an activity by rendering resources unusable or unavailable

But cyber threats change fast!

How to protect against current and future threats?

Potential safety consequences of cyber attack

- Information become inaccessible; theft/deletion/encryption
- Modification of information
- Display of misleading information
- Damage to plant equipment; e.g. reducing defence in depth
- Preventing operation – e.g. stopping electricity generation
- Causing release of radioactive material, or material in the wrong place

Need a security policy that describes risk appetite, to focus defences

Are cyber threats different to other security threats?

Where a cyber threat could affect safety, is this (just) another hazard?

Cyber threats are different to other hazards that could affect safety systems because:

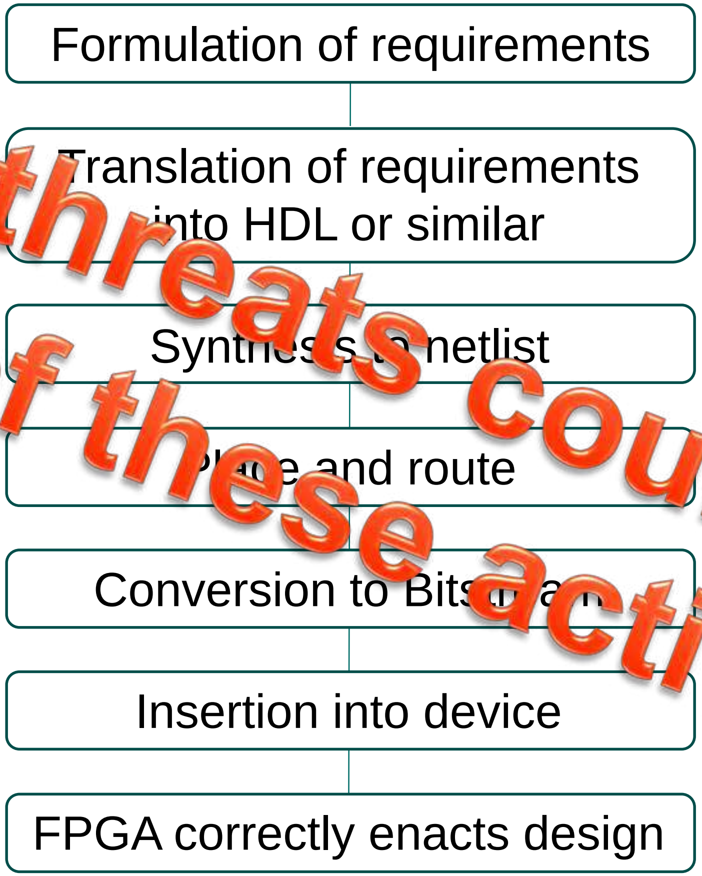
- They are controlled by an ‘intelligent actor’ that can target it to the most vulnerable/risky part(s) of the system
- They can be targeted to have an effect on multiple parts of the plant at the same time, regardless of physical separation
- They can be coordinated with physical attacks on diverse equipment
- They can be designed to lie dormant for many years

So, cyber threats should be treated explicitly

Where are the sources of the cyber challenges to FPGA design?

- People, deliberate or unintended
- Software and other engineering tools
- Pre-developed modules e.g. libraries/macros
- The design processes and quality control of other organisations e.g. device manufacturers
- Connectivity, including wireless and memory transfer

Where could cyber threats affect a FPGA design?



Formulation of requirements

Translation of requirements into HDL or similar

Synthesis to netlist

Place and route

Conversion to Bitstream

Insertion into device

FPGA correctly enacts design

Cyber threats could affect any of these activities

Software Tools for FPGA’s

- There is the potential for software tools to contain faults that could result in a safety consequence. This may be addressed by a number of different approaches:
  - Use of proven in use tools. This is vulnerable to version changes
  - Certification of tools. This is vulnerable to version changes
  - Use of diverse tools and cross compare. Noting some tools may have a common history
  - Assessment of the effects of a fault in a tool, and taking action to add an independent check, or mitigation
  - Use of formal methods to formally prove the correctness of the design at each stage

Use of libraries, macro’s, predeveloped designs

Improves productivity, but:

- Does the predeveloped design come from a trusted source?
- What verification has been performed on it?
- Could it contain malicious code?
- Can you verify it, fully?
- If the pre-developed was to contain malware, what effect could it have?

Bitstream

- Bitstream is generally encrypted – how is it possible to know the bitstream reflects the correct design?
- Has the design been correctly transmitted to the device?
- Are all gates correctly programmed?
- Is there any unwanted functionality?
- Can the design be read back from the device?

Use of complex functionality in the FPGA including

- Microprocessor cores
- Communication processors
- Memory management, and other complex functions

To what extent have these functions been verified and how?

How to manage the risks arising from cyber threats?

- In the UK the licensee will be expected to show how the cyber risks have been managed.
- …and demonstrate that the safety risks arising from safety threats have been reduced, so far as is reasonably practicable.

Standards compliance

- Standards lag behind technology developments e.g. use of open source software
- Security risks have traditionally been viewed separately to safety risks
- New cyber threats are emerging that may require different protection measures

Functional testing

- Even on small systems there are likely to be too many internal states (combinations of potential internal memory states) to achieve even 1% of coverage in a reasonable time
- For testing to be sufficient all potential internal states need to have been covered
- It is difficult to show by testing that an unwanted behaviour will not occur
- Malware may be designed to be triggered by an external event not covered by testing

Supply chain auditing

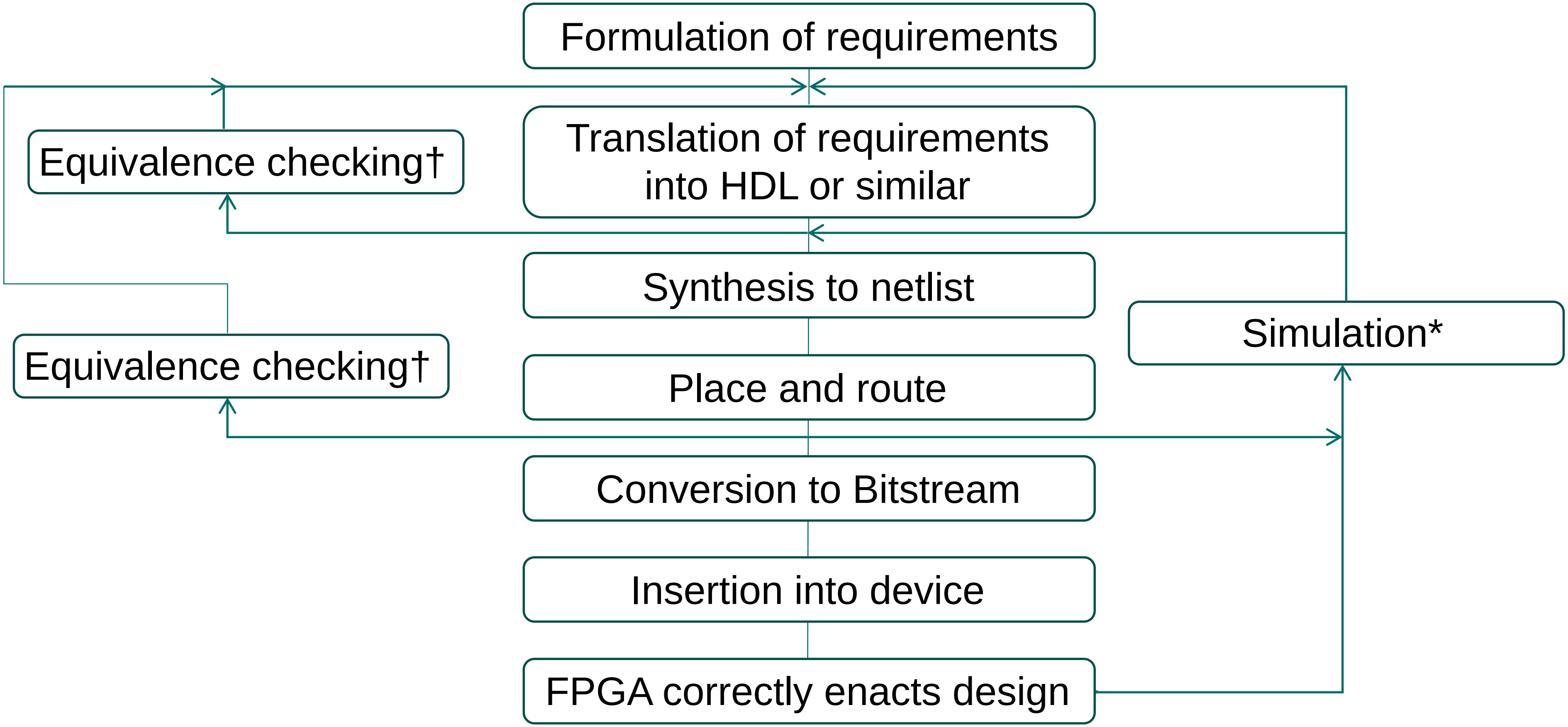
- FPGA design uses multiple software packages to complete the design and programming steps – most efficient use of effort?
- Software packages are likely to contain intellectual property that vendors wish to keep secret, so detection of malware is not easy or even possible
- New versions of software may be introduced at any time, containing unknown modifications and possible malware
- Some packages will be using legacy code that is not traceable or that is not resistant to cyber threats

Operational experience/proven in use

For operational experience to be relevant the device/component has to have been successfully used in a manner that supports the proposed use, including:

- Similar (identical?) use profile and resistance to cyber threat
- Configuration (e.g. software/firmware and hardware versions should be the same)
- Any failures have been identified and analysed
- Needs to be statistically significant (e.g. sufficient running hours, demands, etc.)
- Malware may be designed to be triggered by external event

Software analysis techniques



† = Potentially complete * = Likely incomplete

Conclusions

- Cyber threats present a hazard that can affect safety, even in FPGA based systems
- Cyber threats have some similarities and differences when compared with conventional hazards
- There are a number of activities that provide some evidence the risks arising from cyber threats have been managed:
  - Demonstration that design development standards have been complied with
  - Functional testing
  - Supply chain auditing
  - Operational experience

Conclusions

- There are some activities that can provide strong evidence that cyber threats can be managed:

  - Analysis of software
  - Formal methods to demonstrate correct functionality, and absence of incorrect functionality
  - Use of diverse tools and independent cross check
  - Use of diverse devices and architecture
  - Use of less vulnerable technologies
  - Replace complex devices that cannot be fully analysed with hardwired devices that can.

Office for
Nuclear Regulation

Questions?