Jurnal Pengembangan Energi Nuklir
Laman Jurnal: jurnal.batan.go.id/index.php/jpen

Kajian Implementasi *Field Programmable Gate Array* untuk Rencana Modernisasi Sistem Proteksi Reaktor

Restu Maerani*[1], Tulis Jojok Suryono[1], Sigit Santoso[1], Muhammad Subekti[1]
[1] Pusat Teknologi dan Keselamatan Reaktor Nuklir, BATAN, Kawasan Puspiptek Serpong Gd. 80 Tangerang Selatan 15310, Indonesia

INFORMASI ARTIKEL

Riwayat Artikel:
Diterima:
12 November 2020
Diterima dalam bentuk revisi:
13 Desember 2020
Disetujui:
18 Desember 2020

Kata kunci:
SPR
FPGA
Persyaratan
Verifikasi
Validasi

ABSTRAK

KAJIAN IMPLEMENTASI *FIELD PROGRAMMABLE GATE ARRAY* UNTUK RENCANA MODERNISASI SISTEM PROTEKSI REAKTOR . Penggunaan *Field Programmable Gate Array* (FPGA) pada reaktor nuklir sudah dilakukan sejak 2016, terutama diaplikasikan pada perangkat Sistem Instrumentasi dan Kendali (SIK). FPGA sebelumnya sudah diujikan pada rancangan Sistem Proteksi Reaktor (SPR) dan *Engineered Safety Feature – Component Control System* (ESF-CCS) reaktor daya tipe APR1400. Dengan adanya rencana peremajaan SIK reaktor serbaguna G.A. Siwabessy (RSG-GAS) pada bagian SPR, diharapkan sistem berbasis FPGA juga dapat diimplementasikan pada reaktor riset. Dengan pertimbangan nilai ekonomi, keamanan dan juga keandalannya, FPGA yang berbasis perangkat keras dinilai akan lebih aman dari serangan jaringan, lebih murah dari *Programmable Logic Controller* (PLC) yang berbasis perangkat lunak dan proses verifikasi dan validasinya yang lebih sederhana. Untuk menjamin berlangsungnya performa SPR RSG-GAS, proses digitalisasi perangkat kendali tidak dapat dihindari dan sebaiknya dilakukan. Penelitian ini membahas siklus perancangan berbasis FPGA yang diawali dengan mengkaji dokumen panduan terkait sistem yang penting untuk keselamatan terutama yang berbasis FPGA agar dapat mengacu kepada persyaratan, baik untuk perancangan perangkat keras maupun perangkat lunak, proses *reverse engineering* hingga proses validasi. Hasil dari penelitian ini bertujuan agar pada proses desain dalam upaya peremajaan SPR RSG-GAS dapat mengikuti metode yang telah disyaratkan terkait perancangan SIK berbasis FPGA untuk reaktor riset, sehingga dapat mempermudah proses perolehan ijin dari badan pengawas tenaga nuklir untuk dapat dilakukan penggantian desain SPR berbasis FPGA

ABSTRACT

STUDY ON THE IMPLEMENTATION OF FIELD PROGRAMMABLE GATE ARRAY FOR MODERNIZATION PLAN OF REACTOR PROTECTION SYSTEM. The use of Field Programmable Gate Array (FPGA) in nuclear reactors has been carried out since 2016, especially applied to Instrumentation and Control Systems (I&C System) devices. In previous research, FPGA has been tested on the design of the Reactor Protection System (RPS) and the Engineered Safety Feature - Component Control System (ESF-CCS) of power reactor type APR1400. With the plan to modernize the multipurpose reactor G.A. Siwabessy (RSG-GAS) in the RPS section, it is hoped that the FPGA-based system can also be implemented in research reactors. With considerations of economic value, safety and reliability, FPGAs as the hardware-based system are rated to be more secure from cyber-attacks, less expensive than Programmable Logic Controllers (PLCs) with software-based and the verification and validation processes are simpler. To ensure the continuity of the reactor control system performance which is important for safety, the process of digitizing control devices cannot be avoided and should be done. This study discusses the FPGA-based design cycle, which begins with reviewing guidance documents related to systems that are important for safety, especially those based on FPGA, so that they can refer to requirements, both for hardware and software design, the reverse engineering process to the validation process. The results of this study aim that the design process in an effort to modernize the RPS of RSG-GAS can follow the required methods related to the design of FPGA-based GIS for research reactors, so that it can simplify the process of obtaining permission from the nuclear power regulatory agency to replace the SPR-based design. FPGA.
Keywords: RPS, FPGA, Requirements, Verification, Validation

1. PENDAHULUAN

Desain Sistem Instrumentasi dan Kendali (SIK) pada reaktor nuklir saat ini sudah dapat menggunakan sistem berbasis perangkat keras, salah satunya adalah menggunakan *Field Programmable Gate Array (FPGA)*. Pada tahun 2016, *International Atomic Energy Agency (IAEA)* dalam dokumennya *Nuclear Energy Series* No. NP-T-3.17 memberikan panduan terkait aplikasi FPGA untuk reaktor nuklir [1]. FPGA umumnya diaplikasikan pada perangkat kendali, dalam hal ini SIK pada reaktor nuklir

*Penulis korespondensi.
E-mail: maerani@batan.go.id

untuk dapat menggantikan perangkat analog yang sudah usang [2]. Dari alasan inilah, untuk rencana peremajaan perangkat Sistem Proteksi Reaktor (SPR) Reaktor Serbaguna G.A Siwabesy (RSG-GAS) dikaji untuk dapat menggunakan FPGA sebagai salah satu opsi yang dapat diimplementasikan pada sistem tersebut.

Studi terkait implementasi FPGA pada reaktor nuklir sudah dilakukan sebelumnya pada desain SPR dan *Engineered Safety Features – Component Control System (ESF – CCS)* untuk reaktor daya tipe APR1400 [3, 4]. Tujuan diimplementasikannya FPGA pada reaktor APR1400 adalah dikarenakan SIK berbasis *Programmable Logic Controller (PLC)* yang sudah di implementasikan pada SIK sebelumnya dapat mengalami keusangan, dan kerentanan apabila mendapatkan serangan jaringan karena berbasis komputer, serta sistem berbasis perangkat lunak memiliki kerentanan *Common Cause Failure (CCF)* [3]. Alasan penggunaan FPGA juga dikarenakan pada pengujian di ESF – CCF berbasis perangkat keras (FPGA) terbukti lebih mudah dan dapat terpenuhi 100% *coverage* analisis fungsinya, mengingat pada desain perangkat lunak umumnya banyak terjadi kegagalan [4, 5]. FPGA juga dinyatakan mampu mengurangi kompleksitas sistem jika dibandingkan dengan sistem berbasis PLC, yaitu dengan perancangan berbasis perangkat keras untuk menggantikan elektronik analog pada hasil desain akhirnya [6].

FPGA juga diklaim lebih murah dari PLC, dari segi perangkat yang hanya berupa perangkat keras konvensional, dari segi pelaksanaan proses desain, verifikasi dan validasi yang lebih singkat sehingga dapat menekan biaya operasional pada pengujian perangkat lunak [7, 8]. Penggunaan FPGA pada reaktor riset sebelumnya digunakan untuk sistem pemantauan, dengan pertimbangan *response time* yang baik untuk *real time monitoring* [9].

RSG-GAS hingga saat ini sudah beroperasi lebih dari 30 tahun, dan tim manajemen penuaan reaktor beberapa tahun belakangan ini sudah melakukan tinjauan keselamatan secara periodik pada RSG-GAS. Aktivitas yang dilakukan dalam manajemen penuaan adalah dengan melakukan penilaian dan perawatan sesuai dengan persyaratan peraturan yang harus dilakukan sepanjang masa operasi suatu reaktor nuklir [10]. Beberapa aktivitas tersebut merupakan persyaratan dari dokumen IAEA *Safety of Research Reactor* No. SSR-3, yaitu; memperhitungkan pengalaman operasi, efek kumulatif dari penuaan, standar keselamatan yang berlaku, dan informasi keselamatan dari catatan selama beroperasi baik proses selama operasi dan perawatan [11].

Dalam aktivitas manajemen penuaan reaktor pada kelompok SIK, dalam dokumen IAEA No. SSR-3 tersebut dinyatakan bahwa fitur yang harus diperhatikan adalah *containment building* yang terkait dengan keselamatan dimana didalamnya terdapat kabel sumber daya dan juga kabel untuk sistem kendali agar tidak terjadi interaksi dengan struktur lain akibat adanya kejadian eksternal. SIK harus mampu memastikan tersedianya sistem kendali terkait keselamatan, contohnya apabila reaktor harus dipadamkan pada kondisi tertentu baik karena adanya kecelakaan maupun akibat dari kegagalan fungsi itu sendiri.

Meskipun SPR bukanlah kategori komponen yang dapat mengalami perubahan material, namun fisiknya dapat mengalami keusangan secara *non-physical* yang dapat mempengaruhi performa kinerja reaktor. Penggantian perangkat SPR yang mengalami keusangan merupakan salah satu aktivitas dalam upaya peremajaan reaktor riset, mengingat fungsinya sebagai sistem kendali untuk keselamatan reaktor sehingga perbaruan perangkat ini perlu dipertimbangkan [12]. Disinilah fungsi dari FPGA yang berbasis perangkat keras ini diharapkan dapat mencegah terjadinya CCF [13, 14].

Dalam proses modernisasi SPR RSG-GAS ini, proses *reverse engineering* atau rekayasa terbalik merupakan suatu pilihan yang dapat dilakukan untuk mempermudah proses verifikasi spesifikasi desain dari tipe reaktor ini. Dengan mengacu catatan dari Laporan Analisis Keselamatan (LAK) RSG-GAS, yang mana catatan selama operasi dan perawatan tercatat secara lengkap, diharapkan pelaksanaan pengembangan desain SPR berbasis FPGA ini memenuhi kriteria desain.

Mengingat FPGA yang akan diimplementasikan untuk SPR merupakan desain yang penting untuk keselamatan, maka desain SPR berbasis FPGA ini harus handal

menjalankan fungsinya dengan prediksi waktu dan konsistensi dengan waktu yang diinginkan, dan diharuskan melakukan verifikasi dan validasi di setiap levelnya berupa; *behavior simulation, logic simulation, physical simulation*, dan pengujian prototipe [15]. Pada kajian ini, akan diuraikan dan dijelaskan metodologi perancangan SPR berbasis FPGA, yang berfokus pada persyaratan sistem berbasis FPGA yang penting untuk keselamatan, dimana proses verifikasi dan validasinya memiliki persyaratan khusus bahwa implementasi FPGA pada SIK reaktor nuklir harus dapat melaporkan jika terjadi kondisi *abnormal* [15].

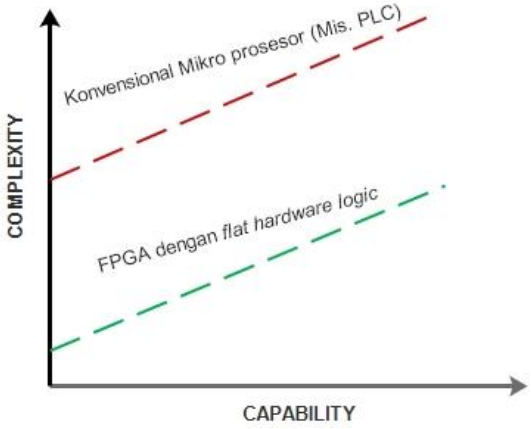
Jenis-jenis pengujian yang akan diterapkan pada desain SPR berbasis FPGA yang akan dijelaskan merupakan persyaratan minimum yang harus terpenuhi dikarenakan implementasi FPGA pada reaktor nuklir masih butuh pengembangan desain dan validasi desain yang terus berlanjut, terutama setelah dilakukan *reliability analysis* harus dilanjutkan dengan *robustness test* [16, 17].

Dengan dilakukannya kajian ini, diharapkan hasil rancangan desain SPR berbasis FPGA dapat di implementasikan pada RSG-GAS dan memenuhi persyaratan desain untuk diajukan ke BAPETEN dengan hasil validasi yang lengkap.

2. TEORI

2.1. Field Programmable Gate Array

Untuk perancangan FPGA ini yang mana terkait dengan sistem penting untuk keselamatan, IAEA merekomendasikan beberapa standar sebagai acuan dalam pengembangan desain sistem berbasis FPGA, yaitu IEC 62566, EPRI TR-1019181 dan NUREG/CR-7006 [1]. Dalam dokumen EPRI TR-1019181 seperti yang tertera pada Gambar 1, diterangkan bahwa perancangan SIK berbasis PLC memiliki tingkat kompleksitas yang lebih tinggi dibandingkan dengan penggunaan FPGA yang berbasis perangkat keras. Meskipun desain berbasis FPGA dengan kompleksitas yang lebih sederhana, namun kemampuannya dapat disetarakan dengan sistem berbasis mikro-prosesor, contohnya PLC.

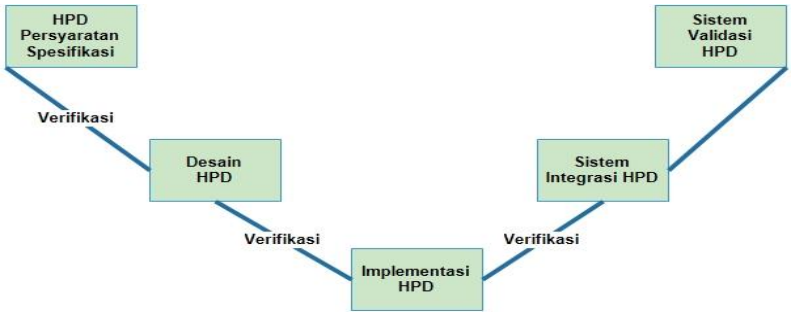


Gambar 1. Perbandingan Kompleksitas Perancangan Sistem berbasis FPGA dan PLC [6, 18].

Berikut hal-hal yang dapat dipertimbangkan terkait pemilihan FPGA sebagai platform untuk SPR RSG GAS: [19]

- Mengurangi kompleksitas perangkat keras karena pengurangan pada jumlah perangkat elektronik yang digunakan.
- Pengurangan kompleksitas logika karena tidak menggunakan sistem operasi seperti berbasis mikro-prosesor.
- Pengurangan kompleksitas dapat dikurangi lagi untuk proses lanjutan dikarenakan dapat dilakukan pemisahan fungsi primer pada SIK dengan sistem yang tidak perlu berinteraksi secara langsung [20].
- Memungkinkan pemakaian jangka panjang, sebab jika dibutuhkan penambahan perangkat yang baru dapat di implementasikan secara *portable*.
- -Pengenalan yang mudah dari keragaman desain SIK.
- Lebih aman untuk melakukan proteksi dari sistem antar muka jika terdapat input yang tidak normal ataupun interaksi yang merugikan.

Meski FPGA berbasis perangkat keras, namun dikarenakan menggunakan bahasa *Hardware Description Language* (HPD), maka perancangannya juga harus mengikuti persyaratan desain perangkat lunak. V-model seperti Gambar 2 pada umumnya digunakan untuk perancangan sistem berbasis perangkat lunak seperti yang direkomendasikan IAEA No. SSG-39 untuk perancangan desain SIK yang mana didalamnya ada perancangan perangkat lunak dan perangkat keras [21]. Namun untuk perancangan sistem berbasis FPGA, siklus hidup perancangan *HDL Programmed Device*



Gambar 2. Siklus hidup pengembangan desain HPD [22].

(HPD) yang ditunjukkan pada V-model Gambar 2 menjelaskan bahwa pada fase tersebut dapat dilakukan secara otomatis dan berulang oleh *tools.* Tujuan dari fase ini adalah untuk menyatakan secara sistematis dan tepat semua persyaratan yang berlaku untuk rangkaian FPGA [22].

BAPETEN sebagai Badan Pengawas Tenaga Nuklir di Indonesia sudah memberikan panduannya dalam perka BAPETEN terkait batasan operasi reaktor non-daya dan keselamatan operasi reaktor non-daya terdapat fungsi-fungsi SIK yang harus menjadi perhatian terutama terkait fungsi SPR yang memantau parameter reaktivitas, sistem proteksi dan sistem pemadaman reaktor [23, 24]. Dengan adanya ketetapan dari BAPETEN tersebut, maka untuk menghindari terjadinya kejadian yang melebihi batasan operasi perlu dijadikan acuan dalam desain SPR berbasis FPGA.

BAPETEN dalam menetapkan kriteria terkait perancangan SIK dengan adanya acuan dari dokumen IAEA, ataupun referensi dari regulasi badan tenaga nuklir internasional lainnya yang dapat diadopsi. Salah satunya adalah *United Stated Nuclear Regulatory Commission (US NRC)* yang memiliki banyak dokumen terkait kriteria desain yang sesuai dengan tipe reaktor yang berbeda beda. US NRC mensyaratkan bahwa perlindungan reaktor dan sistem keselamatan dapat mengacu pada IEEE Standards 603-1991 [25].

2.2. Sistem Proteksi Reaktor

SPR adalah seperangkat komponen yang dirancang untuk dapat memantau parameter operasi reaktor (misalnya daya dan periode neutron, laju aliran pendingin reaktor, *inlet* dan *outlet* temperatur, serta penurun tekanan pada teras reaktor). Tindakan otomatis dimulai atas dasar bahwa pengaturan logika untuk inisiasi tindakan perlindungan sesuai dengan kriteria kegagalan tunggal. Aksi dari SPR ini menghasilkan pemadaman reaktor [26].

Secara umum, SPR untuk reaktor riset harus memiliki kriteria seperti berikut ini: [26].

- Rancangan SPR harus mencakup ketentuan untuk membawa reaktor ke dalam kondisi yang aman dan memeliharanya dalam kondisi yang aman, bahkan jika SPR mengalami CCF yang kredibel (mis. kegagalan perangkat keras karena faktor manusia).
- SPR harus memiliki persyaratan umum untuk memadamkan reaktor.
- Tindakan perlindungan yang sesuai harus dimulai secara otomatis untuk serangkaian penuh peristiwa yang diprakarsai untuk menghentikan reaktor dengan aman
- Perlunya dipertimbangkan penambahan SPR yang fungsinya sama dengan SPR utama, namun SPR kedua ini harus berdiri sendiri secara independen.
- Jika SPR akan di desain dengan berbasis komputer, maka perangkat keras dan perangkat lunak yang digunakan harus berkulitas baik, dan harus dipraktikkan dengan baik dan keseluruhan siklus hidup perancangan harus didokumentasikan secara sistematis dan direview, kemudian harus dilakukan verifikasi dan validasi secara independen.

Apabila keandalan sistem berbasis komputer tidak dapat ditunjukkan dengan dengan tingkat kepercayaan yang tinggi, maka harus dibuktikan dengan pengujian yang lain, yaitu secara internal SPR harus memenuhi kriteria desain dasar secara independent.

3. METODE

Sebelum dilakukannya proses desain SPR berbasis FPGA, terlebih dahulu harus dipelajari

terkait kondisi sistem sebelumnya, sehingga pada saat proses desain dapat ditentukan apakah perlunya ditambahkan fungsi tertentu yang dapat meningkatkan performa dan keselamatan reaktor, atau justru disederhanakan untuk menghindari kompleksitas perangkat keras ataupun perangkat lunak. Hal ini perlu kembali mengacu pada persyaratan SPR pada reaktor riset, dan juga ditambahkan dengan mereview persyaratan implementasi FPGA untuk SIK reaktor yang terkait dengan sistem yang penting untuk keselamatan.

Tabel 1. Proses penting terkait modernisasi SPR berbasis FPGA [28, 29]

No.	Rencana
1.	Analisis persyaratan SPR berbasis FPGA untuk reaktor riset.
2.	Proses rekayasa terbalik untuk SPR dari RSG-GAS.
3.	Implementasi desain berbasis FPGA
4.	Menyusun metode verifikasi dan validasi desain.

Gambar 3 merupakan gabungan siklus hidup rekomendasi IEC 62566 terkait perancangan sistem yang penting untuk keselamatan berfokus pada perancangan HDL program, dan juga NUREG/ CR-7006 dari US. NRC yang berfokus panduan untuk mendapatkan lisensi dari sistem yang didesain berbasis FPGA [15, 18, 27].

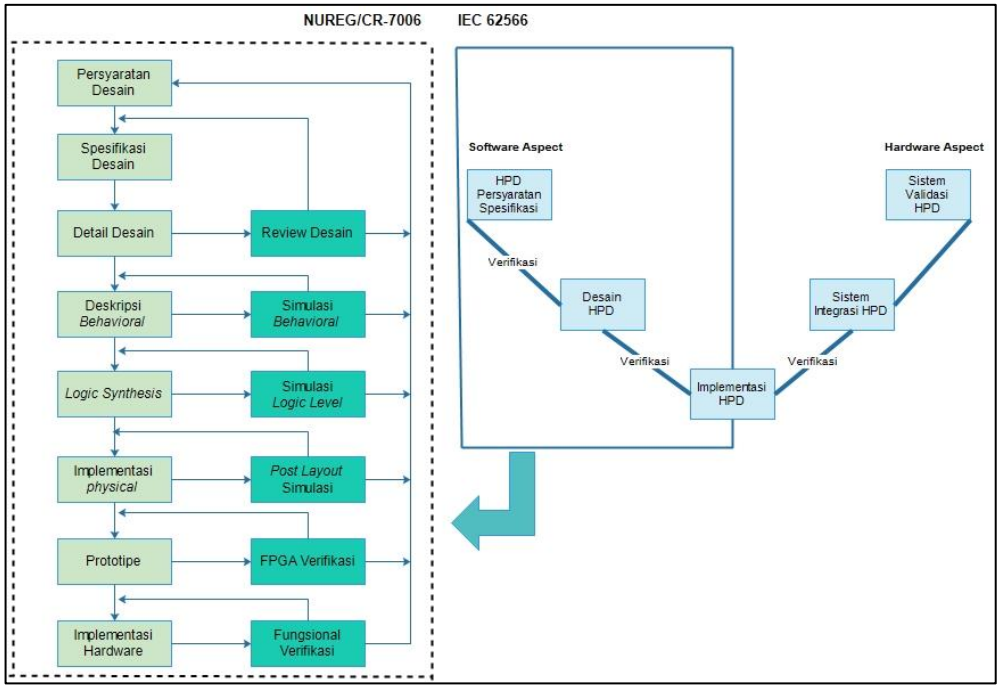
Dari Gambar 3 tersebut, maka pada bahasan penulisan ini di fokuskan pada proses penting yang perlu diperhatikan dalam upaya moderninsasi SPR berbasis FPGA, seperti bahasan yang dirangkum dalam Tabel 1.

4. HASIL DAN PEMBAHASAN

4.1. Analisis Persyaratan

Analisis persyaratan ini dilakukan agar pada saat tinjauan regulasi atau proses perijinan dapat memenuhi kriteria persyaratan desain, terutama karena desain dan konstruksi termasuk dalam salah satu proses yang harus mendapatkan lisensi [30]. Dalam pembahasan ini akan ditampilkan persyaratan apa saja yang harus diperhatikan guna memenuhi kriteria persyaratan dari badan pengawas tenaga nuklir terkait implementasi FPGA pada SPR RSG-GAS.

Beberapa persyaratan terkait SPR berbasis FPGA disusun pada Tabel 2 dan Tabel 3. Tabel 2 merupakan persyaratan umum SPR untuk reaktor riset yang diacu dari Doc. IAEA No.SSR-3. Persyaratan yang diambil pada Tabel 1 tersebut diatas merupakan *shall statement* yang artinya adalah bahwa persyaratan tersebut mutlak harus terpenuhi dalam perancangan desain SPR untuk reaktor riset.



Gambar 3. Alur desain perancangan berbasis FPGA [27].

Tabel 2. Analisis Persyaratan terkait SPR Reaktor Riset Menurut Doc. IAEA No.SSR-3 [11]

	Ref	Deskripsi
Persyaratan umum SPR pada reaktor riset		
6.172	[11]	SPR harus independen dari sistem lain.
6.173	[11]	SPR harus dapat melakukan tindakan otomatis saat melakukan tindakan keselamatan.
6.174	[11]	SPR harus dirancang dengan urutan tindakan otomatis tanpa ada tindakan manual, tidak *self-resetting* dan diperlukan tindakan operator untuk kembali ke kondisi normal.
6.175	[11]	Kemungkinan terjadi *interlock* dan *trip* dari SPR yang mungkin mengakibatkan *bypass* dari fungsi keselamatan harus dievaluasi.
6.176	[11]	SPR didesain agar tidak terjadi kegagalan tunggal yang dapat mengakibatkan hilangnya aksi proteksi otomatis.
6.177	[11]	SPR harus di desain untuk keselamatan reaktor dan terhindar dari CCF.
6.178	[11]	SPR didesain agar dapat diuji fungsinya secara berkala.
6.179	[11]	SPR harus dapat mengendalikan proses sebelum mencapai batas aman.
6.172	[11]	SPR harus independen dari sistem lain.
6.173	[11]	SPR harus dapat melakukan tindakan otomatis saat melakukan tindakan keselamatan.

Selain memperhatikan persyaratan SPR serta perancangan SPR berbasis FPGA, persyaratan terkait perancangan perangkat lunak juga harus diperhatikan, sebab *tools* yang digunakan pada perancangan berbasis FPGA menggunakan bahasa pemograman *VHSIC Hardware Description Language* (VHDL) *code*, yang berfungsi untuk mengkoordinasikan dari beberapa perangkat keras untuk mengimplementasi fungsi dari SPR.

Tabel 3 merupakan persyaratan FPGA yang akan diimplementasikan pada sistem yang penting untuk keselamatan, dalam hal ini SPR merupakan komponen yang penting untuk keselamatan.

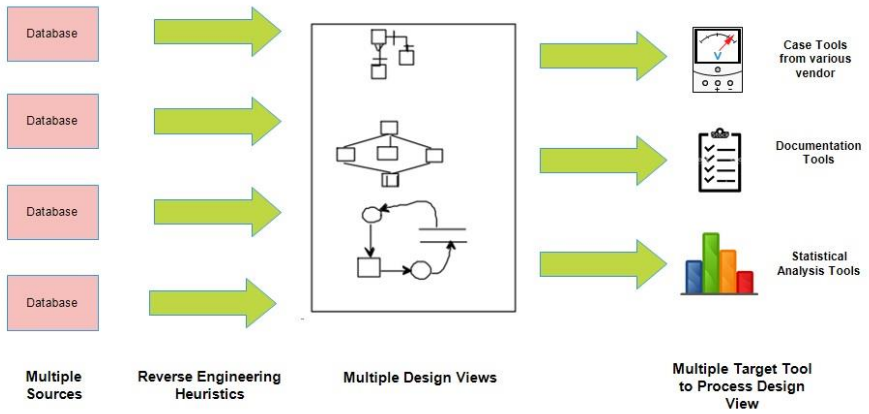
4.2. Rekayasa Terbalik

Rekayasa terbalik merupakan kebalikan daripada proses *forward engineering* dimana prosesnya dimulai dari mereview proses operasi dan perawatan dari operator. Catatan operasional SPR selama dalam proses operasi dan perawatan dapat diacu dari dokumen LAK RSG-GAS. Data tersebut berupa database catatan performa dari SPR RSG-GAS, dengan mempersiapkan *case tools*, *documentation tools* maupun *statistic analysis tools* yang akan dipergunakan, baru kemudian dapat dilakukan proses desain [31]. Gambar 4 merupakan elemen yang diperlukan pada proses rekayasa terbalik untuk keperluan desain SPR yang baru.

Perangkat rekayasa terbalik yang fleksibel memungkinkan seorang *programmer* untuk dapat menyaring dan mendengarkan abstraksi desain yang masih dapat dipergunakan. Dengan perangkat yang generik, memungkinkan perancang alat untuk menyesuaikan alat dengan persyaratan spesifik dari tugas rekayasa terbalik dengan lebih mudah. Perangkat rekayasa terbalik yang praktis harus fleksibel dan generik sehingga dapat berkembang di lingkungan yang masih beroperasi [31].

Tabel 3. Persyarataan Implementasi FPGA pada sistem penting untuk keselamatan (IEC 62566) [22]

	Ref	Deskripsi
HPD	[22]	Spesifikasi persyaratan harus menentukan persyaratan *fault detection* dan *fault tolerant.*
	[22]	Desain dan implementasi harus menggunakan HDL, alat untuk simulasi, sintesis, *place* dan *route*.
	[22]	Pada tahap desain harus menghasilkan formal deskripsi HPD
	[22]	Desain harus memiliki sinyal input yang menempatkan semua *output*, *state machines* dalam keadaan yang diketahui dan terdokumentasi.
	[22]	Setiap fungsi yang diimplementasikan pada HPD harus dapat diujikan.
	[22]	Jika menggunakan *self test*, kemampuan fungsinya harus terverifikasi.
	[22]	Hasil implementasi desain harus menampilkan informasi waktu.
	[22]	Kelengkapan dan kebenaran file parameter dan batasan harus diverifikasi oleh tim verifikasi
	[22]	*Static Timing Analisis* (STA) harus dilakukan.
	[22]	Proses verifikasi harus termasuk pengujian dan analisis.
	[7]	Untuk *test -bench* harus termasuk *test-case* pada semua fitur



Gambar 4. Elemen yang dipergunakan pada proses rekayasa terbalik [30].

Tabel. 4. Metode Verifikasi dan Validasi

Verifikasi	Ref	Validasi	Ref
Membuat *Verification Plan*	[4]	Membuat *Validation Plan*	[4]
Analisis fungsi	[22]	*Test cases*	[4]
*Static timing analysis*x	[7]	*Test bench*	[4]
Dokumentasi *acceptance* (sebelum dan sesudah modifikasi) .	[22]	*White box testing*	[4]
		Functional Black Box Testing	[33]
Formal equivalence checking tools.	[4]	*Statistical Testing*	[33]
Penggunaan HDL untuk simulasi, *synthesis*, *place* dan *route*.	[4]	*Timing Analysis*	[22, 33]
		Reliability Growh Model	[33]
		Periodic Functional Test	[33]
		Robustness Test	[1, 15, 18, 22]

4.3. Impelementasi Desain SPR RSG GAS Berbasis FPGA

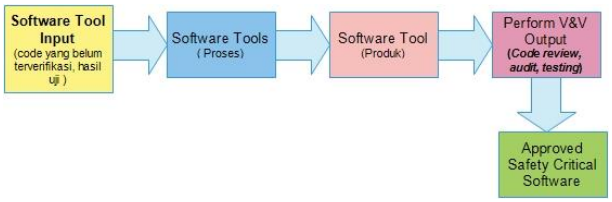
Pada proses implementasi SPR berbasis FPGA, diperlukan dekomposisi dari spesifikasi desain SPR dengan melakukan alokasi fungsi dari SPR berbasis analog menjadi SPR berbasis digital. Hal ini diperlukan untuk mengidentifikasi sub fungsi yang diperlukan untuk mencapai fungsi tersebut [32]. Alokasi ini diambil dari analisis fungsi SPR guna nantinya akan disintesis kedalam arsitektur RPS.

Alokasi persyaratan ke fungsi dari SPR harus mencakup sub fungsi berikut ini: [4]

- Sinyal proses input
- *Component Level Command Processing*
- *System Level Command Processing*
- *Component Command Control*
- *Indication and Alarm Processing*

4.4. Metode Verifikasi dan Validasi

Sesuai dengan penggunaan FPGA pada perancangan SPR ini, maka metode verifikasi dan validasi yang dapat digunakan dan juga mencakup kriteria minimum yang harus terpenuhi adalah dengan acuan dari beberapa rekomendasi, seperti pada Tabel 4. Untuk proses pengujian FPGA agar terbukti keandalannya, badan pengawas dapat meninjau secara independen meninjau nilai masukan dan keluaran dari *tools* untuk memastikan bahwa rancangan VHDL *code* pada rancangan tersebut dapat berfungsi dengan baik, meskipun masih banyak metode testing yang dapat dilakukan, misalnya menggunakan beberapa modeling untuk struktur *code* yang dibuat. Gambar 5 merupakan alur proses uji yang dapat dilakukan agar desain dapat diterima dan membuktikan memiliki kriteria sebagai *safety critical software.*



Gambar 5. V&V Proses untuk *aprroval tools* [1].

5. KESIMPULAN

Pada kajian rencana perancangan SPR berbasis FPGA untuk RSG-GAS ini, siklus hidup yang dilaksanakan sejak saat dilakukannya analisis persyaratan terkait spesifikasi desain pada umumnya serupa dengan persyaratan desain berbasis mikro-prosesor lainnya, yaitu menggunakan V-model yang biasa digunakan pada perancangan perangkat lunak. Hal ini dikarenakan FPGA juga menggunakan perangkat lunak sebagai *tools* untuk mengkonfigurasi parameter fungsi dari sinyal input. Analisis persyaratan yang harus terpenuhi terkait penggunaan FPGA untuk SPR pada reaktor riset meliputi; persyaratan SPR dan FPGA terkait sistem yang penting untuk keselamatan reaktor nuklir. Dari hasil analisis persyaratan ini, dengan ditambahkan adanya data dari rekayasa terbalik, metode pengujian yang mengacu pada rekomendasi verifikasi dan validasi yang ditetapkan, diharapkan dapat mempersiapkan hal-hal yang dibutuhkan untuk memulai perancangan desain agar produk yang dihasilkan sesuai dengan kriteria yang diinginkan, terutama memenuhi kriteria yang ditetapkan oleh badan pengawas tenaga nuklir terkait keselamatan reaktor non daya

UCAPAN TERIMA KASIH

Terima kasih kepada Ibu Ir. Endiah Puji Hastuti, M.T selaku ketua KAK Reaktor Riset - BATAN 2020 yang memberikan bimbingan atas terlaksananya penelitian ini. Penelitian ini didukung oleh DIPA Pusat Teknologi dan Keselamatan Reaktor Nuklir tahun anggaran 2020 Nomor : SP DIPA-080.01.1.450310/2019 tertanggal 14 November 2019.

DAFTAR ACUAN

[1] *IAEA Nuclear Energy Series No. NP-T-3.17, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants*. International Atomic Energy Agency, Vienna, 2016.

[2] Mcnelles P., Lu L. Review of the Current State of FPGA Systems in Nuclear Instrumentation and Control. in: *Proceedings of the 2013 21st International Conference on Nuclear Engineering ICONE21*. 2013. pp. 1–14.

[3] Ahmed I., Jung J., Heo G., "Design Verification Enhancement of Field Programmable Gate Array-Based Safety-Critical I&C System of Nuclear Power Plant," *Nucl. Eng. Des.*, 317:232–41, 2017.

[4] Maerani R., Mayaka J.K., Jung J.C., "Software Verification Process and Methodology for the Development of FPGA-based Engineered Safety Features System," *Nucl. Eng. Des.*, 330, 2018.

[5] Jung J., Chang H.-S., Kim H.-B., ""3+ 3 Process" for Safety Critical Software for I&C System in Nuclear Power Plants," *Nucl. Eng. Technol.* **41**(1):1–8, 2009.

[6] Mayaka J., Jung J.C., "Complexity reduction of the Engineered Safety Features Component Control System," *Nucl. Eng. Des.* 331(January):194–203, 2018.

[7] Habinc S.. 2002 *Lessons learned from FPGA Developments*. Gaisler Research, Sweden.

[8] Villalta I., Bidarte U., Gomez-Cornejo J., Lázaro J., Astarloa A., "Estimating the SEU failure rate of designs implemented in FPGAs in presence of MCUs," *Microelectron. Reliab.* 78:85–92, 2017.

[9] Chen S.Y., Chou H.P., "A FPGA based data acquisition system for research reactor operational monitoring", in *IEEE Nucl. Sci. Symp. Conf. Rec.*, 2013.

[10] Sunaryo G.R., Tarigan A., Wisnubroto D.S., "Recent Status RSG-GAS Ageing Management," in *INIS IAEA*. 2013.

[11] *IAEA Safety Standards: Specific Safety Requirements No. SSR-3 Safety of Research Reactors*. International Atomic Energy Agency, Vienna, 2016.

[12] *IAEA - TECDOC- 1625: Research Reactor Modernization and Refurbishment*. International Atomic Energy Agency, Vienna, 2009.

[13] Lu J.J., Hsu T.C., Chou H.P. "System assessment of an FPGA-based RPS for ABWR nuclear power plant," *Prog. Nucl. Energy*, **85**:44–55, 2015.

[14] Maerani R., Waskita A.A., Pradana S., Saharudin, Deswandri, Jung J.C., "Reliability Program Plan for Field Programmable Gate Array-based I&C System of Nuclear Power Plant," in *AIP Conference Proceedings*. 2019.

[15] Bobrek M., Bouldin D., D.E H., S.M K., S.F S., C W., et al.. 2009. *Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, NUREG/CR-7006.* U.S. Nuclear Regulatory Commission, Washington D.C.

[16] *IEEE Std 1633TM-2008, IEEE Recommended Practice on Software Reliability*. IEEE, *2009*.

[17] Wang X., Holbert K.E., Clark L.T., "Single event upset mitigation techniques for FPGAs utilized in nuclear power plant digital instrumentation and control," *Nucl. Eng. Des.* 241(8):3317–24, 2011..

[18] Flink B., Killian C. *EPRI TR-1019181: Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems*. Electric Power Research Institute. 2009.

[19] Fink R., Killian C., Nguyen T. *EPRI 1022983, Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems*. 2011.

[20] Jung J.-C., "Improved Design Architecture to Minimize Functional Complexity of Plant Protection System for Nuclear Power Plant," *Nucl. Eng. Des.* 2016.

[21] *IAEA Safety Standards, Specific Safety Guide No.SSG-39: Design of Instrumentation and Control*

Systems for Nuclear Power Plants. International Atomic Energy Agency, Vienna, 2016.

[22] *IEC 62566: Nuclear Power Plants – Instrumentation and Control Important to Safety – Development of HDL – Programmed Integrated Circuits for Systems Performing Category A functions*. International Standard IEC, 2012.

[23] BAPETEN, *Peraturan Kepala Badan Pengawas Tenaga Nuklir Nomor. 8 Tahun 2019 Tentang Keselamatan Operasi Reaktor Non Daya*. Badan Pengawas Tenaga Nuklir, Jakarta, 2019.

[24] BAPETEN, *Peraturan Kepala Badan Pengawas Tenaga Nuklir Nomor 9 Tahun 2013 Tentang Batasan dan Kondisi Operasi Reaktor Non Daya*. Badan Pengawas Tenaga Nuklir, Jakarta, 2013.

[25] US Nuclear Regulatory Commission, *Regulatory Guide 1.168, Rev 2, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*. US NRC, 2013.

[26] *IAEA Specific Safety Guide No. SSG-37, Instrumentation and Control and Software Important to Safety for Research Reactors*. International Atomic Energy Agency, Vienna, 2013.

[27] Kim J., Kim E., Yoo J., Lee Y. jun, Choi J., "An Integrated Software Testing Framework for FPGA-based Controllers in Nuclear Power Plants," *Nucl. Eng. Technol.*, 48(2):470–81, 2016.

[28] Maerani R., Deswandri, Santoso S., Sudarno, Irianto I.D., "Reverse Engineering Program Using MBSE to Support Development of I&C System Experimental Power Reactor from PLC to FPGA," *J. Phys. Conf. Ser,* 1198(2), 2019.

[29] *IEEE Std 1012-2012, IEEE Standard for System and Software Verification and Validation.* IEEE. 2012.

[30] Lexvek M., Stevens J., Snyder-mackler L. *IAEA Safety Standards, Safety Series No. 35-S1, Code on the Safety of Nuclear Research Reactor Design*. International Atomic Energy Agency, Vienna, 2001.

[31] Jarzabek S., Wang G., "Model-based Design of Reverse Engineering Tools," *Journal of Software Maintenance: Research and Practice*, (10):353–80, 1998.

[32] Lee J.S., Miller L.E. *INCOSE – Systems Engineering Handbook*. International Council on Systems Engineering, San Diego, 2007.

[33] *IAEA Technical Report Series No.384: Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control*. International Atomic Energy Agency, Vienna, 1999.

HALAMAN INI SENGAJA DIKOSONGKAN