

## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PENGESAHAN .....	ii
PENELITIAN S3 .....	iii
PERNYATAAN .....	iv
PRAKATA.....	vii
DAFTAR ISTILAH.....	ix
DAFTAR ISI.....	xiii
DAFTAR GAMBAR.....	xvi
DAFTAR TABEL.....	xvii
DAFTAR LAMPIRAN.....	xviii
Intisari .....	xix
Abstract.....	xx
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah dan Asumsi .....	4
1.4 Tujuan Penelitian.....	5
1.5 Kontribusi Penelitian .....	5
BAB II TINJAUAN PUSTAKA .....	7
2.1 Keamanan Siber pada Keamanan Nuklir.....	7
2.2 Metode Kajian Risiko untuk Keamanan Siber dalam Keamanan Nuklir .....	7
BAB III DASAR TEORI.....	19
3.1 Konsep Keamanan Nuklir .....	19
3.2 Risiko .....	21
3.2.1 Ancaman .....	25
3.2.2 Kerentanan .....	27
3.2.3 Konsekuensi.....	28

3.2.4	Musuh .....	28
3.3	Metode Kajian Risiko.....	29
3.3.1	Kajian Risiko dalam Konsep Keamanan Nuklir.....	29
3.3.2	Kajian Risiko untuk Keamanan Siber di Fasilitas Nuklir.....	32
3.3.3	Pembangkitan Pohon Kejadian pada Kajian Risiko .....	33
3.3.4	<i>Risk Informed Approach</i> .....	35
3.3.5	Kajian risiko berdasarkan validasi .....	38
3.3.6	<i>Fault Tree Analysis</i> (FTA).....	42
3.3.7	<i>Design Basis Threat</i> (DBT) .....	47
3.4	Risiko Keamanan Siber dalam Fasilitas Nuklir.....	51
3.4.1	Keamanan Komputer dalam Fasilitas Nuklir.....	52
3.4.2	Standar Internasional ISO/IEC 27001 Sistem Manajemen Keamanan Teknologi Informasi .....	53
3.4.3	<i>Common Criteria</i> untuk Standar Keamanan Teknologi Informasi .....	55
BAB IV ANALISIS PERANCANGAN PROSES RISK ASSESSMENT (KAJIAN RISIKO) KEAMANAN SIBER .....		57
4.1	Perancangan Proses <i>Risk Assessment</i> .....	57
4.1.1	Proses Identifikasi Melalui Pengumpulan Data.....	61
4.1.2	Identifikasi Risiko dalam Prosedur Kajian Risiko.....	61
4.1.3	Analisis Risiko dalam Prosedur Kajian Risiko.....	62
4.2	<i>Design Basis Threat</i> (DBT).....	63
4.3	Penyusunan Diagram Pohon Kegagalan dalam <i>Fault Tree Analysis</i> (FTA).....	63
4.4	Evaluasi .....	65
BAB V PENGEMBANGAN METODE <i>RISK ASSESSMENT</i> KEAMANAN SIBER .....		67
5.1	Identifikasi Risiko.....	67
5.2	Ancaman Desain Dasar (DBT - <i>design basis threat</i> ) .....	68
5.2.1	Identifikasi Ancaman .....	69
5.2.2	Identifikasi Musuh dan Jenis Serangan Berdasar DBT .....	69
5.3	Membangun Skenario dengan DBT .....	76

5.3.1	Peristiwa/Kejadian dasar.....	76
5.3.2	Kriteria Sukses/Keberhasilan dan Kegagalan Serangan.....	77
5.3.3	Pembentukan Diagram Pohon Kegagalan berupa FTA dalam Skenario .....	77
5.4	Studi Kasus Serangan terkait Keamanan Siber pada Fasilitas Nuklir	80
5.4.1	Penghitungan Nilai Probabilitas pada FTA Studi Kasus.....	84
5.4.2	<i>Minimum Cut Sets</i> pada FTA.....	89
5.4.3	Hasil Skenario Studi Kasus dalam FTA Berdasar DBT .....	90
BAB VI EVALUASI HASIL DAN PENGEMBANGAN DI MASA MENDATANG.....		93
6.1	Penilaian Kualitatif Pakar .....	93
6.1.1	Validasi atas Metode Kajian Risiko dengan FTA Berdasar DBT ....	93
6.1.2	Penilaian Kualitatif atas Studi Kasus dengan FTA Berdasar DBT ..	95
6.2	Pengembangan Metode FTA berdasar DBT di Masa Mendatang.....	97
BAB VII KESIMPULAN DAN SARAN.....		99
7.1	Kesimpulan.....	99
7.2	Saran .....	100