Annex A: Reference Tables for CVSS Scoring and Impact Criticality Classifications

Table A.1: CVSS 3.1 Metric Value Weights

Metric	Value	Weight
AV (Attack Vector)	N (Network)	0.85
	A (Adjacent)	0.62
	L (Local)	0.55
	P (Physical)	0.20
AC (Attack Complexity)	L (Low)	0.77
	H (High)	0.44
PR (Privileges Required)	N (None)	0.85
	L (Low)	0.62
	H (High)	0.27
UI (User Interaction)	N (None)	0.85
	R (Required)	0.62
S (Scope)	U (Unchanged)	1.00
	C (Changed)	1.00
C (Confidentiality)	H (High)	0.56
	L (Low)	0.22
	N (None)	0.00
I (Integrity)	H (High)	0.56
	L (Low)	0.22
	N (None)	0.00
A (Availability)	H (High)	0.56
	L (Low)	0.22
	N (None)	0.00

Table A.2: Impact Criticality Levels and Descriptions

Impact Type	Level (Value)	Description
Safety	None (0.00)	No injuries.
	Minor (0.25)	Single and/or minor injuries.
	Moderate (0.50)	Multiple minor injuries and/or a severe injury.
	Severe (0.75)	Single fatality and/or multiple severe injuries.
	Catastrophic (1.00)	Multiple fatalities and severe injuries.
Financial	None (0.00)	No damage to equipment or other property.
	Minor (0.25)	Local equipment damage, small damage to other property, or minor loss of income.
	Moderate (0.50)	Damage to CPS, other assets, or significant income loss.
	Severe (0.75)	Severe damage to CPS or other properties, or income loss equivalent to several days of operation.
	Catastrophic (1.00)	Complete loss of CPS or key assets.
Information	None (0.00)	No sensitive data stored, processed, or transmitted; no exposure risk.
	Minor (0.25)	Contains only non-critical config data or system logs; no security impact.
	Moderate (0.50)	Stores security-related data (e.g., local access permissions); limited consequence if exposed.
	Severe (0.75)	Handles privileged credentials or critical configs that could significantly affect system security.
	Catastrophic (1.00)	Stores high-value security artefacts; compromise leads to full security failure.
Operational	None (0.00)	Component has no direct influence on CPS operations.
	Minor (0.25)	Disruptions affect non-essential functions but do not impair CPS operations.
	Moderate (0.50)	Supports critical functions; failure may cause only efficiency loss or temporary disruption without long-term systemic consequences.
	Severe (0.75)	Directly influences primary CPS operations; failure causes major interruptions such as cascading outages or instability.
	Catastrophic (1.00)	Mission-critical component; failure results in complete operational breakdown, requiring extensive intervention.
Staging	None (0.00)	No ability to enable further attacks.
	Minimal (0.25)	May allow minor privilege escalation or expose low-value credentials but lacks persistence or lateral movement capability.
	Moderate (0.50)	Enables credential harvesting or moderate privilege escalation to aid persistence or lateral movement.
	High (0.75)	Facilitates significant escalation, lateral movement, persistence, or C2 operations.
	Maximum (1.00)	Serves as a central attack hub with full access, strong persistence, and high scalability.

Annex B: Formulations for Conditional Probabilities

Conditional Attack Probability Representation

The equations below establish conditional dependencies, enabling the derivation of the posterior probability of a successful cybersecurity attack in the CPS.

Conditional Attack Probabilities for Dependent Vulnerability Nodes.

$$P(Attack|V)_{\text{vuln}} = \begin{cases} P(E)_{\text{vuln}} \cdot \phi, & \text{if } V_p = 1 \text{ and } V_c = 1 \\ 1 - P(E)_{\text{vuln}} \cdot \phi, & \text{if } V_p = 1 \text{ and } V_c = 0 \\ 0, & \text{if } V_p = 0 \text{ and } V_c = 1 \\ 1, & \text{if } V_p = 0 \text{ and } V_c = 0 \end{cases} \tag{.1}$$

where:

- $P(Attack|V)_{\text{vuln}}$ represents the conditional probability of a successful attack given exposure in the vulnerability node.
- $P(E)_{\text{vuln}}$ is the probability of exposure for the vulnerability node.
- V_p represents the exploitation state of the parent vulnerability node (1 if exploited, 0 otherwise).
- V_c represents the exploitation state of the vulnerability node (1 if exploited, 0 otherwise).
- ϕ is the attack feasibility factor, representing the likelihood of successful exploitation.

Conditional Attack Probabilities for Dependent Asset Nodes.

$$P(Attack|A)_{\text{asset}} = \begin{cases} 1, & \text{if } A_p = 1 \text{ and } A_c = 1 \\ 0, & \text{if } A_p = 1 \text{ and } A_c = 0 \\ P(E)_{\text{asset}}, & \text{if } A_p = 0 \text{ and } A_c = 1 \\ 1 - P(E)_{\text{asset}}, & \text{if } A_p = 0 \text{ and } A_c = 0 \end{cases} \tag{.2}$$

where:

- $P(Attack|A)_{\text{asset}}$ represents the conditional probability of a successful attack given exposure in the the asset node.
- $P(E)_{\text{asset}}$ is the probability of exposure for the asset node.
- A_p represents the failure state of the parent asset node (1 if failed, 0 otherwise).
- A_c represents the failure state of the asset node (1 if failed, 0 otherwise).

Conditional Attack Probabilities for Dependent Hazard Nodes.

$$P(Attack|H)_{\text{haz}} = \begin{cases} P(E)_{\text{haz}}, & \text{if } H_p \text{ occurs and } H \text{ occurs} \\ 1 - P(E)_{\text{haz}}, & \text{if } H_p \text{ occurs and } H \text{ does not occur} \\ 0, & \text{if } H_p \text{ does not occur and } H \text{ occurs} \\ 1, & \text{if } H_p \text{ does not occur and } H \text{ does not occur} \end{cases} \tag{.3}$$

where:

- $P(Attack|H)_{\text{haz}}$ represents the conditional probability of a successful attack given exposure in the the hazard node.
- $P(E)_{\text{haz}}$ is the probability of exposure for the hazard node.
- H_p represents the parent hazard state (1 if the hazard occurs, 0 otherwise).
- H_c represents the hazard state (1 if the hazard occurs, 0 otherwise).

Conditional Attack Probabilities for Asset Nodes Linked to Vulnerabilities.

$$P(Attack|V)_{\text{asset}} = \begin{cases} 1, & \text{if } V \text{ is exploited and asset fails} \\ 0, & \text{if } V \text{ is exploited and asset does not fail} \\ P(E)_{\text{asset}}, & \text{if } V \text{ is not exploited and asset fails} \\ 1 - P(E)_{\text{asset}}, & \text{if } V \text{ is not exploited and asset does not fail} \end{cases} \tag{.4}$$

Conditional Attack Probabilities for Hazard Nodes Linked to Assets.

$$P(Attack|A)_{\text{haz}} = \begin{cases} P(E)_{\text{haz}}, & \text{if } A \text{ fails and hazard occurs} \\ 1 - P(E)_{\text{haz}}, & \text{if } A \text{ fails and hazard does not occur} \\ 0, & \text{if } A \text{ does not fail and hazard occurs} \\ 1, & \text{if } A \text{ does not fail and hazard does not occur} \end{cases} \tag{.5}$$

Posterior Probability of Successful Cybersecurity Attack. Applying variable elimination, the posterior probability of a successful cybersecurity attack in the CPS is computed as follows:

$$P(Attack)_{\text{CPS}} = \sum_{\text{X=v,a,h}} \sum_{\text{Y=v,a,h}} P(E)_Y \cdot P(Attack|Y)_X \tag{.6}$$

where:

- $P(Attack)_{\text{CPS}}$ represents the posterior probability of a successful cybersecurity attack in the CPS.
- $P(E)_Y$ denotes the exposure of node Y (Equations **??**, **??**, **??**, **??**).
- $P(Attack|Y)_X$ is the conditional probability of a successful attack in node X given exposure in node Y (Equations .1, .2, .3, .4, .5).
- v, a, h represent vulnerabilities, assets, and hazards respectively.

Conditional Impact Probability Representation

The equations below establish conditional dependencies, enabling the derivation of the posterior probability of a successful cybersecurity attack in the CPS.

Conditional Impact Probabilities for Dependent Vulnerability Nodes.

$$P(Impact|E)_{\text{vuln}} = \begin{cases} 1, & \text{if } V_p = 1 \text{ and } V_c = 1 \\ 0, & \text{if } V_p = 1 \text{ and } V_c = 0 \\ P(Impact)_{\text{vuln}} \cdot \phi, & \text{if } V_p = 0 \text{ and } V_c = 1 \\ 1 - P(Impact)_{\text{vuln}} \cdot \phi, & \text{if } V_p = 0 \text{ and } V_c = 0 \end{cases} \tag{.7}$$

where:

- $P(Impact|E)_{\text{vuln}}$ represents the conditional probability of impact given exposure in the vulnerability node.
- $P(Impact)_{\text{vuln}}$ is the probability of impact for the vulnerability node.
- V_p represents the exploitation state of the parent vulnerability node (1 if exploited, 0 otherwise).
- V_c represents the exploitation state of the vulnerability node (1 if exploited, 0 otherwise).
- ϕ is the attack feasibility factor, representing the likelihood of successful exploitation.

Conditional Impact Probabilities for Dependent Asset Nodes.

$$P(Impact|E)_{\text{asset}} = \begin{cases} 1, & \text{if } A_p = 1 \text{ and } A_c = 1 \\ 0, & \text{if } A_p = 1 \text{ and } A_c = 0 \\ P(Impact)_{\text{asset}}, & \text{if } A_p = 0 \text{ and } A_c = 1 \\ 1 - P(Impact)_{\text{asset}}, & \text{if } A_p = 0 \text{ and } A_c = 0 \end{cases} \tag{.8}$$

where:

- $P(Impact|E)_{\text{asset}}$ represents the conditional probability of impact given exposure in the the asset node.
- $P(Impact)_{\text{asset}}$ is the probability of impact for the asset node.
- A_p represents the failure state of the parent asset node (1 if failed, 0 otherwise).
- A_c represents the failure state of the asset node (1 if failed, 0 otherwise).

Conditional Impact Probabilities for Dependent Hazard Nodes.

$$P(Impact|H)_{\text{haz}} = \begin{cases} 1, & \text{if } H_p \text{ occurs and } H \text{ occurs} \\ 0, & \text{if } H_p \text{ occurs and } H \text{ does not occur} \\ P(Impact)_{\text{haz}}, & \text{if } H_p \text{ does not occur and } H \text{ occurs} \\ 1 - P(Impact)_{\text{haz}}, & \text{if } H_p \text{ does not occur and } H \text{ does not occur} \end{cases} \tag{.9}$$

where:

- $P(Impact|H)_{\text{hazard}}$ represents the conditional probability of impact for the hazard node.
- $P(Impact)_{\text{hazard}}$ is the probability of impact for the hazard node.
- H_p represents the parent hazard state (1 if the hazard occurs, 0 otherwise).
- H_c represents the hazard state (1 if the hazard occurs, 0 otherwise).

Conditional Impact Probabilities for Asset Nodes Linked to Vulnerabilities.

$$P(Impact|V)_{\text{asset}} = \begin{cases} 1, & \text{if } V \text{ is exploited and asset fails} \\ 0, & \text{if } V \text{ is exploited and asset does not fail} \\ P(E)_{\text{asset}}, & \text{if } V \text{ is not exploited and asset fails} \\ 1 - P(E)_{\text{asset}}, & \text{if } V \text{ is not exploited and asset does not fail} \end{cases} \tag{.10}$$

Conditional Impact Probabilities for Hazard Nodes Linked to Assets.

$$P(Impact|A)_{\text{haz}} = \begin{cases} 1, & \text{if } A \text{ fails and hazard occurs} \\ 0, & \text{if } A \text{ fails and hazard does not occur} \\ P(E)_{\text{haz}}, & \text{if } A \text{ does not fail and hazard occurs} \\ 1 - P(E)_{\text{haz}}, & \text{if } A \text{ does not fail and hazard does not occur} \end{cases} \tag{.11}$$

Posterior Probability of Severe Impact in CPS. Applying variable elimination, the posterior probability of a severe impact on the CPS is computed as follows:

$$P(SevereImpact)_{\text{CPS}} = \sum_{\text{X=v,a,h}} \sum_{\text{Y=v,a,h}} P(E)_Y \cdot P(Impact|Y)_X \tag{.12}$$

where:

- $P(Impact)_{\text{CPS}}$ represents the posterior probability of severe impact on the CPS.
- $P(Impact)_Y$ denotes the probability of impact of node Y (Equations **??**, **??**).
- $P(Impact|Y)_X$ is the conditional probability of impact in node X given impact in node Y (Equations .7, .8, .9, .10, .11).
- v, a, h represent vulnerabilities, assets, and hazards respectively.

Annex C: Case Study Vulnerability Details, Parameters, and Estimates

Table C.1: CVE Identifiers and CVSS Vectors in BlackEnergy Case Study

Node	CVE ID	CVSS Vector
V1	CVE-2015-3113	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
V2	CVE-2014-4114	CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
V3	N/A	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
V4	N/A	CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
V5	N/A	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
V6	N/A	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N
V7	N/A	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
V8	N/A	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L
V9	N/A	CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N
V10	N/A	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N
V11	N/A	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:H/A:N

Table C.2: Exposure Estimates and Posterior Parameters in BlackEnergy Case Study

Node	$P(E)_{\textbf{EPSS}}$	$P(E)_{\textbf{CVSS}}$	$\mu_{\textbf{post}}$	$\sigma^2_{\textbf{post}}$	$P(E)^*$
V1	0.824	N/A	N/A	N/A	0.824
V2	0.217	N/A	N/A	N/A	0.217
V3	N/A	0.306	0.489	0.00235	0.489
V4	N/A	0.045	0.274	0.00290	0.274
V5	N/A	0.435	0.592	0.00120	0.592
V6	N/A	0.152	0.338	0.00260	0.338
V7	N/A	0.441	0.503	0.00140	0.503
V8	N/A	0.198	0.364	0.00220	0.364
V9	N/A	0.176	0.349	0.00240	0.349
V10	N/A	0.265	0.420	0.00200	0.420
V11	N/A	0.275	0.460	0.00160	0.460

Table C.3: CVE Identifiers and CVSS Vectors in Solar PV Inverter Case Study

Node	**CVE ID**	**CVSS Vector**
V1	CVE-2024-50684	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
V2	CVE-2024-50691	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
V3	CVE-2024-50688	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H
V4	CVE-2024-50690	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H
V5	CVE-2024-50692	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
V6	CVE-2024-50685	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V7	CVE-2024-50686	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V8	CVE-2024-50687	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V9	CVE-2024-50693	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V10	CVE-2024-50694	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V11	CVE-2024-50695	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V12	CVE-2024-50696	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V13	CVE-2024-50697	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V14	CVE-2024-50698	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
V15	CVE-2024-50696	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H
V16	N/A	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H

Table C.4: Exposure Estimates and Posterior Parameters in Solar PV Inverter Case Study

Node	$P(E)_{\mathbf{EPSS}}$	$P(E)_{\mathbf{CVSS}}$	$\mu_{\mathbf{post}}$	$\sigma^2_{\mathbf{post}}$	$P(E)^*$
V1	0.00049	N/A	N/A	N/A	0.0005
V2	0.00023	N/A	N/A	N/A	0.0002
V3	0.00066	N/A	N/A	N/A	0.0007
V4	0.00055	N/A	N/A	N/A	0.0006
V5	0.00047	N/A	N/A	N/A	0.0005
V6	0.00047	N/A	N/A	N/A	0.0005
V7	0.00047	N/A	N/A	N/A	0.0005
V8	0.00047	N/A	N/A	N/A	0.0005
V9	0.00047	N/A	N/A	N/A	0.0005
V10	0.00047	N/A	N/A	N/A	0.0005
V11	0.00095	N/A	N/A	N/A	0.0010
V12	0.00122	N/A	N/A	N/A	0.0012
V13	0.00095	N/A	N/A	N/A	0.0010
V14	0.00095	N/A	N/A	N/A	0.0010
V15	0.00023	N/A	N/A	N/A	0.0002
V16	N/A	0.4729	0.4984	0.00235	0.4984

Table C.5: Analogous CVE Identifiers and CVSS Vectors in Railway CBTC Case Study

Node	**CVE ID**	**CVSS Vector**
V1	CVE-2022-21882	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
V2	CVE-2017-17740	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
V3	CVE-2018-0171	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
V4	CVE-2017-13077	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
V5	CVE-2019-16336	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
V6	CVE-2020-0601	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
V7	CVE-2022-34718	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
V8	CVE-2017-13078	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Table C.6: CVSS-based Exposure Estimates and Posterior Parameters in Railway CBTC Case Study

Node	$P(E)_{\mathbf{CVSS}}$	$\mu_{\mathbf{post}}$	$\sigma^2_{\mathbf{post}}$	$P(E)^*$
V1	0.2702	0.4865	0.00235	0.4865
V2	0.4729	0.4984	0.00235	0.4984
V3	0.4729	0.4984	0.00235	0.4984
V4	0.4729	0.4984	0.00235	0.4984
V5	0.4729	0.4984	0.00235	0.4984
V6	0.4729	0.4984	0.00235	0.4984
V7	0.2702	0.4865	0.00235	0.4865
V8	0.2702	0.4865	0.00235	0.4865

Table C.7: EPSS-Based Exposure Estimates in Railway CBTC Case Study

Node	$P(E)_{\mathbf{EPSS}}$
V1	0.89101
V2	0.02838
V3	0.9129
V4	0.01057
V5	0.00337
V6	0.93911
V7	0.00838
V8	0.2702