Quantifying security risk level from CVSS estimates of frequency and impact

- Authors:
  - Siv Hilde Houmb, Virginia N.L. Franqueira, Erlend A. Engum
- Journal:
  - The Journal of Systems and Software, Vol. 83, No. 9, September 2010, pp. 1622-1634.

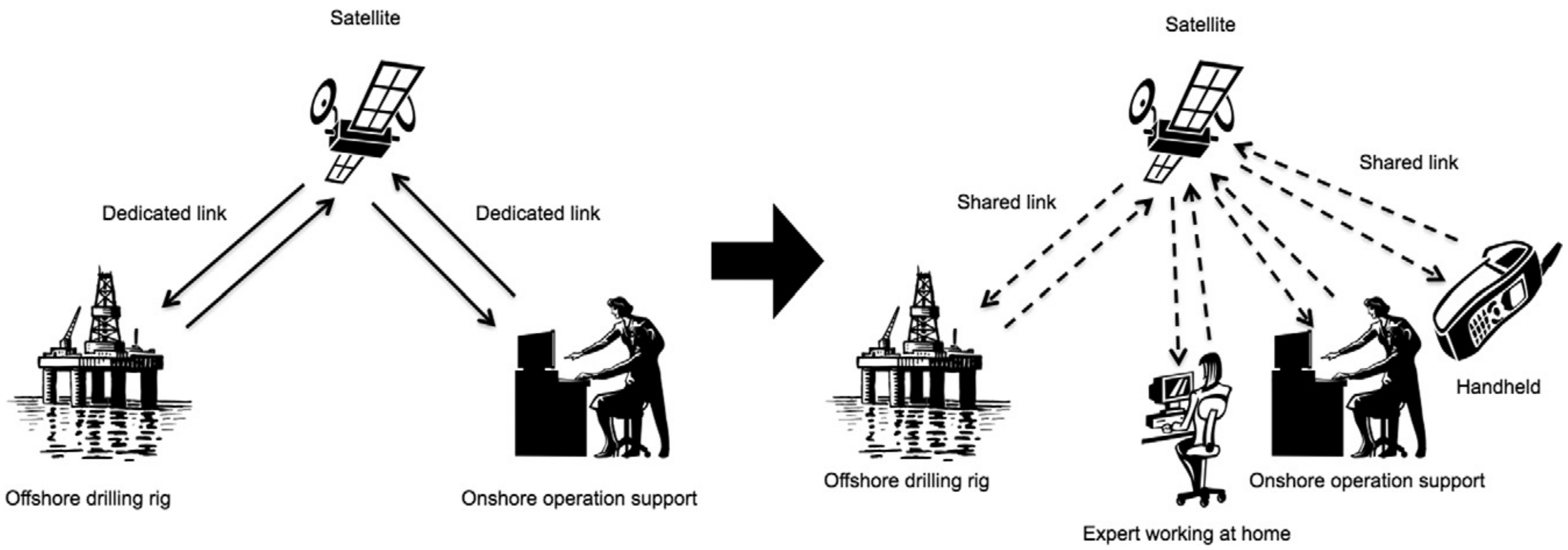
Introduction (1/2)

- Risk management is a good tool for controlling risk but it has the inherent challenge of quantitatively estimating frequency and impact in an accurate and trustworthy way.
- Quantifying the frequency and impact of potential security threats requires experience-based data which is limited and rarely reusable because it involves company confidential data.
- This paper presents a risk estimation model that makes use of one such data source, the Common Vulnerability Scoring System (CVSS).
- The CVSS Risk Level Estimation Model estimates a security risk level from vulnerability information as a combination of frequency and impact estimates derived from the CVSS.

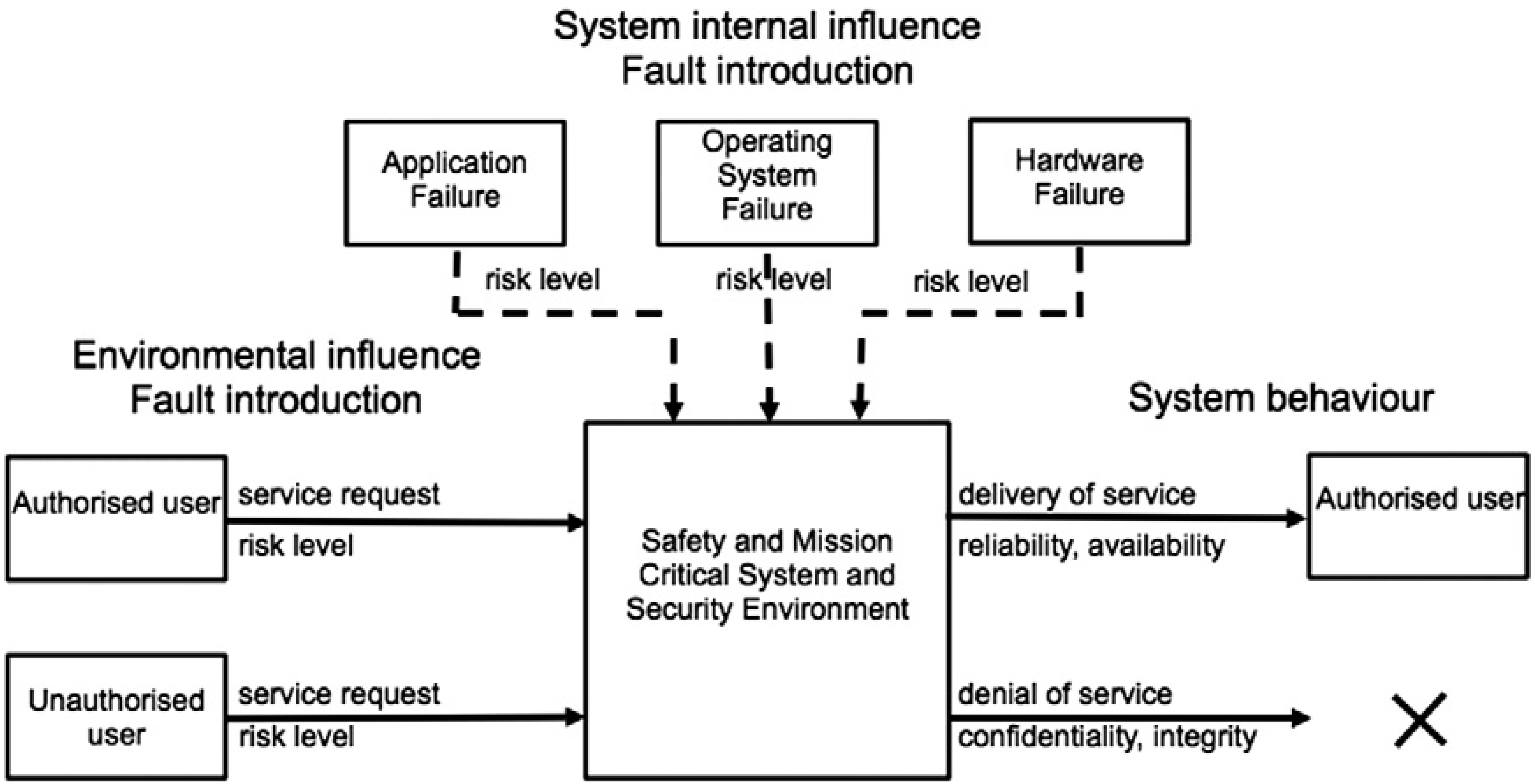
Introduction (2/2)

- One such model is the CVSS Risk Level Estimation Model presented in this paper.
- This model supports trade-off analysis of any type of system but, in this paper, it is applied to the control of risks in a Measurement and Logging While Drilling (M/LWD) system on oil and gas drilling installations.

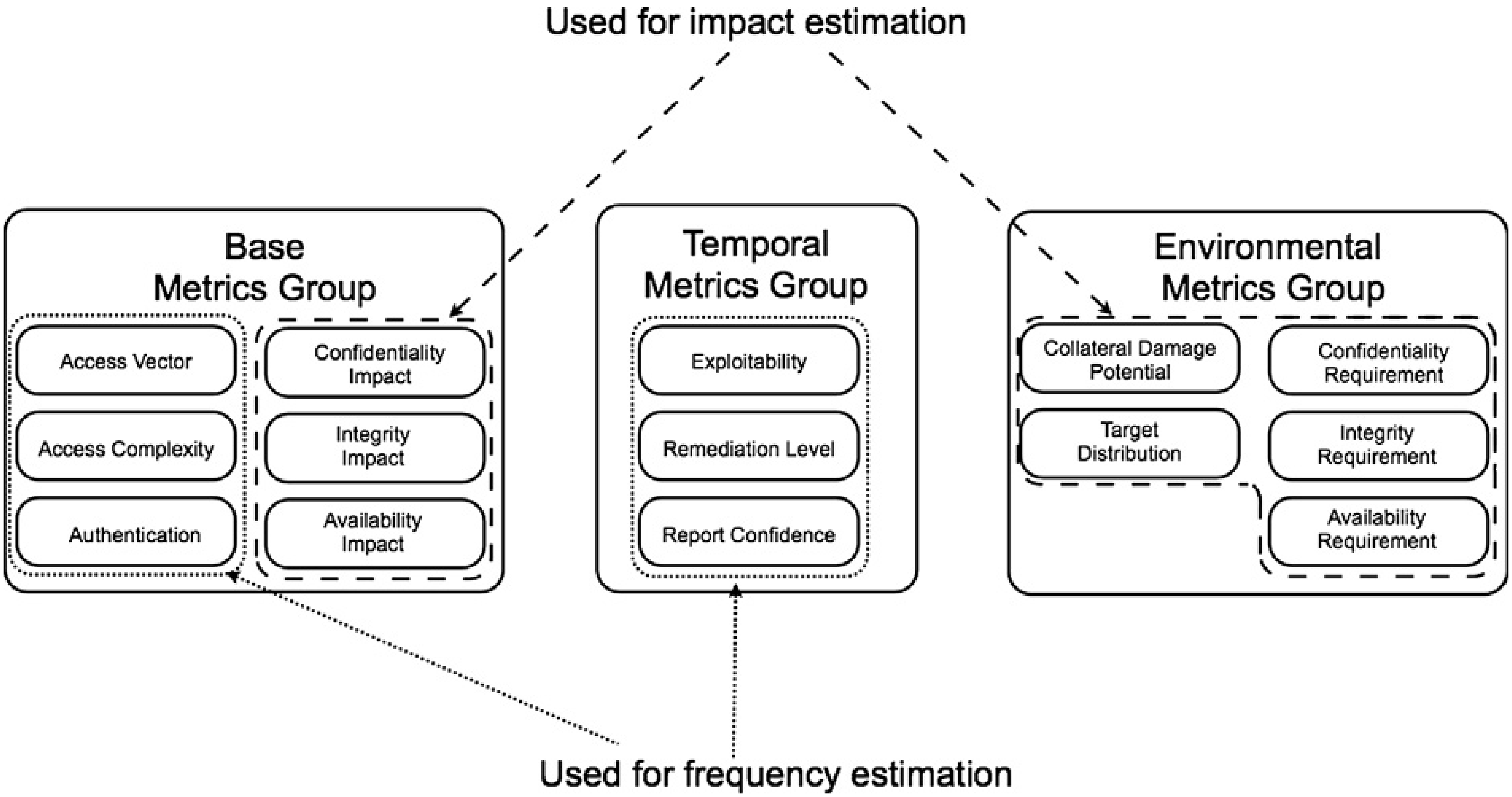
Transition from controlled communication to open communication between drilling rig and onshore experts



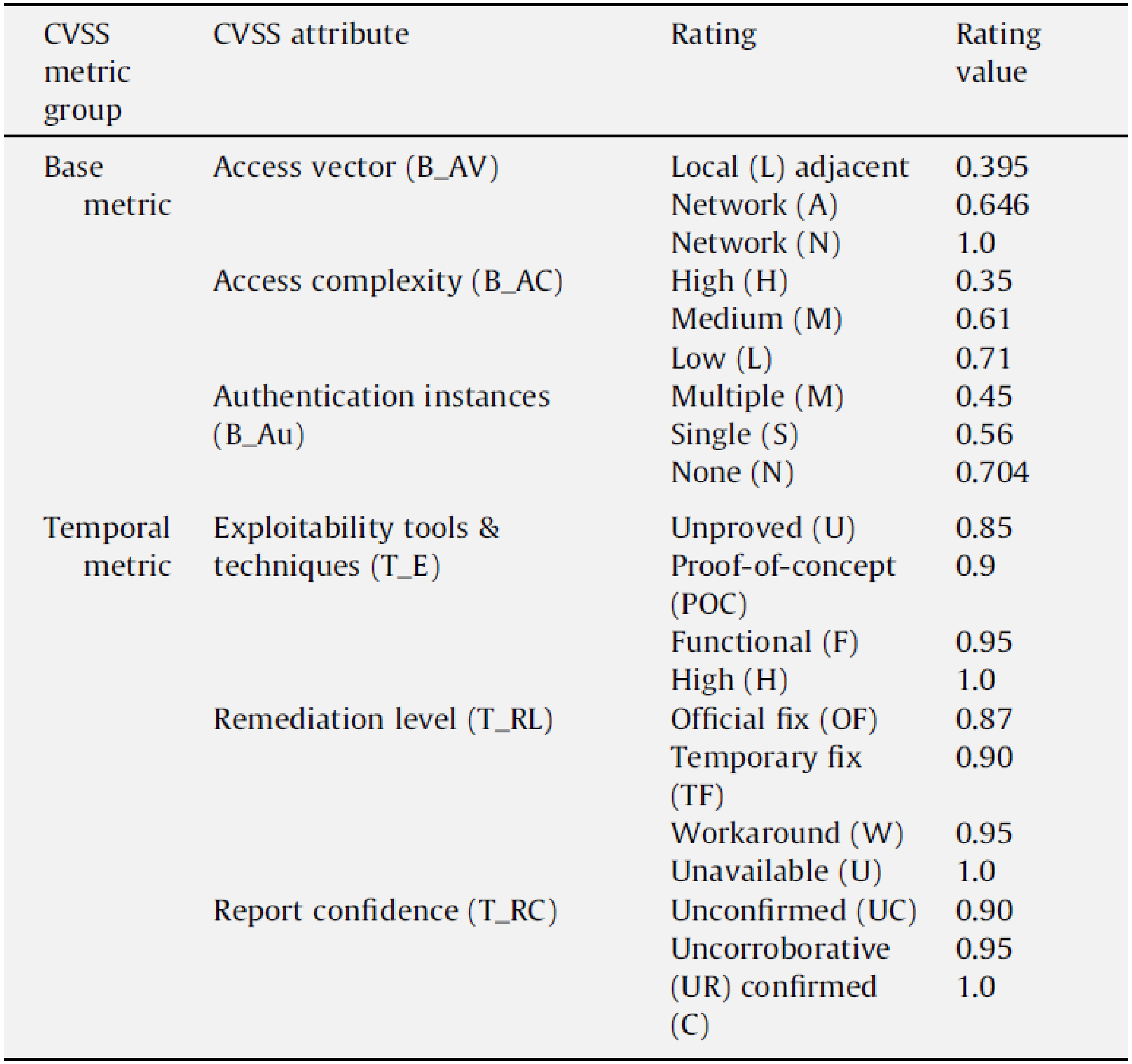
System internal and environmental fault introduction as risk level influence sources and how they may affect the system behaviour



Emphasised subset of attributes from the CVSS

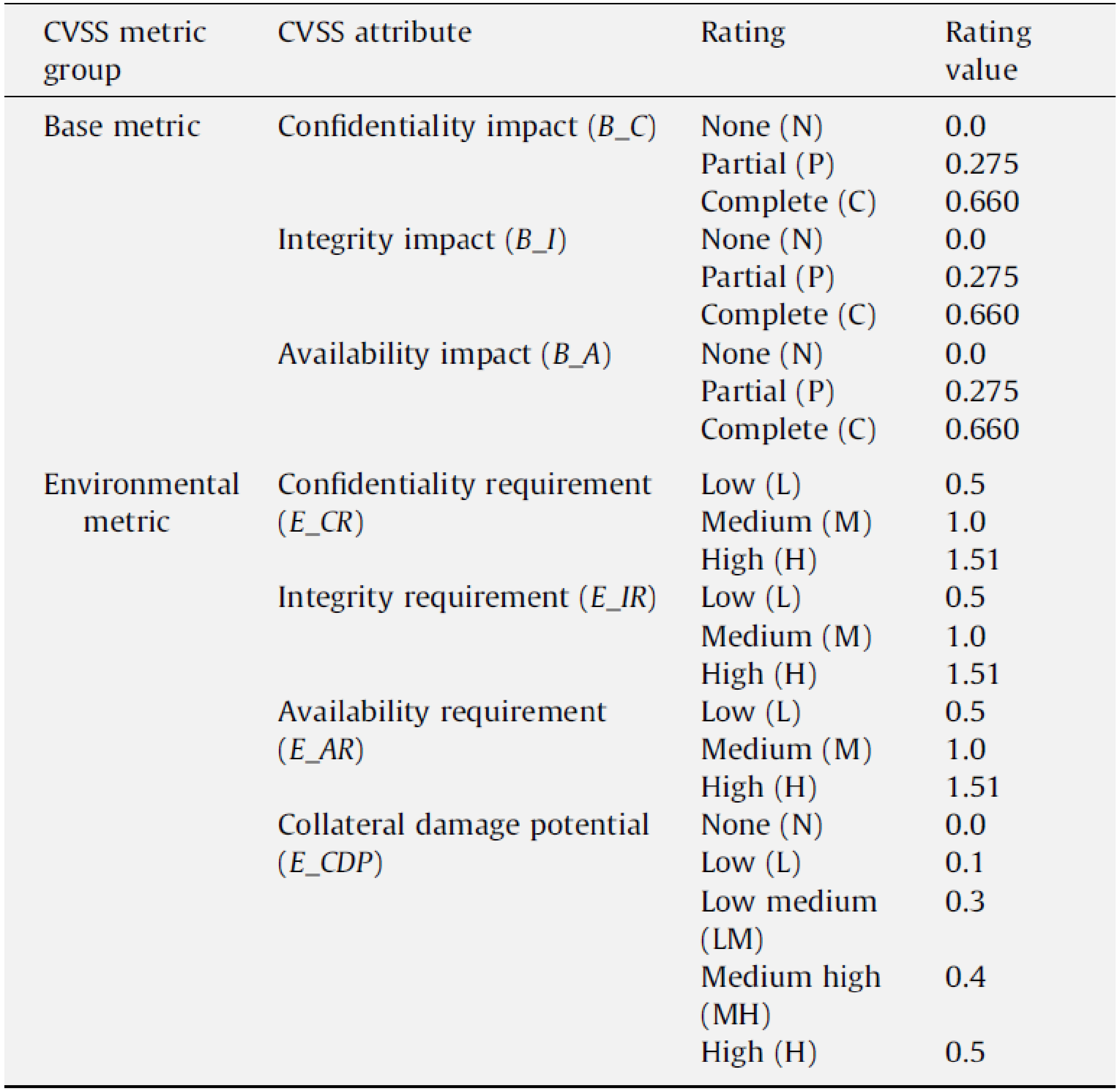


CVSS attributes relevant for the calculation of frequency estimate



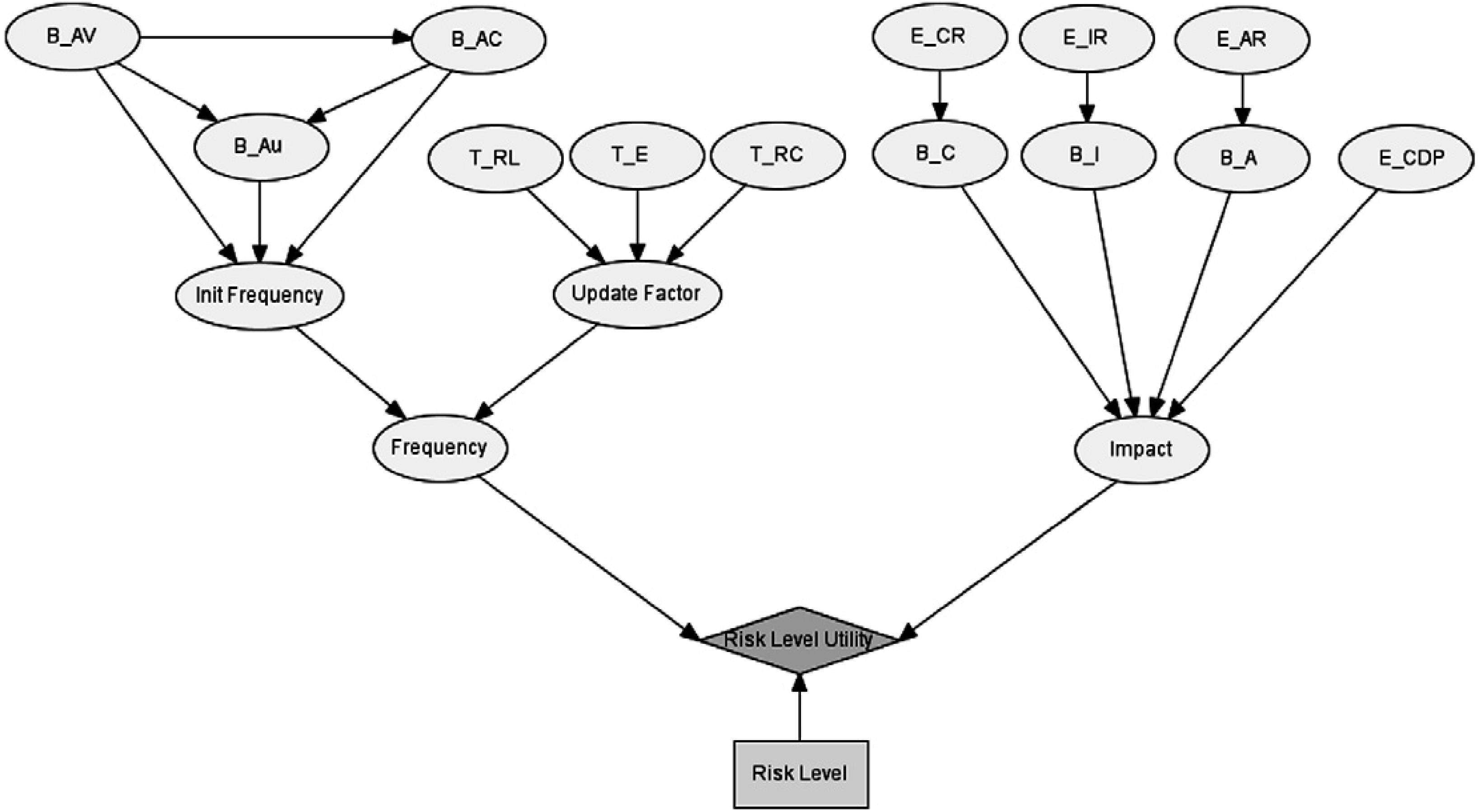
CVSS metric group	CVSS attribute	Rating	Rating value
Base metric	Access vector (B_AV)	Local (L) adjacent	0.395
		Network (A)	0.646
		Network (N)	1.0
	Access complexity (B_AC)	High (H)	0.35
		Medium (M)	0.61
		Low (L)	0.71
	Authentication instances (B_Au)	Multiple (M)	0.45
		Single (S)	0.56
		None (N)	0.704
Temporal metric	Exploitability tools & techniques (T_E)	Unproved (U)	0.85
		Proof-of-concept (POC)	0.9
		Functional (F)	0.95
		High (H)	1.0
	Remediation level (T_RL)	Official fix (OF)	0.87
		Temporary fix (TF)	0.90
		Workaround (W)	0.95
		Unavailable (U)	1.0
	Report confidence (T_RC)	Unconfirmed (UC)	0.90
		Uncorroborative	0.95
		(UR) confirmed (C)	1.0

CVSS attributes relevant for the calculation of impact estimate

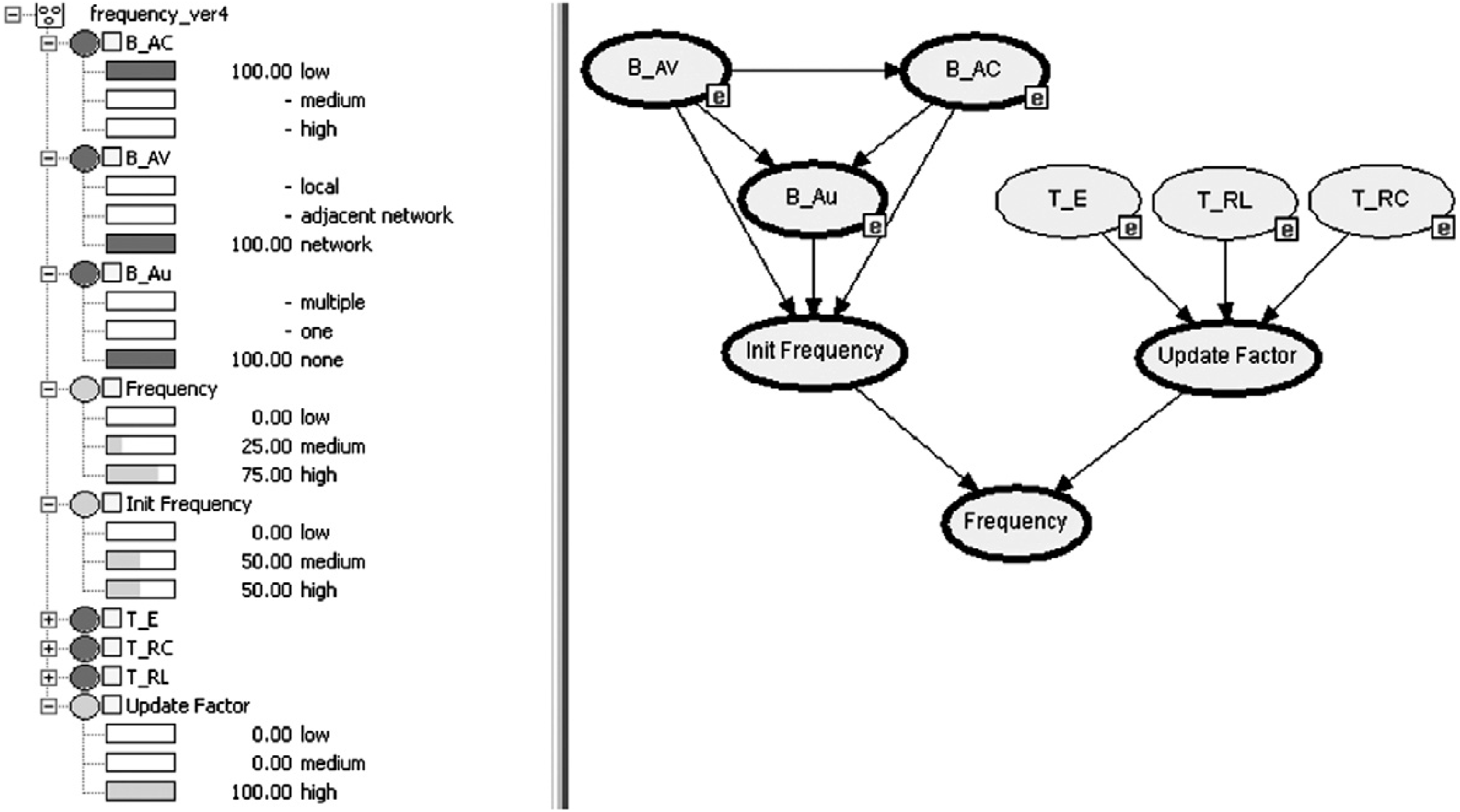


CVSS metric group	CVSS attribute	Rating	Rating value
Base metric	Confidentiality impact (*B_C*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
	Integrity impact (*B_I*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
	Availability impact (*B_A*)	None (N)	0.0
		Partial (P)	0.275
		Complete (C)	0.660
Environmental metric	Confidentiality requirement (*E_CR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Integrity requirement (*E_IR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Availability requirement (*E_AR*)	Low (L)	0.5
		Medium (M)	1.0
		High (H)	1.51
	Collateral damage potential (*E_CDP*)	None (N)	0.0
		Low (L)	0.1
		Low medium (LM)	0.3
		Medium high (MH)	0.4
		High (H)	0.5

BBN topology of the CVSS Risk Level Estimation Model

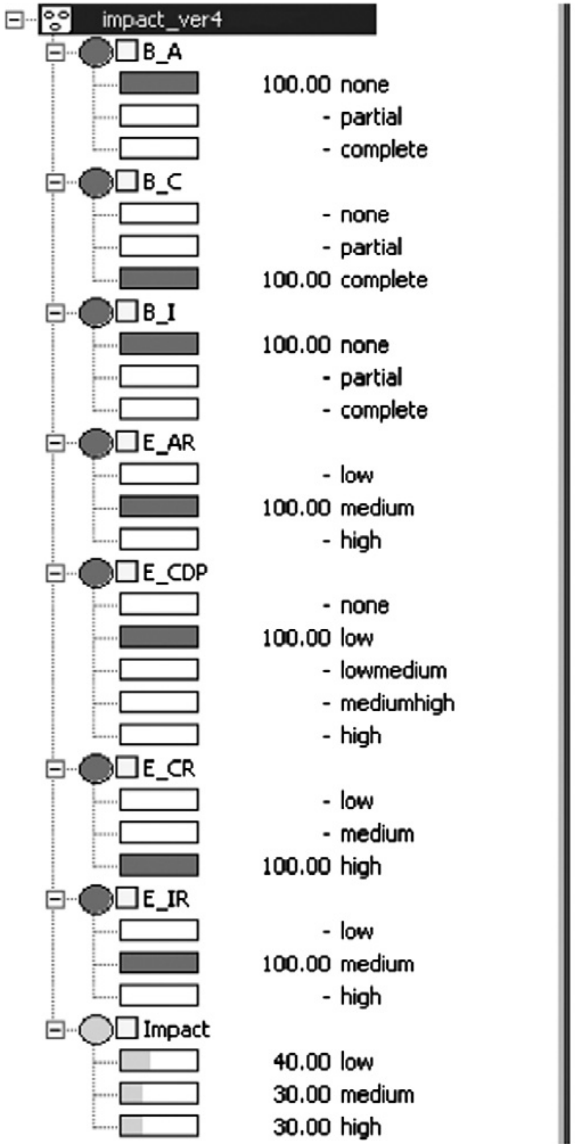


Resulting frequency estimate after information has been inserted

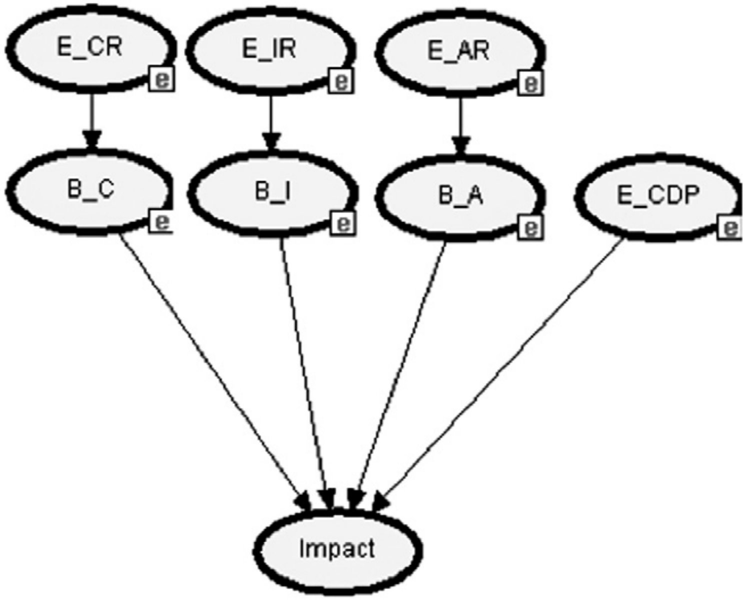


```
frequency_ver4
  B_AC
    100.00 low
         - medium
         - high
  B_AV
         - local
         - adjacent network
    100.00 network
  B_Au
         - multiple
         - one
    100.00 none
  Frequency
      0.00 low
     25.00 medium
     75.00 high
  Init Frequency
      0.00 low
     50.00 medium
     50.00 high
  T_E
  T_RC
  T_RL
  Update Factor
      0.00 low
      0.00 medium
    100.00 high
```

Resulting impact estimate after information has been inserted

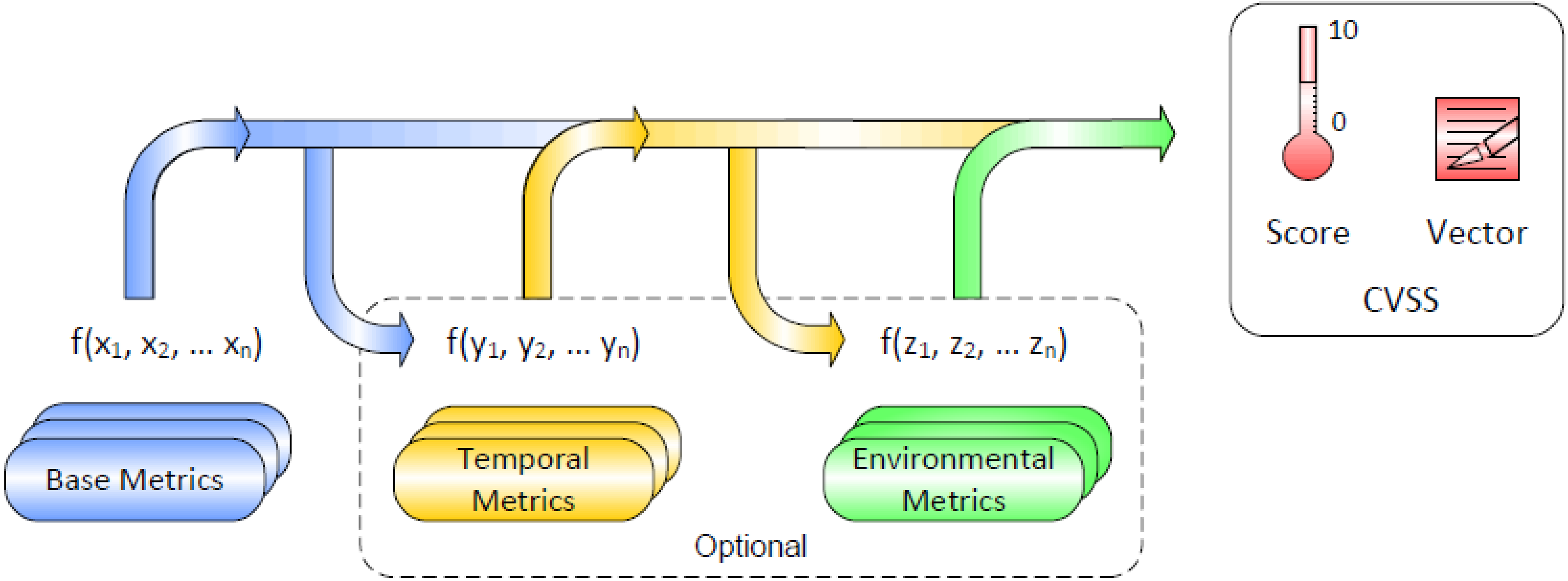


```
impact_ver4
  B_A
        100.00 none
             - partial
             - complete
  B_C
             - none
             - partial
        100.00 complete
  B_I
        100.00 none
             - partial
             - complete
  E_AR
             - low
        100.00 medium
             - high
  E_CDP
             - none
        100.00 low
             - lowmedium
             - mediumhigh
             - high
  E_CR
             - low
             - medium
        100.00 high
  E_IR
             - low
        100.00 medium
             - high
  Impact
         40.00 low
         30.00 medium
         30.00 high
```



CVSS Metrics and Equations

- **A Complete Guide to the CVSS Version 2.0**



Equations (1/2)

- ***Base* Equation**
  - BaseScore = round_to_1_decimal(((0.6 * Impact) + (0.4 * Exploitability) – 1.5) * f(Impact))
  - Impact = 10.41 * (1 - (1 - ConfImpact) * (1 - IntegImpact) * (1 - AvailImpact))
  - Exploitability = 20 * AccessVector * AccessComplexity * Authentication
  - f(impact) = 0 if Impact =0, 1.176 otherwise

- ***Temporal* Equation**
  - TemporalScore = round_to_1_decimal(BaseScore * Exploitability * RemediationLevel * ReportConfidence)

Equations (2/2)

- ***Environmental* Equation**
  - EnvironmentalScore = round_to_1_decimal((AdjustedTemporal + (10-AdjustedTemporal) * CollateralDamagePotential) * TargetDistribution)

  - AdjustedTemporal = **TemporalScore** recomputed with the **BaseScore**’s Impact subequation replaced with the AdjustedImpact equation
  - AdjustedImpact = min(10, 10.41 * (1 - (1 – ConfImpact * ConfReq) * (1 - IntegImpact * IntegReq) * (1 – AvailImpact * AvailReq)))

Example: CVE-1999-0196

- The NVD reports the following information relevant to the **base** metric attributes.
- For example, the vulnerability CVE-1999-0196 has a base vector (AV:N/AC:L/AU:N/C:P/I:N/A:N) which is interpreted as follows:
  - AV:N – the access vector is ‘‘network” (i.e., the vulnerability can be exploited remotely);
  - AC:L – the complexity involved in exploiting the vulnerability is ‘‘low”;
  - AU:N – authentication required for the exploitation of the vulnerability is ‘‘none”;
  - C:P – the impact on confidentiality of a successful exploitation of the vulnerability is ‘‘partial”; and
  - I:N/A:N – the impact on both integrity and availability of a successful exploitation of the vulnerability is ‘‘none”.

Example: CVE-2003-0818

```
----------------------------------------------------
BASE METRIC                   EVALUATION       SCORE
----------------------------------------------------
Access Vector                 [Network]       (1.00)
Access Complexity             [Low]           (0.71)
Authentication                [None]          (0.704)
Confidentiality Impact        [Complete]      (0.66)
Integrity Impact              [Complete]      (0.66)
Availability Impact           [Complete]      (0.66)
----------------------------------------------------
FORMULA                                   BASE SCORE
----------------------------------------------------
Impact = 10.41*(1-(0.34*0.34*0.34)) == 10.0
Exploitability = 20*0.71*0.704*1 == 10.0
f(Impact) = 1.176
BaseScore =((0.6*10.0)+(0.4*10.0)-1.5)*1.176
                                          == (10.0)
----------------------------------------------------
```

```
----------------------------------------------------
TEMPORAL METRIC              EVALUATION        SCORE
----------------------------------------------------
Exploitability               [Functional]     (0.95)
Remediation Level            [Official-Fix]   (0.87)
Report Confidence            [Confirmed]      (1.00)
----------------------------------------------------
FORMULA                               TEMPORAL SCORE
----------------------------------------------------
round(10.0 * 0.95 * 0.87 * 1.00) ==            (8.3)
----------------------------------------------------
```

```
----------------------------------------------------
ENVIRONMENTAL METRIC         EVALUATION        SCORE
----------------------------------------------------
Collateral Damage Potential  [None - High]  {0 - 0.5}
Target Distribution          [None - High]  {0 - 1.0}
Confidentiality Req.         [Medium]          (1.0)
Integrity Req.               [Medium]          (1.0)
Availability Req.            [Low]             (0.5)
----------------------------------------------------
FORMULA                          ENVIRONMENTAL SCORE
----------------------------------------------------
AdjustedImpact = 10.41*(1-(1-0.66*1)*(1-0.66*1)
         *(1-0.66*0.5)) == 9.6
AdjustedBase =((0.6*9.6)+(0.4*10.0)-1.5)*1.176
                                            == (9.7)
AdjustedTemporal == (9.7*0.95*0.87*1.0)     == (8.0)
EnvScore = round((8.0+(10-8.0)*{0-0.5})*{0-1})
                 ==                   (0.00 - 9.0)
----------------------------------------------------
```