CPF Mathematical Formalization Series - Paper 7: Stress Response Vulnerabilities: Mathematical Models and Detection Algorithms

Giuseppe Canale, CISSP
Independent Researcher
g.canale@cpf3.org
ORCID: 0009-0007-3263-6897

September 24, 2025

Abstract

We present the complete mathematical formalization of Category 7 indicators from the Cybersecurity Psychology Framework (CPF): Stress Response Vulnerabilities. Each of the ten indicators (7.1-7.10) is rigorously defined through detection functions combining physiological modeling, behavioral pattern analysis, and stress propagation dynamics. The formalization enables systematic implementation of stress-related security vulnerabilities while maintaining theoretical grounding in Selye's General Adaptation Syndrome and contemporary stress research. We provide explicit algorithms for real-time stress detection, cascade modeling for organizational stress contagion, and validation metrics for continuous calibration. This work establishes the mathematical foundation for operationalizing stress-induced psychological vulnerabilities in cybersecurity contexts.

1 Introduction and CPF Context

The Cybersecurity Psychology Framework (CPF) represents a paradigm shift from reactive security awareness to predictive vulnerability assessment through psychological state modeling [1]. Unlike traditional security frameworks that address technical controls, CPF systematically identifies pre-cognitive psychological vulnerabilities that create systematic security blind spots.

The CPF architecture comprises 100 indicators organized in a 10×10 matrix, each grounded in established psychological research. The framework employs a ternary assessment system (Green/Yellow/Red) while maintaining strict privacy protection through aggregated behavioral analysis rather than individual profiling.

This paper series provides complete mathematical formalization for each CPF category, enabling rigorous implementation and validation. Each indicator receives explicit detection functions, interdependency modeling, and algorithmic specifications. The mathematical approach serves dual purposes: ensuring reproducible implementations across organizations and establishing CPF as a scientifically rigorous methodology suitable for peer review and standardization.

Category 7 focuses on stress response vulnerabilities, drawing primarily from Selye's General Adaptation Syndrome [2] and contemporary psychoneuroimmunology research [3]. These vulnerabilities exploit the fundamental changes in cognitive processing, decision-making, and risk assessment that occur during acute and chronic stress states, creating systematic security weaknesses that attackers can exploit through timing-based and pressure-based attack strategies.

2 Theoretical Foundation: Stress Physiology and Cybersecurity

Stress response vulnerabilities emerge from the intersection of neuroendocrinology, cognitive psychology, and organizational behavior. The human stress response system, evolved for immediate physical threats, creates systematic cognitive impairments when activated by cybersecurity incidents and organizational pressures [4].

Research demonstrates that stress affects security-relevant cognitive processes through multiple pathways: (1) cortisol elevation impairs working memory and executive function [5], (2) sympathetic nervous system activation narrows attention and reduces cognitive flexibility [6], and (3) chronic stress depletes cognitive resources necessary for vigilant security behavior [7].

The mathematical models presented here capture these physiological and behavioral mechanisms through four complementary approaches: (1) stress state estimation using behavioral and physiological proxies, (2) cognitive impairment modeling based on stress levels, (3) contagion dynamics for organizational stress propagation, and (4) recovery modeling for post-stress vulnerability periods.

3 Mathematical Formalization

3.1 Universal Stress Detection Framework

Each stress response indicator employs the unified detection function:

$$D_i(t) = w_1 \cdot S_i(t) + w_2 \cdot C_i(t) + w_3 \cdot B_i(t) + w_4 \cdot R_i(t) \tag{1}$$

where $D_i(t)$ represents the detection score for indicator i at time t, $S_i(t)$ denotes stress state estimation, $C_i(t)$ represents cognitive impairment measure, $B_i(t)$ represents behavioral deviation score, and $R_i(t)$ represents recovery state. Weights w_1, w_2, w_3, w_4 sum to unity and are calibrated through organizational baselines.

The temporal evolution follows a stress-modified exponential model:

$$T_i(t) = \alpha(S(t)) \cdot D_i(t) + (1 - \alpha(S(t))) \cdot T_i(t-1) \tag{2}$$

where $\alpha(S(t)) = \alpha_0 \cdot (1 + \beta \cdot S(t))$ provides stress-dependent decay rates.

3.2 Indicator 7.1: Acute Stress Impairment

Definition: Immediate cognitive and behavioral degradation under acute stress conditions.

Mathematical Model:

The acute stress index combining multiple physiological and behavioral markers:

$$ASI(t) = \sum_i w_i \cdot \tanh\left(\frac{x_i(t) - \mu_i}{\sigma_i}\right) \tag{3}$$

where $x_i(t)$ represents stress markers including typing pattern deviation, response time variance, and error rate increase.

Cognitive Impairment Function:

$$CI(ASI) = 1 - e^{-\lambda \cdot ASI^2} \tag{4}$$

where λ controls the sensitivity of cognitive degradation to stress levels.

Behavioral Deviation Detection:

$$BD(t) = \sqrt{\sum_j \left(\frac{b_j(t) - \mu_{b_j}}{\sigma_{b_j}}\right)^2} \tag{5}$$

where $b_j(t)$ represents behavioral metrics such as session duration, click patterns, and navigation behavior.

Detection Function:

$$D_{7.1}(t) = ASI(t) \cdot CI(ASI(t)) \cdot (1 + \gamma \cdot BD(t)) \tag{6}$$

Threshold Condition:

$$R_{7.1}(t) = \begin{cases} 1 & \text{if } D_{7.1}(t) > \theta_{acute} \text{ and } \Delta t < 3600s \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

3.3 Indicator 7.2: Chronic Stress Burnout

Definition: Long-term stress accumulation leading to sustained security performance degradation.

Mathematical Model:

The chronic stress accumulation model using allostatic load:

$$AL(t) = \int_0^t e^{-\lambda(t-\tau)} \cdot S(\tau)\, d\tau \tag{8}$$

where $S(\tau)$ represents instantaneous stress level and λ is the recovery rate constant.

Burnout Function:

$$B(t) = \begin{cases} 0 & \text{if } AL(t) < \theta_{low} \\ \frac{AL(t) - \theta_{low}}{\theta_{high} - \theta_{low}} & \text{if } \theta_{low} \leq AL(t) < \theta_{high} \\ 1 & \text{if } AL(t) \geq \theta_{high} \end{cases} \tag{9}$$

Performance Degradation Model:

$$PD(t) = PD_0 \cdot (1 - \alpha \cdot B(t)) \cdot e^{-\beta \cdot AL(t)} \tag{10}$$

Detection Threshold:

$$R_{7.2}(t) = \begin{cases} 1 & \text{if } B(t) > 0.6 \text{ and } PD(t) < 0.5 \cdot PD_0 \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

3.4 Indicator 7.3: Fight Response Aggression

Definition: Aggressive behavioral patterns under stress affecting security decision-making.

Mathematical Model:

The fight response probability using stress-aggression mapping:

$$P_{fight}(S, T, C) = \sigma(\alpha \cdot S + \beta \cdot T + \gamma \cdot C) \tag{12}$$

where S is stress level, T is trait aggression, and C is contextual provocation.

Aggression Markers: Linguistic aggression detection:

$$AG_{ling}(m) = \sum_{w \in m} I_{aggressive}(w) \cdot weight(w) \tag{13}$$

Behavioral aggression indicators:

$$AG_{behav}(t) = w_1 \cdot click_{force}(t) + w_2 \cdot type_{intensity}(t) + w_3 \cdot nav_{abrupt}(t) \tag{14}$$

Security Impact Model:

$$SI_{fight}(t) = P_{fight}(t) \cdot (AG_{ling}(t) + AG_{behav}(t)) \cdot override_{rate}(t) \tag{15}$$

Detection Function:

$$D_{7.3}(t) = SI_{fight}(t) \cdot (1 + \delta \cdot incident_{proximity}(t)) \tag{16}$$

3.5 Indicator 7.4: Flight Response Avoidance

Definition: Avoidance behaviors under stress leading to security task abandonment.

Mathematical Model:

The flight response probability:

$$P_{flight}(S, A, E) = \frac{e^{\alpha \cdot S + \beta \cdot A}}{1 + e^{\alpha \cdot S + \beta \cdot A}} \cdot (1 - E) \tag{17}$$

where S is stress level, A is trait anxiety, and E is environmental constraint.

Avoidance Metrics: Task abandonment rate:

$$TAR(t) = \frac{N_{abandoned}(t)}{N_{initiated}(t)} \tag{18}$$

Session termination acceleration:

$$STA(t) = \frac{T_{baseline} - T_{session}(t)}{T_{baseline}} \tag{19}$$

Avoidance Index:

$$AI(t) = w_1 \cdot TAR(t) + w_2 \cdot STA(t) + w_3 \cdot delay_{response}(t) \tag{20}$$

Detection Threshold:

$$R_{7.4}(t) = \begin{cases} 1 & \text{if } P_{flight}(t) > 0.7 \text{ and } AI(t) > 0.5 \\ 0 & \text{otherwise} \end{cases} \tag{21}$$

3.6 Indicator 7.5: Freeze Response Paralysis

Definition: Decision paralysis under stress preventing appropriate security responses.

Mathematical Model:

The freeze response using decision latency modeling:

$$P_{freeze}(S, U, O) = \frac{1}{1 + e^{-(\alpha \cdot S + \beta \cdot U - \gamma \cdot O)}} \tag{22}$$

where S is stress level, U is uncertainty, and O is available options.

Paralysis Indicators: Decision time extension:

$$DTE(t) = \frac{T_{decision}(t) - T_{baseline}}{T_{baseline}} \tag{23}$$

Action frequency reduction:

$$AFR(t) = 1 - \frac{A_{current}(t)}{A_{baseline}} \tag{24}$$

Paralysis Index:

$$PI(t) = \sqrt{DTE(t)^2 + AFR(t)^2} \cdot P_{freeze}(t) \tag{25}$$

Detection Function:

$$D_{7.5}(t) = PI(t) \cdot (1 + \epsilon \cdot criticality(t)) \tag{26}$$

3.7 Indicator 7.6: Fawn Response Overcompliance

Definition: Submissive overcompliance under stress reducing security scrutiny.

Mathematical Model:

The fawn response probability:

$$P_{fawn}(S, H, D) = \sigma(\alpha \cdot S + \beta \cdot H + \gamma \cdot D) \tag{27}$$

where S is stress level, H is hierarchy position, and D is dependency level.

Overcompliance Metrics: Approval seeking frequency:

$$ASF(t) = \frac{N_{approval\_requests}(t)}{N_{decisions}(t)} \tag{28}$$

Authority deference increase:

$$ADI(t) = \frac{compliance_{current}(t)}{compliance_{baseline}} - 1 \tag{29}$$

Fawn Index:

$$FI(t) = P_{fawn}(t) \cdot (w_1 \cdot ASF(t) + w_2 \cdot ADI(t)) \tag{30}$$

Security Risk Model:

$$SR_{fawn}(t) = FI(t) \cdot (1 - verification_{rate}(t)) \tag{31}$$

3.8 Indicator 7.7: Stress-Induced Tunnel Vision

Definition: Attentional narrowing under stress missing security-relevant information.

Mathematical Model:

The attention narrowing function following Easterbrook's cue utilization theory:

$$A_{width}(S) = A_{max} \cdot e^{-\lambda \cdot S^2} \tag{32}$$

where A_{max} is maximum attention span and λ controls narrowing rate.

Tunnel Vision Metrics: Peripheral detection rate:

$$PDR(t) = \frac{N_{peripheral\_detected}(t)}{N_{peripheral\_present}(t)} \tag{33}$$

Context switching frequency:

$$CSF(t) = \frac{N_{context\_switches}(t)}{T_{session}(t)} \tag{34}$$

Tunnel Vision Index:

$$TVI(t) = (1 - PDR(t)) \cdot e^{-\alpha \cdot CSF(t)} \cdot f(A_{width}(S(t))) \tag{35}$$

where $f(A_{width}) = 1 - \tanh(\beta \cdot A_{width})$.

Detection Function:

$$D_{7.7}(t) = TVI(t) \cdot (1 + \gamma \cdot threat_{level}(t)) \tag{36}$$

3.9 Indicator 7.8: Cortisol-Impaired Memory

Definition: Stress hormone effects on memory formation and retrieval affecting security procedures.

Mathematical Model:

The cortisol-memory impairment function:

$$MI(C) = \begin{cases} 0 & \text{if } C < C_{threshold} \\ \alpha \cdot (C - C_{threshold})^{\beta} & \text{if } C \geq C_{threshold} \end{cases} \tag{37}$$

where C represents cortisol level (estimated from behavioral proxies).

Memory Performance Proxies: Password error rate increase:

$$PERI(t) = \frac{errors_{password}(t)}{attempts_{password}(t)} - baseline_{error} \tag{38}$$

Procedure deviation frequency:

$$PDF(t) = \frac{N_{deviations}(t)}{N_{procedures}(t)} \tag{39}$$

Memory Impairment Index:

$$MII(t) = w_1 \cdot PERI(t) + w_2 \cdot PDF(t) + w_3 \cdot recall_{failures}(t) \tag{40}$$

Cortisol Estimation:

$$\hat{C}(t) = \sum_i w_i \cdot proxy_i(t) \tag{41}$$

with proxies including stress indicators, time-of-day, and workload measures.

3.10 Indicator 7.9: Stress Contagion Cascades

Definition: Organizational stress propagation creating collective vulnerability states.

Mathematical Model:

The stress contagion model using network dynamics:

$$\frac{dS_i}{dt} = -\lambda_i S_i + \sum_j \alpha_{ij} \cdot S_j \cdot (1 - S_i) + \beta_i \cdot E_i(t) \tag{42}$$

where S_i is stress level of individual i, α_{ij} is contagion rate from j to i, and $E_i(t)$ represents external stressors.

Network Contagion Metrics: Stress correlation coefficient:

$$SCC(t) = \frac{\text{Cov}(S_i(t), S_j(t))}{\sqrt{\text{Var}(S_i(t)) \cdot \text{Var}(S_j(t))}} \tag{43}$$

Cascade propagation rate:

$$CPR(t) = \frac{d}{dt}\left(\sum_i I_{stressed}(i,t)\right) \tag{44}$$

Contagion Index:

$$CI(t) = SCC(t) \cdot CPR(t) \cdot \sqrt{density(network)} \tag{45}$$

Critical Threshold:

$$R_{7.9}(t) = \begin{cases} 1 & \text{if } CI(t) > \theta_{cascade} \text{ and } \%_{stressed} > 0.3 \\ 0 & \text{otherwise} \end{cases} \tag{46}$$

3.11 Indicator 7.10: Recovery Period Vulnerabilities

Definition: Continued vulnerability during post-stress recovery phases.

Mathematical Model:

The recovery function following bi-exponential decay:

$$R(t) = A \cdot e^{-t/\tau_{fast}} + B \cdot e^{-t/\tau_{slow}} \tag{47}$$

where τ_{fast} and τ_{slow} represent fast and slow recovery time constants.

Recovery State Estimation: Cognitive performance restoration:

$$CPR(t) = 1 - \left(\frac{P_{baseline} - P(t)}{P_{baseline} - P_{minimum}} \right) \tag{48}$$

Vigilance level recovery:

$$VLR(t) = \frac{V(t) - V_{minimum}}{V_{baseline} - V_{minimum}} \tag{49}$$

Recovery Vulnerability Index:

$$RVI(t) = (1 - R(t)) \cdot \left(\frac{1}{1 + e^{\alpha \cdot (CPR(t) - 0.5)}} \right) \tag{50}$$

Vulnerability Window:

$$VW(t) = \begin{cases} 1 & \text{if } RVI(t) > 0.3 \text{ and } t_{post\_stress} < 3\tau_{slow} \\ 0 & \text{otherwise} \end{cases} \tag{51}$$

4 Interdependency Matrix

The stress response indicators exhibit significant interdependencies captured through the correlation matrix $\mathbf{R}_7$:

$$\mathbf{R}_7 = \begin{pmatrix} 1.00 & 0.75 & 0.45 & 0.50 & 0.55 & 0.40 & 0.70 & 0.80 & 0.60 & 0.65 \\ 0.75 & 1.00 & 0.35 & 0.40 & 0.45 & 0.30 & 0.55 & 0.70 & 0.85 & 0.90 \\ 0.45 & 0.35 & 1.00 & -0.60 & -0.70 & 0.25 & 0.40 & 0.50 & 0.30 & 0.20 \\ 0.50 & 0.40 & -0.60 & 1.00 & 0.30 & 0.80 & 0.35 & 0.45 & 0.40 & 0.35 \\ 0.55 & 0.45 & -0.70 & 0.30 & 1.00 & 0.20 & 0.60 & 0.65 & 0.40 & 0.45 \\ 0.40 & 0.30 & 0.25 & 0.80 & 0.20 & 1.00 & 0.25 & 0.35 & 0.30 & 0.25 \\ 0.70 & 0.55 & 0.40 & 0.35 & 0.60 & 0.25 & 1.00 & 0.75 & 0.50 & 0.55 \\ 0.80 & 0.70 & 0.50 & 0.45 & 0.65 & 0.35 & 0.75 & 1.00 & 0.60 & 0.70 \\ 0.60 & 0.85 & 0.30 & 0.40 & 0.40 & 0.30 & 0.50 & 0.60 & 1.00 & 0.80 \\ 0.65 & 0.90 & 0.20 & 0.35 & 0.45 & 0.25 & 0.55 & 0.70 & 0.80 & 1.00 \end{pmatrix} \tag{52}$$

Key interdependencies include:

- Very strong correlation (0.90) between Chronic Stress Burnout (7.2) and Recovery Period Vulnerabilities (7.10)
- Strong correlation (0.85) between Chronic Stress Burnout (7.2) and Stress Contagion Cascades (7.9)
- High correlation (0.80) between Acute Stress Impairment (7.1) and Cortisol-Impaired Memory (7.8)
- Notable negative correlation (-0.70) between Fight Response (7.3) and Freeze Response (7.5)
- Strong correlation (0.80) between Flight Response Avoidance (7.4) and Fawn Response Overcompliance (7.6)

5 Implementation Algorithms

Algorithm 1 Stress Response Vulnerability Assessment

Initialize baseline parameters $\boldsymbol{\mu}, \boldsymbol{\Sigma}, \boldsymbol{w}$, stress thresholds
Initialize stress history buffer and contagion network
for each time step t **do**
  Collect behavioral and physiological proxy data $\mathbf{x}(t)$
  Estimate current stress levels $S(t)$ using multi-modal fusion
  Update allostatic load $AL(t)$ using exponential integration
  for each indicator $i \in \{7.1, 7.2, \ldots, 7.10\}$ **do**
    Compute stress state $S_i(t)$ using indicator-specific models
    Compute cognitive impairment $C_i(t)$ based on stress level
    Compute behavioral deviation $B_i(t)$ from baseline patterns
    Compute recovery state $R_i(t)$ using bi-exponential decay
    Calculate $D_i(t) = w_1 S_i(t) + w_2 C_i(t) + w_3 B_i(t) + w_4 R_i(t)$
    Update temporal state with stress-modified decay
  end for
  Update stress contagion network dynamics
  Compute interdependency corrections using $\mathbf{R}_7$
  Generate alerts based on dynamic stress-adjusted thresholds
  Update baseline parameters and stress models
  Log results for validation and drift detection
end for

6 Validation Framework

Each stress response indicator undergoes continuous validation through multiple metrics adapted for stress-related phenomena:

Classification Metrics:

$$Precision = \frac{TP}{TP + FP} \tag{53}$$

$$Recall = \frac{TP}{TP + FN} \tag{54}$$

$$F_1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall} \tag{55}$$

Temporal Validation with Stress Cycles: Stress-aware drift detection using Kolmogorov-Smirnov test with temporal stratification:

$$D_{KS}^{stress} = \max_x |F_{high\_stress}(x) - F_{low\_stress}(x)| \tag{56}$$

Physiological Correlation Validation: When available, correlation with physiological stress markers:

$$\rho_{physio} = \frac{\text{Cov}(\hat{S}(t), S_{physio}(t))}{\sqrt{\text{Var}(\hat{S}(t)) \cdot \text{Var}(S_{physio}(t))}} \tag{57}$$

Stress Prediction Accuracy: For predictive models, using Mean Absolute Error:

$$MAE_{stress} = \frac{1}{n} \sum_{i=1}^{n} |S_{predicted}(i) - S_{actual}(i)| \tag{58}$$

Contagion Model Validation: Network-based validation using epidemic model metrics:

$$R_0 = \frac{\lambda}{\gamma} \cdot \langle k \rangle \tag{59}$$

where λ is transmission rate, γ is recovery rate, and $\langle k \rangle$ is average network connectivity.

7 Conclusion

This mathematical formalization of stress response vulnerabilities provides rigorous foundation for CPF Category 7 implementation. Each indicator receives explicit detection functions that account for the complex physiological and behavioral manifestations of stress while maintaining computational efficiency for real-time operation.

The interdependency matrix captures important correlations between stress-related vulnerabilities, enabling enhanced detection through multivariate analysis that accounts for the systemic nature of organizational stress. Implementation algorithms provide clear guidance for system integration, while validation frameworks ensure sustained accuracy across different stress conditions.

Future work will focus on integrating this stress response framework with other CPF categories, particularly Authority-Based Vulnerabilities (Category 1) and Cognitive Overload Vulnerabilities (Category 5), which show strong theoretical and empirical correlations with stress states. The mathematical rigor enables reproducible research, standardized implementations, and objective validation of stress-based vulnerability assessment.

The stress response vulnerability category serves as a critical foundation for understanding how physiological and psychological stress states create systematic security blind spots. By formalizing these stress-security mechanisms mathematically, we enable automated detection and mitigation of vulnerabilities that have historically been addressed only through reactive incident response rather than predictive stress management.

References

[1] Canale, G. (2024). The Cybersecurity Psychology Framework: A Pre-Cognitive Vulnerability Assessment Model Integrating Psychoanalytic and Cognitive Sciences. *Preprint*.

[2] Selye, H. (1956). *The Stress of Life*. McGraw-Hill.

[3] McEwen, B. S. (2007). Physiology and neurobiology of stress and adaptation: Central role of the brain. *Physiological Reviews*, 87(3), 873-904.

[4] Sapolsky, R. M. (2004). *Why Zebras Don't Get Ulcers*. Times Books.

[5] Lupien, S. J., McEwen, B. S., Gunnar, M. R., & Heim, C. (2009). Effects of stress throughout the lifespan on the brain, behaviour and cognition. *Nature Reviews Neuroscience*, 10(6), 434-445.

[6] Easterbrook, J. A. (1959). The effect of emotion on cue utilization and the organization of behavior. *Psychological Review*, 66(3), 183-201.

[7] Baumeister, R. F., Vohs, K. D., & Tice, D. M. (2007). The strength model of self-control. *Current Directions in Psychological Science*, 16(6), 351-355.