Appendix C: Proofs of Safety Meta-Properties

In this appendix we include the details of the proofs of the meta-properties of the basic properties. These meta-properties are proved for each property in the context of the three composite system structures: product, cascade, and feedback. Where the proof is straightforward or essentially the same as another proof, we omit the details of the proof, indicating only the major steps of the proof.

$\Phi^{i+j} = \Phi^{i} \cup \Phi^{j}$

$\Phi^{i+j}(i(A),j(A)) = \Phi^{i+j}(i(A)) \cap \Phi^{i+j}(j(A)) = \Phi^{i}(A) \cap \Phi^{j}(A) = \Phi^{i+j}(A)$

C.1 Authenticity

$AU \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{Fma}\{\Phi(i)\} \cdot \sigma\{\mathbf{i}\}(out) \models_x A$

$AU\text{-}E \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{Fma}\{\Phi(\mathcal{E})\} \cdot \sigma\{\mathcal{E}\}(out) \models_x A$

C.1.1 Reflexivity

Examine the reflexivity of authenticity at an arbitrary component.

$\mathbf{sat}(C_i, AU)$

$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A : \mathcal{Fma}\{\Phi(i(A,out))\} \cdot \sigma(i;\mathcal{E})(out) \models_x A$

Let at least one occurrence of ($out^i \rightarrow$ environs) be replaced by ($out^i \rightarrow in^i$)

$= \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{Fma}\{\Phi(i(A,out))\} \cdot \sigma(i;\mathcal{E}+i)(out) \models_x A$

If $\Phi(i(A,out) = \Phi(i(A,in,out)$ then

$\Rightarrow \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{Fma}\{\Phi(i(A,in,out))\} \cdot \sigma(i;\mathcal{E}+i)(out) \models_x A$

$\Rightarrow \mathbf{sat}(C_i^R, AU)$

If $\Phi(i(A,out) \neq \Phi(i(A,in,out)$ then it is possible that an unacceptable event received as an input from the output of that component will in turn cause an unacceptable, unknown output.

$\not\Rightarrow \mathbf{sat}(C_i^R, AU)$

The reflexivity of authenticity for the environment is a non-sequiter as it implies that the environment is connected to itself and removed from the components. The authenticity of the environment is therefore not affected by the reflexive connection of a component with itself.

C.1.2 Transitivity

<u>Product Composition</u>

$\mathbf{sat}(\&^P(C_i, C_j), AU) \wedge \mathbf{sat}(\&^P(C_j, C_k), AU)$

$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbf{N} \cdot \exists A_1, A_2 : \mathcal{Fma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$

$\exists B_1, B_2 : \mathcal{Fma}\{\Phi^{j+k}(j(A),k(A))\} \cdot \sigma(i;\mathcal{E})(out) \models_x A_1 \wedge \sigma(j;\mathcal{E})(out) \models_x A_2$

$\wedge\, \sigma(j;\mathcal{E})(out) \models_x B_1 \wedge \sigma(k;\mathcal{E})(out) \models_x B_2$

If $\Phi^{i+j}(i(A),j(A)) = \Phi^{j+k}(j(A),k(A)) = \Phi^{i+k}(i(A),k(A))$ then

$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,k : \mathbf{N} \cdot \exists X_1, X_2 : \mathcal{Fma}\{\Phi^{i+k}(i(A),k(A))\} \cdot$

$\sigma(i;\mathcal{E})(out) \models_x X_1 \wedge \sigma(k;\mathcal{E})(out) \models_x X_2$

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_k), AU)$

Otherwise

$$\not\Rightarrow \mathbf{sat}(\mathbf{\&}^{P}(C_i, C_k), AU)$$

<u>Cascade Composition</u>

$$\mathbf{sat}(\mathbf{\&}^{C}(C_i, C_j), AU) \wedge \mathbf{sat}(\mathbf{\&}^{C}(C_j, C_k), AU)$$

$$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}\mathit{ma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$$

$$\exists B_1, B_2 : \mathcal{F}\mathit{ma}\{\Phi^{j+k}(j(A),k(A))\} \cdot \sigma(i;\text{Ɇ}+j)(out) \models_x A_1 \wedge \sigma(j;\text{Ɇ})(out) \models_x A_2$$

$$\wedge\, \sigma(j;\text{Ɇ}+k)(out) \models_x B_1 \wedge \sigma(k;\text{Ɇ})(out) \models_x B_2$$

Let all occurrences of ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow in^k$), and ($out^j \rightarrow in^k$) be replaced by ($out^j \rightarrow$ environs).

$$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}\mathit{ma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$$

$$\exists B_1, B_2 : \mathcal{F}\mathit{ma}\{\Phi^{j+k}(j(A),k(A))\} \cdot \sigma(i;\text{Ɇ}+k)(out) \models_x A_1 \wedge \sigma(j;\text{Ɇ})(out) \models_x A_2$$

$$\wedge\, \sigma(j;\text{Ɇ})(out) \models_x B_1 \wedge \sigma(k;\text{Ɇ})(out) \models_x B_2$$

If $\Phi^{i+j}(i(A),j(A)) = \Phi^{j+k}(j(A),k(A)) = \Phi^{i+k}(i(A),k(A))$ then

$$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists X_1, X_2 : \mathcal{F}\mathit{ma}\{\Phi^{i+k}(i(A),k(A))\} \cdot$$

$$\sigma(i;\text{Ɇ}+k)(out) \models_x X_1 \wedge \sigma(k;\text{Ɇ})(out) \models_x X_2$$

$$\Rightarrow \mathbf{sat}(\mathbf{\&}^{C}(C_i, C_k), AU)$$

Otherwise

$$\not\Rightarrow \mathbf{sat}(\mathbf{\&}^{C}(C_i, C_k), AU)$$

<u>Feedback Composition</u>

$$\mathbf{sat}(\mathbf{\&}^{F}(C_i, C_j), AU) \wedge \mathbf{sat}(\mathbf{\&}^{F}(C_j, C_k), AU)$$

$$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}\mathit{ma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$$

$$\exists B_1, B_2 : \mathcal{F}\mathit{ma}\{\Phi^{j+k}(j(A),k(A))\} \cdot \sigma(i;\text{Ɇ}+j)(out) \models_x A_1 \wedge \sigma(j;\text{Ɇ}+i)(out) \models_x A_2$$

$$\wedge\, \sigma(j;\text{Ɇ}+k)(out) \models_x B_1 \wedge \sigma(k;\text{Ɇ}+j)(out) \models_x A_2$$

$$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists A_1, A_2, A_3, A_4 : \mathcal{F}\mathit{ma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$$

$$\exists B_1, B_2, B_3, B_4 : \mathcal{F}\mathit{ma}\{\Phi^{j+k}(j(A),k(A))\} \cdot$$

$$\sigma(i;\text{Ɇ})(out) \models_x A_1 \wedge \sigma(i;j)(out) \models_x A_3 \wedge \sigma(j;\text{Ɇ})(out) \models_x A_2 \wedge \sigma(j;i)(out) \models_x A_4$$

$$\wedge\, \sigma(j;\text{Ɇ})(out) \models_x B_1 \wedge \sigma(j;k)(out) \models_x B_3$$

$$\wedge\, \sigma(k;\text{Ɇ})(out) \models_x B_2 \wedge \sigma(k;j)(out) \models_x B_4$$

Let all occurrences of ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow in^k$), ($out^j \rightarrow in^i$) be replaced by ($out^k \rightarrow in^i$), ($out^j \rightarrow in^k$) be replaced by ($out^i \rightarrow in^k$), ($out^k \rightarrow in^j$) be replaced by ($out^k \rightarrow in^i$)

$$= \forall x : \mathbb{N} \cdot \forall i,j,k : \mathbb{N} \cdot \exists A_1, A_2, A_3, A_4 : \mathcal{F}\mathit{ma}\{\Phi^{i+j}(i(A),j(A))\} \cdot$$

$$\exists B_1, B_2, B_3, B_4 : \mathcal{F}\mathit{ma}\{\Phi^{j+k}(j(A),k(A))\} \cdot$$

$$\sigma(i;\text{Ɇ})(out) \models_x A_1 \wedge \sigma(i;k)(out) \models_x A_3 \wedge \sigma(j;\text{Ɇ})(out) \models_x A_2 \wedge \sigma(k;i)(out) \models_x A_4$$

$$\wedge\, \sigma(j;\text{Ɇ})(out) \models_x B_1 \wedge \sigma(i;k)(out) \models_x B_3$$

$$\wedge\, \sigma(k;\text{Ɇ})(out) \models_x B_2 \wedge \sigma(k;i)(out) \models_x B_4$$

If $\Phi^{i+j}(i(A),j(A)) = \Phi^{j+k}(j(A),k(A)) = \Phi^{i+k}(i(A),k(A))$ then

$$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,k : \mathbb{N} \cdot \exists X_1, X_2, X_3, X_4 : \mathcal{F}ma\{\Phi^{i+k}(i(A),k(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x X_1 \wedge \sigma(i;k)(out) \models_x X_3$$
$$\wedge\, \sigma(k;\mathbb{E})(out) \models_x X_2 \wedge \sigma(k;i)(out) \models_x X_4$$
$$= \forall x : \mathbb{N} \cdot \forall i,k : \mathbb{N} \cdot \exists X_1, X_2 : \mathcal{F}ma\{\Phi^{i+k}(i(A),k(A))\} \cdot$$
$$\sigma(i;\mathbb{E}+k)(out) \models_x X_1 \wedge \sigma(k;\mathbb{E}+i)(out) \models_x X_2$$
$$\Rightarrow \mathbf{sat}(\&^F(C_i, C_k), AU)$$

Otherwise

$$\not\Rightarrow \mathbf{sat}(\&^F(C_i, C_k), AU)$$

C.1.3 Symmetry

Product Composition

$$\mathbf{sat}(\&^P(C_i, C_j), AU)$$
$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x A_1 \wedge \sigma(j;\mathbb{E})(out) \models_x A_2$$
$$= \mathbf{sat}(\&^P(C_j, C_i), AU)$$

Cascade Composition

$$\mathbf{sat}(\&^C(C_i, C_j), AU)$$
$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;\mathbb{E}+j)(out) \models_x A_1 \wedge \sigma(j;\mathbb{E})(out) \models_x A_2$$

Let the connections ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow$ environs) and at least one occurrence of ($out^j \rightarrow$ environs) be replaced by ($out^j \rightarrow in^i$).

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists A_1, A_2 : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x A_1 \wedge \sigma(j;\mathbb{E}+i)(out) \models_x A_2$$
$$\Rightarrow \mathbf{sat}(\&^C(C_j, C_i), AU)$$

C.1.4 Closure

$$\mathbf{sat}(C_i, AU) \wedge \mathbf{sat}(C_j, AU)$$
$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : Fma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{N}+\mathbb{E})(out) \models_x A \wedge \sigma(j;\mathbb{N}+\mathbb{E})(out) \models_x B$$

Product Composition

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : \mathcal{F}ma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x A \wedge \sigma(j;\mathbb{E})(out) \models_x B$$

If $\Phi^i(i(A)) = \Phi^j(j(A))$ then

$$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,j : \mathbb{N} \cdot \exists X_1, X_2 : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x X_1 \wedge \sigma(j;\mathbb{E})(out) \models_x X_2$$
$$\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), AU)$$

Otherwise

$$\not\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), AU)$$

Cascade Composition

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : \mathcal{F}ma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x A \wedge \sigma(j;\mathbb{E})(out) \models_x B$$

Let at least one connection ($out^i \rightarrow$ environs) be replaced by ($out^i \rightarrow in^j$).

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : \mathcal{F}ma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{E}+j)(out) \models_x A \wedge \sigma(j;\mathbb{E})(out) \models_x B$$

If $\Phi^i(i(A)) = \Phi^j(j(A))$ then

$$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A,B : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;j+\mathbb{E})(out) \models_x A \wedge \sigma(j;\mathbb{E})(out) \models_x B$$
$$\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), AU)$$

Otherwise

$$\nRightarrow \mathbf{sat}(\&^C(C_i, C_j), AU)$$

Feedback Composition

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : \mathcal{F}ma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{E})(out) \models_x A \wedge \sigma(j;\mathbb{E})(out) \models_x B$$

Let at least one connection ($out^i \rightarrow$ environs) be replaced by ($out^i \rightarrow in^j$) and let at least one connection ($out^j \rightarrow$ environs) be replaced by ($out^j \rightarrow in^i$) .

$$= \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi^i(i(A))\} \cdot \exists B : \mathcal{F}ma\{\Phi^j(j(A))\} \cdot$$
$$\sigma(i;\mathbb{E}+j)(out) \models_x A \wedge \sigma(j;\mathbb{E}+i)(out) \models_x B$$

If $\Phi^i(i(A)) = \Phi^j(j(A))$ then

$$\Rightarrow \forall x : \mathbb{N} \cdot \forall i,j : \mathbf{N} \cdot \exists A,B : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A))\} \cdot$$
$$\sigma(i;j+\mathbb{E})(out) \models_x A \wedge \sigma(j;i+\mathbb{E})(out) \models_x B$$
$$\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), AU)$$

Otherwise

$$\nRightarrow \mathbf{sat}(\&^F(C_i, C_j), AU)$$

C.2 Pessimistic Confidentiality and Integrity

$$PC \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi(\mathbf{N}(A),obs) \cup \Phi(\mathbf{N},mod)\} \cdot \sigma(\mathbf{N}+\mathbb{E};i)(in) \models_x A$$
$$PI \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi(\mathbf{N},obs) \cup \Phi(\mathbf{N}(A),mod)\} \cdot \sigma(\mathbf{N}+\mathbb{E};i)(in) \models_x A$$

C.2.1 Reflexivity

$$\mathbf{sat}(C_i, PC)$$
$$= \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A : \mathcal{F}ma\{\Phi(i(A),obs) \cup \Phi(i,mod)\} \cdot \sigma(\mathbb{E};i)(in) \models_x A$$

Following the same reasoning as with authenticity, if $\Phi(i(A,out),obs) \subseteq \Phi(i(A),obs)$ then all outputs of a component are acceptable as inputs to that component.

$$\Rightarrow \mathbf{sat}(C_i^R, PC)$$

Otherwise,

$$\nRightarrow \mathbf{sat}(C_i^R, PC)$$

The (ir)reflexivity of pessimistic integrity immediately follows, as the (obs, mod) dual of the reflexivity of pessimistic confidentiality.

C.2.2 Transitivity

Product Composition

$\mathbf{sat}(\&^P(C_i, C_j),PI) \wedge \mathbf{sat}(\&^P(C_j, C_k),PI)$

If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_k),PI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^P(C_i, C_k),PI)$

Cascade Composition

$\mathbf{sat}(\&^C(C_i, C_j),PI) \wedge \mathbf{sat}(\&^C(C_j, C_k),PI)$

Let all occurrences of $(out^i \rightarrow in^j)$ be replaced by $(out^i \rightarrow in^k)$, and $(out^j \rightarrow in^k)$ be replaced by $(out^j \rightarrow environs)$. If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_k),PI)$

Otherwise,

$\not\Rightarrow \mathbf{sat}(\&^C(C_i, C_k),PI)$

Feedback Composition

$\mathbf{sat}(\&^F(C_i, C_j),PI) \wedge \mathbf{sat}(\&^F(C_j, C_k),PI)$

Let all occurrences of $(out^i \rightarrow in^j)$ be replaced by $(out^i \rightarrow in^k)$, $(out^j \rightarrow in^i)$ by $(out^k \rightarrow in^i)$, $(out^j \rightarrow in^k)$ by $(out^i \rightarrow in^k)$, $(out^k \rightarrow in^j)$ by $(out^k \rightarrow in^i)$. If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^F(C_i, C_k),PI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^F(C_i, C_k),PI)$

The (in)transitivity of pessimistic confidentiality immediately follows, as the (obs, mod) dual of the transitivity of pessimistic integrity.

C.2.3 Symmetry

Product Composition

$\mathbf{sat}(\&^P(C_i, C_j),PC)$

$= \forall x : \mathbb{N} \cdot \forall i : \{i,j\} \cdot \exists A,B : \mathcal{F}ma\{\Phi^{i+j}(i(A),j(A),obs) \cup \Phi^{i+j}(i,j,mod)\} \cdot$
$\sigma(\mathcal{E};i)(in) \models_x A \wedge \sigma(\mathcal{E};j)(in) \models_x B$

$\Rightarrow \mathbf{sat}(\&^P(C_j, C_i),PC)$

Cascade Composition

$\mathbf{sat}(\&^P(C_i, C_j),PI)$

$= \forall x : \mathbb{N} \cdot \forall i : \{i,j\} \cdot \exists A,B : \mathcal{F}ma\ \{\Phi^{i+j}(i(A),j(A),obs) \cup \Phi^{i+j}(i,j,mod)\} \cdot$
$\sigma(\mathcal{E};i)(in) \models_x A \wedge \sigma(i{+}\mathcal{E};j)(in) \models_x B$

Let the connections $(out^i \rightarrow in^j)$ be replaced by $(out^i \rightarrow environs)$ and at least one occurrence of $(out^j \rightarrow environs)$ be replaced by $(out^j \rightarrow in^i)$.

$= \forall x : \mathbb{N} \cdot \forall i : \{i,j\} \cdot \exists A,B : \mathcal{F}ma \; \{\Phi^{i+j}(i(A),j(A),obs) \cup \Phi^{i+j}(i,j,mod)\} \cdot$
$\sigma(j^{+}\mathcal{E};i)(in) \models_x A \wedge \sigma(\mathcal{E};j)(in) \models_x B$

By definition, the output events produced by component **j** are defined as $\Phi^{i+j}(j(A,out))$. If $\Phi^{i+j}(j(A,out)) \subset \{\Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod)\}$ then

$\Rightarrow \mathbf{sat}(\&^P(C_j, C_i),PC)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^P(C_j, C_i),PC)$

The (a)symmetry of pessimistic integrity immediately follows, as the (obs,mod) dual of the symmetry of pessimistic confidentiality.

C.2.4 Closure

$\mathbf{sat}(C_i, PI) \wedge \mathbf{sat}(C_j, PI)$

$= \forall x : \mathbb{N} \cdot \forall i : \{i,j\} \cdot \exists A : \mathcal{F}ma \; \{\Phi^{i}(i(A),obs) \cup \Phi^{i}(i,mod)\} \cdot$
$\exists B : Fma \; \{\Phi^{j}(j(A),obs) \cup \Phi^{j}(j,mod)\} \cdot$
$\sigma(\mathcal{E};i)(in) \models_x A \wedge \sigma(\mathcal{E};j)(in) \models_x B$

Product Composition

If $\Phi^{i}(i,obs) = \Phi^{j}(j,obs)$ and $\Phi^{i}(i(A),mod) = \Phi^{j}(j(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), PI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), PI)$

Cascade Composition

If $\Phi^{i}(i,obs) = \Phi^{j}(j,obs)$ and $\Phi^{i}(i(A),mod) = \Phi^{j}(j(A),mod)$ and
$\Phi^{i+j}(j(A,out)) \subset \{\Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod)\}$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), PI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), PI)$

Feedback Composition

If $\Phi^{i}(i,obs) = \Phi^{j}(j,obs)$ and $\Phi^{i}(i(A),mod) = \Phi^{j}(j(A),mod)$ and
$\Phi^{i+j}(j(A,out)) \subset \{\Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod)\}$ and
$\Phi^{i+j}(i(A,out)) \subset \{\Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod)\}$ then

$\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), PI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), PI)$

The closure properties pessimistic confidentiality immediately follow as the (obs, mod) dual of the transitivity of pessimistic integrity.

C.3 Environment Optimistic Confidentiality and Integrity

$EOC \equiv \forall x : \mathbb{N} \cdot \forall i : \mathcal{N} \cdot$

$\quad \exists A : \mathcal{F}ma\{\Phi(\mathcal{N}(A),obs) \cup \Phi(\mathcal{N},mod)\} \cdot \exists B : \mathcal{F}ma\{\Phi(i,obs) \cup \Phi(i,mod)\} \cdot$

$\quad A,B \in \mathcal{F}ma\{\Phi(i(A),obs) \cup \Phi(i,mod)\} \wedge \sigma(\mathcal{N};i)(in) \models_x A \wedge \sigma(\mathcal{E};i)(in) \models_x B$

$EOI \equiv \forall x : \mathbb{N} \cdot \forall i : \mathcal{N} \cdot$

$\quad \exists A : \mathcal{F}ma\{\Phi(\mathcal{N},obs) \cup \Phi(\mathcal{N}(A),mod)\} \cdot \exists B : \mathcal{F}ma\{\Phi(i,obs) \cup \Phi(i,mod)\} \cdot$

$\quad A,B \in \mathcal{F}ma\{\Phi(i,obs) \cup \Phi(i(A),mod)\} \wedge \sigma(\mathcal{N};i)(in) \models_x A \wedge \sigma(\mathcal{E};i)(in) \models_x B$

C.3.1 Reflexivity

$\quad \mathbf{sat}(C_i, EOC)$

$\quad = \forall x : \mathbb{N} \cdot \forall i : \mathcal{N} \cdot \exists B : \mathcal{F}ma\{\Phi(i,obs) \cup \Phi(i,mod)\} \cdot$

$\quad\quad B \in \mathcal{F}ma\{\Phi(i(A),obs) \cup \Phi(i,mod)\} \wedge \sigma(\mathcal{E};i)(in) \models_x B$

Followign the same arguement as with pessimistic confidentiality

$\quad \not\Rightarrow \mathbf{sat}(C_i^R, PC)$

The reflexivity of environment optimistic integrity immediately follows, as the (obs, mod) dual of the reflexivity of environment optimistic confidentiality.

C.3.2 Transitivity

Product Composition

$\mathbf{sat}(\&^P(C_i, C_j),EOI) \wedge \mathbf{sat}(\&^P(C_j, C_k),EOI)$

If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ and environment trusted not to send unacceptable events to **k** then

$\quad \Rightarrow \forall x : \mathbb{N} \cdot \forall i : \{i,j\} \cdot \exists X_1 : \mathcal{F}ma\{\Phi^{i+k}(i,obs) \cup \Phi^{i+k}(i,mod)\} \cdot$

$\quad\quad \exists X_2 : \mathcal{F}ma\{\Phi^{i+k}(k,obs) \cup \Phi^{i+k}(k,mod)\} \cdot$

$\quad\quad X_1 : \in \mathcal{F}ma\{\Phi^{i+k}(i,obs) \cup \Phi^{i+k}(i(A),mod)\} \wedge \sigma(\mathcal{E};i)(in) \models_x X_1$

$\quad\quad \wedge X_2 \in \mathcal{F}ma\{\Phi^{i+k}(k,obs) \cup \Phi^{i+k}(k(A),mod)\} \wedge \sigma(\mathcal{E};k)(in) \models_x X_2$

$\quad \Rightarrow \mathbf{sat}(\&^P(C_i, C_k),EOI)$

Otherwise

$\quad \not\Rightarrow \mathbf{sat}(\&^P(C_i, C_k),EOI)$

Cascade Composition

$\mathbf{sat}(\&^C(C_i, C_j),EOI) \wedge \mathbf{sat}(\&^C(C_j, C_k),EOI)$

As with product composition, if $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ and $\Phi^{i}(i(A,out)) \subset \{\Phi^{i+k}(i(A),k(A),mod) \cup \Phi^{i+k}(i,k,mod)\}$ and environment trusted not to send unacceptable events to **k** then

$\quad \Rightarrow \mathbf{sat}(\&^C(C_i, C_k),EOI)$

Otherwise

$\quad \not\Rightarrow \mathbf{sat}(\&^C(C_i, C_k),EOI)$

Feedback Composition

sat($\&^F(C_i, C_j)$,EOI) $\wedge$ **sat**($\&^F(C_j, C_k)$,EOI)

As with product composition, if Φ^{i+j}(i,j,obs) = Φ^{j+k}(j,k,obs) = Φ^{i+k}(i,k,obs) and Φ^{i+j}(i(A),j(A),mod) = Φ^{j+k}(j(A),k(A),mod) = Φ^{i+k}(i(A),k(A),mod) and environment trusted not to send unacceptable events to **k** then

$\Rightarrow$ **sat**($\&^C(C_i, C_k)$,EOI)

Otherwise

$\nRightarrow$ **sat**($\&^C(C_i, C_k)$,EOI)

The (in)transitivity of pessimistic confidentiality immediately follows, as the (obs, mod) dual of the transitivity of pessimistic integrity.

C.3.3 Symmetry

Product Composition

sat($\&^P(C_i, C_j)$,EOC)

As with pessimistic confidentiality

$\Rightarrow$ **sat**($\&^P(C_j, C_i)$,EOC)

Cascade Composition

sat($\&^C(C_i, C_j)$,EOC)

Let the connections ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow$ environs) and at least one occurrence of ($out^j \rightarrow$ environs) be replaced by ($out^j \rightarrow in^i$). If Φ^i(i(A,out)) $\subset$ { Φ^{i+k}(i(A),k(A),mod) $\cup$ Φ^{i+k}(i,k,mod) } then

$\Rightarrow$ **sat**($\&^C(C_j, C_i)$,EOC)

Otherwise

$\nRightarrow$ **sat**($\&^C(C_j, C_i)$,EOC)

The (a)symmetry of pessimistic integrity immediately follows, as the (obs,mod) dual of the symmetry of pessimistic confidentiality.

C.3.4 Closure

sat(C_i, EOI) $\wedge$ **sat**(C_j, EOI)

$= \forall x : \mathbb{N} \cdot \forall i : \{i\} \cdot \exists A : \mathcal{Fma}\{\Phi^i(i,obs) \cup \Phi^i(i(A),mod)\} \cdot$

$\exists B : \mathcal{Fma}\{\Phi^i(obs) \cup \Phi^i(mod)\} \cdot$

$B \in \mathcal{Fma}\{\Phi^i(i,obs) \cup \Phi^i(i(A),,mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x A \wedge \sigma(\mathbf{E};i)(in) \models_x B$

$\wedge \forall x : \mathbb{N} \cdot \forall j : \{j\} \cdot \exists X : \mathcal{Fma}\{\Phi^j(j,obs) \cup \Phi^j(j(A),mod)\} \cdot$

$\exists \Delta : \mathcal{Fma}\{\Phi^j(obs) \cup \Phi^j(mod)\} \cdot$

$\Delta \in \mathcal{Fma}\{\Phi^j(j,obs) \cup \Phi^j(j(A),mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x X \wedge \sigma(\mathbf{E};i)(in) \models_x \Delta$

Product Composition

sat(C_i, EOI) $\wedge$ **sat**(C_j, EOI)

If Φ^i(i,obs) = Φ^j(j,obs) and Φ^i(i(A),mod) = Φ^j(j(A),mod) and environment trusted not to send unacceptable events to **i** or **j** then

$\Rightarrow$ **sat**($\&^P(C_i, C_j)$, EOI)

Otherwise

$\nRightarrow$ $\mathbf{sat}(\&^P(C_i, C_j), EOI)$

Cascade Composition

$\mathbf{sat}(C_i, EOI) \wedge \mathbf{sat}(C_j, EOI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and $\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ and environment trusted not to send unacceptable events to **i** or **j** then

$\Rightarrow$ $\mathbf{sat}(\&^C(C_i, C_j), EOI)$

Otherwise

$\nRightarrow$ $\mathbf{sat}(\&^C(C_i, C_j), EOI)$

Feedback Composition

$\mathbf{sat}(C_i, EOI) \wedge \mathbf{sat}(C_j, EOI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and

$\Phi^{i+j}(i(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ and

$\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ and environment trusted not to send unacceptable events to **i** or **j** then

$\Rightarrow$ $\mathbf{sat}(\&^F(C_i, C_j), EOI)$

Otherwise

$\nRightarrow$ $\mathbf{sat}(\&^F(C_i, C_j), EOI)$

The closure properties environment optimistic confidentiality immediately follows, as the (obs, mod) dual of the closure properties of environment optimistic integrity.

C.4 Component Optimistic Confidentiality and Integrity

$COC \equiv \forall x : \mathbb{N} \cdot \forall i : \mathcal{N} \cdot \exists A : \mathcal{F}ma\{ \Phi(obs) \cup \Phi(mod)\} \cdot$

$\exists B : \mathcal{F}ma\{\Phi(\mathcal{N}(A),obs) \cup \Phi(\mathcal{N},mod)\} \cdot$

$A \in \mathcal{F}ma\{Fma\{\Phi(i(A),obs) \cup \Phi(mod)\} \wedge \sigma(\mathcal{N};i)(in) \models_x A \wedge \sigma(\mathcal{E};i)(in) \models_x B$

$COI \equiv \forall x : \mathbb{N} \cdot \forall i : \mathcal{N} \cdot \exists A : \mathcal{F}ma\{ \Phi(obs) \cup \Phi(mod)\} \cdot$

$\exists B : \mathcal{F}ma\{\Phi(\mathcal{N},obs) \cup \Phi(\mathcal{N}(A),mod)\} \cdot$

$A \in \mathcal{F}ma\{\Phi(obs) \cup \Phi(i(A),mod)\} \wedge \sigma(\mathcal{N};i)(in) \models_x A \wedge \sigma(\mathcal{E};i)(in) \models_x B$

C.4.1 Reflexivity

$\mathbf{sat}(C_i, COC)$

As with pessimistic confidentiality

$\nRightarrow$ $\mathbf{sat}(C_i^R, COC)$

The (ir)reflexivity of environment optimistic integrity immediately follows, as the (obs, mod) dual of the reflexivity of environment optimistic confidentiality.

C.4.2 Transitivity

Product Composition

$\mathbf{sat}(\&^P(C_i, C_j),COI) \wedge \mathbf{sat}(\&^P(C_j, C_k),COI)$

If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_k),COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^P(C_i, C_k),COI)$

Cascade Composition

$\mathbf{sat}(\&^C(C_i, C_j),COI) \wedge \mathbf{sat}(\&^C(C_j, C_k),COI)$

As with product composition, if $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_k),COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^C(C_i, C_k),COI)$

Feedback Composition

$\mathbf{sat}(\&^F(C_i, C_j),COI) \wedge \mathbf{sat}(\&^F(C_j, C_k),COI)$

As with product composition, if $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_k),COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^C(C_i, C_k),COI)$

The (in)transitivity of pessimistic confidentiality immediately follows, as the (obs, mod) dual of the transitivity of pessimistic integrity.

C.4.3 Symmetry

Product Composition

$\mathbf{sat}(\&^P(C_i, C_j),COC)$

As with symmetry of previous properties,

$\Rightarrow \mathbf{sat}(\&^P(C_j, C_i),COC)$

Cascade Composition

$\mathbf{sat}(\&^C(C_i, C_j),COC)$

Let the connections ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow$ environs) and at least one occurrence of ($out^j \rightarrow$ environs) be replaced by ($out^i \rightarrow in^i$). By definition, the output events produced by component **j** are defined as $\Phi^{i+j}(j(A,out))$.

If $\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^C(C_j, C_i),COC)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^C(C_j, C_i),COC)$

The (a)symmetry of pessimistic integrity immediately follows, as the (obs,mod) dual of the symmetry of pessimistic confidentiality.

C.4.4 Closure

$\mathbf{sat}(C_i, COI) \wedge \mathbf{sat}(C_j, COI)$

$= \forall x : \mathbb{N} \cdot \forall i : \{i\} \cdot \exists A : \mathcal{Fma}\{\Phi^i(obs) \cup \Phi^i(mod)\} \cdot$

$\exists B : \mathcal{Fma}\{\Phi^i(obs) \cup \Phi^i(i(A),mod)\} \cdot$

$A,B \in \mathcal{Fma}\{\Phi^i(iobs) \cup \Phi^i(i(A),mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x A \wedge \sigma(\mathbf{E};i)(in) \models_x B$

$\wedge \forall x : \mathbb{N} \cdot \forall j : \{j\} \cdot \exists X : \mathcal{Fma}\{\Phi^j(obs) \cup \Phi^j(mod)\} \cdot$

$\exists \Delta : \mathcal{Fma}\{\Phi^j(obs) \cup \Phi^j(j(A),mod)\} \cdot$

$X,\Delta \in \mathcal{Fma}\{\Phi^j(j,obs) \cup \Phi^j(j(A),mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x X \wedge \sigma(\mathbf{E};i)(in) \models_x \Delta$

<u>Product Composition</u>

$\mathbf{sat}(C_i, COI) \wedge \mathbf{sat}(C_j, COI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^P(C_i, C_j), COI)$

<u>Cascade Composition</u>

$\mathbf{sat}(C_i, COI) \wedge \mathbf{sat}(C_j, COI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and $\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^C(C_i, C_j), COI)$

<u>Feedback Composition</u>

$\mathbf{sat}(C_i, COI) \wedge \mathbf{sat}(C_j, COI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and $\Phi^{i+j}(i(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ and $\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), COI)$

Otherwise

$\nRightarrow \mathbf{sat}(\&^F(C_i, C_j), COI)$

The closure properties environment optimistic confidentiality immediately follows, as the (obs, mod) dual of the closure properties of environment optimistic integrity.

C.5 Strongly Optimistic Confidentiality and Integrity

$SOC \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A,B : \mathcal{Fma}\{\Phi(obs) \cup \Phi(mod)\} \cdot$

$\exists A,B \in \mathcal{Fma}\{\Phi(i(A),obs) \cup \Phi(mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x A \wedge \sigma(\mathbf{E};i)(in) \models_x B$

$SOI \equiv \forall x : \mathbb{N} \cdot \forall i : \mathbf{N} \cdot \exists A,B : \mathcal{Fma}\{\Phi(obs) \cup \Phi(mod)\} \cdot$

$\exists A,B \in \mathcal{Fma}\{\Phi(obs) \cup \Phi(i(A),mod)\} \wedge \sigma(\mathbf{N};i)(in) \models_x A \wedge \sigma(\mathbf{E};i)(in) \models_x B$

C.5.1 Reflexivity

$\textbf{sat}(C_i, SOC)$

By the irreflexivity of weakly environment optimistic confidentiality and weakly component optimistic confidentiality.

$\not\Rightarrow \textbf{sat}(C_i^R, COC)$

The irreflexivity of strongly optimistic integrity immediately follows, as the (obs, mod) dual of the reflexivity of strongly optimistic confidentiality.

C.5.2 Transitivity

Product Composition

$\textbf{sat}(\&^P(C_i, C_j),SOI) \wedge \textbf{sat}(\&^P(C_j, C_k),SOI)$

If $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \textbf{sat}(\&^P(C_i, C_k),SOI)$

Otherwise

$\not\Rightarrow \textbf{sat}(\&^P(C_i, C_k),SOI)$

Cascade Composition

$\textbf{sat}(\&^C(C_i, C_j),SOI) \wedge \textbf{sat}(\&^C(C_j, C_k),SOI)$

As with product composition, if $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \textbf{sat}(\&^C(C_i, C_k),SOI)$

Otherwise

$\not\Rightarrow \textbf{sat}(\&^C(C_i, C_k),SOI)$

Feedback Composition

$\textbf{sat}(\&^F(C_i, C_j),SOI) \wedge \textbf{sat}(\&^F(C_j, C_k),SOI)$

As with product composition, if $\Phi^{i+j}(i,j,obs) = \Phi^{j+k}(j,k,obs) = \Phi^{i+k}(i,k,obs)$ and $\Phi^{i+j}(i(A),j(A),mod) = \Phi^{j+k}(j(A),k(A),mod) = \Phi^{i+k}(i(A),k(A),mod)$ then

$\Rightarrow \textbf{sat}(\&^C(C_i, C_k),SOI)$

Otherwise

$\not\Rightarrow \textbf{sat}(\&^C(C_i, C_k),S)I)$

The (in)transitivity of pessimistic confidentiality immediately follows, as the (obs, mod) dual of the transitivity of pessimistic integrity.

C.5.3 Symmetry

Product Composition

$\textbf{sat}(\&^P(C_i, C_j),SOC)$

$\Rightarrow \textbf{sat}(\&^P(C_j, C_i),SOC)$

Cascade Composition

$\mathbf{sat}(\&^C(C_i, C_j),sOC)$

Let the connections ($out^i \rightarrow in^j$) be replaced by ($out^i \rightarrow$ environs) and at least one occurrence of ($out^j \rightarrow$ environs) be replaced by ($out^i \rightarrow in^j$). If $\Phi^{i+j}(j(A)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^C(C_j, C_i),SOC)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^C(C_j, C_i),SOC)$

The (a)symmetry of pessimistic integrity immediately follows, as the (obs,mod) dual of the symmetry of pessimistic confidentiality.

C.5.4 Closure

$\mathbf{sat}(C_i, COI) \wedge \mathbf{sat}(C_j, COI)$

$$= \forall x : \mathbb{N} \cdot \forall i : \{i\} \cdot \exists A, B : \mathcal{F}ma\{\Phi^i(obs) \cup \Phi^i(mod)\} \cdot$$
$$A,B \in \mathcal{F}ma\{\Phi^i(iobs) \cup \Phi^i(i(A),,mod)\} \wedge \sigma(\mathbb{N};i)(in) \models_x A \wedge \sigma(\mathbb{E};i)(in) \models_x B$$
$$\wedge \forall x : \mathbb{N} \cdot \forall j : \{j\} \cdot \exists X,\Delta : \mathcal{F}ma\{\Phi^j(obs) \cup \Phi^j(mod)\} \cdot$$
$$X,\Delta \in \mathcal{F}ma\{\Phi^j(j,obs) \cup \Phi^j(j(A),mod)\} \wedge \sigma(\mathbb{N};i)(in) \models_x X \wedge \sigma(\mathbb{E};i)(in) \models_x \Delta$$

Product Composition

$\mathbf{sat}(C_i, SOI) \wedge \mathbf{sat}(C_j, SOI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ then

$\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), SOI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^P(C_i, C_j), SOI)$

Cascade Composition

$\mathbf{sat}(C_i, SOI) \wedge \mathbf{sat}(C_j, SOI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and $\Phi^{i+j}(j(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), SOI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^C(C_i, C_j), SOI)$

Feedback Composition

$\mathbf{sat}(C_i, SOI) \wedge \mathbf{sat}(C_j, SOI)$

If $\Phi^i(i,obs) = \Phi^j(j,obs)$ and $\Phi^i(i(A),mod) = \Phi^j(j(A),mod)$ and $\Phi^{i+j}(i(A,out)) \subset \{ \Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ and $\Phi^{i+j}(j(A,out)) \subset \{\Phi^{i+j}(i,j,obs) \cup \Phi^{i+j}(i(A),j(A),mod) \}$ then

$\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), SOI)$

Otherwise

$\not\Rightarrow \mathbf{sat}(\&^F(C_i, C_j), SOI)$

The closure properties environment optimistic confidentiality immediately follows, as the (obs, mod) dual of the closure properties of environment optimistic integrity.