SYSTEMS SECURITY ENGINEERING

Adequate Security

An Engineering Answer to an Impossible Question

Dr. Ron Ross

CEO, RONROSSECURE, LLC

> **“The goal is not maximum security. The goal is security that is sufficient for the consequences at stake—and defensible by evidence.”**

THE QUESTION

How Much Security Is Enough?

The usual answers are not sufficient

More security is not a requirement.

Best practice does not prove sufficiency.

Compliance alone does not establish that the system is secure enough for its mission.

The engineering question

What security performance is necessary, tolerable, practicable, and demonstrable for this specific system and its stakeholders?

Adequacy replaces an absolute target with a reasoned judgment.

THE CORE TEST

Two Conditions Define Adequate Security

1 Minimum Tolerable Security

Establishes the floor below which security performance is unacceptable.

The threshold must reflect stakeholder protection needs and the consequences of loss.

2 As Secure as Reasonably Practicable

Meeting the floor is only the beginning.

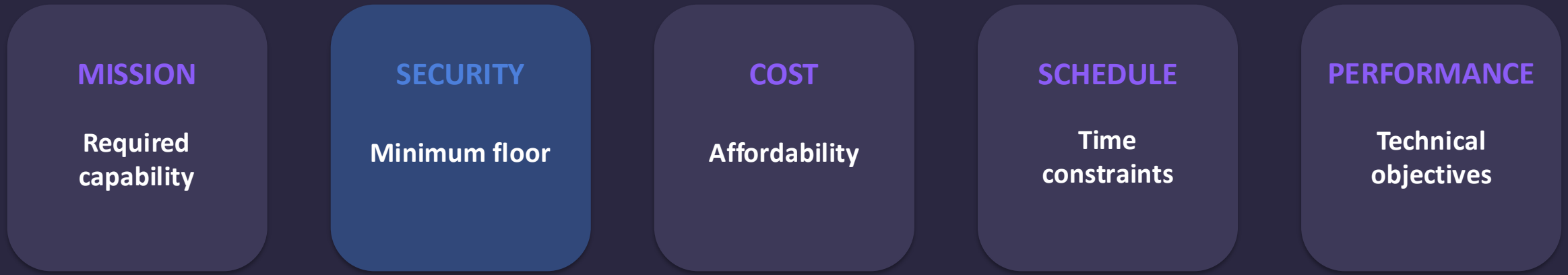
Additional protection should be pursued until further improvement would impose disproportionate degradation, violate constraints, or require unacceptable operational concessions.

Minimum tolerability sets the floor. ASARP asks whether stopping there is justified.

THE TRADE SPACE

Security Is a Trade—But Not Just Another Trade

A system exists to deliver capability. Security must be engineered within the larger system trade space.



Security can be traded within the acceptable region—but not below the minimum tolerable boundary.

CONTEXT MATTERS

There Is No Universal Answer

Adequate security is system-specific.

SYSTEM

What capability must be protected?

ASSETS

What matters to stakeholders?

CONSEQUENCES

What losses are unacceptable?

ADVERSITY

What must the system withstand?

CONSTRAINTS

What limits the solution?

EVIDENCE

How much confidence is required?

SYSTEM BEHAVIOR

Adequacy Must Hold Under Adversity

Systems operate in states—and transition among them.

Protective Failure

Detect and constrain insecure states so failure does not propagate.

Protective Recovery

Move securely toward a reconstituted, alternative, or less insecure state.

Adequate security does not require that nothing bad ever happens—it requires behavior under adversity to remain within defensible bounds.

ASSURANCE

Evidence Turns Opinion into Engineering Judgment

THE ADEQUACY CLAIM

The system meets the minimum tolerable security level and has been made as secure as reasonably practicable.

The consequences of being wrong determine the rigor of evidence required.

- ✓ Analysis & modeling
- ✓ Verification & validation
- ✓ Penetration / red-team testing
- ✓ Recovery demonstrations
- ✓ Operational evidence

Security performance and confidence in that performance are related—but distinct.

DECISION FRAMEWORK

A Practical Adequate-Security Sequence

1. Define capability
2. Define unacceptable consequences
3. Set minimum tolerable security
4. Identify states & transitions
5. Engineer protection & recovery
6. Explore the trade space
7. Determine ASARP
8. Substantiate with evidence
9. Revisit as conditions change

Adequacy is a maintained engineering judgment—not a one-time certificate.

CONCLUSION

From *How Much Security?* to *How Much Confidence?*

The right amount of security is not the most security we can imagine.

It is the level of security we can justify—technically, operationally, economically, and through evidence—against the consequences we cannot afford.

ABOVE THE FLOOR

Is security performance above the minimum tolerable threshold?

ASARP

Is further improvement still reasonably practicable?

EVIDENCE

Is the evidence strong enough to justify the judgment?

That is a question engineering can answer.