TABLE I-3: RESTATEMENTS OF STRATEGIC CYBER RESILIENCY DESIGN PRINCIPLES FOR SELF-DRIVING CARS

STRATEGIC DESIGN PRINCIPLES	RESTATEMENT AND RELATIVE PRIORITY
Focus on common critical assets.	Prevent false geolocation, driving directions, and operating instructions from causing unsafe conditions. (**Priority: Very High**)
Support agility and architect for adaptability.	Provide fail-safe mechanisms and supporting alerting mechanisms; accommodate future interfaces to external sensors and controls. (**Priority: High**)
Reduce attack surfaces.	Enable the operator to take control of the vehicle or to engage fail-safe mechanisms. (**Priority: High**)
Assume compromised resources.	Ensure that the car can fail safely despite cyber-attack, disruption, or interference. (**Priority: Very High**)
Expect adversaries to adapt.	Ensure that in the absence of physical damage, the car's cyber resources can be restored to a known good state. (**Priority: Low**)

Consideration of the relative priorities of the cyber resiliency objectives and strategic design principles, along with the architectural context, enables the applicability of the structural cyber resiliency design principles to be determined as illustrated in Table I-4.

TABLE I-4: APPLICABILITY OF STRUCTURAL CYBER RESILIENCY DESIGN PRINCIPLES TO SELF-DRIVING CARS

STRUCTURAL DESIGN PRINCIPLE	APPLICABILITY
Limit the need for trust.	Applicable; consistent with and reinforcing of safety.
Control visibility and use.	Applicable in principle but may be infeasible depending on needs and capability limitations of constituent sub-systems.
Contain and exclude behaviors.	Applicable; consistent with and reinforcing of safety.
Layer defenses and partition resources.	Applicable in principle but may be infeasible due to added complexity.
Plan and manage diversity.	Not applicable; diversity in components restricted by limited number of original equipment manufacturers (OEMs).
Maintain redundancy.	Applicable in principle but may be infeasible due to added complexity or size, weight, and power concerns.
Make resources location-versatile.	Not applicable.
Leverage health and status data.	Applicable; consistent with and reinforcing of safety.
Maintain situational awareness.	Applicable; consistent with and reinforcing of safety.
Manage resources (risk-) adaptively.	Not applicable.
Maximize transience.	Potentially applicable to infotainment and telematics.
Determine ongoing trustworthiness.	Applicable in principle but may be infeasible depending on capability limitations of constituent sub-systems.
Change or disrupt the attack surface.	Not applicable.
Make the effects of deception and unpredictability user-transparent.	Applicable; given the assumption about the operator and maintenance communities, this is crucial.

Similarly, the relative applicability of the structural design principles, in conjunction with the architectural context, enables the applicability of the cyber resiliency techniques and approaches to be determined as illustrated in Table I-5.