

NANOARC

ACE Program, Routine, Verb, Noun, and Operator-Flow Architecture Manual

Revision A.0 - CMC-Informed Control-System Baseline

Apollo-derived operating principles adapted for the NanoArc Arc Control Executive

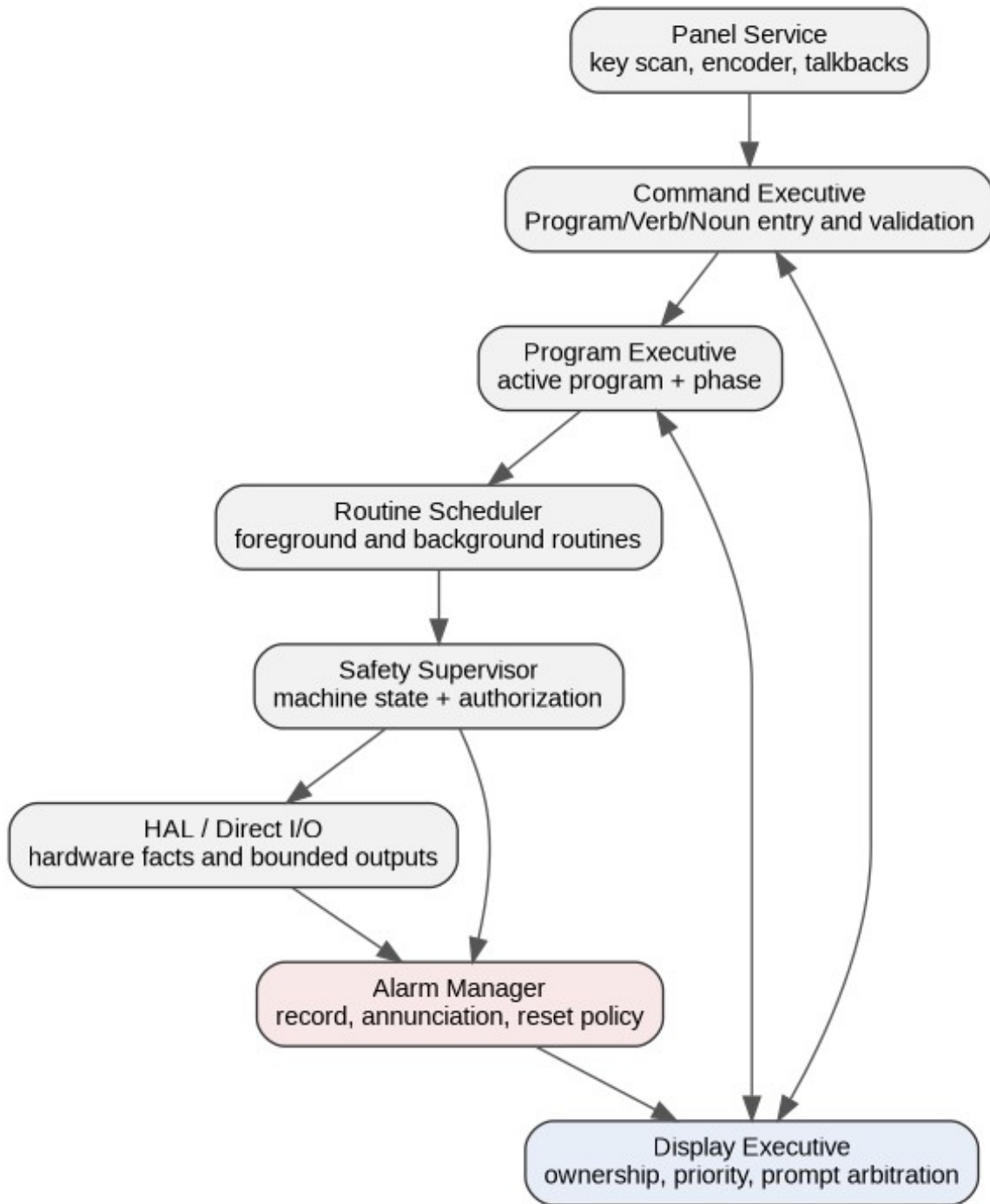


Figure 1. Revised ACE executive architecture and ownership boundaries.

Document identifier	Value
Document	NA-ACEPVN-001
Revision	A.0
Status	Architectural baseline for RevA control-module development
Primary controller	Arduino Nano Every / ATmega4809
Source basis	Apollo 15 Delco CMC/Colossus operating procedures, PDF pages 2-103
Related documents	NA-ACEHW-001 and NanoArc Control System and HID Architecture Manual

Document Control

Revision	Date	Description
A.0	2026-06-24	Initial program/routine/command architecture derived from the Apollo 15 CMC section and integrated with the ACE firmware and panel baseline.

Contents

1. Purpose and Scope
2. CMC Analysis and Design Lessons
3. Revised ACE Executive Architecture
4. Operator-Panel Integration
5. Code Spaces and Descriptor Model
6. ACE Program Catalogue
7. ACE Routine Catalogue
8. ACE Verb Catalogue
9. ACE Noun Catalogue
10. Option, Checklist, Prompt and Alarm Tables
11. Program Operating Flows
12. Automatic Sequencing and Background Services
13. Firmware Mapping and Migration
14. Verification and Acceptance
15. Integration Impact and Open Decisions
- Appendix A. Program/State Compatibility
- Appendix B. Event Catalogue
- Appendix C. Source Traceability
- References

Executive Summary

The Apollo 15 CMC material changes one central assumption in the preliminary ACE design: a Program is not a machine state. The CMC always had a major program, including its idle program P00, while hardware mode, display ownership, routines, alarms and automatic sequences existed as separate dimensions. ACE shall adopt the same separation in a modern typed architecture.

The resulting design retains the NanoArc safety boundary while adding a Program Executive, Routine Scheduler, Command Executive, Display Executive, Prompt Manager and table-driven data dictionary. The previous direct transition `SAFE + PROGRAM_REQUEST -> PROGRAM` is therefore superseded. Program requests are validated and dispatched independently from the Safety Supervisor.

The CMC structure is used as a design pattern, not copied literally. ACE keeps decimal two-digit codes and logical R1/R2/R3 components, but uses an OLED, typed descriptors, explicit access control and modern fault containment.

1. Purpose and Scope

This manual defines the operator-visible program structure and the firmware architecture that supports it. It integrates lessons from the Apollo 15 CMC/Colossus operating procedures into the existing NanoArc ACE control-system and operator-panel design.

- Define the distinction between machine state, active Program, routine execution and authorization state.
- Define the Program, Routine, Verb, Noun, Option, Checklist, Prompt and Alarm code spaces.
- Define display ownership, flashing prompts, operator responses and program recycling.
- Define a preliminary program catalogue and detailed flow for RevA control-module development.
- Define the firmware descriptor tables and event routing required to implement the interface without dynamic allocation.
- Identify changes required to the RevA.0 panel hardware baseline.

The manual does not define the high-current output stage, capacitor-bank construction or final process parameters. Nouns that refer to energy or pulse characteristics are interfaces whose numerical limits remain provisional until hardware characterization is complete.

2. CMC Analysis and Design Lessons

2.1 Source boundary

The analysis covers the CMC/Colossus section of the Apollo 15 Delco manual, PDF pages 2 through 103. The LGC/Luminary section begins on PDF page 104 and is intentionally outside this revision. The source includes DSKY behaviour, Program and Routine catalogues, complete Verb and Noun tables, option/checklist/alarm codes, display arbitration flagwords, channel assignments, detailed Program procedures and the R07 MINKEY automatic sequencer [1].

2.2 Structural findings

- P00 is an idling Program, proving that a program can remain active while the machine is merely waiting.
- Major Programs own long-lived mission procedures; reusable Routines perform shared operations and displays.
- Regular Verbs are highly systematic: display, monitor, load, recycle, proceed, terminate, test, restart and change Program.
- Nouns are data descriptors with one to three components, units, formats and load restrictions.
- Option codes and checklist codes are separate namespaces rather than overloaded Nouns.
- Flashing displays are response contracts. PRO, ENTR, KEY REL and RSET have different meanings.
- Display ownership is arbitrated. Internal priority displays can be held while the operator owns the keyboard.
- Programs can call background routines or coexist with other functions; P20 is a clear example.
- Automatic sequencing is implemented above individual Programs by R07 MINKEY.
- Program changes can be inhibited during critical computations; invalid requests raise an operator-visible error.

2.3 Patterns adopted by ACE

CMC pattern	ACE adaptation
P00 idling program	P00 SAFE IDLE becomes the default active Program after startup.
Programs separate from hardware modes	ProgramCode is independent from MachineState and AuthorizationState.
Routines	Reusable services receive RoutineCode values and completion events.
Regular Verb families	V01-06 display, V11-16 monitor, V21-25 load, V32-37 executive control.
Three-component Nouns	Each Noun has zero to three typed components with units, range and access policy.
Flashing display	PromptDescriptor defines response type, priority, timeout and fallback.
KEY REL / OPR ERR	Panel gains KEY REL and OPR ERR semantics; invalid sequences cannot silently disappear.
Option and checklist codes	Separate descriptor tables support choices and physical operator actions.
MINKEY sequencer	R07 Automatic Sequence Controller performs multi-Program flows.
Alarm history	ACE records first, second and latest alarm plus persistent history.

2.4 Patterns deliberately rejected

- No operator Verb may write arbitrary memory or raw hardware channels in normal builds.
- No Program directly drives a safety-critical output; it requests a bounded service through the Supervisor and HAL.
- No restart may restore an armed or active-output condition.
- No hidden, untyped FLAGWORD maze is used as the primary software model. Typed facts and compact bitsets replace it.
- No display-only confirmation can arm or enable the physical output path.
- No fixed five-digit octal presentation is required; display formatting is selected by each Noun descriptor.

3. Revised ACE Executive Architecture



Figure 2. Machine state, Program state and authorization state are independent.

3.1 Three independent state dimensions

Dimension	Owner	Baseline values
Machine state	Safety Supervisor	BOOT, SAFE, STANDBY, OPERATE, FAULT
Active Program	Program Executive	P00, P01, P06, P10, P11, P20, P30, ...
Authorization	Safety Supervisor / hardware facts	INHIBITED, PREPARED, ARMED
Program phase	Active Program instance	Program-specific phase code
Output fact	HAL feedback	inactive or active; never inferred from Program alone

The current MachineState::program value should be renamed to MachineState::operate. Program selection is tracked separately. After BOOT_COMPLETE, the Supervisor enters SAFE and the Program Executive starts P00.

3.2 Program Executive

- Owns the active Program code and current phase.
- Validates manual and automatic Program requests against a ProgramDescriptor.
- Performs explicit entry, suspend, resume, terminate and fallback actions.
- Posts program_started, program_phase_changed, program_completed and program_aborted events.
- Never changes safety authorization directly; it submits requests to the Supervisor.

3.3 Routine Scheduler

- Runs short reusable Routines without pretending that each Routine is a major Program.
- Supports one foreground Routine owned by the active Program and a bounded set of background services.
- Rejects duplicate ownership of exclusive hardware services.
- Uses completion events rather than blocking calls or nested modal loops.

3.4 Command Executive



Figure 3. Table-driven command construction and dispatch.

- Builds a command from Program, Verb, Noun, digit, sign, CLR and ENTR key events.
- Validates Verb existence, Noun existence, component compatibility, access policy, Program permission and machine-state permission.
- Stages writes before commit. A partially entered value never changes the live system.
- Reports operator errors through OPR ERR, an error message and a rejected-command event.

3.5 Display Executive and Prompt Manager

- Own the logical R1/R2/R3 display image and the OLED page composition.
- Arbitrate operator pages, monitor pages, Program prompts, safety prompts and alarms.
- Preserve one interrupted operator context so a priority display does not destroy an unfinished command.
- Interpret ENTR, PRO, ACK, KEY REL and RSET according to the active prompt contract.

3.6 Alarm Manager

- Records active, first, second and latest alarm codes.
- Drives the FAULT and OPR ERR annunciators through the panel service.
- Allows ACK to acknowledge presentation without clearing the cause.
- Allows RSET to clear eligible annunciation only after the underlying condition is no longer active.
- Persists restart-relevant records where appropriate.

4. Operator-Panel Integration

The CMC analysis requires a panel revision before the hardware layout is frozen. The original 4 x 4 keypad does not provide distinct PRO, KEY REL and RSET functions while retaining Program, Verb, Noun, digits, CLR and ENTR.

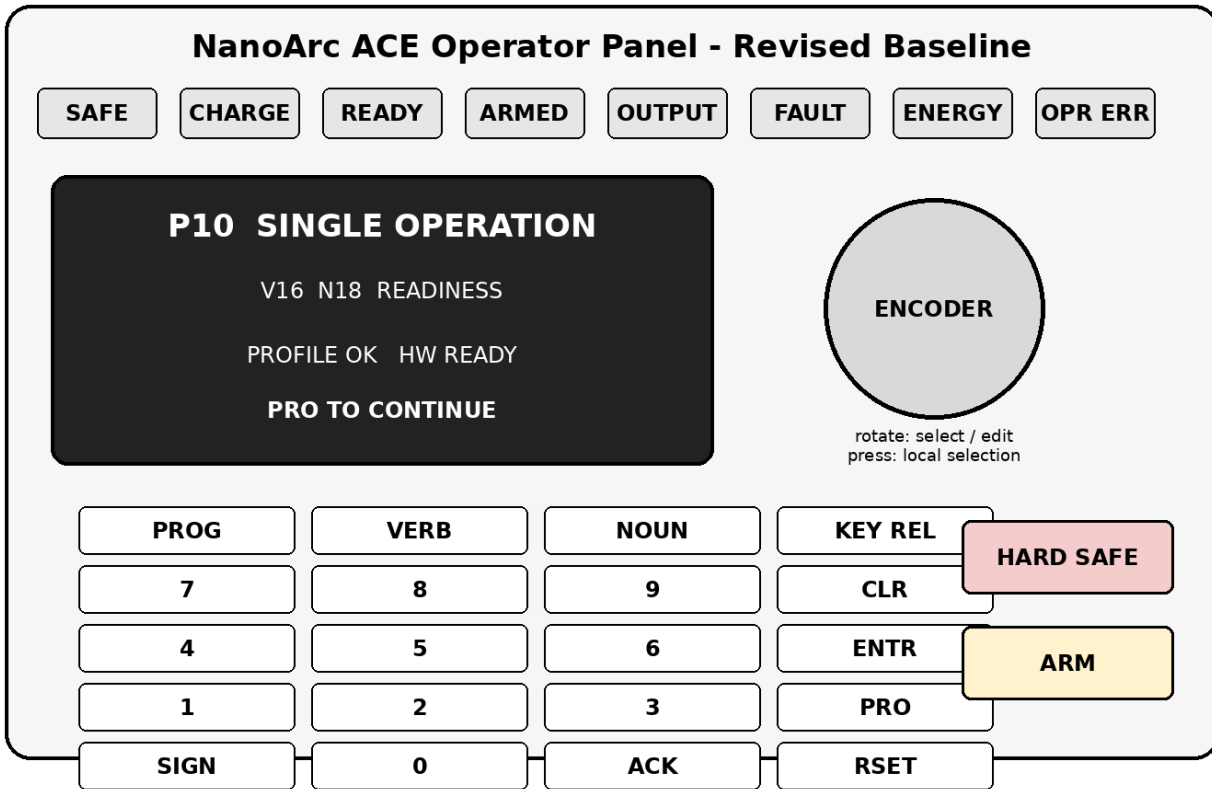


Figure 4. Revised 5 x 4 matrix and eight-talkback panel baseline.

4.1 Revised keypad matrix

Row	Key 1	Key 2	Key 3	Key 4
1	PROG	VERB	NOUN	KEY REL
2	7	8	9	CLR
3	4	5	6	ENTR
4	1	2	3	PRO
5	SIGN	0	ACK	RSET

The 5 x 4 matrix consumes nine expander lines. With encoder A, encoder B, encoder push and panel-present input, the MCP23017 input expander uses thirteen of sixteen lines and retains three spare inputs.

4.2 Key semantics

Key	ACE meaning
PROG	Select the Program field. It is a convenience front end to the same validated program-request mechanism as V37.
VERB / NOUN	Select the corresponding two-digit command field.
ENTR	Commit a complete command, accept staged data, or provide the ENTR response requested by a prompt.
PRO	Proceed or approve the active Program prompt without implying that data were entered.
KEY REL	Release an operator-owned display to a waiting internal display, or return to the Program default page when no internal display is waiting.
ACK	Acknowledge an informational message or alarm presentation without clearing the cause.
RSET	Reset eligible annunciations after the cause has cleared; never bypass an active fault.
CLR	Clear the current staged field or back out of an incomplete entry.

Key	ACE meaning
SIGN	Toggle the sign of the selected signed component.
Encoder	Browse lists and edit bounded values. Encoder push is a local selection, not a substitute for ENTR or PRO.

4.3 Talkbacks

Talkback	Meaning
SAFE	The hardware and software inhibit chain is asserted.
CHARGE	Preparation/charging activity is present.
READY	All current Program readiness conditions are satisfied.
ARMED	Physical arm authorization is present.
OUTPUT	Output-active feedback is present.
FAULT	A blocking fault or alarm is active.
ENERGY	Stored-energy presence or equivalent hazardous condition is detected.
OPR ERR	The most recent operator sequence was invalid or rejected.

This supersedes the seven-talkback RevA.0 panel allocation. The output expander uses all eight pins of one port for talkbacks. KEY REL state is shown on the OLED rather than consuming another lamp.

4.4 Logical registers on the OLED

- ACE retains logical R1, R2 and R3 components even though the OLED can display labels and units.
- Display and Monitor Verbs select which Noun components occupy the logical registers.
- Each field shows the component label, formatted value, unit and validity state.
- Flashing is reserved for a required response, not decoration.
- The Program, Verb and Noun codes remain visible in the command/status header.

4.5 Display ownership and priority

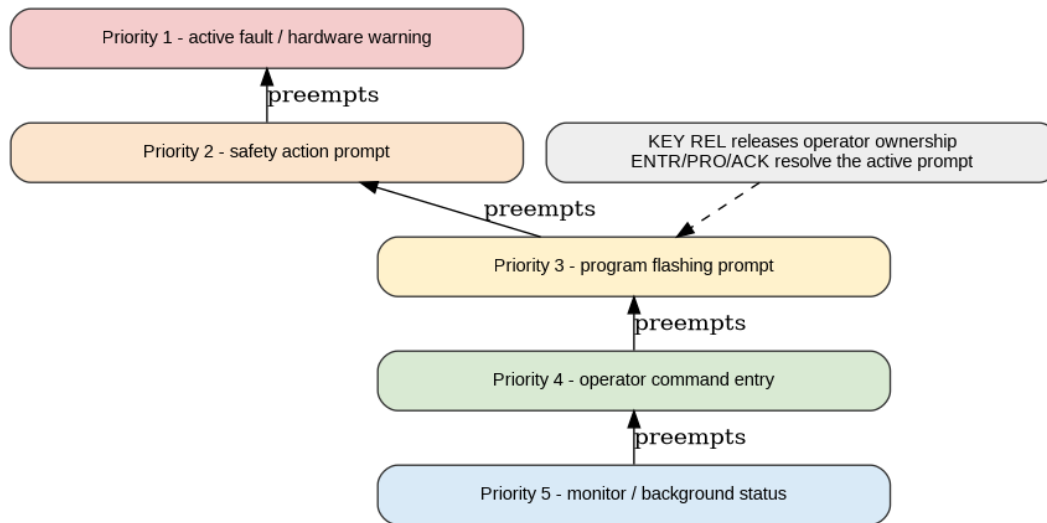


Figure 5. ACE display-priority and response hierarchy.

Priority	Owner	Examples	Resolution
1	Alarm Manager	active fault, gate mismatch, bus failure affecting safety facts	ACK presents detail; RSET only after cause clears
2	Safety Supervisor	set SAFE, release trigger, disarm	Required physical action plus PRO/ACK as specified
3	Active Program	load value, confirm profile, inspect result	ENTR, PRO, V32 recycle or V34 terminate
4	Operator command entry	Program/Verb/Noun and staged digits	ENTR commit, CLR edit, KEY REL release
5	Monitor/background	status, measurements, logs	Replaced by higher priority; restored afterward

5. Code Spaces and Descriptor Model

5.1 Code types

```

using ProgramCode    = uint8_t;
using RoutineCode    = uint8_t;
using VerbCode       = uint8_t;
using NounCode       = uint8_t;
using OptionCode     = uint16_t;
using ChecklistCode  = uint16_t;
using PromptCode     = uint16_t;
using AlarmCode      = uint16_t;

```

Two-digit Program, Routine, Verb and Noun codes are operator-visible decimal values. Option, Checklist, Prompt and Alarm codes may use wider numeric ranges. Strong wrapper types or enum classes should prevent accidental interchange in firmware.

5.2 Descriptor relationships

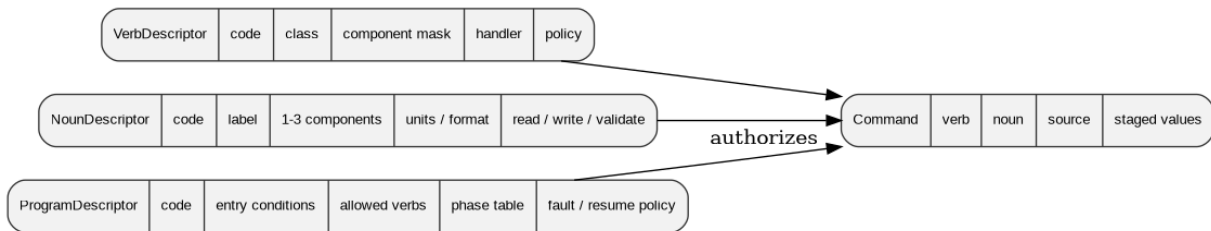


Figure 6. Commands are validated against immutable Verb, Noun and Program descriptors.

Descriptor	Required fields
ProgramDescriptor	code, title, entry states, allowed Programs, allowed Verb mask, phase table, fallback Program, restart policy
RoutineDescriptor	code, title, exclusivity class, request event, completion event, timeout, abort policy
VerbDescriptor	code, class, component mask, access operation, handler/request type, prompt behaviour
NounDescriptor	code, title, component count, component descriptors, read/write/validate hooks, Program/state permissions
ComponentDescriptor	label, data type, scale, units, format, min, max, sign rule, persistence and source
PromptDescriptor	code, priority, required response, flashing fields, timeout, default action and cancel path
AlarmDescriptor	code, subsystem, severity, latch policy, reset rule, default display and safe action

5.3 Storage policy

- Immutable descriptor tables and strings live in flash memory.
- RAM holds only the active Program instance, one foreground Routine, bounded background-service state, the current command builder, active prompt and current display values.
- No heap allocation is permitted in the executive path.
- Every table has an explicit count and compile-time uniqueness test where practical.

6. ACE Program Catalogue

6.1 Allocation policy

Range	Class
P00-P09	Executive, startup, recovery and standby
P10-P19	Normal operation and simulation
P20-P29	Profiles, tools and calibration
P30-P39	Status, diagnostics and logs
P40-P49	Restricted service and factory functions
P50-P89	Reserved
P90-P99	Development-only harnesses; removed from release builds

6.2 Baseline catalogue

Code	Program	Status	Purpose
P00	SAFE IDLE	Baseline	Default readiness state, command entry and safe monitoring.
P01	STARTUP SELF-TEST	Internal	Validate firmware invariants, panel presence, buses, storage and direct safety facts.
P02	RECOVERY	Internal	Interpret reset cause, reconstruct safe persistent state and return to P00 or FAULT.
P06	STANDBY / POWER-DOWN	Baseline	Enter low-activity standby while preserving safe restart behaviour.
P10	SINGLE OPERATION	Baseline	Prepare and execute one authorized operation, capture result and return to P00.
P11	REPEAT JOB SESSION	Planned	Sequence repeated P10-equivalent cycles with counters, interval and cooldown policy.
P12	DRY RUN / SIMULATION	Baseline	Exercise the complete command and Program flow while all physical output remains inhibited.
P20	PROFILE SELECT / REVIEW	Baseline	Browse, inspect and select a stored or temporary profile.
P21	PROFILE EDIT	Planned	Edit a working copy, validate and commit to storage.
P22	MATERIAL CALIBRATION	Future	Collect controlled test results and derive provisional profile data.
P23	SENSOR CALIBRATION	Planned	Calibrate low-voltage sensing channels against references.
P24	TOOL CONFIGURATION	Planned	Select and verify electrode/tool configuration and reference values.
P30	SYSTEM STATUS	Baseline	Read-only live status and measurement monitoring.
P31	PANEL TEST	Baseline	Test keypad, encoder, OLED, talkbacks and sounder without energizing output hardware.
P32	I/O DIAGNOSTICS	Baseline	Inspect direct inputs, feedback and bus devices; output tests remain bounded and safe.
P33	ALARM / RESTART REVIEW	Baseline	Inspect active alarm, history, reset cause and clearing conditions.
P34	STORAGE INTEGRITY	Planned	Verify profile and log records, checksums and directory consistency.
P40	SERVICE MODE	Restricted	Authorized maintenance functions requiring an explicit service build or hardware condition.
P90	DEVELOPMENT HARNESS	Development	Synthetic events, simulated sensors and deterministic test sequences; excluded from release firmware.

6.3 Program-request rules

- P00 is automatically selected after successful startup and after normal Program termination.

- A Program request is rejected if its descriptor disallows the current MachineState, authorization state or active fault condition.
- A Program request never directly changes the Safety Supervisor state. Entry code requests any needed transition and waits for approval.
- Only P01 and P02 may run during BOOT. Read-only P30 and P33 may be available in FAULT.
- P10 and P11 may enter from SAFE but require OPERATE before preparation can proceed.
- Program changes are inhibited during a timed action and other descriptor-marked critical phases.

7. ACE Routine Catalogue

Code	Routine	Purpose
R00	FINAL REQUEST / RETURN P00	Terminate current function and request the Program fallback path.
R01	COMMAND ENTRY	Build and edit Program/Verb/Noun commands.
R02	HARDWARE FACT SAMPLE	Acquire direct and bus-based low-voltage facts into a coherent snapshot.
R03	STARTUP TEST	Execute startup invariant and device-presence checks.
R04	DISPLAY SERVICE	Compose logical registers and OLED pages.
R05	PANEL SERVICE	Scan keypad/encoder, debounce and update talkbacks.
R06	ALARM SERVICE	Record alarms, select priority display and apply latch policy.
R07	AUTOMATIC SEQUENCE CONTROLLER	Execute bounded tables of Program/Routine steps and conditions.
R10	PROFILE LOAD	Load a profile into a working context.
R11	PROFILE VALIDATE	Validate ranges, integrity, hardware compatibility and revision.
R12	READINESS EVALUATE	Combine profile, hardware, contact, cooldown and authorization facts.
R13	CONTACT TEST	Request and evaluate a low-energy contact/readiness measurement interface.
R14	PREPARATION SERVICE	Prepare the requested operation within Supervisor limits.
R15	TIMED ACTION SERVICE	Own the bounded timing request and independent cutoff interface.
R16	POST-ACTION CAPTURE	Capture measured results and hardware feedback.
R17	COOLDOWN MANAGER	Enforce time and temperature recovery policy.
R20	PROFILE EDITOR	Stage component edits and validation.
R21	MATERIAL CALIBRATION ENGINE	Collect calibration samples and calculate provisional results.
R22	SENSOR CALIBRATION ENGINE	Calculate and verify sensor offset/scale records.
R23	TOOL CONFIGURATION	Validate electrode/tool identity and references.
R30	STATUS DISPLAY	Provide the P30 default monitor page.
R31	ALARM DISPLAY	Provide active and historical alarm pages.
R32	PANEL TEST	Exercise panel hardware in a safe pattern.
R33	I/O TEST	Observe direct I/O and bounded feedback tests.
R34	BUS RECOVERY	Perform bounded I2C recovery and device rescan.
R35	STORAGE INTEGRITY	Verify directories, record headers and checksums.
R40	RESTART RECONSTRUCTION	Interpret reset records and restore safe, non-armed state.

R07 is the ACE equivalent of the CMC MINKEY pattern. It coordinates major steps but does not absorb their implementation. Each called Program or Routine still owns its own entry checks and completion event.

8. ACE Verb Catalogue

8.1 Regular Verbs

Code	Meaning
V00	Invalid / unused
V01	Display component 1
V02	Display component 2
V03	Display component 3
V04	Display components 1 and 2
V05	Display components 1, 2 and 3
V06	Display Noun using its normal formatted page
V07	Display raw diagnostic representation - restricted
V08-V10	Reserved
V11	Monitor component 1
V12	Monitor component 2
V13	Monitor component 3
V14	Monitor components 1 and 2
V15	Monitor components 1, 2 and 3
V16	Monitor Noun using its normal formatted page
V17	Monitor raw diagnostic representation - restricted
V18-V20	Reserved
V21	Load component 1
V22	Load component 2
V23	Load component 3
V24	Load components 1 and 2
V25	Load components 1, 2 and 3
V26	Validate staged load without committing
V27	Display Noun descriptor metadata
V28-V29	Reserved
V30	Request a Routine by code
V31	Schedule a permitted deferred Routine
V32	Recycle the current Program phase
V33	Proceed without changing displayed data
V34	Terminate the current Routine or Program through its defined exit
V35	Panel/lamp test
V36	Controlled software restart to inhibited recovery
V37	Change major Program
V38	Display contextual help
V39	Reserved

8.2 Extended Verb ranges

Range	Domain
V40-V49	Profile, calibration and reference operations
V50-V59	Internal operator prompts
V60-V69	Test and maintenance Routine requests
V70-V79	Alarm, log, standby and recovery functions
V80-V89	Reserved application extensions
V90-V99	Factory/development only

8.3 Initial extended Verbs

Code	Meaning
V40	Zero selected calibration quantity
V41	Calibrate selected Noun/channel
V42	Capture reference sample
V43	Select active profile
V44	Save working profile
V45	Load profile
V46	Copy profile
V47	Delete eligible profile
V48	Validate profile
V49	Restore documented defaults
V50	Please perform the checklist action
V51	Please inspect or confirm contact
V52	Please connect/configure the specified tool

Code	Meaning
V53	Please set HARD SAFE
V54	Please release trigger
V55	Please arm when READY
V56	Please disarm
V57	Please wait for cooldown
V58	Please acknowledge
V59	Please service
V60	Request contact test
V61	Request preparation service
V62	Abort preparation and return safe
V63	Accept current result/disposition
V64	Request panel test
V65	Request I/O diagnostics
V66	Request bus recovery/rescan
V67	Request storage integrity test
V68	Request diagnostic export - future
V69	Reserved
V70	Display alarm summary
V71	Display alarm history
V72	Reset eligible annunciations
V73	Clear eligible non-safety log entries
V74	Enter standby
V75	Return to P00
V76-V89	Reserved
V90-V99	Development/factory functions

8.4 Verb safety rules

- No Verb means ARM, FIRE, BYPASS, FORCE OUTPUT or IGNORE FAULT.
- V21-V25 can only write Nouns marked writable and only through staged validation.
- V32 recycle returns to a Program-defined checkpoint; it is not an arbitrary jump.
- V34 termination follows a safe exit path and cannot interrupt the independent cutoff service.
- V36 always returns through P02 RECOVERY and cannot resume ARMED authorization.
- Internal prompt Verbs V50-V59 are generated by firmware, not accepted as unrestricted operator requests.

9. ACE Noun Catalogue

9.1 Noun descriptor requirements

- Every Noun has zero to three components.
- Each component declares data type, scale, unit, display format, valid range, sign rule and source.
- Access is Read-only, Read/Select, Read/Write, Restricted or Internal.
- A Noun can be visible in several Programs while remaining writable in only one.
- Load-locked measurements and safety facts can never be modified through V21-V25.

Executive and command nouns

Code	Noun	Components	Access
N00	Invalid / unused	-	None
N01	Machine status	state; primary inhibit; readiness	Read-only
N02	Active Program	Program; phase; progress	Read-only
N03	Command state	Verb; Noun; entry status	Read-only
N04	Prompt state	prompt; response required; priority	Read-only
N05	Option request	option ID; selection; validity	Read/Select
N06	Checklist request	code; status; source	Read-only
N07	Event queue	depth; rejected; high-water	Read-only
N08	Alarm summary	first; second; latest	Read-only
N09	Alarm detail	code; source; latch state	Read-only

Power, safety and hardware facts

Code	Noun	Components	Access
N10	Input power	source; voltage; current	Read-only
N11	Logic rails	5 V; 3.3 V; status	Read-only
N12	Energy status	measured level; target; condition	Read-only
N13	Temperatures	controller; power stage; auxiliary	Read-only
N14	Interlocks	arm; grip; trigger	Read-only
N15	Output path	inhibit; gate feedback; watchdog	Read-only
N16	Bus status	device count; error count; recovery state	Read-only
N17	Panel status	last key; encoder; panel health	Read-only
N18	Readiness	profile; hardware; cooldown	Read-only
N19	Reset status	cause; count; recovery result	Read-only

Profile and configuration nouns

Code	Noun	Components	Access
N20	Profile identity	slot; profile code; revision	Read/Select
N21	Material pair	material A; material B; class	Read/Write in P21/P22
N22	Action parameters	energy target; duration; stage count	Read/Write in P21; limits provisional
N23	Tool configuration	electrode type; spacing; revision	Read/Write in P21/P24
N24	Repetition policy	count; interval; cooldown	Read/Write in P21
N25	Profile integrity	format; CRC; compatibility	Read-only
N26	Contact criteria	measured value; threshold; result	Restricted write
N27	Preparation policy	target; limit; timeout	Restricted write
N28	Operation limits	max duration; max energy; max temperature	Restricted
N29	Profile flags	source; validity flags; dirty state	Read-only

Operation and result nouns

Code	Noun	Components	Access
N30	Current job	job ID; cycle; state	Read-only
N31	Operation request	profile; mode; sequence ID	Read-only
N32	Operation result	duration; peak current; delivered energy	Read-only
N33	Quality result	pre-contact; post-contact; disposition	Read/Select disposition
N34	Timing statistics	preparation; action; cooldown	Read-only
N35	Cycle counters	session; lifetime; failures	Read-only
N36	Last operation fault	code; phase; recovery	Read-only
N37	Simulation result	expected path; blocked step; reason	Read-only

Measurement and calibration nouns

Code	Noun	Components	Access
N40	Raw sensor group A	bank sense; current sense; temperature raw	Restricted read
N41	Raw sensor group B	supply sense; tool sense; auxiliary	Restricted read
N42	Calibrated measurements	voltage; current; temperature	Read-only
N43	Calibration coefficients	offset; scale; revision	Restricted
N44	Comparator status	overvoltage; contact; fault	Read-only
N45	Timing capture	start tick; stop tick; watchdog margin	Read-only

Alarm, log and service nouns

Code	Noun	Components	Access
N50	Current alarm	code; source; active	Read-only
N51	Alarm history	first; second; latest	Read-only
N52	Alarm counts	active; session; lifetime	Read-only
N53	Inhibit reason	primary; secondary; clear condition	Read-only
N54	Restart record	cause; Program; result	Read-only
N55	Event history cursor	index; type; timestamp	Read/Select
N56	Service request	code; severity; action	Read-only

Diagnostic and identity nouns

Code	Noun	Components	Access
N60	Panel diagnostics	keypad; encoder; talkbacks	Read-only
N61	Display diagnostics	controller; update rate; errors	Read-only
N62	Bus diagnostics	bus state; device; fault count	Read-only
N63	Direct I/O diagnostics	inputs; outputs; mismatch	Read-only
N64	Storage diagnostics	slots; valid records; errors	Read-only
N65	Firmware build	version; build ID; profile format	Read-only
N66	Resource status	RAM; queue high-water; uptime	Read-only
N67	Hardware identity	controller rev; panel rev; unit ID	Read-only
N68	Test selection	test code; iterations; result	Read/Select
N69	Test detail	step; measured; expected	Read-only

Calibration working nouns

Code	Noun	Components	Access
N80	Calibration selection	channel; method; reference	Read/Select
N81	Calibration coefficients	offset; scale; checksum	Restricted
N82	Calibration sample	raw; reference; residual	Restricted
N83	Calibration result	channel; pass/fail; revision	Read-only
N84	Tool reference	type; resistance; revision	Restricted
N85	Material calibration	pair; sample; result	Restricted
N86-N89	Reserved	-	None
N90-N99	Development/factory	build-specific	Restricted

10. Option, Checklist, Prompt and Alarm Tables

10.1 Option codes

Code	Purpose	Choices
O001	Operation mode	1 single; 2 repeat; 3 simulation
O002	Profile source	1 stored; 2 temporary; 3 documented default
O003	Contact-test sensitivity	1 normal; 2 sensitive; 3 characterization
O004	Monitor refresh	1 slow; 2 normal; 3 fast
O005	Result disposition	1 accept; 2 retry; 3 reject/record
O006	Calibration method	1 verification; 2 one-point; 3 two-point
O007	Standby policy	1 display on; 2 dim; 3 low-power

10.2 Checklist codes

Code	Operator action
C001	Set HARD SAFE
C002	Release trigger
C003	Connect handpiece/control cable
C004	Install the specified electrode/tool
C005	Place the test article or workpiece
C006	Remove the workpiece
C007	Wait for cooldown
C008	Connect the specified calibration reference
C009	Inspect and classify the result
C010	Disconnect output hardware before service

10.3 Prompt codes

Code	Prompt	Allowed response
Q001	Confirm Program start	PRO or V34
Q002	Accept staged data	ENTR, V32 or CLR
Q003	Set SAFE	physical action then PRO
Q004	Release trigger	physical action; automatic completion
Q005	Arm when READY	physical action; no display command can substitute
Q006	Inspect result	ACK, V63 or V32
Q007	Acknowledge fault detail	ACK
Q008	Reset eligible annunciation	RSET after cause clears
Q009	Release display ownership	KEY REL

10.4 Alarm-code allocation

Range	Subsystem	Examples
1000-1999	Executive and scheduling	1001 startup invariant; 1002 queue admission
2000-2999	Panel and buses	panel expander missing; I2C recovery failed
3000-3999	Measurements and sensors	sensor out of range; calibration invalid
4000-4999	Safety and interlocks	trigger active at arm request; gate feedback mismatch
5000-5999	Profiles and storage	profile CRC; incompatible revision
6000-6999	Preparation and timed action	preparation timeout; watchdog cutoff
7000-7999	Reset and power	brownout restart; watchdog restart
8000-8999	Service and diagnostics	test failed; storage directory inconsistency
9000-9999	Development only	synthetic fault injection

The active alarm display shall expose code, source and clearing condition. N08 and N51 preserve the first, second and latest pattern used effectively by the CMC, while the persistent log may retain more entries.

11. Program Operating Flows

Each Program specification follows the Delco structure: Purpose, Assumptions/Entry Conditions, Sequence of Events and Exit/Recycle Behaviour. The flows below are the RevA architecture baseline; exact process limits remain external configuration.

P00 - SAFE IDLE

Purpose. Maintain ACE in a safe, responsive condition while accepting commands and monitoring hardware facts.

Assumptions / entry conditions.

- Startup or recovery completed successfully.
- Safety Supervisor is SAFE or STANDBY; authorization is INHIBITED.
- No timed action is active.

Sequence of events.

1. Select P00 automatically.
2. Assert the software inhibit request and show SAFE.
3. Run R02 hardware-fact sampling, R04 display service, R05 panel service and R06 alarm service.
4. Display N01/N02 default status.
5. Accept permitted Program, Verb and Noun commands.

Exit and recycle behaviour.

- Valid Program request transfers through Program Executive entry checks.
- Active blocking fault transfers to FAULT display while P00 remains the fallback Program.
- P06 request enters standby.

P01 - STARTUP SELF-TEST

Purpose. Prove control-module invariants before normal command acceptance.

Assumptions / entry conditions.

- Entered only from BOOT.
- Output hardware remains independently inhibited.

Sequence of events.

1. Run static/runtime invariant checks.
2. Verify queue, program table and descriptor-table integrity.
3. Verify panel and required bus devices.
4. Read reset cause and direct safety inputs.
5. Verify storage headers and load defaults.
6. If all mandatory checks pass, post BOOT_COMPLETE and start P00; otherwise raise an alarm and remain inhibited.

Exit and recycle behaviour.

- P01 cannot be selected manually in release firmware.
- Failure enters FAULT or restricted P30/P33 visibility.

P02 - RECOVERY

Purpose. Recover from reset without recreating an unsafe operating condition.

Assumptions / entry conditions.

- Entered automatically after watchdog, brownout or software restart.
- Authorization state is forced to INHIBITED before persistent data are interpreted.

Sequence of events.

1. Capture reset cause and previous Program record.
2. Validate persistent configuration and alarm record.
3. Reconstruct only non-hazardous session state.
4. Run the required subset of P01 checks.
5. Record recovery result in N54.
6. Return to P00 or enter FAULT.

Exit and recycle behaviour.

- Never restores ARMED, OUTPUT or an unfinished timed action.
- Operator must explicitly reselect any prior Program.

P06 - STANDBY / POWER-DOWN

Purpose. Reduce control-module activity while preserving deterministic wake-up and safe state.

Assumptions / entry conditions.

- Entered from P00 with no active fault requiring display ownership.
- Authorization is INHIBITED.

Sequence of events.

1. Prompt for confirmation.
2. Blank or dim nonessential display elements.
3. Stop optional monitors and retain minimal panel wake path.
4. Maintain required watchdog, energy-presence and fault indications.
5. Wake on permitted panel or power event.
6. Run wake checks and return P00.

Exit and recycle behaviour.

- Any detected fault wakes the panel into the fault display.
- Standby never disables independent hazard indication.

P10 - SINGLE OPERATION

Purpose. Prepare and execute one authorized operation using the selected profile, then capture and present the result.

Assumptions / entry conditions.

- Active profile exists and passes R11 validation.
- Entry begins in SAFE; Supervisor must authorize OPERATE before preparation.
- Physical arm, grip and trigger facts are direct inputs, not command values.

Sequence of events.

1. Load and validate the active profile.
2. Sample hardware facts and evaluate readiness.
3. Run bounded preparation service.
4. Present READY-SAFE status and wait for required physical conditions.
5. Evaluate contact/readiness criteria.
6. Submit a timed action request to R15.
7. Capture feedback and result data.
8. Apply cooldown policy.
9. Present result and disposition prompt.
10. Return P00.

Exit and recycle behaviour.

- V32 recycles only to the last safe checkpoint.
- V34 terminates through inhibit and safe cleanup.
- Any failed invariant or hardware mismatch asserts inhibit and raises an alarm.

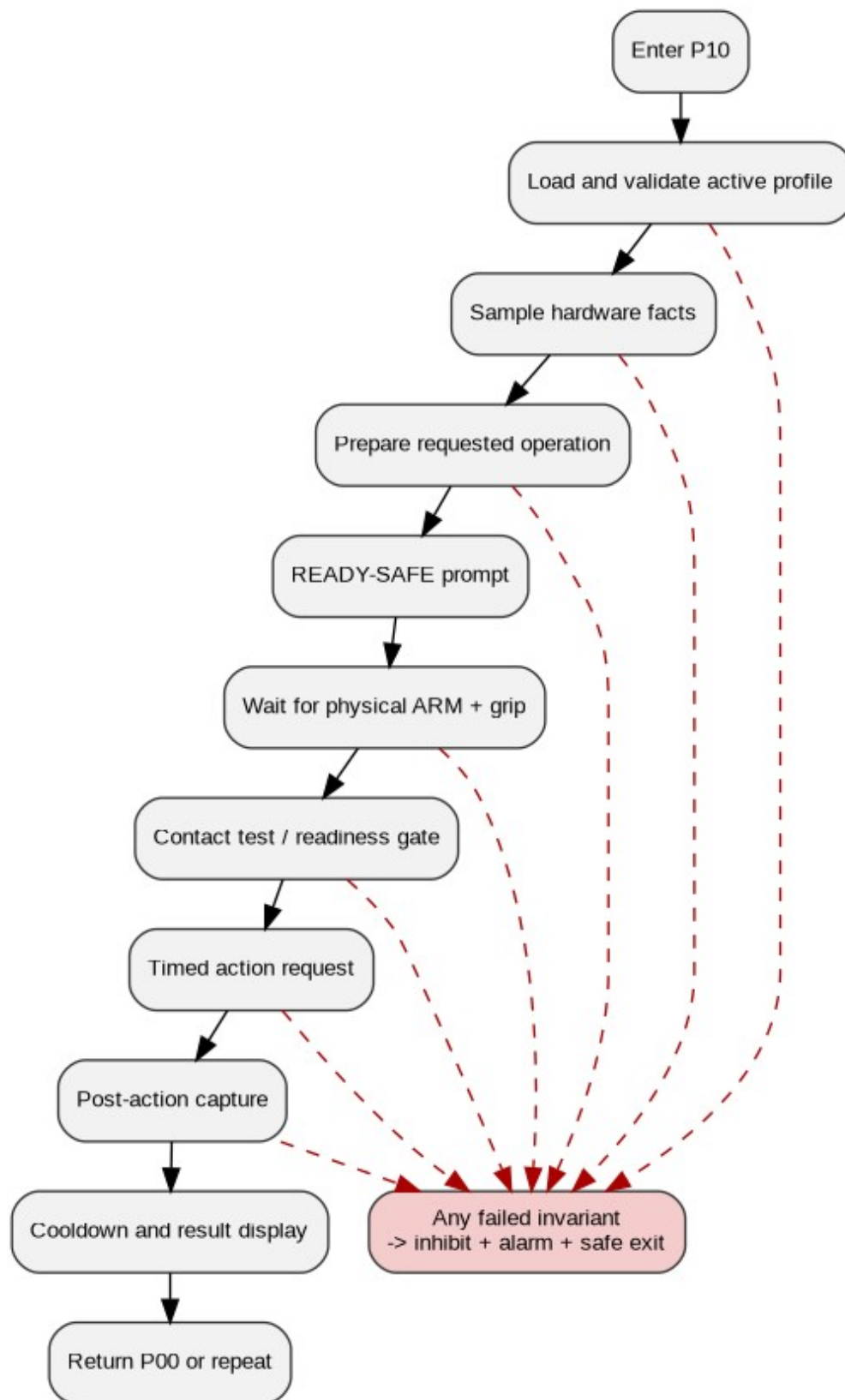


Figure 7. P10 single-operation control flow.

P11 - REPEAT JOB SESSION

Purpose. Repeat the P10 operation flow under a bounded count, interval and cooldown policy.

Assumptions / entry conditions.

- P24 repetition policy is valid.
- P10 entry requirements are satisfied for every cycle.

Sequence of events.

1. Create a job/session record.
2. Use R07 to invoke the P10 preparation/action/result stages.
3. Increment N35 counters after each completed cycle.
4. Apply interval and cooldown checks.
5. Pause on operator result, fault or readiness loss.
6. Complete at requested count or operator termination.

Exit and recycle behaviour.

- No automatic retry after a safety fault.
- A rejected cycle does not silently advance the completed-count field.
- Termination returns P00 with session summary.

P12 - DRY RUN / SIMULATION

Purpose. Exercise Program, command, prompt, display, alarm and sequencing paths without permitting physical output.

Assumptions / entry conditions.

- Development or authorized diagnostic build.
- Supervisor remains SAFE and authorization remains INHIBITED.

Sequence of events.

1. Load a selected profile and synthetic hardware-fact set.
2. Execute the P10 phase table using simulated completion events.
3. Display every required prompt and transition.
4. Record the first blocked or invalid transition in N37.
5. Return P00 with a simulation report.

Exit and recycle behaviour.

- No HAL path capable of active output is called.
- Simulation events are clearly marked and cannot enter persistent production counters.

P20 - PROFILE SELECT / REVIEW

Purpose. Browse and select a valid profile without editing live records.

Assumptions / entry conditions.

- Machine state SAFE or STANDBY.
- No profile-storage fault is active.

Sequence of events.

1. Display profile directory.
2. Select a slot with encoder or N20.
3. Load the profile into a read-only working view.
4. Display N21-N29 pages.
5. Validate compatibility.
6. Commit the active-profile selection with PRO/ENTR.
7. Return P00.

Exit and recycle behaviour.

- Invalid profiles remain viewable with reason but cannot become active.
- CLR or V34 returns without changing selection.

P21 - PROFILE EDIT

Purpose. Edit a working copy, validate it and commit an atomic profile record.

Assumptions / entry conditions.

- Machine state SAFE.

- Storage is healthy and a writable slot is selected.

Sequence of events.

1. Copy source profile or defaults into a working record.
2. Edit writable components using V21-V25.
3. Validate each component and the complete profile.
4. Display differences and integrity result.
5. Prompt to save.
6. Write a new revision atomically and verify checksum.
7. Optionally select the saved profile.
8. Return P20 or P00.

Exit and recycle behaviour.

- Live profile is unchanged until the final atomic commit.
- V32 discards the current field; V34 discards the whole working copy after confirmation.

P22 - MATERIAL CALIBRATION

Purpose. Collect controlled samples and create provisional material-pair data.

Assumptions / entry conditions.

- Restricted mode and documented test setup.
- Calibration reference and tool configuration are valid.

Sequence of events.

1. Select material pair and method.
2. Request checklist actions.
3. Collect bounded samples through existing measurement/action services.
4. Reject outliers according to a documented rule.
5. Calculate provisional values and confidence.
6. Present result for acceptance.
7. Store only as a new provisional profile revision.

Exit and recycle behaviour.

- No calibration result overwrites a validated profile automatically.
- Faults terminate the sequence and retain an incomplete record for diagnosis.

P23 - SENSOR CALIBRATION

Purpose. Derive and verify calibration coefficients for low-voltage measurement channels.

Assumptions / entry conditions.

- Machine SAFE; physical output disabled.
- Specified references are connected.

Sequence of events.

1. Select channel and calibration method.
2. Capture raw/reference pairs.
3. Compute offset and scale.
4. Verify residual and range.
5. Write a versioned calibration record.
6. Re-read and verify checksum.
7. Return P30 or P00.

Exit and recycle behaviour.

- Failed verification leaves the previous valid record active.
- Restricted channels require a service condition.

P24 - TOOL CONFIGURATION

Purpose. Select and verify electrode/tool identity and reference data.

Assumptions / entry conditions.

- Machine SAFE.
- Tool identity mechanism may be manual in RevA.

Sequence of events.

1. Select tool type and revision.
2. Load expected geometry/reference values.
3. Optionally perform a contact/reference check.
4. Validate compatibility with active profile.
5. Commit the working selection.
6. Return P00 or P20.

Exit and recycle behaviour.

- Incompatible tool/profile combination blocks P10 readiness.

P30 - SYSTEM STATUS

Purpose. Provide read-only monitoring of machine, hardware, program and resource facts.

Assumptions / entry conditions.

- Available in SAFE and OPERATE; limited pages available in FAULT.

Sequence of events.

1. Display N01/N02 default page.
2. Allow V11-V16 monitor requests for read-only Nouns.
3. Permit KEY REL and priority preemption.
4. Return to the prior Program default page or P00.

Exit and recycle behaviour.

- No load Verb is accepted for a read-only fact.
- Monitoring cannot acquire exclusive control of a hardware service.

P31 - PANEL TEST

Purpose. Verify operator-panel input and output hardware without affecting the physical output path.

Assumptions / entry conditions.

- Machine SAFE; authorization INHIBITED.

Sequence of events.

1. Show keypad matrix state and encoder count.
2. Require each key once or run a selected subset.
3. Exercise OLED patterns.
4. Exercise talkbacks and sounder with bounded patterns.
5. Record missing/stuck inputs and output mismatches.
6. Return P00 with result.

Exit and recycle behaviour.

- HARD SAFE and ARM are observed but not simulated.
- FAULT and ENERGY hardware override indications are never suppressed by the test.

P32 - I/O DIAGNOSTICS

Purpose. Observe direct inputs, bus devices and feedback while maintaining safe ownership boundaries.

Assumptions / entry conditions.

- Machine SAFE; release build permits read-only tests only.

Sequence of events.

1. Sample direct inputs and compare against expected idle states.
2. Enumerate required bus devices and addresses.
3. Display comparator and feedback status.
4. Run permitted bounded feedback tests.
5. Record mismatches and recovery results.
6. Return P00.

Exit and recycle behaviour.

- No diagnostic can force the timed output path.
- Potentially disruptive tests require P40/service authorization.

P33 - ALARM / RESTART REVIEW

Purpose. Present active alarms, history, restart cause and clearing requirements.

Assumptions / entry conditions.

- Available in SAFE and FAULT.

Sequence of events.

1. Display N50 current alarm.
2. Display N51 first, second and latest codes.
3. Browse persistent history.
4. Show N53 clear condition and N54 restart record.
5. Allow ACK.
6. Allow RSET only when the alarm descriptor reports that its cause is clear.
7. Return P00 or the fault display.

Exit and recycle behaviour.

- ACK never clears the active condition.
- History clearing is a separate restricted command.

P34 - STORAGE INTEGRITY

Purpose. Verify the integrity of profile, calibration and log storage.

Assumptions / entry conditions.

- Machine SAFE.
- No atomic write is in progress.

Sequence of events.

1. Scan record headers and directories.
2. Verify checksums and revision compatibility.
3. Identify orphaned or incomplete records.
4. Offer only descriptor-authorized repair operations.
5. Write an integrity report.
6. Return P00.

Exit and recycle behaviour.

- Repairs are atomic and never discard the last valid profile revision without explicit service authorization.

12. Automatic Sequencing and Background Services

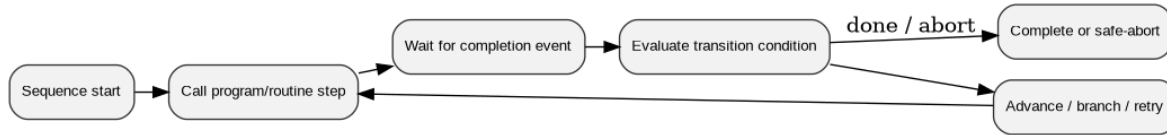


Figure 8. R07 automatic sequencing pattern.

12.1 R07 sequence tables

- Each sequence step identifies a Program or Routine request, completion event, timeout, next-step condition and safe-abort target.
- The sequence controller does not call deep blocking subroutines. It waits through the normal event system.
- Every automatic transition is also legal as a manual transition unless explicitly internal.
- Sequence progress is exposed through N02 and N30.
- A restart invalidates the active sequence and records the interrupted step; recovery returns inhibited.

12.2 Foreground and background ownership

Class	Examples	Rule
Foreground Program	P10, P20, P31	One active major Program.
Foreground Routine	R13 contact test, R15 timed action	One Program-owned modal Routine at a time.
Background service	R02 fact sample, R04 display, R05 panel, R06 alarm	Bounded periodic/event-driven service.
Exclusive hardware service	R15 timed action, storage write	Ownership token prevents simultaneous use.
Priority service	Alarm display and independent cutoff	Can preempt display or hardware request according to policy.

12.3 Optional displays

The CMC allowed optional monitor displays during many Programs without terminating them. ACE adopts the same concept: P30 pages and V11-V16 monitor commands may temporarily own the OLED while the active Program continues. KEY REL or Program prompts restore the appropriate owner.

13. Firmware Mapping and Migration

13.1 Required type changes

```
enum class MachineState : uint8_t {
    boot = 0,
    safe,
    standby,
    operate,
    fault
};

enum class AuthorizationState : uint8_t {
    inhibited = 0,
    prepared,
    armed
};
```

MachineState::program is removed or renamed to operate. ProgramCode active_program and ProgramPhase active_phase are owned by a new ProgramExecutive.

13.2 Event additions

Event family	Representative events
Program	program_requested, program_started, program_phase_changed, program_completed, program_aborted
Routine	routine_requested, routine_started, routine_completed, routine_failed
Command	key_pressed, command_committed, command_rejected, staged_data_changed
Prompt/display	prompt_raised, prompt_resolved, display_preempted, display_released
Safety facts	arm_changed, grip_changed, trigger_changed, inhibit_changed, feedback_changed
Alarm/recovery	alarm_raised, alarm_acknowledged, alarm_reset_requested, restart_detected, recovery_completed
Timing	tick, timeout, watchdog_restart

13.3 Current code correction

- Remove the Supervisor rule SAFE + program_request -> PROGRAM.
- Route program_request events to ProgramExecutive.
- After boot_complete, Supervisor enters SAFE and ProgramExecutive starts P00.
- ProgramExecutive may request SAFE -> OPERATE for P10/P11 entry, but the Supervisor decides based on current facts.
- Executive::run_once remains the single-event dispatcher, but dispatch order expands to Supervisor, ProgramExecutive, RoutineScheduler, CommandExecutive and other subscribers according to explicit routing.

13.4 Suggested implementation slices

1. Introduce ProgramCode, RoutineCode, VerbCode and NounCode wrappers plus P00.
2. Replace MachineState::program with operate and move program_request out of Supervisor.
3. Add ProgramExecutive with P00 and P30 descriptors and host tests.
4. Add CommandBuilder and regular V01/V06/V16/V37 behaviour against a small Noun table.
5. Add DisplayExecutive with ownership and KEY REL tests.
6. Add PromptManager with ENTR, PRO, ACK and RSET response contracts.
7. Add P12 simulation before P10 touches any real preparation interface.
8. Add P10 phase table using simulated HAL events, then bind individual Routines to real RevA hardware as it becomes available.

13.5 Test expectations

- Every descriptor code is unique and within its allocated range.

- Every writable Noun has a validator; every read-only Noun rejects load Verbs.
- Every Program has an entry policy, fallback Program and fault exit.
- Every flashing prompt has at least one terminating response and a safe timeout/default.
- No restart test returns authorization other than INHIBITED.
- Display preemption preserves or intentionally discards operator context according to a testable rule.
- Host tests exercise all Program/Verb/Noun compatibility entries without hardware.

14. Verification and Acceptance

14.1 Architectural acceptance

Requirement	Acceptance evidence
Program and machine state are independent	Unit tests show P20/P30 can run in SAFE and P10 requests OPERATE separately.
P00 is the default Program	BOOT_COMPLETE test results in SAFE + P00.
Table-driven command validation	Generated compatibility tests cover every Verb/Noun pair.
Prompt responses are distinct	ENTR, PRO, ACK, KEY REL and RSET have separate tests.
Display arbitration is bounded	Priority/preemption tests prove no unbounded stack or lost alarm.
Restart is inhibited	Recovery tests prove no armed/output state survives reset.
Panel revision fits expander budget	5 x 4 matrix + encoder + panel-present uses 13 input-expander lines.
Immutable tables fit flash/RAM budget	Build report and size regression recorded for each slice.

14.2 RevA control-module test progression

1. Host-only descriptor and flow tests.
2. Nano Every firmware build and memory-budget checks.
3. Panel emulator or serial-injected key events.
4. Actual keypad/encoder/OLED/talkback daughterboard.
5. Simulated sensor and direct-input harness.
6. P12 end-to-end dry run.
7. P10 with preparation and timed-action interfaces stubbed.
8. Hardware-in-the-loop binding only after each safety fact and feedback path is independently verified.

15. Integration Impact and Open Decisions

15.1 Superseded preliminary decisions

Earlier decision	Integrated decision
MachineState includes PROGRAM	Replace with OPERATE; Program code is independent.
Supervisor handles program_request	ProgramExecutive handles request; Supervisor only authorizes machine-state changes.
4 x 4 keypad	5 x 4 keypad to add PRO, KEY REL, SIGN, ACK and RSET while retaining Program/Verb/Noun entry.
Seven talkbacks	Eight talkbacks; add OPR ERR.
Simple menu model	Table-driven Program/Verb/Noun model plus Options, Checklists, Prompts and Routines.
Single display owner	Priority-arbitrated DisplayExecutive with one preserved operator context.
Program flow encoded ad hoc	Every Program has purpose, entry assumptions, phase table, recycle points and safe exit.

15.2 Hardware-manual revision impact

- NA-ACEHW-001 Section 11.1 changes from a 4 x 4 to a 5 x 4 matrix.
- Input-expander allocation changes to nine keypad lines, three encoder lines, panel-present and three spares.
- Talkback allocation uses eight outputs and adds OPR ERR.
- Panel legends add PRO, KEY REL, SIGN, ACK and RSET.
- No change is made to the direct safety-input policy or the separation of safety-critical outputs from I2C expansion.

15.3 Open decisions

- Exact profile component formats and ranges after output hardware characterization.
- Whether P21 profile editing is included in RevA firmware or deferred to RevB.
- Persistent-storage technology and number of profile/log slots.
- Exact alarm severity levels and which alarms permit automatic return to P00.
- Whether the Program field accepts one or two ENTR presses for complete Apollo-style compatibility.
- Whether a KEY REL lamp is worth adding in a later panel revision.
- LGC and AGS review may add useful sequence or abort conventions but must not collapse the ownership boundaries defined here.

Appendix A. Program/State Compatibility

Program	Permitted machine state	Authorization rule
P00	SAFE, STANDBY, FAULT fallback	INHIBITED
P01	BOOT	INHIBITED
P02	BOOT / recovery	INHIBITED
P06	SAFE -> STANDBY	INHIBITED
P10	SAFE entry; OPERATE run	INHIBITED -> PREPARED -> ARMED
P11	SAFE entry; OPERATE run	INHIBITED -> PREPARED -> ARMED
P12	SAFE	INHIBITED only
P20-P24	SAFE	INHIBITED
P30	SAFE, OPERATE, limited FAULT	Any; read-only
P31-P34	SAFE; limited FAULT for P33	INHIBITED
P40	SAFE with service condition	INHIBITED

Appendix B. Event Catalogue

Event	Meaning
EV_BOOT_COMPLETE	Startup invariants passed.
EV_PROGRAM_REQUEST	Manual or automatic Program request.
EV_PROGRAM_STARTED	Program entry completed.
EV_PROGRAM_PHASE	Program phase changed.
EV_PROGRAM_COMPLETE	Program completed normally.
EV_PROGRAM_ABORT	Program followed fault/termination exit.
EV_ROUTINE_REQUEST	Routine request accepted for scheduling.
EV_ROUTINE_COMPLETE	Routine completion result.
EV_COMMAND_COMMIT	Complete Program/Verb/Noun command committed.
EV_COMMAND_REJECT	Command rejected with operator-error reason.
EV_PROMPT_RAISED	Prompt acquired display ownership.
EV_PROMPT_RESPONSE	ENTR, PRO, ACK, KEY REL or RSET response.
EV_DISPLAY_RELEASE	Operator or prompt released display ownership.
EV_ALARM_RAISED	Alarm Manager receives a new alarm.
EV_ALARM_ACK	Presentation acknowledged.
EV_ALARM_RESET_REQUEST	Reset requested; descriptor decides eligibility.
EV_ARM_CHANGED	Physical arm input changed.
EV_GRIP_CHANGED	Grip input changed.
EV_TRIGGER_CHANGED	Trigger input changed.
EV_FEEDBACK_CHANGED	Gate/output or comparator fact changed.
EV_TIMEOUT	Bounded phase/routine timeout.
EV_RESTART_DETECTED	Reset cause captured for P02.

Appendix C. Source Traceability

Design topic	Source pages	ACE use
DSKY keys and lights	Delco PDF pp. 3-4	Distinct PRO, ENTR, KEY REL, RSET and OPR ERR behaviour.
Program and Routine catalogues	pp. 5-6	Separate major Programs and reusable Routines.
Verb catalogue	pp. 7-8	Systematic display/monitor/load families and executive Verbs.
Noun catalogue	pp. 9-14	One-to-three component descriptors, units, formats and load restrictions.
Alarm/option/checklist tables	pp. 15-17	Separate code spaces and explicit operator actions.
Display arbitration flags	pp. 23-24	Priority, normal and operator-owned display contexts.
Program procedures	pp. 40-101	Purpose, assumptions, sequence, flashing prompts, recycle and termination patterns.
R07 MINKEY	pp. 102-103	Automatic sequencing above individual Programs.

References

- [1] Delco Electronics, Apollo 15 - CM Software, Colossus 3 (Artemis Revision 72), CMC section, PDF pages 2-103.
- [2] NanoArc ACE Hardware and Operator-Panel Architecture Manual, NA-ACEHW-001, Revision A.0.
- [3] NanoArc Control System and HID Architecture Manual, Revision A.