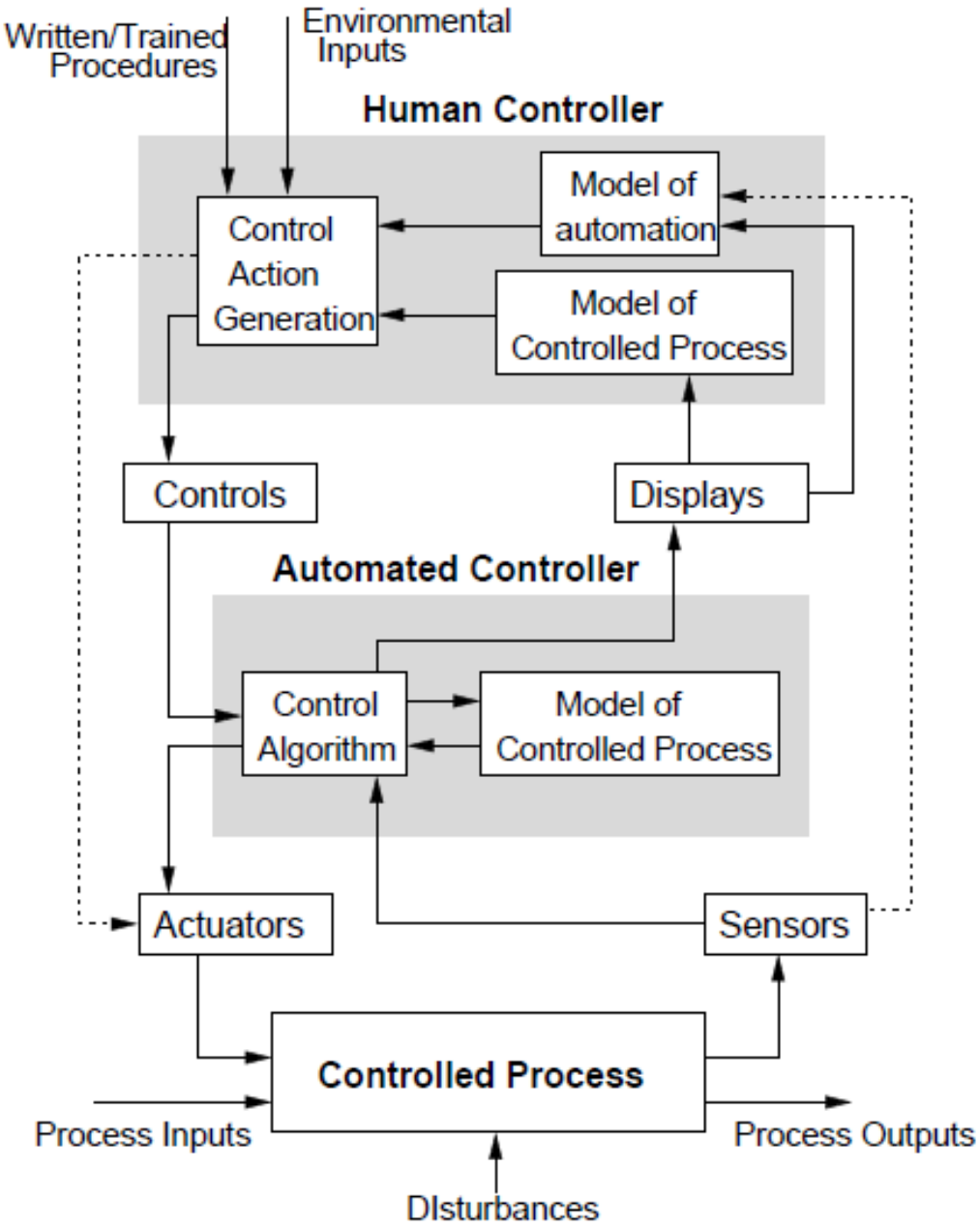
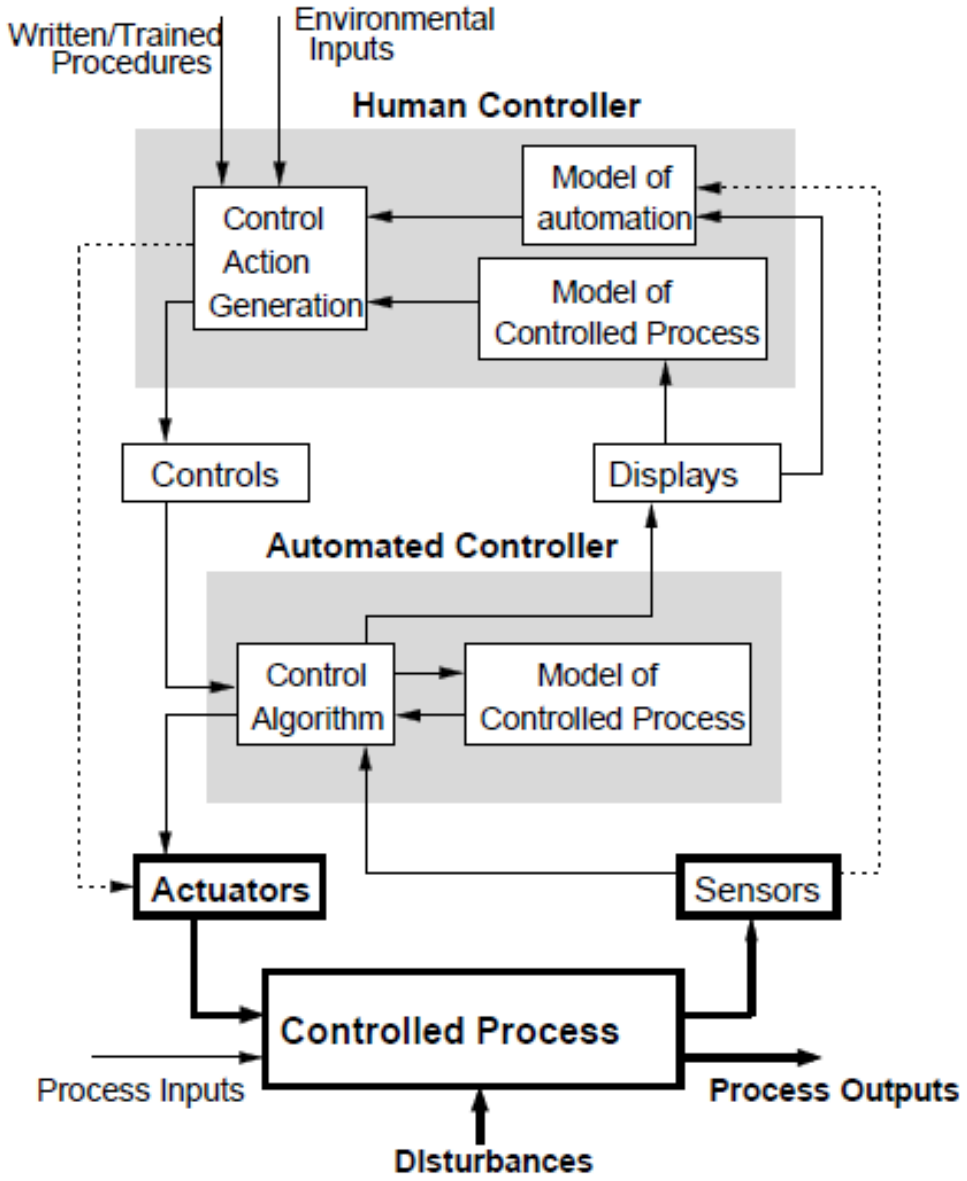
Design for Safety



Controlled Process/Physical Component



Safe Design Precedence

HAZARD ELIMINATION

- Substitution
- Simplification
- Decoupling
- Elimination of human errors
- Reduction of hazardous materials or conditions

HAZARD REDUCTION

- Design for controllability
- Barriers
  - Lockins, Lockouts, Interlocks
- Failure Minimization
  - Safety Factors and Margins
  - Redundancy

HAZARD CONTROL

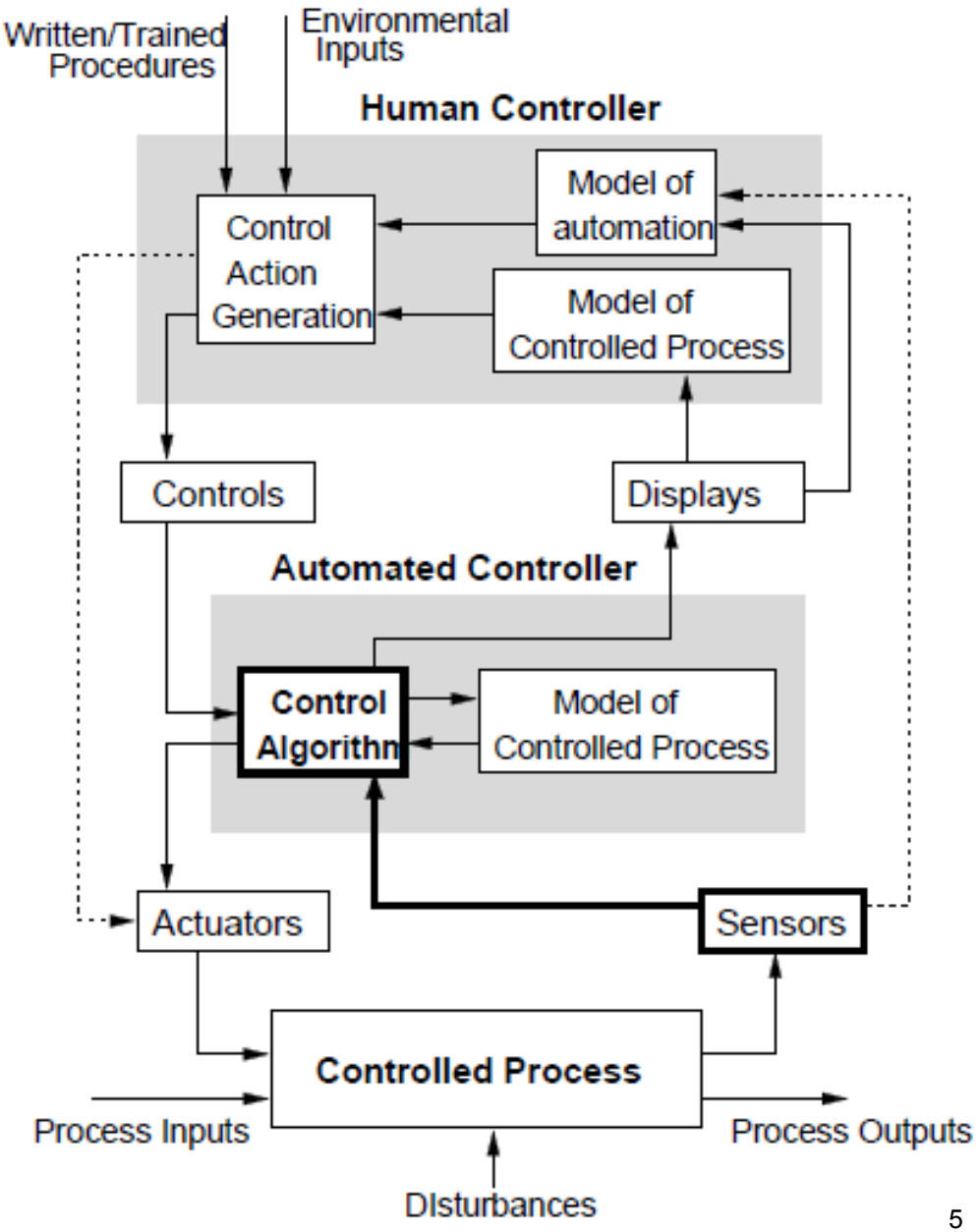
- Reducing exposure
- Isolation and containment
- Protection systems and fail-safe design

DAMAGE REDUCTION

Decreasing cost

Increasing effectiveness

Designing and Processing Inputs and Feedback



Designing and Processing Inputs and Feedback

- STPA provides information about what types of feedback needed
- Additional general design principles:
  - Design to respond appropriately to arrival of any possible input at any time and lack of expected input over a given time period.

    (e.g., target detection report from shutdown radar)
  - Check all inputs for out-of-range or unexpected values. Design response into control algorithm.
  - Specify max time computer waits until before first input and what to do if violated

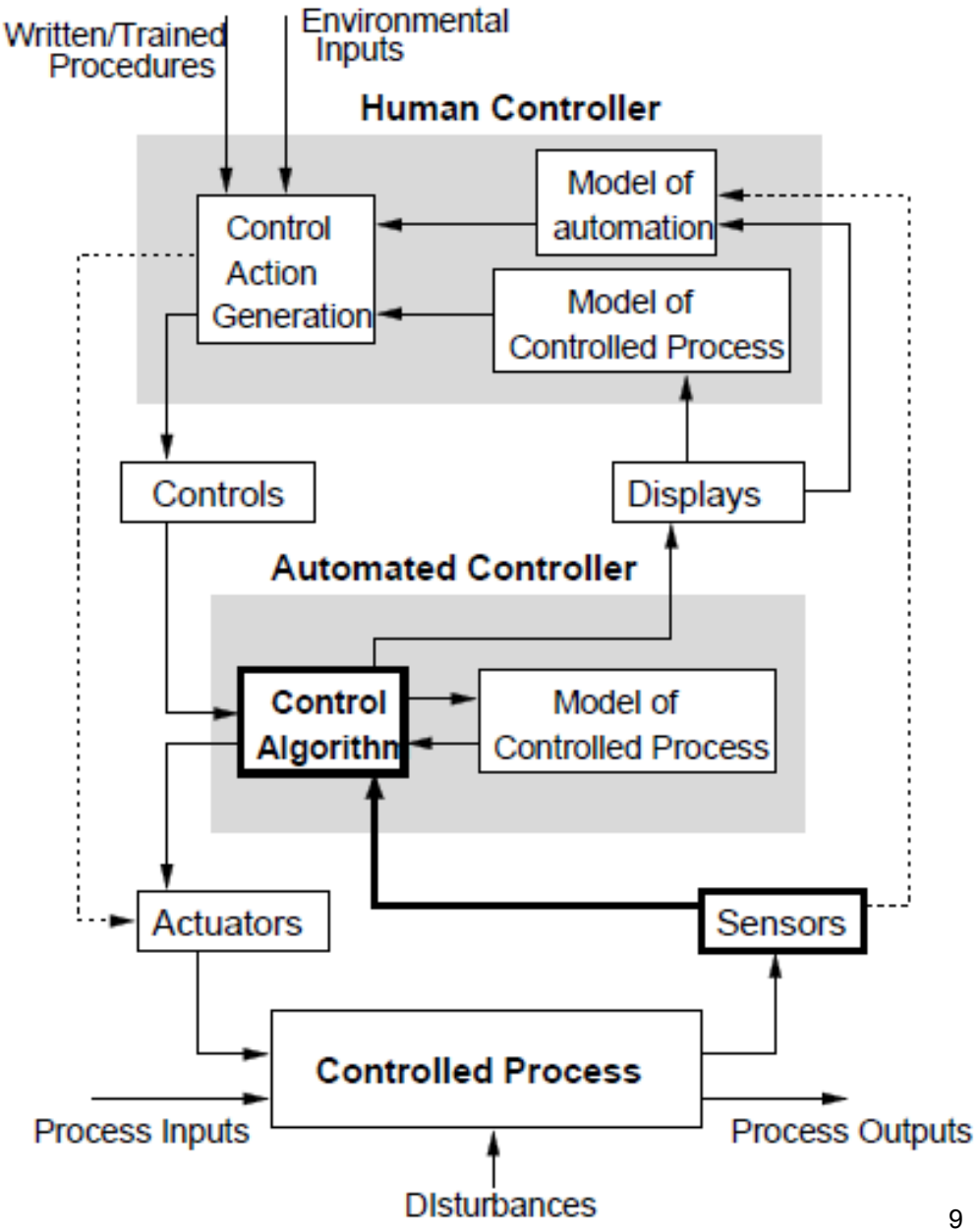
Designing and Processing Inputs and Feedback (2)

- Time bounds (min and max) should be checked for every input and appropriate behavior provided in case does not arrive within bounds.
- Specify response for non-arrival of an input (timeout) and excessive inputs (overload condition)
- Minimum arrival check for each physically distinct communication path (sanity or health check). Software should have the capability to query its environment with respect to inactivity over a given communication path

Feedback Loops

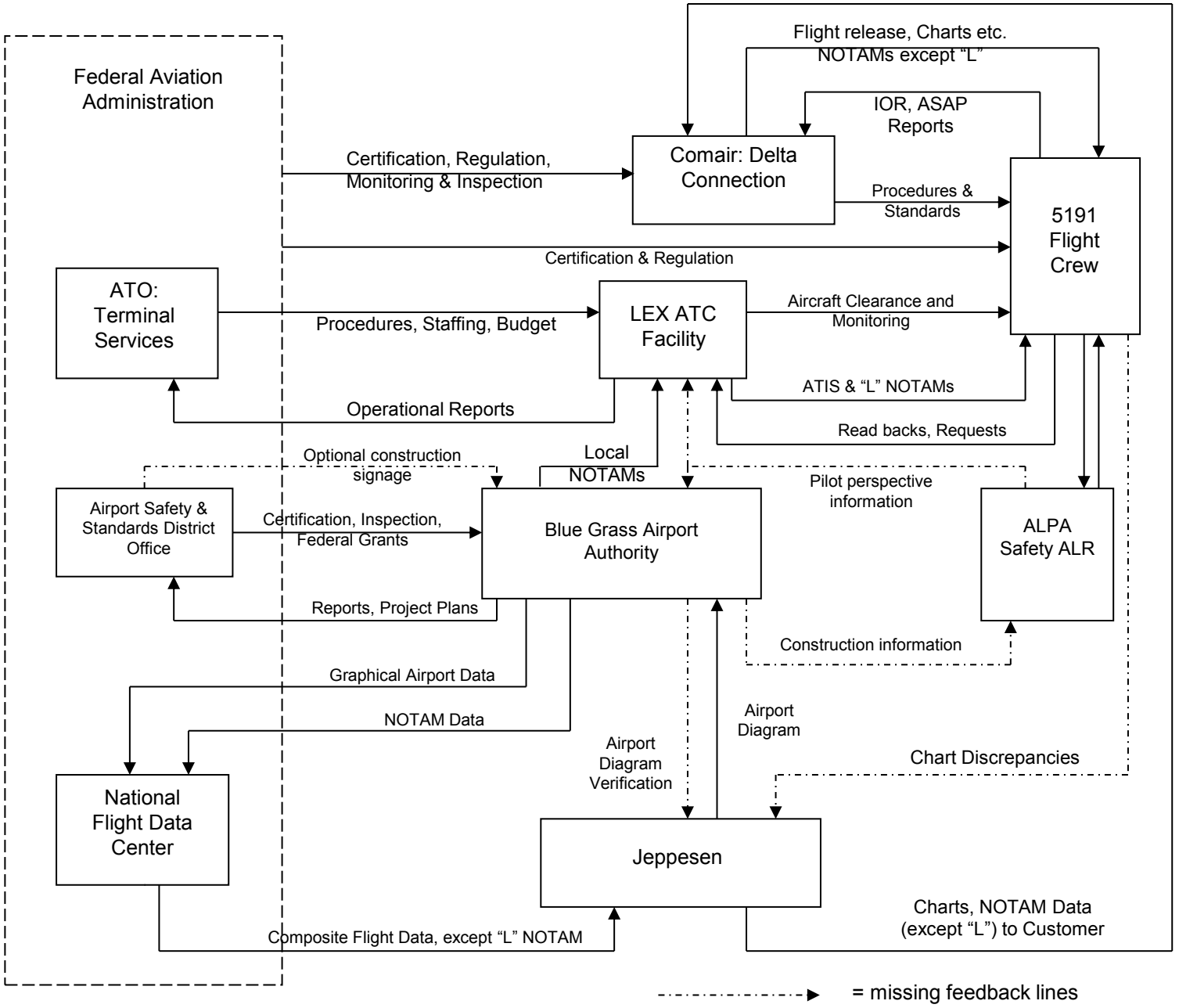
- Basic feedback loops, as defined by the process control function, must be included in algorithm along with appropriate checks to detect internal or external failures or errors.
- There should be an input that the software can use to detect the effect of any output on the process.
  - Not just that command arrived but actual execution
- Every output to which a detectable input is expected must have associated with it:
  1. Behavior to handle the normal response
  2. Behavior to handle a response that is missing, too late, too early, or has an unexpected value.

Initializing and Updating the Process Model

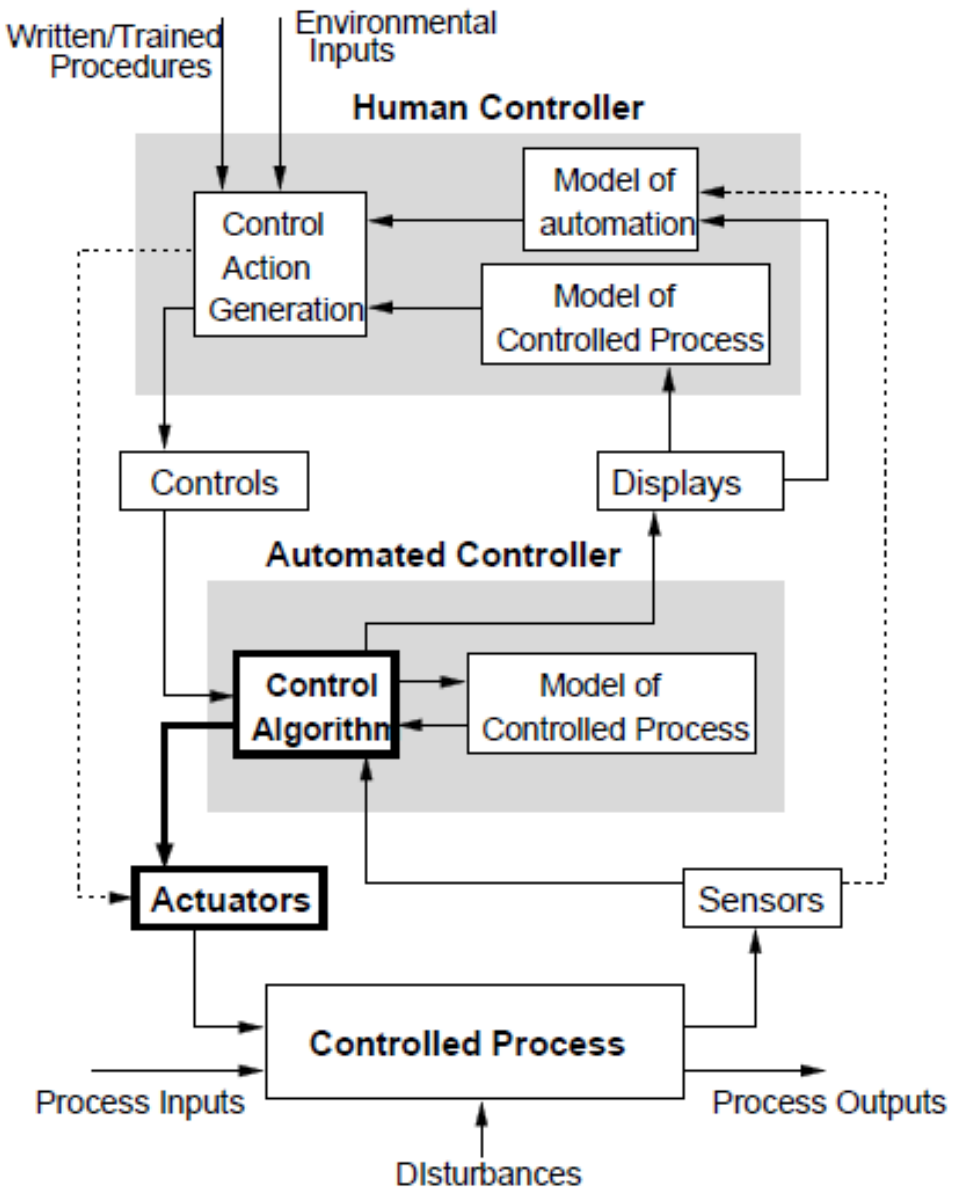


Initializing and Updating Process Model

- Process model must reflect actual process state at initial startup and after temporary shutdown.
  - Unknown state
- Must start in a safe state. Interlocks should be initialized or checked to be operational at system startup, including startup after temporarily overriding interlocks.
- Behavior of software with respect to inputs received before startup, after shutdown, or when computer is temporarily disconnected from process (off-line) must be specified or it must be determined that this information can be safely ignored.
  - National Flight Data Center (led to airport charts inconsistent with reality)



Producing Control Outputs



Producing Outputs

- For the largest interval in which both input and output loads are assumed and specified, the absorption rate of the output environment must equal or exceed the input arrival rate.
- Contingency action must be specified when the output absorption rate limit is exceeded.
- Behavior should be deterministic: only one behavior specified for arrival of any input in a particular state.

Data Age

- All inputs used in specifying output events must be properly limited in the time they can be used
- Output commands that may not be able to be executed immediately must be limited in the time they are valid.
- Incomplete hazardous action sequences (transactions) should have a finite time specified after which the software should be required to cancel the sequence automatically and inform the operator.
- Revocation of partially completed transactions may require:
  1. Specification of multiple times and conditions under which varying automatic cancellation or postponement actions are taken without operator confirmation
  2. Specification of operator warnings to be issued in case of such revocation

Latency Criteria

- Latency is the time interval during which receipt of new information cannot change an output even those it arrives prior to the output
  - Influenced by hardware and software design (e.g., interrupt vs. polling)
  - Cannot be eliminated completely
  - Acceptable length determined by controlled process

Fault Handling

Need to handle:

- Off-nominal states and transitions
- Performance degradation
- Communication with operator about fail-safe behavior
- Partial shutdown and restart (paths to and from fail-safe states)
- Hysteresis in transitions between off-nominal and nominal
  - Conditions that caused it to leave normal state may still exist
- Failure into safe state

16.630J / ESD.03J System Safety
Fall 2012