Control Design and Verification of Cyber-physical Systems: The Industrial Perspective

Leonardo Mangeruca
September 2017

Leonardo.Mangeruca@utrc.utc.com

Export Controlled: ECCN: No License Required.

This document contains no technical data subject to the EAR and the ITAR.
OUTLINE

The systems engineering process
Design drivers for cyber-physical systems
System controllability and requirements compliance
Refrigeration cycle and compressors
Compressor capacity control and anti-surge control
System-level control considerations
CYBER-PHYSICAL SYSTEM WIDE SCOPE

External Perturbation

Atmosphere (air, heat, pressure, radiation)
HMI (e.g. pilot/user commands, malicious attacks)
M2M (e.g., remote system reconfiguration, BITE, diagnostics monitoring, malicious attacks, user's devices)
Faults (HW/SW failures, equipment failures)

External Environment

Air, exhausts, contaminants (e.g., oil, refrigerant), data, etc.

External Interactions

Controller
(Possibly Distributed)

Sensing

Physical Plant

Actuating

Cloud
(Private/Public/Hybrid)

Cyber-physical System

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
CYBER-PHYSICAL SYSTEM

Atmosphere (air, heat, pressure, radiation)
HMI (e.g. pilot/user commands, malicious attacks)
M2M (e.g., remote system reconfiguration, BITE, diagnostics monitoring, malicious attacks, user's devices)
Faults (HW/SW failures, equipment failures)

Air, exhausts, contaminants (e.g., oil, refrigerant), data, etc.

Controller (Possibly Distributed)

Physical Plant

Cyber-physical System
Author(s): Leon Osborne, Jeffrey Brummond, Robert Hart, Mohsen (Moe) Zarean Ph.D., P.E, Steven Conger; Redrawn by User:Slashme.
Source: https://en.wikipedia.org/wiki/V-Model_(software_development)
License: This picture is in the public domain
SYSTEMS DEVELOPMENT LIFE CYCLE

Systems Development Life Cycle (SDLC)
Life-Cycle Phases

Initiation
- Begins when a sponsor identifies a need or an opportunity.
- Concept Proposal is created.

System Concept Development
- Defines the scope or boundary of the concepts.

Planning
- Develops a Project Management Plan and other planning documents.
- Provides the basis for acquiring the resources needed to achieve a solution.

Requirements Analysis
- Analyses user needs and develops user requirements.
- Create a detailed Functional Requirements Document.

Design
- Transforms detailed requirements into complete, detailed designs.
- Focuses on how to deliver the required functionality.

Development
- Converts a design into a complete information system.
- Includes acquiring and installing systems environment; creating and testing databases; preparing test case procedures; preparing test files; coding, compiling, refining programs; performing test readiness review and procurement activities.

Integration and Test
- Demonstrates that developed system conforms to requirements as specified in the Functional Requirements Document.
- Conducted by Quality Assurance staff and users.
- Produces Test Analysis Reports.

Implementation
- Includes implementation preparation, implementation of the system into a production environment, and resolution of problems identified in the Integration and Test Phases.

Operations & Maintenance
- Describes tasks to operate and maintain information systems in a production environment.
- Includes Post-Implementation and In-Process Reviews.

Disposition
- Describes end-of-system activities, emphasis is given to proper preparation of data.

Author(s): US Department of Justice (redrawn by Eugene Vincent Tantong)
License: This picture is in the public domain.
DESIGN CRITERIA

Design problem
Design a cyber-physical system with minimal cost for the customer and for the company subject to system requirements constraints

Cost and Efficiency
Availability
Reliability and Safety
Performance
Controllability
Observability

Business needs
System requirements (customer, regulations)
Design needs
Systems Development Life Cycle (SDLC)
Life-Cycle Phases

Initiation
- Begins when a sponsor identifies a need or an opportunity.
- Concept Proposal is created.

System Concept Development
- Defines the scope or boundary of the concepts.

Planning
- Develops a Project Management Plan and other planning documents.
- Provides the basis for acquiring the resources needed to achieve a solution.

Requirements Analysis
- Analyses user needs and develops user requirements.
  - Create a detailed Functional Requirements Document.

Design
- Transforms detailed requirements into complete detailed Systems Design Document.

Development
- Converts a design into a complete information system.
  - Includes acquiring and installing systems environment, creating and testing databases, preparing test case procedures, preparing test files, coding, compiling, refining programs, performing test readiness reviews, and procurement activities.

Integration and Test
- Demonstrates that developed system conforms to requirements as specified in the Functional Requirements Document.
  - Conducted by Quality Assurance staff and users.
  - Produces Test Analysis Reports.

Implementation
- Includes implementation preparation, implementation of the system into a production environment, and resolution of problems identified in the Integration and Test Phases.

Operations & Maintenance
- Describes tasks to operate and maintain information systems in a production environment.
  - Includes Post-Implementation and In-Process Reviews.

Disposition
- Describes end-of-system activities; emphasis is given to proper preparation of data.

Costs
- Non-Recurring Engineering (NRE) costs
- Operations and Maintenance costs
- Disposition costs

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
AVAILABILITY

Availability: $A = \frac{T_m}{T_m + T_d}$  

where

$A = availability$

$T_m = duration \ of \ mission$

$T_d = Down \ Time$

Operational availability: down time is observed during operations

Predicted availability: downtime is predicted using a model

$T_d = T_m \times \frac{MTTR + MLDT + MAMDT}{MTBF}$

$MTTR = Mean \ Time \ To \ Recover$

$MLDT = Mean \ Logistics \ Delay \ Time$

$MAMDT = Mean \ Active \ Maintenance \ Down \ Time$

$MTBF = Mean \ Time \ Between \ Failures$

Source: [https://en.wikipedia.org/wiki/Availability_(system)](https://en.wikipedia.org/wiki/Availability_(system))
AVAILABILITY

\[
A = \frac{T_m}{T_m + T_d}
\]
\[
T_d = T_m \times \frac{MTTR + MLDT + MAMDT}{MTBF}
\]

**Mean Time To Recover (MTTR)** is the length of time required to restore operation to specification. This includes three values: Mean Time To Discover, Mean Time To Isolate, Mean Time To Repair.

**Mean Time To Discover (MTTD)** depends on the failure detection system. In condition-based maintenance on-line diagnostics is used to discover failures. In planned maintenance systems periodic off-line diagnostics instruments are used during planned maintenance events.

**Mean Time To Isolate (MTTI)** is the average length of time required to identify a setting that needs to be adjusted or a component that needs to be replaced.

**Mean Time To Repair (MTTR)** is the average length of time to restore operation.

**Mean Logistics Delay Time (MLDT)** is the average time required to obtain replacement parts from the manufacturer and transport those parts to the work site.

**Mean Active Maintenance Down Time (MAMDT)** is the average time while the system is not 100% operational because of (planned) diagnostic testing that requires down time.
RELIABILITY

Reliability is defined as the probability that a device will perform its intended function during a specified period of time under stated conditions.

\[ R(T) = 1 - P_f\{t \leq T\} = P_f\{t > T\} = \int_T^\infty f(t)dt \]

where \( f(t) \) = failure probability density function

Terminology
System fault \( \rightarrow \) cause
System error \( \rightarrow \) effect
System failure \( \rightarrow \) observation

Source: https://en.wikipedia.org/wiki/Reliability_engineering
SYSTEM CRITICALITIES

Safety-critical system
Failure causes loss of life, injury, damage to the environment

Mission-critical systems
Failure causes failure of reaching some goal

Business-critical systems
Failure causes relevant economic losses
PERFORMANCE

Probability

Requirements  Capacity

Probability of unsatisfactory performance

Performance Value

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
External Perturbation

External Environment

External Interactions

\[ \dot{b} = F(x, d, u, b) \]

\[ y = G(x, d, u, b) \]

\[ \dot{z} = C(z, y, b) \]

\[ u = D(z, y, b) \]

Controller

Physical Plant

Cyber-physical System
**CYBER-PHYSICAL SYSTEM**

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
\[
F = D \ast (d_0 + b - d)
\]

\[
\dot{x}_1 = x_2
\]

\[
\dot{x}_2 = -\frac{c}{m}x_2 - \frac{k}{m}x_1 + \frac{F}{m}
\]

\[
d = x_1 + d_0
\]
HYBRID DYNAMICAL SYSTEMS

\[ \dot{x} = F(x, d, u, b) \quad y = G(x, d, u, b) \quad d' = n(x, d, u, b) \quad x' = r(x, d, u, b) \]

Continuous state \quad Discrete state \quad Manipulated Variables \quad External Interactions \quad External Perturbation \quad Next State Function \quad Reset Function

Bouncing Ball

Hybrid System

\[ H_P[[u, b]; \{y\}] \]

System Requirements (safety properties)

\[ H_R[[x, d, b, y]; \{R\}] \quad R \geq 0 \]

Author(s): Michael Maggs Edit by Richard Bartz
Source: https://en.wikipedia.org/wiki/Bouncing_ball
License: This picture is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license.


Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
SYSTEM CONTROLLABILITY

\[ \dot{x} = F(x, d, u, b) \quad y = G(x, d, u, b) \quad d' = n(x, d, u, b) \quad x' = r(x, d, u, b) \]

Controllability: The Linear Time Invariant Formulation

An LTI system is controllable if, for every \( x^* \) and every finite \( T > 0 \), there exists a control function \( u(t), 0 < t \leq T \), such that the system state goes from \( x(0) = 0 \) to \( x(T) = x^* \)

Controllability: A Formulation Suitable for Industrial Applications

A hybrid dynamical system is controllable if for every external perturbations there exists a control such that the system satisfies its requirements.

A hybrid dynamical system is controllable if for every \( b(t) \) there exists \( u(t) \) such that \( R(t) \geq 0 \).
Compliance: A Formulation Suitable for Industrial Applications

A hybrid dynamical system with a specific controller is compliant with the system requirements if for every external perturbations the system satisfies its requirements.

A hybrid dynamical system with a specific controller is not compliant with the system requirements if there exists b(t) and T > 0 such that R(T) < 0.

Compliance Falsification


\[
\begin{align*}
\dot{z} &= C(z, y, b) \\
u &= D(z, y, b) \\
\end{align*}
\]

Controller

\[
\begin{align*}
x &= F(x, d, u, b) \\
y &= G(x, d, u, b) \\
\end{align*}
\]

Physical Plant

\[
\begin{align*}
H_C[\{y, b\}; \{u\}] & \quad \parallel \quad H_P[\{u, b\}; \{y\}] \\
H_{PC}[\{b\}; \{y\}] & \quad \parallel \quad H_{PR}[\{x, d, b, y\}; \{R\}] \\
H_{PCR}[\{b\}; \{R\}] &
\end{align*}
\]
Domain Estimation Problem

Consider a function $f : D \to R$ and an interval $I \subseteq R$. We define the domain estimation problem requires us to identify a set $B$ of size $|B| = n$ of points $x \in D$ such that $f(x) \in I$: $B = \{x \in D | f(x) \in I\} \subseteq D$

Compliance Falsification

$$H_{PCR}[[b]; \{R\}] : D \to \mathbb{R} \text{ where } D = \{b(t)\} \text{ and } I = ]-\infty, 0]$$

S. Silvetti et al., "An Active Learning Approach to the Falsification of Black Box Cyber-Physical Systems", Logic in Computer Science, submitted May 2017
Enthalpy (H): Measurement of energy in a thermodynamic system. Thermodynamic quantity equivalent to the total heat content of a system.

Entropy (S): Measurement of the disorder or randomness of a system. $\Delta S = \frac{\Delta H}{T}$
REFRIGERANT PRESSURE TEMPERATURE CHART

Phase Diagram

Temperature-Pressure Chart

http://www.engineeringtoolbox.com/refrigerant-temperature-pressure-chart-d_1683.html

http://www.ref-wiki.com/

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
The compressor is the heart of the refrigeration system and it serves two basic functions:
Maintain the pressure in the evaporator so that the liquid refrigerant can evaporate at the required temperature
Compress the refrigerant so that it can condense at a normal temperature.

Protections
Over-pressurization (valve malfunction), overheating (loss of cooling, improper lubrication, valve malfunction), surging, leaks, vibrations (impeller imbalance or damage, worn bearings, misaligned shaft), loss of capacity (leaking valves or piston rings), motor overload (high discharge pressure, high motor amperage, bearing failure), high/low flow (excessive speed, suction restriction)

https://en.wikipedia.org/wiki/Compressor
The basic function of compressor control is to adjust the capacity of the compressor to the actual demand of the refrigeration system so that the required evaporating temperature can be maintained.

Compressor unloading
Reciprocating compressors utilize unloaders that lift the suction gas valve so that the piston do no compress the gas.
Screw compressors utilize a slide valve to cover the suction inlet ports, effectively shortening the length of the screws and reducing the resulting amount of compressed refrigerant vapor.

Compressor cycling
Cycling the compressor is a cost-effective and energy-efficient method for reducing capacity, especially when multiple compressors are used in the systems. However, cycling the compressors too frequently may result in compressor motor damage and failure.

Hot gas bypass
Hot gas bypass is a method that bypasses some of the high-pressure refrigerant gas (hot gas) discharged from the compressor back to the evaporator line without going through the condenser.

Variable speed control
Compressor capacity is varied by varying the speed of the motor driving the air compressor. The motor is controlled by an electronic system referred to as an inverter, frequency controller or variable speed drive. This is unlike conventional techniques that work by throttling the air flow into the compressor. Thus variable speed control is inherently more efficient in part-load conditions.
COMPRESSOR SURGE

A. Compressor operates at point A with flow $m_A$ at constant speed $N_4$

B. If flow rate is reduced to $m_B$ by closing a control valve on the delivery pipe.
   - The static pressure upstream of the valve is increased to $p_B$
   - Increased pressure $p_B$ is matched by the increased delivery pressure at B which is developed by the compressor

C. If the flow is further reduced to $m_C$ first and then to $m_S$
   - The increased pressures in the delivery pipe are again matched by the compressor delivery pressures at C and S

D. If the flow is further reduced to the point D
   - The pipe pressure is higher than the pressure at D

E. Due to lower compressor pressure, the pressure falls to $p_E$

This unbalance (at D and E) between the pipe pressure and the compressor delivery pressure only exist for a very short time. This is because there is higher pressure in the pipe than the gas pressure produced by the compressor and due to this reversing of the flow takes place and it leads to a complete break-down of the normal steady flow from the compressor to the pipe.

Due to flow reversal, pressure in the pipe falls and the compressor regains its normal stable operation (at B) delivering the gas at higher flow rate $m_B$. But the control valve still corresponds to the flow rate $m_D$. Due to this compressor’s operating conditions will again return to D through points C and S. And due to lower compressor pressure, the pressure falls further to $p_E$ and the entire phenomenon from point E to D repeats again and again and this cycle EBCSDE known as the surge cycle.

https://en.wikipedia.org/wiki/Centrifugal_compressor
ANTI-SURGE CONTROL

Suction Line

Vapor In

Compressor 1

Vapor Out

Discharge Line

Anti-surge control

ASV

Process control

\( \omega_1 \)
Gravdahl-Egeland

\[ \frac{d\omega}{dt} = \frac{1}{J} (\tau_{\text{drive}} - \tau_{\text{comp}}) \]  \hspace{1cm} (1)

\[ \frac{d\psi_c}{dt} = \frac{1}{t_\psi} (\psi_{c,ss}(\hat{m}_1, \omega) - \psi_c) \]  \hspace{1cm} (2)

\[ \frac{dm_c}{dt} = \frac{A_c}{L_c} (p_1 \cdot \psi_c - p_2) \]  \hspace{1cm} (3)

\[ \psi_{c,ss} = c_0(\omega) + c_1(\omega) \cdot \hat{m}_1 + c_2(\omega) \cdot \hat{m}_1^2 + c_3(\omega) \cdot \hat{m}_1^3 \]  \hspace{1cm} (4)

\[ \tau_{\text{comp}} = \sigma \cdot r^2 \cdot |\hat{m}_1| \cdot \omega \]  \hspace{1cm} (5)

**Author(s):** Sunilchaudhary2  
**Source:** [https://en.wikipedia.org/wiki/Compressor_characteristic](https://en.wikipedia.org/wiki/Compressor_characteristic)  
**License:** This picture is licensed under the [Creative Commons Attribution-Share Alike 3.0 Unported license](https://creativecommons.org/licenses/by-sa/3.0/).


*Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.*
Limitations on pressure rise per stage and economic considerations lead to process designs utilizing compressors in series and parallel configurations or combinations of both to meet operability requirements.

The safe operating envelope of centrifugal compressors is defined by the constraints due to surge and choke phenomena as well as minimum and maximum speed limits.

The interactions between process and anti-surge control, already present in a single compressor, become more difficult to handle when multiple compressors are considered.

Poor control design can lead to undesirable oscillations in process operating conditions, cascaded surge events and complete plant shut-downs.

Increasing the compressor speed leads to more mass flow through the whole system and to a higher discharge pressure. The speeding up compressor takes more compression load and moves towards the surge line. Increasing speed of 1st compressor leads to increase of discharge pressure for both. Increasing speed of 2nd compressor leads to reduction of discharge pressure of 1st compressor. ASV action moves the compressor away from the surge line. The recycling compressor takes a lower share of compression load and moving the other compressor towards the surge line.

Compressor 1

Compressor 2

Anti-surge Control 1

Anti-surge Control 2

ASV

ASV

ω₁

ω₂

Speed Control 1

Speed Control 2

M. Mercangoz et al., "Coordinated Operation of Centrifugal Compressors in Series via Model Predictive Control", ASME Proceedings
M. Mercangoz et al., "Coordinated Operation of Centrifugal Compressors in Series via Model Predictive Control", ASME Proceedings

Created at UTRC-Italy – This document contains no technical data subject to the EAR and the ITAR.
SUMMARY

The design of cyber-physical systems is driven by cost subject to system requirements compliance constraints.

System requirements impose performance, reliability/safety and availability constraints.

The physical plant design is subject to controllability under perturbations to maintain system requirements compliance.

Compliance violation detection (falsification) can be formulated as a domain estimation problem.

Physical plant architecture drastically affects controllability under perturbations.

Control architecture significantly affects controllability under perturbations.
THANK YOU

Contact: Leonardo.Mangeruca@utrc.utc.com
Leader of System Analysis, Control & Optimization Group in UTRC-Italy

United Technologies Corporation: http://www.utc.com
United Technologies Research Center: http://www.utrc.utc.com

More resources:
United Technologies Corporation, Moving the World Forward – Overview
United Technologies Corporation, UTC Investor and Analyst Meeting, 2017 Webcast
United Technologies Corporation, Moving the World Forward – 2015 Annual Report
United Technologies Corporation, Innovation – 2011 Annual Report