INTERACTIVE CONTROL ENGINEERING
Principles and Applications

Volume 20 Motion Control, Robotics, and Autonomous Systems

CHAPTER 15

Collaborative Robot Speed and Separation Simulator With a Truth Audit

Pages 354–379

Edited by John D. Hedengren

How to cite this chapter. "Collaborative Robot Speed and Separation Simulator With a Truth Audit," in *Motion Control, Robotics, and Autonomous Systems*, John D. Hedengren, Ed., vol. 20 of *Interactive Control Engineering: Principles and Applications*. Advanced Process Solutions, LLC, 2026, ch. 15, pp. 354–379.

The page numbers in this file are those of the printed volume.

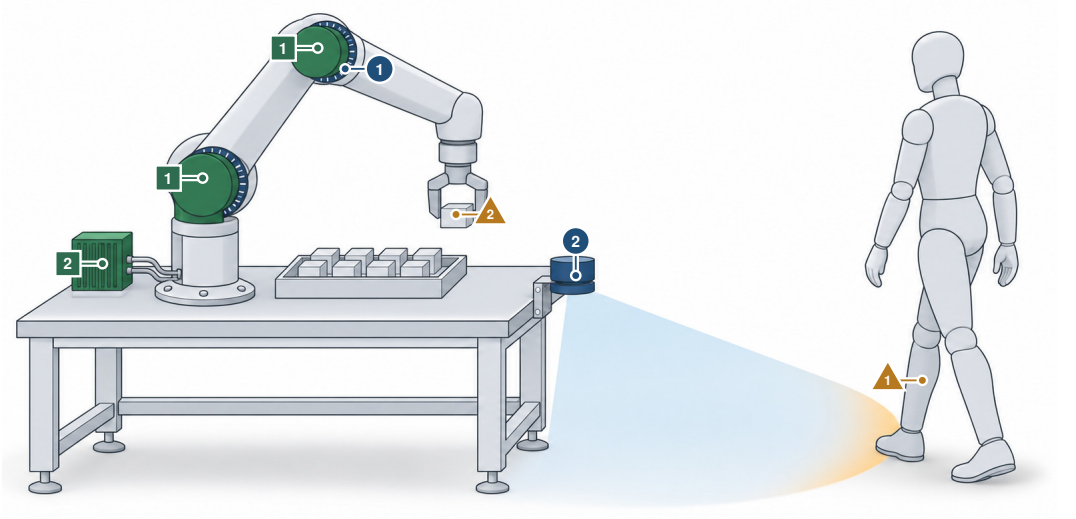
The app for this chapter
https://apmonitor.com/apps/cobot-safety/

The volume online: contents, other chapters and citation records
https://apmonitor.com/apps/books/v20-motion-robotics/#cobot-safety

Copyright © 2026 Advanced Process Solutions, LLC. All rights reserved. Produced by Advanced Process Solutions, LLC.

CHAPTER 15

Collaborative Robot Speed and Separation Simulator With a Truth Audit



The controller moves 1 drives at the shoulder and the elbow 2 the controller that sets the arm's speed ceiling

The controller reads 1 joint encoders 2 safety laser scanner that finds the person

What disturbs it 1 the person walking in 2 a part heavier than the program believes

Notice that the scanner, not a fence, keeps the person safe: the arm slows as the person comes closer and must always be able to stop in time. Illustration, not to scale.

IN PLAIN TERMS A Robot Arm That Slows for People

The main idea. A collaborative robot works beside people with no fence between them. A scanner watches each person, and the arm slows as a person comes closer, so that it can always stop in time.

The challenge. The scan is always a little late and a little off, and a loaded arm needs more time to stop. A supervisor that trusts a hopeful braking figure acts too late, and only a replay of the truth shows how close the person came.

Why it matters. Every bit of safety distance costs parts made, so an honest stopping model keeps a shared cell both safe and busy.

THREE WAYS TO READ THIS CHAPTER

Explore	12 min	the first page, the two history segments (Section 15.2), the fact on walking speed (Section 15.4), the try-it segments of cases 2 and 5 and the fact on latency (Section 15.6) and the key points
Study	50 min	the whole chapter with its three pause points and the twelve exercises at its end
Practice	20 min	the first page, the measured cases (Section 15.6), Technology in Practice (Section 15.7), Limitations (Section 15.8) and the open challenges

The control question A collaborative robot without a fence must be able to stop before a person walking in can reach it, so its safe speed shrinks as the person comes closer. How large is that protective distance term by term, what does each term cost in throughput, and how can a supervisor that sees only a late, noisy scan be checked against the truth?

Learning objectives

- Compute the protective separation distance and its terms from the reaction chain, the braking model and the uncertainties.
- Solve the speed law for the fastest tool speed a measured separation allows, and explain why it needs a margin and a restart hysteresis.
- Explain why an optimistic braking figure misjudges the stop mostly in time, and read a truth audit that exposes it.
- Compute the contact speed that power and force limiting allows for a body region from the reduced mass and the region's stiffness.
- Weigh a raised collision threshold against a corrected friction model.

Prerequisites Sections 1.4.9 (stopping distance, protective separation and speed law), 1.4.2 (arm dynamics), 1.4.8 (landing force), 1.3 (loop action) and 1.6.4 (scenarios, scorecard and CSV file). Chapter 9 treats believed against true braking on a mobile robot.

The app https://apmonitor.com/apps/cobot-safety/

See also Volume 4, Chapter 2 for a protective override that rests at its clamp and is judged by its margin to a limit. Volume 8, Chapter 13 for a latched supervisor whose product history is logged apart from its instruments, and Volume 8, Chapter 2 for a safety layer that guards a hazard with no symptom in the controlled variable.

15.1 Introduction

Collaborative robots are bought to work in the same space as people, and the fence that used to separate the two was a safety function in its own right. New paradigms in industrial robotics no longer require physical separation between manipulators and people, and safety can then be posed as a hard constraint on the robot's motion, met while productivity is kept as high as possible [1]. A survey of collaborative robotics for industry relates actuation, control, safety, physical interaction, usability and productivity, and finds that the way an application is organized affects both its quality and its safety [2]. The requirements for industrial robots are set by ISO 10218 [3], and ISO/TS 15066 supplements them for collaborative operation [4, 5]. Two of its methods are feedback problems. Speed and separation monitoring, as the specification presents it, keeps a minimum protective distance between the robot and the person [6], and power and force limiting, which the application takes from the same specification, admits contact at a speed whose impact a body region can bear, the question that crash tests of robots address [7].

The protective distance is a budget of distances that all move at once. In the cell of this chapter it is 1448 mm at 1.00 m/s with a 3 kg part and a 170 ms reaction chain, and 840 mm of that is the person's own approach while the arm reacts and brakes. At rest it is still 532 mm, more than the 214 mm that the arm's path leaves a person standing at the table. The simulator is built against three beliefs. The first is that a slow enough arm is safe near a person, but an unmonitored arm held at 25 % of its speed still gives 6 violation episodes in a minute, the worst 410 mm short of the distance the truth requires. The second is that the stopping distance is the term to get right, but a brochure braking figure of 5 m/s^2 misjudges the stop of the loaded arm by 67 mm in distance and by 440 ms in time, and the time costs 704 mm of the person's walk. The third is that an optimistic model at least buys throughput. With the brochure figure the cell completes 7 cycles in a minute, the same 7 as with an honest model, and a truth audit finds 6 violation episodes, the worst 506 mm short.

The class of problem is general. A supervisor that watches a primary controller and intervenes when a safety constraint is about to be lost is a runtime assurance system, of which the automatic ground collision avoidance of military aircraft is a working example, and safety filtering of this kind

is now studied for complex control systems in general [8]. In a robot cell the filter acts on a speed. The separation can be adapted to the direction of the robot's motion as well as to the distance, and continuous adaptation of the velocity was found to beat zone-based supervision and physical barriers in productivity, by an amount that depends on how often and when an operator comes near [9]. Metrics for speed and separation monitoring accordingly quantify both the safety and the effect on production [10]. A mobile robot braking for a walker, a crane slewing near a worker and a road vehicle with automatic braking have the same shape, with a stopping model that must be honest, a measurement that is old when it is used, a threshold that needs hysteresis, and a verdict that only the true state can give. A transfer function from speed override to tool speed carries none of these.

However, the monitoring literature measures implementations on physical cells [6, 9], and the collision literature evaluates detection on physical arms [11], so a student has no plant on which the budget can be read term by term while a person walks in, one term changed, and the throughput and a verdict of safety compared side by side. This chapter itemizes the protective separation distance on a collaborative cell simulator in which every term of the budget is a setting, the stopping behavior comes from the arm's own torque limits, and each supervisory decision is audited against where the person truly was and how the arm truly stops. The protective separation distance, the speed law, power and force limiting and the momentum observer follow the standard's formulas and the literature. The model can be rebuilt from this text alone. Its controller sees nothing but its encoders, its drive torques, a hand-over button and a delayed scanner, its braking model is derived from the drives' torque limits along the program, and its audit replays the controller's own trajectory generator and servos on a copy of the true arm. Eight cases and a graded shift isolate the terms of the budget one at a time.

Section 15.2 traces the domain. Section 15.3 gives the model of the cell, and Section 15.4 the budget, the speed law built on it, the stop it assumes, the contact allowed instead and the truth audit. Section 15.5 describes the controller as implemented, and Section 15.6 measures the eight cases and the shift. Section 15.7 sets the model beside the scanners, drives and controllers of real cells, Section 15.8 states the limitations, Section 15.9 draws the results together, and the exercises of Section 15.10 work through the budget, the law and the cases.

15.2 From Fenced Cells to Shared Workspaces

For most of their history industrial robots moved where no person was meant to be, and robot accidents were being analyzed for their causes and effects by 1987 [12]. The requirements for the robot itself were collected in ISO 10218, whose 2011 edition of part 1 is one of the two parts the simulator follows [3]. BSI records that edition as withdrawn on 17 March 2025, when a new edition replaced it.

Robots built to work with a person rather than apart from one came next. The collaborative robot, or cobot, was described in 2001 as a machine for direct physical interaction with a human operator, one that creates smooth and strong virtual surfaces in a shared workspace while it steers a single mechanical degree of freedom [13]. The question of how hard a robot may strike a person was then taken to measurement, as the first history segment below tells.

> ⧖ HISTORY **Crash-Testing a Robot Arm, 2009**
>
> How hard a robot may strike a person was taken to measurement. A lightweight robot arm was impact-tested at the standard crash-test facilities used for automobiles, and industrial robots of different weights were then evaluated from the results, with the influence of the robot's mass and velocity investigated. Free impacts captured only part of the problem. The study identified the quasi-static constrained impact, in which the robot presses a body part against something, as a possible serious threat to a person even from a robot of low inertia, and it classified the injuries relevant to robotics [7].

Detecting a contact without extra sensors followed, and the second history segment, at the end of this section, traces it from 2005 to 2017. The two-link planar robot of its first study is the plant that carries the observer in this simulator.

Standards then gave the methods a common form. ISO/TS 15066 was published in February 2016 as a supplement to ISO 10218 [5], and it specifies safety requirements for collaborative industrial robot systems and their work environment [4]. Its minimum protective distance for speed and separation monitoring was examined analytically and in tests, with its input values, implementation specifications and performance expectations [6]. The approach speed of the person belongs to an older standard, which positions safeguards, laser scanners among them, by the approach speeds of parts of the body, walking and upper-limb movement, and gives a method for the minimum distance from a detection zone to a hazard [14]. Compliance does not remove every hazard, and a residual hazard potential in case of an incident has been illustrated with an experiment on a standard collaboration scenario [5]. What the simulator of this chapter adds to these pieces is a record that a physical cell cannot keep, the true separation and the true stop behind every decision of its supervisor.

> ⧖ HISTORY **A Collision Sensed Without a Sensor, 2005 to 2017**
>
> In 2005 a collision between a robot arm and an obstacle of unknown shape and place was treated as a fault of the arm's actuating system. A dynamic fault detection and isolation technique, which needs neither acceleration nor force measurements, found a collision at any point along the arm with the joint encoders alone and named the link that was struck. Its results were simulations of a two-link planar robot [15]. A survey of 2017 reviewed, extended and evaluated experimentally such model-based detection, isolation and identification from proprioceptive sensors only. It reported that the physically motivated solution had been applied to manipulators, humanoids, flying robots and commercial products [11].

15.3 The Shared Cell

Figure 15.1 shows the cell from above. The origin is at the arm's shoulder, $+y$ points from the robot toward the aisle, and the front edge of the robot's table lies at $y = 0.90\,\mathrm{m}$. A feeder P at $(-0.56, 0.26)$ m supplies parts, a fixture Q at $(0.56, 0.26)$ m receives them, and a hand-over point H at $(0.06, 0.72)$ m, with a lamp, is where a part can be handed to the person. The twelve integrated states are the two joint angles q_1 and q_2, their rates ω_1 and ω_2, and for the person's torso and hand a two-dimensional displacement from a scripted anchor with its rate. The person's script, the gripper, contact episodes, the reflex timing and the truth audit are discrete and are updated after each integration step, never inside the derivative function. The signals are classified in Table 15.1.

15.3.1 The Arm

The two joints have vertical axes, so the links sweep the plane of the table, gravity does no work, and the arm obeys Equation (15.1), the arm dynamics of Equation (1.2) with a friction scale and a contact torque added.

$$M(q)\,\ddot{q} + C(q,\dot{q})\,\dot{q} + \varphi F(\dot{q}) = \tau + J_c^{\mathsf{T}} f_c, \qquad |\tau_i| \le \tau_{i,max} \tag{15.1}$$

where $q = [q_1, q_2]^{\mathsf{T}}$, both angles counterclockwise seen from above, F is the joint friction with its true scale φ, and $J_c^{\mathsf{T}} f_c$ is the torque of any contact force. The links are uniform rods of lengths l_1, l_2

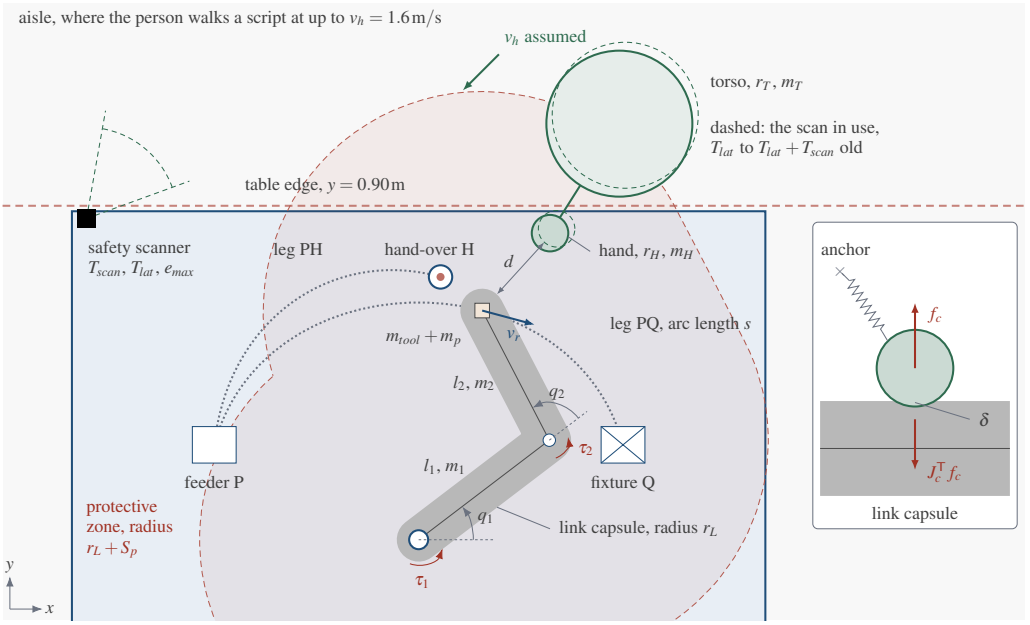


Figure 15.1 Plan view of the shared cell, to scale apart from the magnified contact on the right. The upper arm of length l_1 turns through q_1 from the x axis and the forearm of length l_2 through q_2 from the upper arm, driven by τ_1 and τ_2, and each link is a capsule of radius r_L. The tool carries m_{tool} and, while a part is held, its mass m_p along leg PQ at v_r. The person's torso and hand are discs of radii r_T and r_H carrying the effective masses m_T and m_H on supports to a scripted anchor, and the dashed discs are the scan the supervisor is using, from which it measures the separation d. The shaded capsule of radius $r_L + S_p$ is the protective zone at $S_p = 0.54\,\mathrm{m}$, a little above its value at rest. A contact overlap δ pushes the body with f_c and the arm with $-f_c$ through the contact Jacobian J_c. The scanner is drawn at the table's corner but has no geometry in the model.

Table 15.1 Signals of the Cell by Role, With Their Defaults

Symbol	Role	Default	Range
q_1, q_2	states, CVs of the servos	114.8°, 87.0°	the paths
ω_1, ω_2	states, joint rates	0	—
ξ_T, $\dot{\xi}_T$	states, torso on its support	0	—
ξ_H, $\dot{\xi}_H$	states, hand on its support	0	—
τ_1, τ_2	MVs, joint torques	held 10 ms	±20, ±14 N m
v_{cap}, α	MV of the supervisor, ceiling	v_{nom}, 100 %	0–100 %
—	DV, the person's script	per case	scripted legs
λ_v	DV, walking speed scale	100 %	30–100
λ_m	DV, true part mass	100 % of m_L	50–200
φ	DV, true gearbox friction	100 %	50–300
—	DV, scanner dropout	off	1.5 s event
q_m	measured, joint encoders	17 bit	—
τ	measured, drive torques	as applied	—
$\hat{p}_T$, $\hat{p}_H$	measured, scan of the person	40 ms, 100 ms late	≤ 40 mm off
—	measured, hand-over button	off	on, off
d, S_p	supervisor's separation, budget	—	—
d_{true}	truth, the audit's separation	—	—

and masses m_1, m_2, and a point mass $m_{tip} = m_{tool} + m_p$ at the tip carries the wrist, the gripper and any part held. With $l_{ci} = l_i/2$ and $I_i = m_i l_i^2/12$ the inertia coefficients and the remaining terms are given by Equation (15.2).

$$\begin{aligned} a_1 &= m_1 l_{c1}^2 + I_1 + (m_2 + m_{tip})\, l_1^2 + J_{1m} \\ a_2 &= m_2 l_{c2}^2 + I_2 + m_{tip}\, l_2^2, \qquad a_3 = (m_2 l_{c2} + m_{tip} l_2)\, l_1 \\ M &= \begin{bmatrix} a_1 + a_2 + 2a_3 \cos q_2 & a_2 + a_3 \cos q_2 \\ a_2 + a_3 \cos q_2 & a_2 + J_{2m} \end{bmatrix} \\ C\dot{q} &= a_3 \sin q_2 \begin{bmatrix} -(2\dot{q}_1\dot{q}_2 + \dot{q}_2^2) \\ \dot{q}_1^2 \end{bmatrix} \\ F_i &= b_i \dot{q}_i + f_{ci} \tanh(\dot{q}_i / 0.05) \end{aligned} \tag{15.2}$$

where J_{1m} and J_{2m} are the motors' rotor inertias reflected through their gears, b_i and f_{ci} are the viscous and Coulomb coefficients of each joint, and the hyperbolic tangent smooths the Coulomb term over 0.05 rad/s. At the feeder pose the empty arm has $M_{11} = 2.273\,\mathrm{kg\,m^2}$ and $M_{22} = 0.483\,\mathrm{kg\,m^2}$, and the 3 kg part raises them to 3.416 and $0.963\,\mathrm{kg\,m^2}$. The generalized momentum $p = M(q)\dot{q}$ obeys $\dot{p} = \tau + C^{\mathsf{T}}\dot{q} - \varphi F + J_c^{\mathsf{T}} f_c$, because $\dot{M} = C + C^{\mathsf{T}}$, and for this arm $C^{\mathsf{T}}\dot{q} = [0,\ -a_3 \sin q_2\, (\dot{q}_1^2 + \dot{q}_1\dot{q}_2)]^{\mathsf{T}}$. That identity is what the collision observer of Section 15.5 integrates.

Velocity is affine along each rigid link, so the fastest point of the arm is the elbow or the tip, and its speed $v_r = \max(l_1|\dot{q}_1|,\ \|J(q)\dot{q}\|)$ is the robot speed in the protective distance. On every path of this program the tip is the fastest point. A body struck at a point of the arm along a direction $\hat{n}$ meets the operational-space mass $m_{eff} = 1/(\hat{n}^{\mathsf{T}} J_p M^{-1} J_p^{\mathsf{T}} \hat{n})$ of that point [16]. Along its direction of travel the gripper presents 3.3 to 5.4 kg empty and 6.5 to 9.0 kg with the part.

15.3.2 The Person

The person is a torso disc of radius $r_T = 0.20\,\mathrm{m}$ and a hand disc of radius $r_H = 0.05\,\mathrm{m}$ in the plane of the links. A script moves an anchor through legs that walk to a point, accelerating and stopping at $2\,\mathrm{m/s^2}$ and never faster than 1.6 m/s, pause, reach the hand out to at most 0.62 m from the torso's center, hold it, withdraw it, move it across, lean over the table, press the hand-over button, wait for the lamp, wait for a part with a given patience, or repeat. A walking-speed disturbance λ_v scales every walk. The torso and the hand are each a mass on a soft support to the anchor, so a strike pushes a body part of the right effective mass, as shown in Equation (15.3).

$$\begin{aligned} m_B \ddot{\xi}_B &= f_{c,B} - m_B \omega_B^2\, \xi_B - 2\zeta_B m_B \omega_B\, \dot{\xi}_B \\ p_B &= a_B(t) + \xi_B \end{aligned} \tag{15.3}$$

where $B \in \{T, H\}$, $a_B(t)$ is the scripted anchor, ξ_B the displacement from it, $m_T = 40\,\mathrm{kg}$ and $m_H = 0.6\,\mathrm{kg}$ are the effective masses of the chest and hand regions, $\omega_T = 2\pi \cdot 2\,\mathrm{Hz}$, $\omega_H = 2\pi \cdot 5\,\mathrm{Hz}$ and $\zeta_B = 0.7$. A hand that is not reached out lies inside the torso and cannot be struck on its own. A struck person reacts after 0.15 s, straightening up from a lean or pulling a held hand back.

15.3.3 Contact

Where a body disc overlaps a link capsule, a unilateral spring pushes the two apart along the line between their closest points, as shown in Equation (15.4).

$$\begin{aligned} \delta &= r_L + r_B - \|p_B - p_L\| \\ F &= \max\big(0,\ k_B\,\delta + c_B\,\dot{\delta}\,\min(1,\ \delta/1\,\mathrm{mm})\big), \qquad f_c = F\,\hat{n} \end{aligned} \tag{15.4}$$

where p_L is the closest point on the link's centerline, $\hat{n}$ the unit vector from it to the body, k_B the body region's effective stiffness and $c_B = 2\zeta_c\sqrt{k_B m_B}$ with $\zeta_c = 0$, an elastic contact. The force enters the

arm through the Jacobian of the contact point. The body-region values of Table 15.2 are illustrative teaching values, in the manner of the body model of ISO/TS 15066 as the application describes them, and not the standard's tables. For two bodies meeting through such a spring the peak force is $v\sqrt{\mu k}$, Equation (1.15) with the reduced mass μ in place of the moving mass, and the application's check drives the tip at 0.6 m/s into a hand and a chest and finds peaks of 121.0 and 186.5 N against predictions of 119.2 and 187.0 N, with contacts lasting 9 ms and 40 ms. An episode starts above 0.5 N and its peak is compared with the region's limit.

15.3.4 Scanner and Separation

Every T_{scan} the safety scanner captures the torso and, once the hand is out of the torso's outline, the hand, as shown in Equation (15.5).

$$\hat{p}_B(t_k) = p_B(t_k) + \mathrm{sat}_{e_{max}}\big(\sigma\, v_{B,k}\big), \qquad \sigma = e_{max}/3 \tag{15.5}$$

where $v_{B,k}$ is a pair of independent standard normal deviates from the scenario's seeded generator and the saturation shortens any error longer than $e_{max} = 40\,\mathrm{mm}$ to that length, so $\sigma = 13.3\,\mathrm{mm}$ per axis. The scan reaches the supervisor T_{lat} later, and none is taken during a dropout. The scanner sees the person anywhere, and the arm never hides the person from it. The supervisor's separation is the distance from its own links to the scanned body, as shown in Equation (15.6).

$$d = \min_{B}\Big[\,\mathrm{dist}\,\big(\hat{p}_B,\ \mathscr{L}(q_m)\big) - r_L - r_B\Big] \tag{15.6}$$

where $\mathscr{L}(q)$ is the pair of link segments from the shoulder to the elbow and from the elbow to the tip, evaluated at the encoder angles q_m, and the minimum runs over the torso and a scanned hand. The fixed base is not part of either segment. The true separation d_{true} is the same expression with the true angles and positions, and a check against 2000 sampled link points agrees with the segment distance to $4.4 \times 10^{-8}\,\mathrm{m}$.

15.3.5 Program, Paths and Braking Capability

The program picks a part at P, carries it along leg PQ, places it at Q and returns along QP, dwelling 0.5 s at each station, and a cycle is a part placed or handed over. Asked for a part, it takes leg PH to the hand-over point and HP back. Each leg is a cubic Bézier curve, PQ with control points $(-0.42, 0.78)$ and $(0.42, 0.78)$ m, 1.470 m long, and PH with $(-0.52, 0.62)$ and $(-0.22, 0.80)$ m, 0.885 m long. It is parameterized by its arc length s through a table of 240 intervals, each integrated by three-point Gauss-Legendre quadrature. A reference $(s, \dot{s}, \ddot{s})$ gives the joint reference through the inverse kinematics with the elbow bent counterclockwise, $q = \mathrm{IK}(B(s))$, $\dot{q} = J^{-1} t\,\dot{s}$ and $\ddot{q} = J^{-1}(t\ddot{s} + \kappa \dot{s}^2 - \dot{J}\dot{q})$, with t the unit tangent and κ the curvature vector. The tool reaches $y = 0.74\,\mathrm{m}$ at most, 0.80 m with the capsule.

The torque that follows a path at speed $\dot{s}$ while braking at a is affine in a, $\tau = \tau_0 + a\,\tau_a$, so each drive's limit bounds the deceleration as shown in Equation (15.7).

$$\begin{aligned} a_{cap}(s, \dot{s}) &= \min_{j} \frac{\mathrm{sgn}(\tau_{a,j})\,\tau_{j,max} - \tau_{0,j}}{\tau_{a,j}} \\ a_{wc} &= \min_{\text{program}} a_{cap}(s, \dot{s}) \end{aligned} \tag{15.7}$$

where the worst case a_{wc} runs over the four legs, 49 positions on each and speeds of 0 to 1.2 m/s in five steps, and a point whose constant-speed torque already exceeds a limit counts as zero. With the arm's nominal friction the worst case is $4.74\,\mathrm{m/s^2}$ empty, 3.13 with the 3 kg part and 2.04 with a 6 kg one. The correct braking model plans on $a = 0.9\,a_{wc}$ for the payload the program believes it holds, 4.26, 2.81 or $1.84\,\mathrm{m/s^2}$, and the optimistic one on a single brochure figure of $5\,\mathrm{m/s^2}$ whatever the payload.

Table 15.2 Model Constants. Class V Is a Slider in the Show Model Dialog, H a Hidden Parameter and C Fixed in the Code

Symbol	Meaning	Value	Class
Arm and drives			
l_1, l_2	link lengths	0.45, 0.40 m	V
m_1, m_2	link masses	8, 4 kg	V
m_{tool}	wrist and gripper	1.5 kg	V
r_L	link capsule radius	60 mm	V
$\tau_{1,max}$, $\tau_{2,max}$	drive torque limits	20, 14 N m	V
J_{1m}, J_{2m}	rotor inertias, reflected	0.10, 0.03 kg m^2	H
b_1, b_2	viscous friction	1.0, 0.5 N m s/rad	H
f_{c1}, f_{c2}	Coulomb friction	1.0, 0.5 N m	H
—	encoder count	$2\pi/131072$ rad	H
Program			
a_{nom}	path acceleration	1.5 m/s^2	V
—	dwell at P and Q	0.5 s	V
—	longest hand-over wait	8 s	H
Person and contact			
r_T, r_H	torso and hand radii	0.20, 0.05 m	C
—	walking acceleration, top speed	2 m/s^2, 1.6 m/s	C
—	reach, reaction time	0.62 m, 0.15 s	C
f_T, f_H, ζ_B	body supports	2, 5 Hz, 0.7	H
ζ_c	contact damping ratio	0	H
Body regions, m_B, k_B and F_{max} (illustrative)			
—	hand	0.6 kg, 75 N/mm, 280 N	C
—	lower arm	2.0 kg, 40 N/mm, 320 N	C
—	chest	40 kg, 25 N/mm, 280 N	C
—	head	no contact permitted	C
Scanner and budget			
e_{max}	true scan error bound	40 mm	V
v_h, Z_r	approach speed, robot uncertainty	1.6 m/s, 10 mm	C
T_{sup}, T_{act}	supervisor and servo cycles	20, 10 ms	C
—	braking share, brochure figure	0.9, 5 m/s^2	C

15.3.6 Initial State and Numerics

Table 15.2 lists the constants, and Table 15.3 the supervisor and controller settings, which are the student's controls. Every case starts with the arm at rest at the feeder, holding nothing, and the person at the case's own starting point, and the scanner's queue is seeded with error-free samples of the person taken before $t = 0$ so that the supervisor has a reading at once. The twelve states advance by the fourth-order Runge-Kutta method on a fixed 2 ms step, in the engine of Section 1.6.1. Whenever a body part lies within $(v_r + 2.5\,\mathrm{m/s}) \times 6\,\mathrm{ms} + 4\,\mathrm{mm}$ of a link, the reach of the arm and a fast body part in three steps, the step is split into eight sub-steps of 0.25 ms, because a hand strike rings at 360 to 390 rad/s, and the peak force is taken at every sub-step. The servos and the observer run every 10 ms from $t = 0$, the supervisor every 20 ms, and the historian logs at 20 Hz. Inside a step the controller acts first, the integrator second, and then come the discrete events, the outputs and the log, as in Figure 1.11. The scan errors come from a generator seeded at 20261103, so every reset replays the same scans. Halving the step moves the worst violation of case 4 from 506 to 517 mm, and a second halving leaves it at 517 mm, and moves the first hand strike of case 8, with its friction model corrected, from 68.13 to 68.18 N. Sixteen sub-steps move a hand strike's peak by 0.008 % from eight, and without torque or friction the arm keeps its kinetic energy over 2 s to 2×10^{-13}. The application passes its 43 verification checks.

15.3.7 Assumptions

A planar arm at table height. The two-link arm stands in for a six-axis collaborative robot working in one horizontal layer, with no wrist, no vertical motion and rigid links. Its drive limits are teaching values chosen so that its braking, 2 to 5 m/s^2 at the tool, is of the order that collaborative robots' stopping data show, as the application states.

A person of two discs on a script. The legs, the head and the arm between shoulder and hand have no geometry, the head appears only as a body region a risk assessment could name, and the person never changes their mind.

An ideal scanner. It has a period, a latency and a bounded error, and nothing else. It has no detection capability, response-time tables, muting or multiple fields, the arm never hides the person from it, and its error is independent from scan to scan.

Elastic transient contact. Only free impacts are modeled. Clamping against a fixture, the quasi-static constrained impact that the crash tests found dangerous [7], pressure limits and edges are outside the model.

A path-following stop. The protective stop decelerates the reference along the path at the braking model's deceleration, which the application calls a category 2 stop in the terms of IEC 60204-1, and the arm then holds position under power. Brakes and stops of other categories are not modeled.

Friction as a scale factor. The true gearbox friction is the nominal model times φ, the same shape at every temperature and load, although the static friction of a real robot joint changes with both load torque and temperature [17].

Teaching values. Every limit and threshold is a teaching value. The method follows ISO 10218 and ISO/TS 15066, and real values come from those standards, ISO 13855, the robot maker's stopping data and a risk assessment [3, 4, 14].

15.4 The Budget and the Law

The protective separation distance is where the cell stops being a trajectory tracking problem. It turns the scanner's delay, the arm's speed and braking and the uncertainties into one moving limit, and the supervisor schedules the speed against it.

15.4.1 The Budget

The supervisor writes the protective separation distance in the form of ISO/TS 15066, as shown in Equation (15.8).

$$S_p = \underbrace{v_h(T_r + T_s)}_{S_h} + \underbrace{v_r T_r}_{S_r} + \underbrace{\frac{v_r^2}{2a}}_{S_s} + C + Z_d + Z_r$$
$$T_s = \frac{v_r}{a}, \qquad T_r = T_{scan} + T_{lat} + T_{sup} + T_{act} \tag{15.8}$$

where $v_h = 1.6\,\mathrm{m/s}$ is the approach speed the application takes from ISO 13855, v_r the speed of the arm's fastest point as the encoders report it, a the braking model's deceleration, C the intrusion distance that fingers reach past what the sensor resolves, and Z_d and Z_r the position uncertainties the supervisor assumes for the scanner and the robot. It is Equation (1.18) of Chapter 1 with the two uncertainties added, written with T_r for t_r, T_s for t_s and a for A_b. The reaction time budgets the whole chain from a movement of the person to the arm starting to brake. A movement just after a scan waits up to one period to be seen, the scan then takes T_{lat} to arrive, and the supervisor and the servos are each allowed one cycle, so $T_r = 40 + 100 + 20 + 10 = 170\,\mathrm{ms}$ by default. The intrusion distance is 200 mm, which the application sizes after the $8(d_s - 14)$ mm that its model panel quotes from ISO 13855 for a sensor resolving $d_s = 40\,\mathrm{mm}$.

> **+ DID YOU KNOW? Walking Faster Than the Budget Assumes**
>
> ISO 13855 takes the approach of a person as 2000 mm/s, or 1600 mm/s where the separation exceeds 500 mm. Studies of gait put average normal walking on level ground at 1250 to 1510 mm/s, and average fast walking at 1710 to 1840 mm/s [6].

With the 3 kg part and the correct model at 1.00 m/s, the terms are $840 + 170 + 178 + 200 + 50 + 10 = 1448\,\mathrm{mm}$. The empty arm, which brakes at $4.26\,\mathrm{m/s^2}$, needs 1195 mm, a 6 kg part 1845 mm, the

brochure figure 1122 mm, and a 300 ms latency 1968 mm. At rest only $v_h T_r + C + Z_d + Z_r = 532$ mm is left, the person's approach through the reaction chain, the intrusion and the uncertainties. The stopping time enters twice, once through the arm's braking distance and again as time during which the person keeps walking. With round inputs, 1 m/s of tool speed, $T_r = 0.2$ s, 5 m/s^2, $C = 0.2$ m and 0.06 m of uncertainty, the formula gives 1.200 m, and 0.716 m at 0.25 m/s, and a shortcut that leaves out the person's approach during the stop gives 0.880 m, short by the 0.32 m a person walks while the arm brakes. The application's own check reproduces the first two.

15.4.2 The Speed Law

S_p is a quadratic in v_r, so the fastest speed whose budget fits in a distance D is its positive root, Equation (15.9), the speed law of Section 1.4.9 with these terms.

$$v_{allow}(D) = a\left[\sqrt{\beta^2 + \frac{2(D - D_0)}{a}} - \beta\right], \qquad \beta = \frac{v_h}{a} + T_r \tag{15.9}$$

where $D_0 = v_h T_r + C + Z_d + Z_r$ and $v_{allow} = 0$ for $D \le D_0$. The supervisor applies it to the measured separation less a margin $m = 50$ mm. With the 3 kg part it allows 1.00 m/s at 1.5 m, 0.50 m/s at 1.0 m, 0.28 m/s at 0.8 m and nothing at or below 582 mm, as shown in Figure 15.2(a). Full speed needs 1498 mm with the part, 1245 mm empty, 1895 mm with 6 kg and 1172 mm under the brochure figure, which is how the optimistic model buys its extra speed near a person.

15.4.3 Sampling and the Margin

The speed law acts only through scans, and a scan arrives every 40 ms. A person walking in at 1.6 m/s closes 64 mm between scans (Section 1.4.9), and in case 2 the measured separation falls by 64 to 96 mm per scan in the 0.3 s before the first stop, the arm's own motion and the scan error included. The band in which the law can slow the arm before the stop test $d < S_p(v_r)$ trips is only the margin wide, so a head-on approach at full speed can cross it between two scans. In case 2 the scan used at 3.96 s puts the person 1271 mm from the empty arm, where 1.00 m/s is still allowed, the next, at 3.98 s, reads 1207 mm and trims the ceiling to 0.95 m/s, and the one after, at 4.02 s, reads 1112 mm against an S_p of 1149 mm at 0.94 m/s, so the arm stops from nearly full speed. The margin decides how the approach ends. With no margin the first stop latches at 1.00 m/s, at 50 mm at 0.94 m/s, at 100 mm at 0.72 m/s, and at 150 mm and 200 mm the law has brought the arm to rest when the stop latches at 4.42 s. The cell completes 7 cycles in the minute with every margin tried from 0 to 200 mm and 6 with 300 mm, while the protective stops fall from 8 with no margin to 2 at 50 mm and 1 at 150 mm.

15.4.4 Hysteresis, Stop and Restart

The ceiling follows the speed law with backlash, as shown in Equation (15.10).

$$\begin{aligned} v^s_{cap} &\leftarrow \mathrm{clamp}\big(v^s_{cap},\ v_{allow}(d - m - h),\ v_{allow}(d - m)\big) \\ \mathrm{stop} &\Leftarrow d < S_p(v_r) \\ \mathrm{restart} &\Leftarrow v_r < 0.01\,\mathrm{m/s} \ \wedge\ d \ge S_p(0) + m + h \end{aligned} \tag{15.10}$$

where $h = 100$ mm is the restart hysteresis. The ceiling comes down at once when the separation shrinks and goes back up only when the separation would allow it with h to spare. A protective stop latches, and the arm restarts on its own once it is at rest and the separation exceeds $S_p(0) + m + h = 682$ mm. Without h every scan that reads a little farther lets a slowed arm creep, and the next one stops it again, which is the chattering of case 5.

15.4.5 The Stop the Budget Assumes

The budget is only as good as its deceleration. The protective stop commands a reference that slows along the path at the braking model's a, and Figure 15.2(b) shows what the loaded arm does with

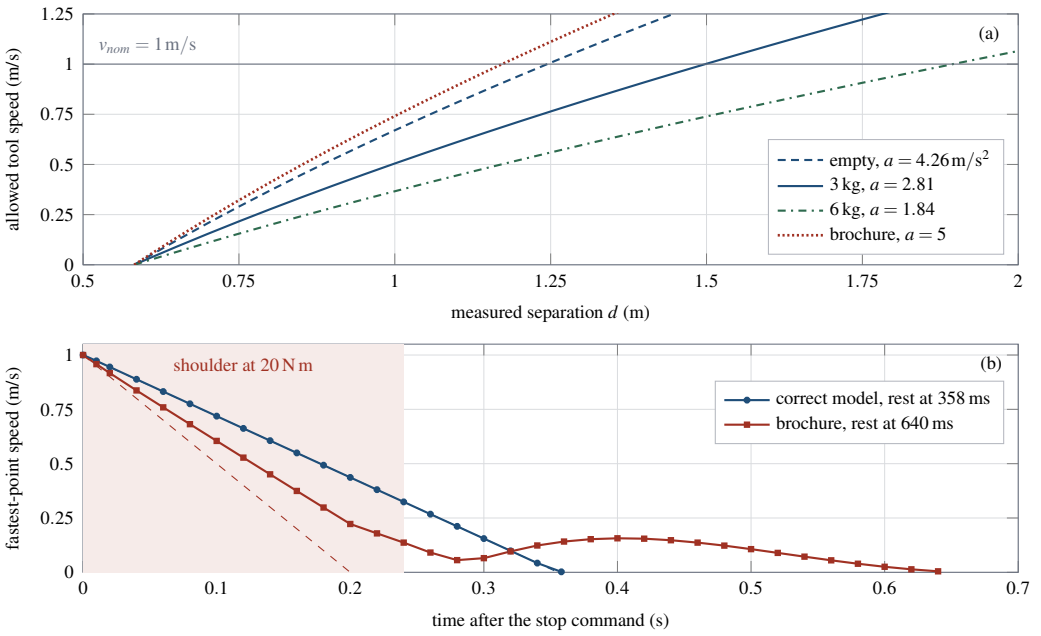


Figure 15.2 The speed law and the stop it relies on, both from the application. (a) The fastest tool speed whose protective distance fits in the measured separation less the 50 mm margin, at the default 170 ms reaction chain, empty (densely dashed), with the 3 kg part (solid), with a 6 kg part (dash-dotted) and under the brochure figure (dotted). Every curve starts at 582 mm, and full speed needs 1245, 1498, 1895 and 1172 mm. (b) The speed of the arm's fastest point after a protective stop commanded from 1.00 m/s with the 3 kg part, at a servo cycle, under the correct model (circles) and the brochure figure (squares). The thin dashed references reach rest at 355 and 200 ms. The shaded interval is where the shoulder drive sits at its limit, and the brochure's second hump is the arm moving back to a reference that has already stopped.

it from 1.00 m/s. Under the correct model the reference stops after the model's 178 mm, the drives never reach a limit, and the arm comes to rest after 178 mm in 358 ms against the model's 355 ms, within 0.1 mm of the model's distance. Under the brochure figure the reference stops after 100 mm in 200 ms. The shoulder drive cannot supply the torque, sits at its 20 N m limit for the first 240 ms, and lets the tool run 30 mm past the stopped reference before the servo pulls it back. The arm comes to rest 640 ms after the command, having moved 167 mm at its fastest point. The distance is 67 mm longer than the brochure promises, but the time is 440 ms longer, and at 1.6 m/s that time is 704 mm of the person's walk. An optimistic stop is wrong mostly in time. Chapter 9 meets the same error on a pallet robot that plans its stop on the braking of the empty robot.

🕮 **Pause.** Try Exercise 15.2 before reading on.

15.4.6 Contact Instead of Separation

On the hand-over legs the person must come close, and speed and separation monitoring would only stop the arm. Power and force limiting admits contact instead, at the speed at which the energy of a transient impact is stored in the body's spring at its force limit, as shown in Equation (15.11).

$$\tfrac{1}{2}\,\mu\, v^2 = \frac{F_{max}^2}{2k_B} \;\Rightarrow\; v_{PFL} = \frac{F_{max}}{\sqrt{\mu k_B}} \qquad \mu = \left(\frac{1}{m_B} + \frac{1}{m_R}\right)^{-1} \tag{15.11}$$

where $m_R = (m_1 + m_2)/2 + m_{tool} + m_L$ is the standard's estimate of the robot's effective mass as the application implements it, half the moving mass of the arm plus the tool and the programmed payload m_L. With the 3 kg part $m_R = 10.5$ kg, the chest allows 0.61 m/s, the lower arm 1.23 m/s and the hand 1.36 m/s, and the head permits no contact. Empty, $m_R = 7.5$ kg and the chest allows 0.70 m/s. The limit has to be taken for the most vulnerable region the motion could reach, which here is the chest. The estimate is conservative for this arm, whose own operational-space mass at the gripper is below it. Struck head-on at the empty-arm limit of 0.70 m/s in the pose of the application's contact check, the chest takes 219 N against its 280 N, because the arm presents only 4.3 kg there.

15.4.7 The Truth Audit

The supervisor decides from an old, noisy scan and a braking model. At every supervisor cycle in which the arm moves or is about to, the audit replaces each measured or assumed term by its true value and checks the inequality of Equation (15.12).

$$d_{true}(t_c) \;\geq\; v_h\,(\text{age} + T_{rest}) + D + C + Z_r \tag{15.12}$$

where $d_{true}(t_c)$ is the true separation between the arm now and the person where they truly were when the scan in use was taken at t_c, age is that scan's age, T_{rest} is how long the arm truly takes, from now, to come to rest, and D is how far its fastest point travels meanwhile. T_{rest} and D come from replaying the controller's own trajectory generator and servos on a copy of the true arm, with the true payload, the true friction and the drives' limits, for the T_r − age left of the reaction chain at the ceiling just set and then through the stop the braking model commands. The replay feeds the servos the true angles and rates, without the encoder quantization or the half-period lag of the backward difference, and it holds no bodies, so it is a slightly idealized copy of the controller. Rest means within 2 mm of where the arm finally stops. There is no Z_d term, because the truth has no sensor error. A cheap bound skips the replay when the person is far enough that no stop of this arm could matter. A violation episode starts when the inequality fails and ends when it holds with 20 mm to spare, and it means that a person walking straight in at 1.6 m/s from where they really were could have reached the arm while it still moved. The audit writes nothing the controller reads, and it stands aside on the legs that power and force limiting governs, where the contact force against its limit is the test. Volume 8, Chapter 13 keeps a record of the same kind, the treatment of every parcel of milk logged apart from the instruments its diversion valve acts on.

15.5 The Controller as Implemented

The controller works from its 17-bit joint encoders, the torques its drives delivered, the scans that have arrived and the hand-over button, and from nothing else. It is built in layers, a servo and a collision observer every $\Delta t = 10$ ms, a supervisor every 20 ms, and the program above them. The framework's velocity-form PID of Section 1.6.2 is not used. No loop integrates its error, so the servos carry no integral term for a torque limit to wind up and need no anti-windup. The settings are listed in Table 15.3.

15.5.1 Trajectory Generator and Servos

The reference is a point $(s, \dot{s}, \ddot{s})$ on the current leg, advanced once per control period with $\ddot{s}$ held over it, a trapezoid profile in the sense of Section 1.4.4. Its target speed is $\dot{s}^*$ of

$$\dot{s}^* = \max\big(0,\ \min(v_{prof}(s),\ v_{cap})\big), \qquad v_{prof}(s) = \min\left(v_{nom},\ \sqrt{2\min(a_{nom}, a)\,(L - s)}\right)$$

where v_{prof} is the leg's own profile into its station at the end of the leg's length L, and v_{cap} is the supervisor's ceiling. The reference speeds up at a_{nom} and slows at $\max(a_{nom}, a)$, the same deceleration that the budget assumes for S_s, and it advances by the trapezoid rule. The servo law of each joint is Equation (15.13).

$$\tau_i = \text{clip}_{\tau_{i,max}}\left(\tau_{ff,i} + K_{p,i}\,e_i + K_{d,i}\big(\dot{q}_{ref,i} - \tfrac{\Delta t}{2}\ddot{q}_{ref,i} - \hat{\omega}_i\big)\right) \tag{15.13}$$

Table 15.3 Supervisor and Controller Settings, Defaults and Ranges

Symbol	Setting	Default	Range
—	speed and separation monitoring	on	on, off
v_{nom}	tool speed at 100 %	1.00 m/s	0.2–1.2
m, h	margin, restart hysteresis	50, 100 mm	0–300
α_{man}	manual speed override	100 %	0–100
T_{lat}	scanner latency	100 ms	20–400
T_{scan}	scan period	40 ms	40–100
Z_d	declared scan uncertainty	50 mm	0–300
C	intrusion distance	200 mm	0–600
—	braking model	correct	or optimistic
m_L	programmed payload	3 kg	0–6
—	PFL on hand-over legs, region	on, chest	4 regions
—	collision detection	on	on, off
r_{th}	residual threshold	3 N m	0.5–20
T_{reflex}	declared reflex time	50 ms	10–200
K_O	observer gain	40 s^{-1}	5–100
$\hat{\varphi}$	friction in the model	100 %	50–300
K_{p1}, K_{d1}	shoulder gains	400, 40	to 1500, 120
K_{p2}, K_{d2}	elbow gains	200, 16	to 800, 60
—	computed-torque feedforward	on	on, off

Gains in N m/rad and N m s/rad, lower bounds 50, 0, 20 and 0.

where $\mathrm{clip}_c(x) = \max(-c, \min(c, x))$, $e_i = q_{ref,i} - q_{m,i}$ and $\hat{\omega}_i = (q_{m,i,k} - q_{m,i,k-1})/\Delta t$ is the unfiltered backward-difference rate, half a period old, which the shift $\frac{\Delta t}{2}\ddot{q}_{ref}$ matches. The feedforward $\tau_{ff} = \hat{M}\ddot{q}^* + \hat{C}\dot{q}^* + \hat{\varphi}\hat{F}$ is the torque that the controller's arm model assigns to the reference half a period ahead, since the torque computed at the start of a period is applied until its end, with the programmed payload m_L while a part is carried and the friction scaled by $\hat{\varphi}$. The clip at each drive's limit is the only output limit, and the torque has no rate limit. Against the diagonal inertias along the paths, the shipped gains give the shoulder 11.7 to 13.3 rad/s at damping ratios of 0.59 to 0.66 empty and 9.3 to 10.8 rad/s at 0.47 to 0.54 with the part, and the elbow 20.3 rad/s at 0.81 empty and 14.4 rad/s at 0.58 loaded. The loops are reverse acting in the convention of Section 1.3, $a = +1$, because the torque rises when a joint falls short of its reference, as the application's sign check confirms. With no gravity on the links and the friction in the feedforward, no steady torque is left for an integral term to find.

15.5.2 Collision Observer and Reflex

The generalized-momentum residual estimates the external joint torque without differentiating the joint rates [11, 15], and the implementation is the discrete form of Equation (15.14).

$$\begin{aligned} p_k &= \hat{M}(q_{m,k})\,\hat{\omega}_k, \qquad \hat{\beta}_k = \hat{C}^{\mathsf{T}}\hat{\omega}_k - \hat{\varphi}\hat{F}(\hat{\omega}_k) \\ I_k &= I_{k-1} + \left[\tfrac{1}{2}(\tau_{k-1} + \tau_{k-2}) + \hat{\beta}_k + r_{k-1}\right]\Delta t \\ r_k &= K_O\,(p_k - p_0 - I_k) \end{aligned} \tag{15.14}$$

where τ_{k-1} and τ_{k-2} are the torques the drives held over the last two periods, averaged because the backward-difference rate makes p_k the momentum of half a period ago, and the model uses the programmed payload and the modeled friction. For a constant external torque the residual approaches it through a first-order lag of rate $K_O = 40\,s^{-1}$. When either joint's residual exceeds r_{th} the reflex stops the arm and holds it for 2 s, and then until the scanned person is at least 200 mm from the arm. A reflex with no contact under way is booked as a nuisance stop, and one that comes later than the declared T_{reflex} after the first touch as late. With the model right the residual stays within about 1 N m in free motion.

Table 15.4 The Eight Cases and the Shift

#	Change from the reference line	Teaching point
1	manual override, no monitoring, walk-in at 1.2 m/s	the budget by hand
2	walk-in at 1.6 m/s, stand 5 s	the law and its price
3	$T_{lat} = 300$ ms, aisle walk 1.9 m away	time and uncertainty are distance
4	brochure 5 m/s^2, walk-in at 1.6 m/s	an optimistic stop
5	$h = 0$, person stands 1.47 m away	chattering
6	hand-over asked for, eager reach across	contact allowed, and the head
7	$m_L = 6$ kg, aisle walk	payload in stop and contact
8	no monitoring, 0.5 m/s, friction 250 %, hand in the path	threshold against model error
9	600 s of mixed traffic, $T_{lat} = 150$ ms, brochure, $h = 0$, PFL off	graded shift

15.5.3 Supervisor and Program

Every 20 ms the supervisor computes the reaction chain, the braking model's deceleration for the payload the program believes it holds, the measured separation of Equation (15.6) from the latest scan and the budget of Equation (15.8) at the measured speed, and it updates the ceiling and the latches of Equation (15.10). The chain T_r is a budget. At the default timing each scan arrives on a supervisor cycle, and the generator and the servos begin a stop in the same execution as the decision, so the code applies at most 140 ms of the 170 ms. A scan older than $T_{lat} + 3T_{scan} = 220$ ms trips a watchdog that stops the arm like a protective stop. Volume 4, Chapter 2 has a protective layer of the same kind, an override that rests at its clamp in healthy operation and is judged by its margin to a limit. On legs PH and HP and at the hand-over point, with power and force limiting on and a body region that permits contact, the ceiling is $\min(v_{nom}, v_{PFL})$ instead, and any latched stop is released. A stop, a fault or a reflex sets the ceiling to zero, and the speed override the scene shows is $\alpha = v_{cap}/v_{nom}$. A halt is counted each time the ceiling reaches zero while the arm is on a leg, whether a stop or the speed law brought it there. Asked for a part, the program waits at the feeder with the lamp lit until the scanner sees a hand within 0.30 m of the hand-over point, carries the part there, and opens the gripper for 0.4 s once it sees the hand within 0.15 m of the gripper. It gives up after 8 s at either wait, and a person whose patience runs out leaves.

In manual mode the operator's override α_{man} replaces the speed law, as the override knob of a teach pendant does, while the stop latch, the power and force limit, the watchdog and the reflex keep acting and the servos keep running. In automatic mode the manual override tracks the supervisor's, so a switch of mode moves nothing.

15.5.4 Simulation, Controller and Audit Models

Equations (15.1) to (15.6) make up the simulation model. The controller holds four internal models, the arm model of the feedforward and the observer with the programmed payload and the modeled friction, the braking model, the budget with its declared Z_d, and the estimate m_R for contact. The audit's model is the controller's generator and servos on a copy of the true arm, without contact. No control model is identified from data, and a wrong payload or friction is a wrong model in every safety function at once.

15.6 Eight Cases and a Shift

Table 15.4 lists the cases. Each opens on the reference line of Tables 15.2 and 15.3, with monitoring on, the correct braking model, the 3 kg part, the 50 mm margin, 100 mm of hysteresis, power and force limiting at the chest and detection at 3 N m, and alters that line in the ways its row gives. The numbers below come from headless runs at the default seed, over the first simulated minute unless another span is named. Every variant is set at $t = 0$ before Run, the same run as one carried through Reset, and a run that pauses at its first violation is continued. The results are collected in Table 15.5.

Table 15.5 Truth-Audit Scorecard of Each Case and Variant. Runs Last 60 s Except Where Named

Case and configuration	Result
1, override 100 %	11 cycles, 13 violations, worst 1054 mm, first at 4.18 s
1, override 50 and 25 %	8 cycles, 9 violations (598 mm); 5 cycles, 6 (410 mm)
1, override 0	no cycle, no violation
2, as shipped	7 cycles, no violation, closest 118 mm, 2 stops
2, monitoring off	11 cycles, 12 violations, worst 1054 mm
3, T_{lat} 100, 200, 300 ms, 240 s	660, 600, 540 h^{-1}, no violation
3, T_{lat} 50, 150, 400 ms, 240 s	675, 630, 495 h^{-1}, no violation
3, $Z_d = 200$ mm or $T_{scan} = 100$ ms	615 h^{-1} either way, no violation
3, monitoring off, 240 s	690 h^{-1}, 44 violations, worst 604 mm
4, brochure	7 cycles, 6 violations, worst 506 mm, first at 6.22 s
4, correct model	7 cycles, no violation, closest 61 mm
5, $h = 0$	13 stops, 178 halts, no cycle
5, $h = 100$ mm	1 stop, 2 halts, no cycle
5, h 0 and 100 mm, 90 s	17 stops, 4 cycles; 2 stops, 3 cycles
6, PFL at the chest	3 hand-overs, 8 cycles, peak 76 N, reflex 12.5 ms
6, PFL at the hand or lower arm	3 hand-overs, 8 cycles, peak 76 N
6, PFL off, or the head named	no hand-over, 1 cycle
7, 6 kg and 3 kg, 240 s	615 and 660 h^{-1}, no violation
7, 6 kg undeclared, 240 s	110 nuisance stops, 1 cycle
7, undeclared, reflex off, 240 s	630 h^{-1}, 83 violations, worst 567 mm
8, $r_{th} = 3$ N m	19 nuisance stops, 1 cycle
8, $r_{th} = 5$ N m	no nuisance stop, 7 reflexes within 16.5 ms, 6 cycles
8, $r_{th} = 12$ N m	one reflex 117 ms late, 6 cycles
8, model at 250 %	no nuisance stop, within 18.5 ms, 6 cycles
8, model right, $r_{th} = 12$ N m	no detection, 32 contacts, 8 cycles

15.6.1 The Budget in the Operator's Hands

In case 1 nothing monitors the cell and the operator holds the override while a person walks in from 2.85 m at 1.2 m/s, stands at the table for 5 s and walks back. At 100 % the arm completes 11 cycles in the minute and the audit finds 13 violation episodes, the first 4.18 s after the run starts and the worst 1054 mm short of the true protective distance, while the moving arm comes within 214 mm of the person. Held at 50 % for the minute it makes 8 cycles with 9 episodes, the worst 598 mm, and at 25 % 5 cycles with 6, the worst 410 mm. Only a standstill avoids them all, and then nothing is made. The reason is Section 15.4's 532 mm at rest. At any speed above zero the person's approach through the 170 ms chain, the intrusion distance and the uncertainties are due, and they exceed the 214 mm the path leaves.

🕮 **Pause.** Try Exercise 15.1 before reading on.

15.6.2 The Law Against a Person Walking In

Case 2 turns monitoring on and sends the person in at 1.6 m/s. The first protective stop comes at 4.02 s from 0.94 m/s, for the sampling reason of Section 15.4. The arm restarts at 4.26 s, at rest with the person still coming and 754 mm away, creeps, stops again at 4.38 s at 579 mm against an S_p of 583 mm, and restarts at 10.70 s once the person, walking away, is 709 mm off. In the minute the cell completes 7 cycles against 11 unmonitored, the audit never finds it late, its closest call leaving 118 mm, and the arm spends 30.8 s at full speed, 22.7 s slowed by the law and 6.6 s stopped. Unmonitored, the same walk gives 12 violation episodes, the worst 1054 mm. The price of the law is 4 cycles in a minute of a person coming and going.

TRY IT IN THE APP **2 · The Separation Law at Walking Speed**

Load the case and press Run. Watch the override dial as the person walks in: it falls before they reach the table, and the arm stops while they stand there. Over the minute the scorecard counts 7 cycles and no separation violated. Set Speed and separation monitoring Off on the supervisor card and run again: 11 cycles and 12 violation episodes.

15.6.3 Latency and Uncertainty Are Distance

Case 3 walks the person along the aisle 1.9 m from the robot, never within 0.99 m of the arm, with the scanner's latency at 300 ms. The chain grows to 370 ms and S_p at 1 m/s with the part to 1968 mm, so a person the arm used to pass at full speed now slows it. Over four minutes the cell makes 540 cycles an hour, against 600 at 200 ms, 660 at 100 ms and 675 at 50 ms, and it spends 158 s of the four minutes slowed at 300 ms against 52 s at 100 ms. At 100 ms a declared uncertainty of 200 mm instead of 50 mm costs 45 cycles an hour, as does a 100 ms scan period, while 25 mm gains 15. None of the monitored runs violates, with closest calls of 103 to 301 mm, because the terms are honest. The same walk unmonitored makes 690 cycles an hour with 44 violation episodes at 300 ms, the worst 604 mm, and 23 at 100 ms, the worst 276 mm, because the audit charges the person's walk through the whole reaction chain.

DID YOU KNOW? **Safety Nearly Free on a Fast Scanner**

From the simulator: along the aisle walk of case 3, the unmonitored cell makes 690 cycles an hour, and the audit, charging the person's walk through a 300 ms latency, finds 44 violation episodes. Monitored with 50 ms of latency, the cell makes 675 cycles an hour with none (Table 15.5).

15.6.4 An Optimistic Braking Model

Case 4 has the supervisor plan with the brochure's 5 m/s^2 and sends the person straight at the table at 1.6 m/s as the arm starts its loaded leg. The audit finds 6 violation episodes in the minute, the first at 6.22 s and the worst 506 mm short. At the first one the supervisor measured 1486 mm against an S_p of 970 mm at 0.77 m/s and ran at full override, while the truth asked for 1558 mm and had 1478 mm. Figure 15.3 shows the Separation view at that moment, with the measured separation, the budget, the override and the audit's true distances. The truth places the person where they really were when the 100 ms-old scan was taken, and it has the arm come to rest 620 ms after the decision, 70 ms of reaction chain and the rest braking, after 196 mm of travel. The cell completes 7 cycles with either model, and the brochure's 7 protective stops keep the arm stopped for 20.6 s of the minute against 16.5 s for the correct model's 9. With the correct model the audit's closest call leaves 61 mm. Unmonitored, the same walk gives 11 cycles and 11 episodes, the worst 1468 mm.

15.6.5 Chattering at the Boundary

Case 5 parks the person 1.47 m from the robot for a minute with no restart hysteresis, then steps them back to 1.72 m. At that distance the speed the law allows is small. The restart threshold and the speed ceiling keep the arm on the boundary, and the scanner's 40 mm of error adds variation. The run makes 13 protective stops and 178 halts of the ceiling in the first minute with no cycle completed. The halts do not need the scan error. With the true error bound at the smallest value the Show Model dialog allows, the protective stops disappear and the ceiling still halts nearly as often, because the person stands where the law allows almost nothing and the ceiling flickers on and off zero. The scan error turns that flicker into latched protective stops. With 100 mm of hysteresis the arm stops once, halts twice and waits. The hysteresis is not free. After the step back, which begins at 61.4 s, the arm speeds up only with 100 mm to spare, its first cycle ends at 65.7 s instead of 64.5 s, and each cycle takes about 8.9 s instead of 8.1 s, so the 90 s run completes 3 cycles against 4. For that it ends the chatter, 2 protective stops in the 90 s instead of 17. Smaller values bracket the choice, since 20 mm still halts the ceiling 75 times in the first minute and 50 mm 9 times. Collaborative applications are judged on

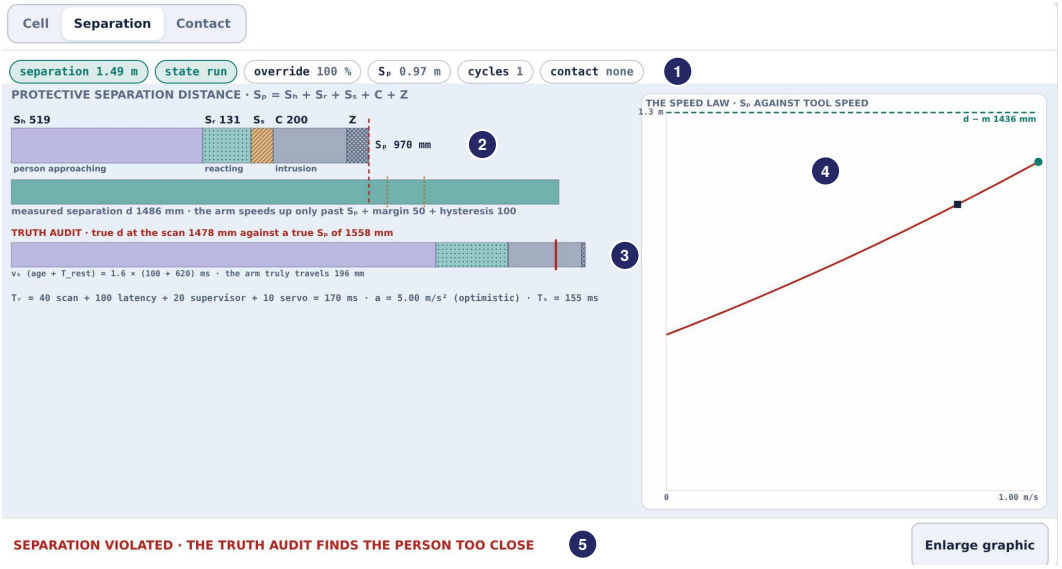


Figure 15.3 The cell in case 4, An optimistic braking model, at $t = 6.22$ s, where the application paused itself at the first separation violation, with no control changed, in the Separation view, cropped to the plant view. (1) The badge row with the separation, the state, the override and S_p. (2) The stacked bars give S_p of 970 mm as S_h 519, S_r 131, S_s (60 mm, too narrow for its value), C 200 and Z (60 mm), with the measured separation of 1486 mm below them and the margin and hysteresis marked beyond S_p. (3) The truth-audit bar reads a true d of 1478 mm at the scan against a true S_p of 1558 mm, the person walking $1.6\,\text{m/s} \times (100 + 620)$ ms while the arm truly travels 196 mm, and the chain below it reads $40 + 100 + 20 + 10 = 170$ ms with $a = 5.00\,\text{m/s}^2$ and $T_s = 155$ ms. (4) The speed law draws S_p against the tool speed up to 1.00 m/s, entirely below $d - m = 1436$ mm. (5) The status line reads Separation violated, the truth audit finds the person too close.

human factors as well as on production figures [2], and the application's briefing adds that an arm which stops and starts on every scan wears its drives and is hard for the person beside it to read.

> **TRY IT IN THE APP** **5 · A Person at the Boundary**
>
> Press Run and watch the protective stops climb while the person stands still: 13 in the first minute, with 178 halts of the speed ceiling and no cycle. Press Reset, set Restart hysteresis to 100 mm on the supervisor card and run again. The arm stops once, halts twice and waits for the person to step back.

15.6.6 Contact Allowed at the Hand-Over

In case 6 the person presses the hand-over button, comes to the table when the lamp shows that the robot is ready at the feeder, and holds out a hand. Under power and force limiting at the chest, leg PH runs at 0.61 m/s with the part and HP at 0.70 m/s empty, and the hand-overs complete at 12.14, 33.06 and 54.26 s, 3 in the minute with 8 cycles. Each time, with the part in hand, the person reaches across for the next one and meets the returning gripper 65.5 ms after the hand-over, at 76 N, 27 % of the hand's 280 N. The reflex stops the arm 12.5 ms after the first touch and has it at rest 163 ms after, while the hand bounces off it four more times, at 62, 52, 45 and 39 N. With power and force limiting off, the person at the table is inside the protective distance of any moving arm. A protective stop latches at 9.46 s while the arm waits at the feeder, the person gives up at 30.1 s, and the arm, released once they have gone, reaches an empty hand-over point at 35.2 s, waits 8 s and carries the part back, so the minute has no hand-over and one cycle. Naming the head as the region the motion

could reach forbids contact and gives the same result, an honest infeasibility rather than a slower success. Naming the hand or the lower arm lets the legs run at the full 1.00 m/s, because their limits of 1.36 and 1.23 m/s do not bind, and gives the same 76 N strike, because the gripper is still gathering speed out of the hand-over point, at 0.11 m/s, when the hand meets it. The chest is why the legs run at 0.61 m/s.

15.6.7 A Heavier Part

Case 7 programs a 6 kg part and walks the person along the aisle. The drives' worst case falls from 3.13 to 2.04 m/s^2 and the model's plan to 1.84 m/s^2, S_p at 1 m/s grows by 397 mm to 1845 mm, and the arm slows for the person sooner, 615 cycles an hour over four minutes against 660 with 3 kg, with no violation. Contact tightens as well, since m_R rises to 13.5 kg and the chest allows 0.56 m/s. With 3 kg programmed and the part truly twice as heavy, the observer, whose model expects 3 kg, reads every acceleration of the loaded arm as a contact, and the arm makes 110 nuisance stops and one cycle in the four minutes. Chapter 10 shows the torque budget that a payload left out of the controller's model breaks on an arm of the same form. Those stops hide a worse fault. With the reflex off, the same undeclared part lets the cell make 630 cycles an hour while the audit finds 83 violation episodes, the worst 567 mm short, because the braking model still plans for 3 kg.

15.6.8 A Threshold Against a Wrong Model

Case 8 switches monitoring off and runs the arm at 0.5 m/s, relying on detecting contact, while a person holds a hand in the path after the feeder and the gearboxes run at 250 % of the friction the model expects, a change of the kind that temperature causes in the friction of a robot joint [17]. With the 3 N m threshold the residual reaches 3.3 N m in free motion and trips, 19 nuisance stops and one cycle in the minute. At 5 N m the nuisance stops end and every strike on the hand, 100 N at the worst, is caught within 16.5 ms, and at 12 N m the first reflex comes 117 ms after the touch, past the declared 50 ms. Re-identifying the friction, the model at 250 %, lets 3 N m work. The first strike, 68 N at 1.312 s, is caught 18.5 ms later, the rest within 7.5 ms, the free-motion residual stays below 1.1 N m, and the arm makes 6 cycles with no nuisance stop. With the model right and the threshold at 12 N m no strike is detected at all, and the arm makes 8 cycles through 32 contacts. Monitoring is off, so the audit flags separation violations throughout, 14 in the shipped minute. A raised threshold trades false alarms for late ones, and identifying the model is the fix.

Pause. Try Exercise 15.3 before reading on.

OPEN CHALLENGE **Choosing a Collision Threshold**

Selecting the threshold on the monitoring signal, so that it avoids false positives and stays sensitive at the same time, is a major practical problem of collision detection. In an observer, unknown friction torques, quantization, measurement noise and delay all enter the estimate of the external torque, so the residual is not zero even without contact [11]. The threshold has to clear a model error that changes with load and temperature. Progress would be a threshold that adapts to what the model is known to get wrong, catching a light strike in time without stopping on every acceleration.

15.6.9 The Shift

The challenge runs 600 s of mixed traffic at 150 ms of latency and 50 mm of declared uncertainty. Its loop, a walk along the aisle, a 1.6 m/s approach toward the fixture side, 20 s standing at 1.47 m, a request for a part and a reach into the fixture, repeats every 76 to 94 s, depending on how quickly the hand-over goes. The target asks for at least 55 cycles, no violation, no contact above its region's limit and at most 30 protective stops. Changing a model parameter or a disturbance voids an attempt. Table 15.6 compares the configurations. As shipped, with the brochure figure, no hysteresis and power and force limiting off, the cell makes 39 cycles with 47 violation episodes, the worst 466 mm, 46 stops and 552 halts, and no hand-over completes. Each shipped setting fails a different part of the

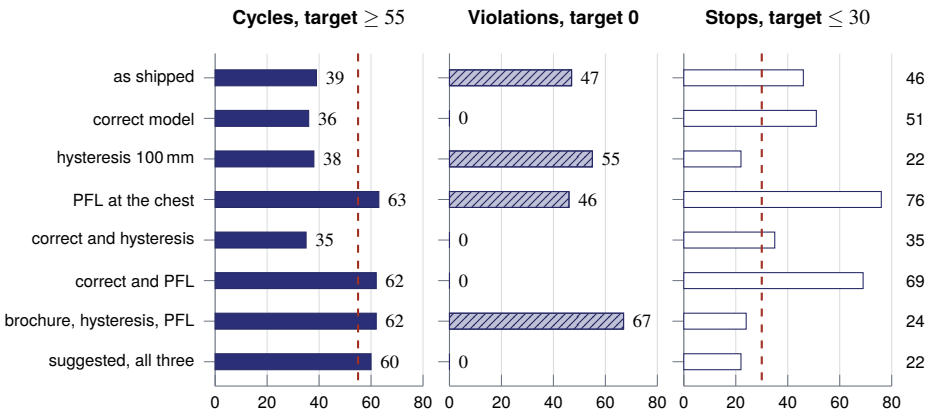


Figure 15.4 The shift of 600 s in its eight configurations, from Table 15.6: cycles (solid bars), violation episodes (hatched bars) and protective stops (open bars), with the targets as dashed lines. Notice that each single change fails a different part of the target, and only the suggested configuration, with the correct model, hysteresis and power and force limiting together, passes all three.

Table 15.6 The Shift of 600 s in Eight Configurations

Configuration	Cycles	Hand-overs	Violations	Stops
as shipped	39	0	47	46
correct model	36	0	0	51
hysteresis 100 mm	38	0	55	22
PFL at the chest	63	8	46	76
correct and hysteresis	35	0	0	35
correct and PFL	62	8	0	69
brochure, hysteresis and PFL	62	8	67	24
suggested, all three	60	7	0	22

target. The correct model alone removes the violations and loses 3 cycles, hysteresis alone removes the chatter, and power and force limiting alone finds the throughput in the hand-overs. The suggested configuration makes 60 cycles, 7 of them hand-overs, with no violation, no contact and 22 stops, and the audit's closest call leaves 120 mm. Figure 15.4 sets the cycles, violations and stops of the eight configurations against their targets.

15.7 Technology in Practice

The cell of Section 15.3 reads joint encoders, drive torques, a hand-over button and a delayed safety scanner, and it moves the arm through two torque-limited joint drives. Figure 15.5 draws its loops with real devices in the place of the schematic's symbols.

What Measures It

A fenceless cell detects people with safety-rated sensing equipment. The accepted technologies are light curtains, laser scanners that respond to diffuse reflection, standardized in IEC 61496-3, and pressure-sensitive mats. A sensor without a performance standard, such as a thermal camera, may only support a primary safety-rated one. Mats respond quickly but resolve poorly, while cameras and lasers resolve well but depend on lighting, processing time, capture rate and occlusion [6]. The scanner of Section 15.3, 40 ms between scans, 100 ms late and up to 40 mm off, stands for such a device with its occlusion left out. Contact has no sensor of its own. The drive torque follows from the motor current, and an observer compares it with the model, but unknown friction, quantization, noise

and delay leave a residual even with no contact [11]. The residual of about 1 N m in free motion in Section 15.5 stands for that floor.

> **TECHNOLOGY** **Sensor: The Safety Laser Scanner**
>
> A laser scanner sweeps a laser rangefinder over a plane and finds the range to what it strikes from the time of flight divided by the speed of light [18]. In one testbed for speed and separation monitoring, two scanners about 0.4 m above the floor watched the work area. Software removed a recorded background, grouped the returns into legs and people, and a Kalman filter estimated each person's position and velocity [19]. The range depends on the target's reflectivity and the beam's angle, and a beam that falls across an edge can report phantom points [18]. A person hidden behind another is not seen at all [19]. In the model a lost scan leaves the supervisor an ever older position of the person until its watchdog stops the arm.

What Moves It

Each joint has a servo drive whose torque saturates, and a protective stop is a deceleration commanded through those drives. Arms built for power and force limiting are typically lighter, slower and of shorter reach, while a conventional arm converted to collaborative work has no power and force limiting and needs speed and separation monitoring instead [6]. The torque limits of Table 15.2 stand for the drives, and the worst-case braking of Equation (15.7) for the stopping data a maker would measure.

> **TECHNOLOGY** **Final Element: Joint Drives and the Protective Stop**
>
> A robot is stopped by removing power from its drives, by applying brakes or by controlling the motors against the motion. IEC 60204-1 sorts stops into three categories: category 0 removes power and applies the brakes at once, category 1 brakes under control and then removes power, and category 2 brakes under control and keeps the power on [6]. The stopping time and distance measured under ISO 10218-1 are functions of the initial speed and the payload. Pose, path, brake wear and a shifted center of mass of the payload change them, so they should be measured again from time to time [6].

Where the Controller Runs

A discrete-part plant may give each cell a supervisor above a machine controller and a robot controller, and such loops run with cycle times from milliseconds to minutes [20]. In one testbed the monitoring ran on an external computer, which sent slow, pause and resume commands over a network socket to tasks written in the robot's own language, and the slow command set the controller's general speed override [19]. A delay of about 220 ms was measured on one arm between being at a place and reporting it [6]. In this chapter the servos and the observer act every 10 ms and the supervisor every 20 ms, and the ceiling reaches the arm as the speed override α.

> **IN PRACTICE** **Measuring the Reaction Time and Proving the Stop**
>
> No standard method measures the reaction time of a sensor that detects people, so the integrator supplies it. One way drives the robot along a line past a laser beam wired to its inputs, records where it stops at several speeds, and fits the stop positions to a quadratic in speed whose coefficients give the reaction time and the worst-case deceleration. Repeated trials of a rail-mounted six-axis arm gave 0.113 s [6]. A testbed proved its stops with a mannequin on a rolling platform, pushed toward the moving robot while an independent measurement system tracked both, and the robot had to stop before the contact threshold [19].

What Is Modernizing It

Sensing is the first development. Safety-rated cameras and sensors on the robot are expected to be critical for cells that are not structured, and people will have to be told apart from parts [6]. Thermal cameras have been used to tell a person from a machine, so that the protective distance can shrink

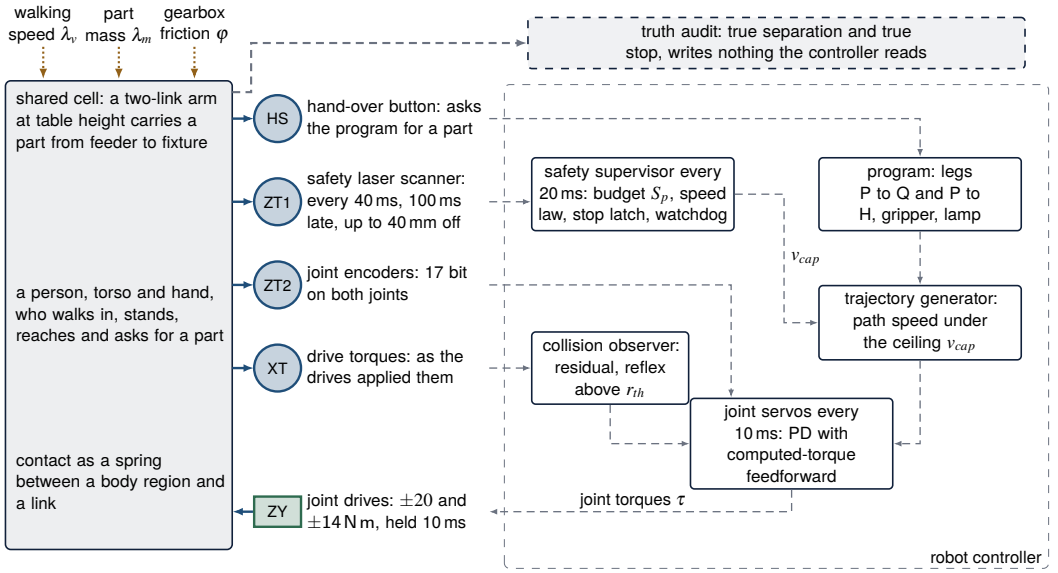


Figure 15.5 The loops of the chapter with real devices in place of the schematic's symbols. A safety supervisor acting every 20 ms reads the safety laser scanner ZT1 and the encoders ZT2, computes the budget and sets the speed ceiling. The trajectory generator follows the program under that ceiling, the servos turn the reference into torques for the joint drives ZY, and the collision observer compares the drive torques XT with the arm model to trigger the reflex. Notice that the truth audit (dashed) reads the cell itself and feeds nothing back, and that no sensor measures contact.

when what approaches is not a person [21]. Detection without sensors is the second: momentum-observer methods for collisions have reached commercial products [11]. Wireless networking is the third. A collaborative work-cell testbed links programmable logic controllers, robot arms and machine tools over wired and wireless industrial networks and measures how the wireless links perform [22].

15.8 Limitations

The arm is planar, rigid and at table height, the person two discs on a script, and the scanner an ideal sensor with a bounded error, no occlusion and no detection capability. Contact is elastic and transient, so clamping, pressure limits and the constrained impacts the crash tests found dangerous [7] are absent. The protective stop follows the path, and brakes, other stop categories and the safety-rated monitoring of the stop itself are not modeled. The truth audit replays the stop with the controller's own servos on the true arm, an idealized validation rather than a measurement on a robot.

Every limit is a teaching value. The body-region masses, stiffnesses and force limits are illustrative, and the standard's estimate m_R stands for the robot's effective mass. The method follows the 2011 editions of ISO 10218, now replaced, and ISO/TS 15066 of 2016, and a real cell takes its values from the current standards, ISO 13855, the robot maker's stopping data, measured transient forces and a risk assessment [3, 4, 14]. The targets of the shift were chosen for teaching, and none of the numbers is a measure of industrial performance.

OPEN CHALLENGE **Proving a Fenceless Cell Safe**

Speed and separation monitoring still lacks methods to verify and validate that it works and keeps working. No method captures the measurement and performance uncertainty of the robot system as a whole, no standard exists for measuring where a person is, and the minimum distance has not been validated as safe for every robot configuration. People vary, sensors are uncertain, and it is hard to tell when a robot actually began its stop [6]. Progress would be a repeatable test, with a human surrogate and an independent measurement synchronized to the robot, that grades a whole cell as the truth audit grades the simulator.

15.9 Conclusion

A collaborative cell earns its missing fence only if the arm can always stop in time, and this simulator makes the budget behind that guarantee, and its truth, measurable. At 1.00 m/s with a 3 kg part the protective separation distance is 1448 mm, and at rest it is still 532 mm, more than the 214 mm the arm's path leaves a person at the table, so no override lets the arm work safely beside them. The speed law costs 4 cycles in a minute of a person coming and going, each 100 ms of latency from 100 to 400 ms costs 45 to 60 cycles an hour, and a brochure braking figure buys no cycle while it produces 6 violation episodes, the worst 506 mm, because the loaded arm takes 640 ms rather than 200 ms to stop. Hysteresis turns 17 protective stops into 2 for one cycle in 90 s, power and force limiting at the chest makes the hand-over possible at 0.61 m/s, and a threshold raised against a wrong friction model detects a strike 117 ms late. The shift improves from 39 cycles with 47 violations to 60 cycles with none. The model is planar with an ideal scanner and elastic contact. A fuller model would add a vertical axis, clamping contact and pressure limits, a scanner with occlusion and detection capability, and a person who changes course. The simulator treats safety as a feedback loop whose price is paid in throughput and whose verdict belongs to the truth.

KEY POINTS

- A collaborative arm without a fence is safe only if it can always stop before a person walking in could reach it.
- At rest the protective separation distance is still 532 mm, more than the 214 mm the path leaves a person at the table.
- A brochure braking figure buys no cycle and gives 6 violation episodes, because the loaded arm takes 640 ms rather than 200 ms to stop.
- Hysteresis turns 17 protective stops into 2 for one cycle in 90 s.
- A threshold raised against a wrong friction model detects a strike 117 ms late, and identifying the model is the fix.

Where else this applies. A record kept apart from the instruments a supervisor acts on also judges the diversion valve of Volume 8, Chapter 13.

References

[1] A. M. Zanchettin, N. M. Ceriani, P. Rocco, H. Ding, and B. Matthias, "Safety in human-robot collaborative manufacturing environments: Metrics and control," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 2, pp. 882–893, 2016.

[2] F. Vicentini, "Collaborative robotics: A survey," *Journal of Mechanical Design*, vol. 143, no. 4, p. 040802, 2021.

[3] *Robots and robotic devices. Safety requirements for industrial robots. Robots*, BSI British Standards Standard BS EN ISO 10 218-1:2011, Sep. 2011.

[4] *Robots and robotic devices. Collaborative robots*, BSI British Standards Published Document PD ISO/TS 15 066:2016, Mar. 2016.

[5] M. J. Rosenstrauch and J. Krüger, "Safe human-robot-collaboration-introduction and experiment using ISO/TS 15066," in *2017 3rd International Conference on Control, Automation and Robotics (ICCAR)*, 2017, pp. 740–744.

[6] J. A. Marvel and R. Norcross, “Implementing speed and separation monitoring in collaborative robot workcells,” *Robotics and Computer-Integrated Manufacturing*, vol. 44, pp. 144–155, 2017.

[7] S. Haddadin, A. Albu-Schäffer, and G. Hirzinger, “Requirements for safe robots: Measurements, analysis and new insights,” *The International Journal of Robotics Research*, vol. 28, no. 11-12, pp. 1507–1527, 2009.

[8] K. L. Hobbs, M. L. Mote, M. C. L. Abate, S. D. Coogan, and E. M. Feron, “Runtime assurance for safety-critical systems: An introduction to safety filtering approaches for complex control systems,” *IEEE Control Systems*, vol. 43, no. 2, pp. 28–65, 2023.

[9] C. Byner, B. Matthias, and H. Ding, “Dynamic speed and separation monitoring for collaborative robot applications – concepts and performance,” *Robotics and Computer-Integrated Manufacturing*, vol. 58, pp. 239–252, 2019.

[10] J. A. Marvel, “Performance metrics of speed and separation monitoring in shared workspaces,” *IEEE Transactions on Automation Science and Engineering*, vol. 10, no. 2, pp. 405–414, 2013.

[11] S. Haddadin, A. De Luca, and A. Albu-Schäffer, “Robot collisions: A survey on detection, isolation, and identification,” *IEEE Transactions on Robotics*, vol. 33, no. 6, pp. 1292–1312, 2017.

[12] B. C. Jiang and C. A. Gainer, “A cause-and-effect analysis of robot accidents,” *Journal of Occupational Accidents*, vol. 9, no. 1, pp. 27–45, 1987.

[13] M. A. Peshkin, J. E. Colgate, W. Wannasuphoprasit, C. A. Moore, R. B. Gillespie, and P. Akella, “Cobot architecture,” *IEEE Transactions on Robotics and Automation*, vol. 17, no. 4, pp. 377–390, 2001.

[14] *Safety of machinery. Positioning of safeguards with respect to the approach speeds of parts of the human body*, BSI British Standards Standard BS EN ISO 13 855:2010, May 2010.

[15] A. De Luca and R. Mattone, “Sensorless robot collision detection and hybrid force/motion control,” in *Proceedings of the 2005 IEEE International Conference on Robotics and Automation*, 2005, pp. 999–1004.

[16] O. Khatib, “Inertial properties in robotic manipulation: An object-level framework,” *The International Journal of Robotics Research*, vol. 14, no. 1, pp. 19–36, 1995.

[17] A. C. Bittencourt and S. Gunnarsson, “Static friction in a robot joint—modeling and identification of load and temperature effects,” *Journal of Dynamic Systems, Measurement, and Control*, vol. 134, no. 5, p. 051013, 2012.

[18] W. C. Stone, M. Juberts, N. Dagalakis, J. Stone, and J. Gorman, “Performance analysis of next-generation LADAR for manufacturing, construction, and mobility,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency/Internal Report 7117, 2004.

[19] S. Szabo, W. Shackleford, R. Norcross, and J. Marvel, “A testbed for evaluation of speed and separation monitoring in a human robot collaborative environment,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency/Internal Report 7851, 2012.

[20] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, and M. Thompson, “Guide to operational technology (OT) security,” National Institute of Standards and Technology, Gaithersburg, MD, Special Publication 800-82r3, 2023.

[21] U. B. Himmelsbach, T. M. Wendt, N. Hangst, P. Gawron, and L. Stiglmeier, “Human–machine differentiation in speed and separation monitoring for improved efficiency in human–robot collaboration,” *Sensors*, vol. 21, no. 21, p. 7144, 2021.

[22] Y. Liu, M. Hany, K. Montgomery, and R. Candell, “A collaborative robot work-cell testbed for industrial wireless communications,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Interagency/Internal Report 8365, 2021.

15.10 Exercises

15.1 ⌕ Concept check · 2 min

In scenario 1 nothing monitors the cell, and a person stands at the table for 5 s, where the moving arm passes within 214 mm of them. Why does no speed override above zero keep the arm working safely while they stand there?

(a) Below about half speed the drives brake so gently that the arm's stopping distance stays longer than the gap

(b) The scanner cannot resolve a person who stands inside the intrusion distance of the edge of the table

(c) A lower override lengthens the reaction chain, because the supervisor then waits longer between its cycles

(d) Even a crawling arm owes the person's approach through the reaction chain, the intrusion and the uncertainties

15.2 Concept check · 2 min

In scenario 4 the supervisor plans the stop of the loaded arm on a brochure braking figure of $5\,\mathrm{m/s^2}$, while the drives can supply only about $3.13\,\mathrm{m/s^2}$ with the part. How does the true stop from $1.00\,\mathrm{m/s}$ compare with the one the model promises?

(a) It is somewhat longer in distance and much longer in time, and the person keeps walking through that time

(b) It is much longer in distance, because both drives saturate and the arm coasts at nearly full speed

(c) It matches the promise, because the servos follow the stopping reference to within a millimeter

(d) It is shorter than promised, because the joint friction adds its torque to the braking of the drives

15.3 Concept check · 2 min

In scenario 8 the gearboxes run at 250 % of the friction that the observer's model expects, and the 3 N m residual threshold gives 19 nuisance stops in a minute. What does raising the threshold to 12 N m, with the model unchanged, do?

(a) The nuisance stops end and every strike is caught sooner, because the residual is larger

(b) The nuisance stops end, but a strike can be caught later than the declared reflex time

(c) Nothing changes, because the observer gain and not the threshold sets the reflex timing

(d) The nuisance stops grow, because a higher threshold admits more of the friction error

15.4 Theory and calculation · 5 min

The arm moves at $v_r = 1.00\,\mathrm{m/s}$ with the 3 kg part. The correct braking model plans on $a = 0.9 \times 3.13\,\mathrm{m/s^2}$. The reaction chain is $T_r = 170\,\mathrm{ms}$, the approach speed $v_h = 1.6\,\mathrm{m/s}$, the intrusion distance $C = 200\,\mathrm{mm}$ and the uncertainties $Z_d = 50\,\mathrm{mm}$ and $Z_r = 10\,\mathrm{mm}$.

(a) Compute a, the stopping time T_s and the terms S_h, S_r and S_s of Equation (15.8). *Checkpoint:* $a = 2.817\,\mathrm{m/s^2}$, $T_s = 355\,\mathrm{ms}$, $S_h = 840\,\mathrm{mm}$, $S_r = 170\,\mathrm{mm}$, $S_s = 178\,\mathrm{mm}$, each within 1 mm.

(b) Add the terms to S_p, and give S_p with the arm at rest. *Checkpoint:* 1448 mm within 2 mm, and 532 mm.

(c) How much of S_h is the person's walk during the stop, and how does it compare with the arm's own braking distance S_s? *Checkpoint:* 568 mm, more than three times S_s.

15.5 Theory and calculation · 6 min

Use the speed law of Equation (15.9) with the values of the previous exercise, $a = 2.817\,\mathrm{m/s^2}$ and $T_r = 170\,\mathrm{ms}$, and the margin $m = 50\,\mathrm{mm}$ that the supervisor subtracts from the measured separation.

(a) Compute β and D_0. *Checkpoint:* $\beta = 0.738\,\mathrm{s}$ and $D_0 = 532\,\mathrm{mm}$.

(b) Compute the speed allowed at a measured separation of 1.0 m. *Checkpoint:* 0.50 m/s, within 0.01 m/s.

(c) Find the measured separation at which full speed, 1.00 m/s, is first allowed, the separation at or below which nothing is allowed, and the separation a stopped arm needs before it restarts with $h = 100$ mm. *Checkpoint:* 1498 mm within 2 mm, 582 mm and 682 mm.

15.6 Theory and calculation · 5 min

Power and force limiting allows the speed of Equation (15.11), with $m_R = (m_1 + m_2)/2 + m_{tool} + m_L$. The links weigh 8 and 4 kg and the wrist and gripper 1.5 kg. The chest has $m_B = 40$ kg, $k_B = 25$ N/mm and $F_{max} = 280$ N, and the hand $m_B = 0.6$ kg, $k_B = 75$ N/mm and the same 280 N.

(a) With the 3 kg part, compute m_R, the reduced mass μ for the chest and the speed the chest allows. *Checkpoint:* 10.5 kg, 8.32 kg and 0.61 m/s.

(b) Compute the speed the hand allows, and say which limit the hand-over legs must obey and why. *Checkpoint:* 1.36 m/s; the chest's.

(c) Repeat (a) for a 6 kg part. *Checkpoint:* 13.5 kg and 0.56 m/s.

15.7 App challenge · 9 min

Load scenario 4, An optimistic braking model, and change no setting. Press Run at 1x with the default seed. The run pauses itself at the first separation violation.

(a) On the Separation view, read the measured separation d and S_p on the supervisor card, and the true separation and true S_p on the truth audit line, with the clock reading. *Checkpoint:* 6.22 s; $d = 1486$ mm against $S_p = 970$ mm; true 1478 mm against 1558 mm.

(b) Press Run again, at 2x if you wish, and let the run reach 60 s, pressing Run after any pause. Read the Separation violated and Cycles tiles. *Checkpoint:* 6 episodes, worst 506 mm; 7 cycles.

(c) Press Reset, switch to Advanced and set Braking model to Correct on the scanner card before Run. Run 60 s and read the same two tiles. What did the optimistic model buy? *Checkpoint:* never violated; 7 cycles; nothing.

15.8 App challenge · 9 min

Load scenario 3, Latency and uncertainty are distance, which ships with a scanner latency of 300 ms, and use the default seed and a speed of 5x. Each run lasts 240 s.

(a) Run with no change. Read the Cycles tile, the Separation violated tile, and T_r on the scanner card. *Checkpoint:* 36 cycles, 540 h^{-1}; never; 370 ms.

(b) Press Reset, set Scanner latency to 100 ms before Run and run again. Read the Cycles tile and compute the cost of each 100 ms of latency between the two runs. *Checkpoint:* 44 cycles, 660 h^{-1}; 60 cycles an hour per 100 ms.

(c) Press Reset, keep 100 ms and set Position uncertainty the supervisor assumes to 200 mm before Run. Read the Cycles tile and say why none of the three runs violates. *Checkpoint:* 41 cycles, 615 h^{-1}; the terms are honest.

15.9 App challenge · 8 min

Load scenario 5, A person at the boundary, which ships with no restart hysteresis. Use the default seed and a speed of 5x, and read the Protective stops and Cycles tiles at the end of each run.

(a) Run 60 s with no change. *Checkpoint:* 13 protective stops, 0 cycles.

(b) Press Reset, set Restart hysteresis to 100 mm before Run, and run 90 s, through the step back at about 61 s. *Checkpoint:* 2 protective stops, 3 cycles.

(c) Press Reset, set Restart hysteresis back to 0 before Run and run 90 s. What does the hysteresis cost and what does it buy? *Checkpoint:* 17 protective stops, 4 cycles.

15.10 Application area · 3 min

A cell integrator proposes to copy the chapter's 1448 mm into the protective field of a safety scanner on a real collaborative cell that runs at 1.00 m/s with a 3 kg part. Give two reasons the number cannot be used, and name where the real values must come from.

15.11 Application area · 4 min

A person reaches a hand into fixture Q while the arm places a part there.

(a) Which contact hazard does the model leave out, and why does the speed of Equation (15.11) not cover it?

(b) Name two idealizations of the scanner in the model, and say what a real scanner's occlusion by the arm would do to the separation the supervisor uses.

15.12 Review the agent · 5 min

An AI assistant is asked how to pass the challenge, Ten minutes of mixed traffic, and replies as follows. "Keep the brochure braking figure, because it lets the arm run faster near the person. Add 100 mm of restart hysteresis and power and force limiting at the chest on the hand-over legs. The shift then makes 62 cycles with 8 hand-overs and 24 protective stops, so it beats the target of 55 cycles and 30 stops with more cycles than the configuration the app suggests." Find the flaw and say how you would check it.