



Bridge Security Guidelines

2nd Edition | May 2022





American Association of State Highway and Transportation Officials
555 12th Street, NW, Suite 1000
Washington, DC 20004
202-624-5800 phone/202-624-5806 fax
www.transportation.org

© 2022 by the American Association of State Highway and Transportation Officials. All rights reserved. Printed in the United States of America. This book or parts thereof may not be reproduced in any form without written permission of the publishers.

ISBN: 978-1-56051-789-4

Pub Code: BSG-2



© 2022 by the American Association of State Highway and Transportation Officials.
All rights reserved. Duplication is a violation of applicable law.

**AASHTO EXECUTIVE COMMITTEE
2021–2022**

Voting Members

Officers

President: Shawn Wilson, Louisiana*

Vice President: Roger Millar, Washington*

Secretary-Treasurer: Russell McMurry, Georgia

Executive Director: Jim Tymon, Washington, DC

Regional Representatives

Region I: Marie Therese Dominguez, New York
Nicole Majeski, Delaware

Region II: Brad White, Mississippi
Vacant

Region III: Julie Lorenz, Kansas
Jack Marchbanks Ohio

Region IV: Bill Panos, North Dakota
Kristina Swallow, Nevada

Nonvoting Members

Immediate Past President: Victoria Sheehan, New Hampshire

*Elected at the 2021 Annual Meeting

**AASHTO COMMITTEE ON BRIDGES AND STRUCTURES
2020–2021**

Carmen Swanwick, Utah, *Chair*
Scot Becker, Wisconsin, *Vice Chair*

Joseph Hartmann, *Liaison*, FHWA
Patricia Bush, *Liaison*, AASHTO

Alabama

Jeffrey Huner
William Tim Colquett
Eric Christie

Alaska

Elmer Marx
Leslie Daugherty
Richard Pratt

Arizona

David Benton
David Eberhart
Pe-ShenYang

Arkansas

Joe Sartini
Michael Hill
Rick Ellis

California

Gudmund Setberg
Michael Johnson
Thomas Ostrom

Colorado

Jessica Martinez
Michael Collins
Stephen Harelson

Connecticut

Andrew Cardinali
Bart Sweeney
Timothy Fields

Delaware

Craig Stevens
Jason Arndt
Jason Hastings

Dist of Columbia

Konjit Eskender
Richard Kenney
Waseem Dekelbab

Florida

Don Cooney
Sam Fallaha
William Potter

Georgia

Donn Digamon
Douglas Franks
Steve Gaston

Hawaii

James Fu
Nicholas Groves

Idaho

Matt Farrar

Illinois

Ruben Boehler
Tim Armbrecht

Indiana

Andrew Fitzgerald
Stephanie Wagner
Anne Rearick

Iowa

James Nelson
Michael Nop

Kansas

Calvin Reed
Karen Peterson
Mark Hurt

Kentucky

Michael Carpenter
Royce Meredith

Louisiana

Chris Guidry
Artur DAndrea
Zheng Zheng Jenny Fu

Maine

Jeffrey Folsom
Wayne Frankhauser
Michael Wight

Maryland

Jesse Creel
Maurizio Agostino
Jeffery Robert

Massachusetts

Justin Slack
Matthew Weidele
Alexander Bardow

Michigan

Rebecca Curtis
Richard Liptak
Matthew Chynoweth

Minnesota

Ed Lutgen
Kevin Western
Arielle Ehrlich

Mississippi

Bradnado Turnquest
Scott Westerfield

Missouri

Bryan Hartnagel
Darren Kemna

Montana

Amanda Jackson
Nathan Haddick
Stephanie Brandenberger

Nebraska

Fouad Jaber
Mark Ahlman

Nevada

David Chase
Jessen Mortensen

New Hampshire

Loretta Doughty
David Scott

New Jersey

Xiaohua Cheng

New Mexico

Kathy Crowell
Shane Kuhlman
Jeff Vigil

New York

Brenda Crudele
Ernest Holmberg
James Flynn

North Carolina

Brian Hanks
Girchuru Muchane
Scott Hidden

North Dakota

Jason Thorenson
Jon Ketterling

Ohio

Alexander Dettloff
Jeffrey Syar
Timothy Keller

Oklahoma

Justin Hernandez
Tim Tegeler
Walter Peters

Oregon

Albert Nako
Raymond Mabey
Tanarat Potisuk

Pennsylvania

Richard Runyen
Shane Szalankiewicz
Thomas Macioce

Rhode Island

Mary Vittoria-Bertrand
Keith Gaulin

South Carolina

Hongfen Li
Terry Koon
Jeff Sizemore

South Dakota

Steve Johnson
Dave Madden
Todd Thompson

Tennessee

Ted Kniazewycz

Texas

Bernie Carrasco
Graham Bettis
Jamie Farris

Utah

Mark Daniels
Rebecca Nix
Cheryl Hersh Simmons
Carmen Swanwick

Vermont

Carolyn Cota
Jim Lacroix
Robert Klinefelter
Kristin Higgins

Virginia

Andrew Zickler
Kendal Walus

Washington State

Mark Gaines
Bijan Khaleghi
Tony Allen

West Virginia

Chad Robinson
Tracy Brown

Wisconsin

Aaron Bonk
Josh Dietsche
Scot Becker
William Oliva

Wyoming

Jeff Booher
Michael Menghini
Paul Cortez

FOREWORD

The events that unfolded during the September 11 attacks on the United States of America motivated bridge engineers to face a new and unusual extreme design scenario prompting the engineering community to consider blast-resistant design for vulnerable bridges and transportation structures. Historically, designers considered only natural extreme events, such as earthquakes and floods. Until September 11, 2001, rarely in the history of bridge design had engineers considered designing bridges for an intentionally destructive event caused by humans.

Shortly after September 11, concerns of possible attacks on our nation's bridges led the Federal Highway Administration (FHWA) to assemble a Blue Ribbon Panel (BRP) of experts comprised of the country's most accomplished and renowned bridge engineers, transportation infrastructure managers, and academic researchers. This panel was tasked to develop a long-term strategy for deterring, disrupting, and mitigating potential attacks and providing guidance to highway infrastructure owners and operators (Blue Ribbon Panel on Bridge and Tunnel Security, 2003).

The knowledge and expertise of the BRP members laid the foundation for the understanding of bridge and tunnel security issues. Among the many BRP findings and recommendations were that outreach and education were needed to develop a greater awareness and professional capacity to address bridge and tunnel security challenges. In their opinion, trained professionals were needed to understand and meet these new challenges (Blue Ribbon Panel on Bridge and Tunnel Security, 2003).

Subsequently, the National Cooperative Highway Research Program (NCHRP) funded a study to develop *Blast-Resistant Highway Bridges: Design and Detailing Guidelines*, hereafter referred to as NCHRP 12-72. The study focused on developing design and detailing guidelines to improve structural performance and resistance of new and existing bridges to explosive effects. The study was endorsed by the newly formed AASHTO T-1 Technical Committee on Bridge Security and Hazards of the Subcommittee on Bridges and Structures (SCOBS) and led by Eric B. Williamson, Ph.D., P.E., professor of civil engineering at the University of Texas at Austin. The Transportation Research Board (TRB) published the results of NCHRP 12-72 in February 2010 as *NCHRP Report 645: Blast-Resistant Highway Bridges: Design and Detailing Guidelines* (Williamson et al., 2010). The study focused on substructures and provides scientific experiments, background, and analytical research for bridge engineers looking for design solutions to enhance the structural performance and resistance of concrete bridge columns.

Following this report, AASHTO and FHWA supported the development of an AASHTO guide specification incorporating the findings of NCHRP 12-72. The 1st edition of the *AASHTO Bridge Security Guidelines* received a favorable vote at the annual meeting of SCOBS in 2011, and the document was titled as a guideline rather than a specification.

Since the adoption of the 1st edition, numerous research results have become available through collaborative efforts of FHWA, the Department of Homeland Security (DHS), and the U.S. Army Corps of Engineers (USACE). Research has addressed critical bridge components in addition to reinforced concrete columns such as cable stays (Chiarito, Ray, et al., 2011) (FHWA, 2018a) (Ocel et al., 2019), steel bridge towers (Walker et al.; 2011a, 2011b, 2011c, 2011d, 2011e), and reinforced concrete bridge towers (Chiarito, Minor, et al., 2011). This 2nd edition of the *AASHTO Bridge Security Guidelines* incorporates the knowledge gained through these efforts. A bibliography is provided with references to research reports, some of which are considered Security Sensitive (SSI) and available on a need-to-know basis. Access to these SSI documents may be obtained by contacting the original authors or agencies.

How to Use These Guidelines

This 2nd edition of the *AASHTO Bridge Security Guidelines* is provided to the designer as a guidance document, and it is not intended to be a specification. This document should be used with both signature and common bridges, as historically both have been targets of attacks (Jenkins, 2001). Although this document provides the designer with information on the response of bridge components subjected to blast loads as well as blast-resistant design and detailing guidelines and analytical models of blast load distribution, it is not the end-all answer to every question that exists on this subject. In contrast, this guideline document and its underlying research are considered as continual progress toward educating all bridge stakeholders on the subject of bridge security.

The content of these guidelines concerns situations where resisting blast, impact, or other intentional manmade extreme loads is a valid load case considered by the owner or designer. In such situations, these loads are applied in accordance with AASHTO requirements (AASHTO, 2020) for the Extreme Load II case. The underlying philosophy is that these extreme loads should be considered in combination with all other applicable loads and other factors that may be present at the time of an event, such as the possibility of scour or intentional vehicle or vessel collision (FHWA, 2018c).

Ultimately, mitigation measures may provide the most cost-effective and practical means to enhance bridge security against intentional extreme threats. In some situations, however, depending on the nature and size of the assumed threat, these guidelines can result in outcomes that the owner or designer may consider infeasible and perhaps even unreasonable, such as excessive construction cost or reduced functionality. In such scenarios, owners and designers are encouraged to reevaluate their design assumptions and site layout, considering such factors as accessibility and standoff distance, until they are able to arrive at tolerable design and detailing solutions. When designing a bridge to resist a potential design threat is not

feasible, bridge owners must either accept the risk or make changes to the planning process (e.g., increase or reallocate budget, provide surveillance) as required to mitigate the risk.

Finally, these guidelines are not comprehensive; in fact, there are no recommendations in this document to design for a specific size of threat or standoff distance. Such parameters are left to the discretion of owners because they are in the best position to evaluate the specifics of a given situation.

ACKNOWLEDGMENTS

Many individuals as well as organizations have contributed their time, knowledge, and resources to allow for this document to be created and updated. Recognizing every individual who has contributed to a major project such as this often is difficult and even may be impossible because of their many numbers and because their participation is usually in various periods over a long range of time. Despite this fact, this attempt is made to recognize as many individuals as possible. Only because of them was this knowledge developed and made available.

Blue Ribbon Panel (BRP)

James E. Roberts, ERP Chair, Consulting Bridge Engineer, Imbsen and Associates, Inc.
John M. Kulicki, BRP Vice Chair, Modjeski and Masters, Inc.
Dwight Beranek, U.S. Army Corp of Engineers
Joseph M. Englot, Port Authority of New York and New Jersey
John W. Fisher, Lehigh University
Henry Hungerbeeler, Missouri DOT and Chair AASHTO Transportation Security Task Force
Jeremy Isenberg, Weidlinger Associates, Inc.
Frieder Seible, Jacobs School of Engineering, University of California at San Diego
Kenneth E. Stinson, Peter Kiewit Sons, Inc.
Dan Chung Tang, T.Y. Lin International
Kary H. Witt, Golden Gate Bridge, Highway and Transportation District

NCHRP 12-72 Research Team

Eric B. Williamson, Principal Investigator; Professor, University of Texas at Austin
Oguzhan Bayrak, Professor, University of Texas at Austin
G. Daniel Williams, II, University of Texas at Austin
Carrie E. Davis, University of Texas at Austin
Kirk A. Marchand, Managing Principal, Protection Engineering Consultants
Aldo E. McKay, Project Engineer, Protection Engineering Consultants
John M. Kulicki, President, Modjeski and Masters, Inc.
Wagdy Wassef, Project Manager, Modjeski and Masters, Inc.

Technical Committee on Bridge and Tunnel Security, T-1

Bernie Carrasco, Chair, Texas DOT
Vincent Chiarito, Federal Highway Administration
Andrew Joseph Fitzgerald, Indiana DOT
Arthur Wagner D'Andrea, Louisiana DOT
Kristin Higgins, Vermont DOT
James Harkness, Maryland Transportation Authority

Technical Support to T-1 Committee

Lisa Carter Powell, P.E. Structural Consultants, Inc.
Carrie E. Davis, C. Davis Consulting, LLC
Eric B. Williamson, University of Texas, Austin
G. Daniel Williams, II, Consultant

SCOBs First Technical Committee on Bridge and Tunnel Security, T-1

Hossein Ghara, Chair, Louisiana State Bridge Engineer
Barton Newton, Vice Chair, California State Bridge Engineer
Steve Ernst, FHWA
Sheila R. Duwadi, FHWA
Albert Wahid, New York State Bridge Engineer
Paul V. Liles, Georgia State Bridge Engineer
Kendal “Ken” Walus, Virginia State Bridge Engineer
Dennis Heckman, Missouri State Bridge Engineer
Jugesh Kapur, Washington State Bridge Engineer
Kary H. Witt, Golden Gate Bridge

Special Thanks

Mary Lou Ralls, Principal, Ralls Newman, LLC
George A. Christian, Former New York State Bridge Engineer
Kelley Severns, Former Program Manager for Engineering, AASHTO
Malcolm T. Kerley, Former Chief Engineer, Virginia DOT
David Beal, Former Program Director, NCHRP
Waseem Dekelbab, Former Implementation Coordinator, NCHRP
Dolores Valls, Former Deputy Division Chief, Structure Policy & Innovation, Caltrans
Sheila R. Duwadi, Former Research Engineer, Team Leader, Hazard Mitigation, FHWA
Cheryl Hersh-Simmons, Chief Structural Engineer, Utah DOT Structures Division

TABLE OF CONTENTS

AASHTO EXECUTIVE COMMITTEE	iii
AASHTO COMMITTEE ON BRIDGES AND STRUCTURES.....	iv
FOREWORD	v
ACKNOWLEDGMENTS	vii
SECTION 1—INTRODUCTION	1-1
1.1—GENERAL	1-1
1.2—PRIORITIZATION OF BRIDGES IN INVENTORY	1-3
1.3—RISK-BASED PRIORITIZATION OF BRIDGE COMPONENTS	1-4
1.4—DESIGN DEMAND	1-8
1.5—MITIGATION MEASURES	1-15
1.5.1—Deter.....	1-15
1.5.2—Deny.....	1-15
1.5.3—Detect.....	1-15
1.5.4—Defend (Structural Hardening).....	1-16
SECTION 2—LOADS AND LOAD FACTORS	2-1
2.1—LOAD FACTORS AND COMBINATIONS	2-1
2.2—CHANGE IN FOUNDATIONS BECAUSE OF LIMIT STATE FOR SCOUR.....	2-1
2.3—VEHICULAR COLLISION: <i>CT</i>	2-2
2.3.1—Security Considerations	2-2
2.4—VESSEL COLLISION: <i>CV</i>	2-2
2.4.1—Security Considerations	2-2
2.5—BLAST LOADING	2-3
2.5.1—Introduction.....	2-3
2.5.2—Blast Load Modeling Software	2-4
SECTION 3—STRUCTURAL ANALYSIS OF BLAST EFFECTS.....	3-1
3.1—BLAST ANALYSIS FACTORS.....	3-1
3.1.1—General.....	3-1
3.1.2—Dynamic Increase Factors (DIFs)	3-1
3.1.3—Strength Increase Factors (SIFs)	3-2
3.2—REINFORCED CONCRETE COLUMNS	3-2
3.2.1—Blast Design Categories	3-2
3.2.2—Column Blast Design Shear Analysis	3-3
3.3—OTHER COMPONENTS	3-6
3.3.1—Flexural Members	3-6
SECTION 4—PROVISIONS FOR THREAT DESIGN	4-1
4.1—REINFORCED CONCRETE COLUMNS	4-1
4.1.1—Blast Design Category A.....	4-1
4.1.2—Blast Design Categories B and C.....	4-1
4.1.3—Selection of Component Geometry	4-2
4.1.4—Lateral Reinforcement Detailing.....	4-3
4.1.5—Longitudinal Splices	4-4
4.2—REINFORCED CONCRETE TOWERS.....	4-4
4.2.1—General.....	4-5
4.2.2—Rebar Detailing and Placement.....	4-5

4.3—STEEL TOWERS	4-7
4.3.1—General	4-7
4.3.2—Design Considerations	4-7
4.4—STEEL CABLES	4-8
4.4.1—General	4-8
4.4.2—Design Considerations	4-9
4.5—OTHER COMPONENTS.....	4-10
4.5.1—Flexural Members	4-10
SECTION 5—PERFORMANCE QUALIFICATIONS	5-1
5.1—SCOPE	5-1
5.2—PEER REVIEW	5-1
5.3—BRIDGE STRUCTURAL COMPONENTS	5-2
5.3.1—Performance Qualification by Large-Scale Testing	5-2
5.3.2—Performance Qualification by Analysis and Design	5-3
 APPENDIX A—BRIDGE PRIORITIZATION ASSESSMENT.....	 A-1
A.1—BRIDGE PRIORITIZATION AND RISK-BASED COMPONENT PRIORITIZATION	A-1
A.1.1—Bridge Prioritization Example.....	A-1
A.1.2—Bridge Component Prioritization Example	A-3
APPENDIX B—BRIDGE COLUMN BLAST DESIGN EXAMPLES	B-1
B.1—OVERVIEW	B-1
B.2—DESIGN EXAMPLES.....	B-1
B.3—SUMMARY	B-1
B.4—DESIGN EXAMPLE 1: REINFORCED CONCRETE BRIDGE COLUMN IN DESIGN CATEGORY C	B-2
B.4.1—Design Category C Column.....	B-2
B.5—DESIGN EXAMPLE 2: REINFORCED CONCRETE BRIDGE COLUMN FOR A LARGER THREAT WITHIN DESIGN CATEGORY C.....	B-8
B.5.1—Design Category C Column.....	B-8
B.6—DESIGN EXAMPLE 3: CHANGES REQUIRED FOR A COLUMN IN DESIGN CATEGORY B.....	B-16
B.6.1—Design Category B Column.....	B-16
B.7—DESIGN EXAMPLE 4: REINFORCED CONCRETE BRIDGE COLUMN IN DESIGN CATEGORY A.....	B-21
B.7.1—Design Category A Column	B-21
APPENDIX C—RETROFIT OF EXISTING BRIDGES	C-1
C.1—RETROFITS OF EXISTING BRIDGES.....	C-1
C.2—RETROFIT OPTIONS FOR REINFORCED CONCRETE COLUMNS	C-1
C.3—RETROFIT OPTIONS FOR STEEL TOWERS	C-1
C.4—RETROFIT OPTIONS FOR REINFORCED CONCRETE TOWERS.....	C-2
C.5—RETROFIT OPTIONS FOR STEEL CABLES	C-2
C.6—RETROFIT OPTIONS FOR STEEL TRUSSES	C-2
APPENDIX D—BREACH AND SPALL CURVES FROM UFC-3-340-02	D-1
D.1—USING BREACH AND SPALL CURVES FROM UFC-3-340-02.....	D-1

SECTION 1 INTRODUCTION

1.1—GENERAL

To aid in asset management of bridges, it is advisable that bridge owners prioritize the importance of both new bridges in the planning phase and existing bridges already in inventory to plan the appropriate allocation of limited resources.

Bridge owners should conduct a formal vulnerability study to determine appropriate structural hardening or other countermeasures to include in new designs or in the retrofit of existing bridges to mitigate the identified risks or vulnerabilities on bridges deemed important. A risk management approach should be developed to outline and aid the decision-making process to mitigate risks of vulnerabilities.

Articles 1.2 and 1.3 provide uniform procedures for prioritizing the importance of bridges and assessing the risk to bridge components, respectively, and should be used by bridge engineers and planners unless bridge owners have developed alternate procedures for prioritizing bridge importance.

C1.1

These guidelines provide uniform methods bridge owners can use to prioritize the importance of bridges and assess the risk to bridge components. While these guidelines advise bridge owners to prioritize the importance of their bridges and the risk to components for the allocation of limited resources, they do not advocate the use of a particular method. Previously, no uniform procedure existed, and in the absence of another option, some states developed their own procedures, incorporating security prioritization methods that, while similar, differ in the details. In addition, state procedures to assess bridge importance have been developed by some departments of transportation to assist in prioritizing seismic rehabilitation. These procedures also may be used in conjunction with security considerations, provided some procedure approved by the bridge owner is used for this purpose.

The first step in the risk assessment process provided in these guidelines is to identify bridge assets in a bridge owner's inventory. The second step is to prioritize the criticality of those bridges based on symbolic and economic importance to the region or nation using the procedure outlined in Article 1.2 or another method approved by the bridge owner. Prioritization according to criticality first is important before conducting vulnerability analyses of individual bridges and components to focus limited time and resources toward vulnerability assessments of the most critical bridges. Given the vast number of assets in many bridge owners' inventories, it would be impractical and costly to include vulnerability analyses of all bridges as part of the process to determine criticality.

When determining criticality of bridges, many procedures include the following factors, and they should be considered for any method used for this purpose:

- Social and economic impact of bridge loss;
- Role played by bridge in defense or security of a region, state, and nation;
- Average daily traffic (ADT);
- Average daily truck traffic (ADTT);
- Distance to nearest detour;
- Symbolic importance;
- Contributing resilience to the community or areas served; and
- Multimodal traffic carried by the bridge.

The third step is to conduct a risk assessment of the individual bridges deemed critical and their components to determine the most effective and cost-efficient mitigation measures. To this end, the risk assessments should include, at a minimum, potential threat characterization and probability, likelihood of threats to specific bridge components, analysis of component response, replacement time and cost, and impact on overall bridge integrity.

Once the risk assessment process is complete, the results should be used to inform decisions on resource allocation and mitigation efforts. It is recommended that the risk analysis procedure be used in an iterative manner considering proposed countermeasures both when determining initial mitigation measures and afterward when considering new mitigation measures with subsequent resources. Completing the process in an iterative manner will allow bridge owners to reduce risk to an acceptable level over a specified time given available resources.

Guidance on security strategies and risk reduction may be found in the following documents: *Design of Critical Bridges for Security against Terrorist Attacks* (Winget and Williamson, 2003), *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection* (AASHTO, 2002), *Improving Surface Transportation Security: A Research and Development Strategy* (Transportation Research Board and National Research Council, 1999), *Protecting Public Surface Transportation against Terrorism and Serious Crime: An Executive Overview* (Jenkins, 2001), and *Recommendations for Bridge and Tunnel Security* (Blue Ribbon Panel on Bridge and Tunnel Security, 2003), as well as in the ASCE *Journal of Bridge Engineering* articles “Analysis and Design of Critical Bridges Subjected to Blast Loads” (Winget, Marchand, and Williamson, 2005), “Risk-based Prioritization of Terrorist Threat Mitigation Measures on Bridges” (Ray, 2007), and “Risk Management and Design of Critical Bridges for Terrorist Attacks” (Williamson and Winget, 2005).

It is important to note that once critical/vulnerable bridges have been identified, bridge owners should consider developing a process for restricted access to bridge plans for such structures. Such processes should be in compliance with guidance provided under the U.S. Department of Transportation Federal Highway Administration (FHWA) 49 CFR Part 15—Protection of Sensitive Security Information. The Department of Homeland Security’s Form 11054 may be used as a coversheet for bridge records deemed Sensitive Secure Information (SSI).

1.2—PRIORITIZATION OF BRIDGES IN INVENTORY

Equation 1.2-1, or another method approved by the bridge owner, can be used by bridge owners to prioritize their bridges for the appropriate allocation of available resources. If another method is used, it at a minimum should consider the risk of attack based on a bridge's symbolic or historic importance, the potential economic impact on the region or municipality, and availability of alternate detours.

$$\text{Criticality Factor, } CF = S^2 + E \times D \quad (1.2-1)$$

where:

S = Symbolic Importance
 E = Economic Importance
 D = Detour Impact

using the values in the following table. When bridges obtain the same Criticality Factor, the first tie-breaker shall be the result of $E \times D$, and the second shall be the value of E .

Table 1.2-1—Criticality Factor Variables

Criteria	Value	Definition
Symbolic Importance, S	1	Largely invisible in the community
	2	Visible within the community
	3	Visible statewide
	4	Visible nationwide
	5	Visible worldwide
	6	Iconic national symbol
Economic Importance, E	1	Fewer than 100 vehicles per day
	2	100 to 5,000 vehicles per day
	3	5,000 to 25,000 vehicles per day
	4	25,000 to 100,000 vehicles per day
	5	100,000 to 200,000 vehicles per day
	6	More than 200,000 vehicles per day
Detour Impact, D	1	Two or more <u>comparable</u> detours within 10 miles
	2	One within 10 miles
	3	None within 10 miles
	4	None within 20 miles
	5	None within 50 miles
	6	None within 100 miles, or no alternate route

C1.2

This section provides a uniform procedure to assess the importance of bridges in an inventory based on their relative symbolic and economic importance, and it should be used in the absence of an existing method developed internally by a bridge owner. This method is based on a collective review of several similar procedures, including that proposed by AASHTO (2002) and information provided by state departments of transportation.

The method is based on three objective characteristics that contribute to a bridge's criticality: Symbolic Importance, S , which can be determined either qualitatively by familiarity with comparable bridges or quantitatively by counting visitors, mentions in public media, or another quantifiable value; Economic Importance, E , as determined by average daily traffic; and Detour Impact, D , as determined by distance to comparable detours. The impact of bridge loss is equal to $E \times D$, or the multiple of the economic loss and the detour hardship.

While the $E \times D$ value should objectively characterize the relative impact of bridge loss for the majority of bridges, exceptional scenarios may exist that warrant a modified approach, such as when bridges provide the only access to emergency services or public utilities. In such cases, it may be appropriate to modify $E \times D$ by a factor α , such that the impact of bridge loss then equals $\alpha \times E \times D$, where α is a value defined by the bridge owner. However, the use of this modification should be exceptionally rare. In the majority of such cases, the value of $E \times D$ will already be exceptionally high based on the long detour required to reach the service or utility, or if there truly is no available detour, it would be infinity and already be at the top of the priority list.

Replacement time and cost intentionally are not included for three reasons. First, both are inherently included in this method. In general, the bridges with high symbolic importance, high daily traffic, and minimal detour options are also the ones with high replacement time and cost due to long spans, large structures, and difficult construction conditions. Second, the replacement time and cost depend on the type of attack, location of attack, and component attacked, all of which are not characteristic solely to the bridge itself, and therefore they are to be considered during the individual risk assessments rather than during an inventory-wide determination of criticality of entire bridges. Finally, replacement time and cost should not be used to justify expensive mitigation efforts for a bridge that has little to no visibility, minimal traffic or economic value, or multiple other detour options that minimize the impact of loss of the bridge. Whether or not a bridge is critical is independent of its vulnerability, and the determination of those two values should be done independently.

Notes: When selecting a comparable bridge, consideration should be given to both daily vehicle capacity and vehicle weight limits.

When selecting Detour Impact, D , consider capacity (or lack thereof) of comparable bridges within the detour radii and apply judgement in selecting a value of D that accounts for both distance and delay.

If $E \geq 4$ for two nearby bridges with no third comparable bridge within 50 miles, set D for one of the two bridges ≥ 4 based on the value corresponding to the second available detour (third bridge).

Bridge owners may use decimal values in lieu of integer values if they believe it will more accurately rank bridges in each of these categories.

1.3—RISK-BASED PRIORITIZATION OF BRIDGE COMPONENTS

Bridge owners should establish criteria for the size and location of the threats to be considered when analyzing bridges for security. Section 2 provides descriptions of threats which can be used for this purpose. These threat criteria should consider the type, geometry, and importance of the structure being considered. The criteria also should consider multitier threat sizes and define the associated level of structural performance for each tier.

Engineers can use Equations 1.3-1 through 1.3-4, or another method approved by the bridge owner, to evaluate the total risk to an individual bridge and its critical components. These equations should not be used to compare the risk between bridges. These equations, or another method approved by the bridge owner, should also be used in an iterative manner to determine the value of available countermeasures with competing costs.

$$\text{Total Bridge Risk, } R = \sum [I_j \sum (O_{tj} V_{tj})] \quad (1.3-1)$$

where:

- j = individual bridge component
- t = basic threat
- I_j = importance of a component, j , to the bridge
- O_{tj} = relative likelihood of a basic threat
- V_{tj} = relative vulnerability of a given component

C1.3

Once bridges are prioritized for mitigation efforts, individual components within bridges should be prioritized. This prioritization should be risk-based because not all components have the same risk of being attacked, nor does the failure of all components yield the same risk of structural instability.

Previously, no codified method existed for bridge owners to complete a component-level risk analysis of a bridge, and therefore many bridge owners may have internally developed procedures for this purpose. The method presented in these guidelines is not intended to replace custom methods in use by individual bridge owners, but it is recommended as a standardized procedure in the absence of another preferred method.

This method is based on basic risk equations used for natural hazard risk assessments as adapted and implemented by Ray (2007), and it uses the standard risk equation, $\text{Risk} = OVI$, where O = occurrence, V = vulnerability, and I = importance. As applied to bridges, this method considers several factors to determine the relative risk to bridge components, including likelihood of threat occurrence, vulnerability of components to threats, structural importance of components, historic importance of each component, attractiveness of a component to an attacker, and expected replacement time and cost.

The result of this method is not an actual probability, but rather a subjective measure of expected bridge failure from given threats against given components. While it might appear that these equations can be used to compare components on one bridge with those on another, the resulting values are only relative indicators of risk within a given bridge because they are functions of the total number of components and corresponding attributes in a given bridge, both of which can vary greatly among bridges. Therefore, this procedure is not to be used to compare bridges or components across bridges. Once complete, this process may be done iteratively for individual bridges, either to evaluate the relative effectiveness of mitigation measures or to allocate resources in subsequent years after implementing initial mitigation measures.

$$\text{Component Importance, } I_j = \sum[wf_i a_i]SR \quad (1.3-2)$$

$$\text{Threat Occurrence, } O_{ij} = \sum[wf_o a_o] \quad (1.3-3)$$

$$\text{Component Vulnerability, } V_{ij} = \sum[wf_v a_v] \quad (1.3-4)$$

where:

wf = weighting factor applied to the attribute
 a = attribute
 SR = ratio of span length to main (or largest) span

The Component Importance factor, I_j , measures the importance of an individual component, j , to the bridge. This factor is most important because structural failure is the worst possible outcome, and this has the greatest impact on this outcome.

Table 1.3-1—Component Structural Importance Attribute, a_i

Value	Definition
1.00	Critical component with no alternate load path nor the additional capacity needed to withstand the threat while maintaining its service load, whose failure is likely and would lead to global structural instability
0.75	Critical component with robustness but no redundancy, whose failure is not likely but would lead to global structural instability
0.50	Important component that has at least one other load path
0.25	Important component with multiple other load paths
0.00	Noncritical to overall stability

The Structural Importance Attribute captures the importance of an individual component to the overall stability of the bridge. In some respects, it is the most important attribute because it directly reflects the worst possible outcome of a hazard event, which is complete collapse of a bridge. Example considerations regarding component redundancy and criticality include differences in risk between single-column structures and multicolumn bents, single main suspension cables and multiple hanger cables, and girders comprising main structural spans or bracing for stability and floor beams that are secondary structural members.

Table 1.3-2—Component Historic Importance Attribute, a_i

Value	Definition
1.00	Historically irreplaceable and not reproducible by any method
0.75	Historically irreplaceable and not easily reproducible
0.50	Historically irreplaceable but easily reproducible
0.25	Historic but replaceable
0.00	None

The Historic Importance Attribute captures the potential importance of components that have a high profile in the public sphere or that cannot be replaced directly or indirectly because the manufacturer no longer exists. This attribute should be evaluated for individual components rather than bridges as a whole.

Table 1.3-3—Relative Repair Cost Importance Attribute, a_i

Value	Definition
1.00	Very high
0.75	High
0.50	Medium
0.25	Low
0.00	Little to none

Table 1.3-4—Relative Time Out of Service Attribute, a_i

Value	Definition
1.00	Very long
0.75	Long
0.50	Medium
0.25	Short
0.00	Little to none

Table 1.3-5—Likelihood of Threat Occurrence, a_o

Value	Definition
1.00	Very high
0.75	High
0.50	Medium
0.25	Low
0.00	Little to none

Table 1.3-6—Likelihood of Threat Occurrence against a Given Component, a_o

Value	Definition
1.00	Very high
0.75	High
0.50	Medium
0.25	Low
0.00	Little to none

The Relative Repair Cost attribute addresses the relative repair costs between components of a given bridge. It is particularly important when the loss of components may not cause overall structural collapse, but differing components have different replacement costs and therefore may warrant differing levels of protection.

The Relative Time Out of Service attribute captures the importance of a component based on how long the bridge will be out of service after loss of the component. In some cases, an important component may be replaceable in a matter of days, whereas another may be replaceable in months. Both would have different levels of impact on the local community and therefore may warrant different levels of protection.

The Span Ratio, SR , is the ratio found by the length of the span to which the component contributes divided by the main span length. It is a separate factor by which the importance factor is multiplied to account for the importance of a component to the overall functionality and cost of the entire bridge rather than just to a single span. In many cases, the loss of the main, or longest, span would be more catastrophic and require more replacement time and cost than that of a shorter approach span.

The Threat Occurrence factor, O_{ij} , is the likelihood a given threat, i , will be used against a given component, j . Unlike the vulnerability and importance factors, this value is a subjective expectation that a threat, i , will occur and does not represent an actual probability. There are several attributes to consider.

The first is the Likelihood of Threat Occurrence, which is the likelihood a given threat will be used against a bridge at any time. This attribute does not consider the attractiveness, vulnerability, or importance of any particular component, but rather the chances a given attack method will be used based on historical trends and the capabilities of adversaries.

The next is the Likelihood of Threat Occurrence against a Given Component, independent of component attractiveness or accessibility. For example, is it likely a cutting device will be used against a large reinforced concrete column or against a cable, or a large explosive device against a large column or a cable? In many cases, this attribute will be zero because the likelihood of a threat being used against a component is negligible.

Table 1.3-7—Likelihood of Threat against a Component Based on Visibility or Attractiveness, a_o

Value	Definition
1.00	Very high
0.75	High
0.50	Medium
0.25	Low
0.00	Little to none

Table 1.3-8—Likelihood of Threat Based on Access to a Component, a_a

Value	Definition
1.00	Completely accessible, $RT \gg AT$
0.75	RT probably $> AT$
0.50	$RT = AT$
0.25	RT probably $< AT$
0.00	Access completely denied, or $AT \gg RT$

Note: The bridge owner shall approve appropriate values for the Attack Time (AT) and Response Time (RT) based on past events and response times of local emergency services.

Table 1.3-9—Vulnerability Attribute for Explosive Threats, a_v

Value	Definition
1.00	Component destruction with less than x explosive weight
0.67	Component destruction with x to $6x$ explosive weight
0.36	Component destruction with $6x$ to $20x$ explosive weight
0.20	Component destruction with $20x$ to $60x$ explosive weight
0.10	Component destruction with $60x$ to $120x$ explosive weight
0.06	Component destruction with $120x$ explosive weight
0.00	Little to none

Note: The bridge owner shall approve the size and location of threats to be considered for both hand-placed and vehicle-borne explosives.

The Likelihood of Threat against a Component Based on Visibility or Attractiveness represents the likelihood the component will be attacked based on the odds an attacker would view the component as an attractive or effective target. In many cases, it is clear—even to a non-engineer—that a component is critical to the structural stability of a bridge, and it is reasonable to expect an attacker will view such components as desirable targets. This attribute is given a low weighting factor because it is impossible to evaluate with certainty the knowledge of, or support provided to, an attacker.

The Likelihood of Threat Based on Access to a Component captures the risk based on the ability of an attacker to access a component quicker than emergency services can respond. In some cases, a component may not warrant additional protection because it may be extremely difficult for an attacker to access, or in other cases the time required to access a component due to existing mitigation measures may be greater than the time required for emergency services to intervene, such as primary columns blocked by fencing. The standoff distance—or distance from the center of the explosive charge to the target—for some threats, such as large Vehicle-Borne Improvised Explosive Devices (VBIEDs), should not be considered for this attribute if those threats may be used or attempted at the existing standoff, regardless of their effectiveness. Those factors and the resulting effectiveness of the threats should be considered when determining the vulnerability factor.

The Component Vulnerability factor, V_{ij} , attempts to capture the relative vulnerability of a given component, j , to a threat, i . The only attribute contributing to the vulnerability factor is the structural resistance to a given threat based on its existing configuration and mitigation measures.

The Vulnerability Attribute for Explosive Threats captures the likelihood a component will be destroyed based on the amount of explosive required to render it unable to support its load. This attribute may be used repeatedly considering multiple explosive threats. In most cases, the more explosive material needed to destroy a component, the harder it will be for an attacker to obtain and deliver that material, and therefore the less risk the threat poses to the component. Many explosive threats should be considered, and as a minimum, suggested threats include VBIEDs, Hand-Emplaced Improvised Explosive Devices (HEIEDs), and various shaped and cutting charges. The coefficients and value for x can and should vary from those listed in the table based on the sizes of the explosive threats likely to be used. The coefficients shown were originally developed by Ray (2007) using the analytical hierarchy methodology by Ragsdale (2002). It is recommended that the coefficients be nonlinear and represent the decreasing probability of obtaining and using a device as the charge weight increases.

Table 1.3-10—Vulnerability Attribute for Cutting, a_v

Value	Definition
1.00	Strength loss in less than x min
0.75	Strength loss in less than $2x$ min
0.50	Strength loss in less than $6x$ min
0.25	Strength loss in greater than $6x$ min
0.00	Not applicable or not vulnerable to cutting

Note: The bridge owner shall approve the time intervals to be considered based on the accessibility of the components, ability to detect cutting, and the response times of local emergency services.

Table 1.3-11—Vulnerability Attribute for Fire, a_v

Value	Definition
1.00	Strength loss in less than x min
0.75	Strength loss in less than $3x$ min
0.50	Strength loss in less than $6x$ min
0.25	Strength loss in greater than $6x$ min
0.00	Not applicable or not vulnerable to fire

Note: The bridge owner shall approve the time intervals to be considered based on the accessibility of the components and response times of local emergency services.

Table 1.3-12—Vulnerability Attribute for Vehicular Impact, a_v

Value	Definition
1.00	Complete destruction from a “small weight vehicle” impact
0.75	Complete destruction from a “medium weight vehicle” impact
0.50	Complete destruction from a “large weight vehicle” impact
0.25	Partial destruction from a “large weight vehicle” impact
0.00	Not applicable or can withstand all vehicular impacts

Table 1.3-13—Weight Factor for Vehicular Impact, w_f

Risk Factor	Component Attribute, a	Weight Factor, w_f
Importance	Structural importance	0.5
	Historic importance	0.1
	Repair cost	0.2
	Time out of service	0.2
Occurrence	Threat likelihood	0.1
	Threat likelihood against component	0.3
	Visibility or attractiveness of component	0.1
	Access to component	0.5
Vulnerability	Resistance of component to basic threat, t	1.0

The Vulnerability Attribute for Cutting captures the ability of an attacker to complete a cut to the point it renders a component unable to support its load, prior to emergency services responding to stop an attack. Similar to the attribute for explosive threats, the coefficients and value for x can and should vary from those listed in the table based on the components being evaluated. While not rigorously developed from past events (none within the United States exist for a basis), the values shown attempt to reflect the likelihood that a terrorist would choose a cutting method based on the degree of difficulty in cutting. These values may be adjusted by engineers; it is recommended that the coefficients be nonlinear and represent the decreased risk based on increased difficulty and time required to complete larger cuts.

The Vulnerability Attribute for Fire captures the risk of fire destroying a component based on the ability of emergency services to stop the fire before the component loses its ability to support its load. Partial damage and time for the fire to reach a component should not be considered. Limits on truck sizes may be an upper bound to consider. Also consider potential flammable cargo that may cross a bridge and whether storage of flammable material under bridges is limited or eliminated.

The Vulnerability Attribute for Vehicular Impact captures the risk of various vehicles destroying critical components. In most cases, the larger the vehicle required to destroy a component, the more difficult it is for an attacker to acquire that vehicle to conduct an attack. This attribute can be used for ground-, water-, or air-based vehicles. Vehicles to consider range from small sedans to large semitrucks for ground vehicles; from small, personal recreational boats to large barges and shipping vessels for water-based vehicles; and from unmanned drones and single-engine aircraft to large jets for air-based vehicles.

1.4—DESIGN DEMAND

Bridge owners should establish criteria for the size and location of the threats to consider when analyzing bridges for security. These criteria should account for the type, geometry, and importance of the structure. The criteria should also consider multitier threat sizes and define the associated level of structural performance desired for each tier.

Design demands result from analyses of given design threats, accounting for the associated performance levels. A design strategy based on these demands shall be approved by the bridge owner.

C1.4

The following are issues to consider in the security design of a bridge:

- Threat identification,
- Bridge importance,
- Vulnerability assessment,
- Mitigation,
- Cost-benefit analysis of implementing protective measures,
- Selection of strategy of implementing protective measures, and
- Historical attacks and capabilities of adversaries.

Protecting a bridge from every conceivable threat is not possible. The most likely threat scenarios are based on attacker capabilities, the bridge structural system and geometry, and identified vulnerabilities. The most likely scenarios will minimize the attacker's required time on target, possess simplicity in planning and execution, and have a high likelihood of achieving maximum damage.

The level of acceptable damage may be proportionate to the size of the attack. For example, linear behavior, local damage, or both may be expected in a high-probability, small-sized attack, while significant permanent deformations, significant damage, partial failure of some components, or some combination thereof may be acceptable under lower probability, larger sized attacks.

The level of threat, location of the threat and targeted components, and the importance of the bridge matter when determining the level of analysis used in determining the demands. Approximate methods may be used for low-force threats to low-importance bridges whereas more sophisticated analyses should be used for high-force threats to important bridges.

Type of threat, vulnerability, and method of mitigation vary depending on the type, geometry, location, and importance of the structure. The following are examples for each of the factors:

- Type of threat:
 - VBIED or HEIED;
 - Impact from motor vehicles, intentionally derailed trains, aircraft, or watercraft;
 - Mechanical or exothermic cutting devices;
 - Fire; or
 - Other.

- Potential attack modes against bridge components:
 - Substructure components: The most likely threats to substructure components are vehicle impact and explosives (VBIEDs). For most bridges, explosive charges are most likely to be placed at or near ground level. However, for bridges over waterways, watercraft could deliver charges. For bridges with towers (i.e., cable-stayed and suspension bridges) vehicles on the deck in the vicinity of the towers could deliver explosive charges.
 - Superstructure components: Potential superstructure components attacked vary depending on the structural system. The following examples show potential modes of attack for different types of structural systems:
 - Deck bridges: Damage to main supporting elements because of explosives or fire under or on the bridge.
 - Cast-in-place (CIP) and segmental box concrete girder bridges: Damage from fire, intentional cutting, or explosives to post-tensioning tendons and their anchorages. Damage to the concrete from explosives placed inside or outside the box.
 - Truss bridges: Loss of a member due to removal or severing with either a cutting device or an explosive charge. Loss of stability of compression members when subjected to excessive deformations caused by explosives, collision, or overloading because of redistribution of forces following the failure of other members. Loss of tension members from nonexplosive cutting devices or from precision demolition explosive devices.
 - Cable-stayed bridges: Loss of main girder because of the instability caused by severe local damage from explosive charges on the deck, particularly in regions where compression forces in a main girder are high. Loss of more than one cable stay because of damage to the cables or their anchorages caused by cutting or explosive charges. Damage to one cable stay is not expected to lead to the collapse of a bridge, however, because that scenario is routinely considered in design.
 - Suspension bridges: Loss of a series of suspension cables by cutting devices (nonexplosive or explosive).

- Arch bridges: Likely modes of attack differ based on the type of arch. Potential causes of damage to each component are as follows: (1) explosive charges on spandrel columns in conventional arches, (2) cutting devices or explosive devices deployed against arch ties, and (3) cutting devices or explosive devices deployed against the cable suspenders of tied arches.

Evaluation of force effects in bridges due to natural disasters, such as wind, scour, and seismic, have been codified in the *AASHTO LRFD Bridge Design Specifications* (AASHTO, 2020), hereinafter referred to as LRFD Design, inclusive of vulnerability. However, determining design forces from human-made disasters such as attackers using explosive charges involves significant uncertainty. For example, the size, shape, and location of an explosive charge relative to a structural component determine the magnitude and direction of the load on the component. The following broad guidelines identify factors to consider when evaluating the vulnerability of a structure to different types of threats. In all these cases, discussions with local emergency response officials can help determine bridge vulnerabilities and the response time for an event on the bridge for the best and worst traffic scenarios.

- Vehicle-borne explosives:
 - Size: Maximum size depends on the type of vehicle used in delivering the explosives. Table C1.4-1 shows the effective maximum explosive capacity of different types of vehicles.
 - Location: Below or on the bridge.

Table C1.4-1—Maximum Explosives Capacity of Different Types of Vehicles (U.S. Department of Homeland Security, n.d.)

Vehicle Configuration	Vehicle Description	Maximum Explosives (Capacity, lb)
	Briefcase	50
	Compact Sedan	500
	Full-Size Sedan	1,000
	Passenger or Cargo Van	4,000
	Small Box Van (14-ft box)	10,000
	Semitrailer	60,000

- Rail-borne explosives:
 - Size: May be large because of the high load capacity of rail cars. Achieving full effectiveness of a large quantity of explosives is difficult, however, and using the full capacity of a rail car for estimating explosive threat size is not recommended.
 - Location: May be detonated below or on a bridge.
- Hand-placed explosives:
 - Types: May be contact charges or shaped charges.
 - Size: Will be small to allow a person to handle and place them.
 - Location: May be placed in areas within reach of the persons placing the charges.
- Cutting devices:
 - Components potentially vulnerable to cutting devices: Only those physically within reach of the person placing or operating a cutting device. For example, pure tension members in bridges may be of concern if they are immediately adjacent to the roadway and are relatively small.

- Types of mechanical devices:
 - Explosively actuated device: In this device, the force of an exploding charge drives a cutting wedge through a component to sever it. This type of mechanical device is small, lightweight, and readily lifted and installed by one person.
 - Hydraulic-driven cutting device: An engine or electric motor may be used to drive a hydraulic pump, which then drives a cutting device. These units are heavy and are likely transported by a vehicle. In case of an electrically powered hydraulic pump, a generator is likely needed for the necessary power because the vehicle's electrical system is insufficient to operate the pump.
 - Grinding wheel: To complete the cutting in a short time, handheld grinding wheels may be deployed against the smallest of bridge components. These tools require a relatively low-level power supply, such as a battery.
- Exothermic torches: These devices may be used to cut through a variety of structural materials such as ceramics, concrete, metal, and steel components, including cables. These devices utilize expendable, replaceable rods and a portable oxygen source. One person could carry a portable system with enough resources to cut large structural members quickly.
- Impact vulnerability:
 - Components exposed to impact: Impact threat is most likely to be directed against the substructure. Superstructure components such as towers on cable-stay and suspension bridges and truss members also may be vulnerable to deliberate impact. Low-level movable structures over waterways are potentially vulnerable to impact by watercraft.
 - Delivery method:
 - A motor vehicle: Most likely a truck.
 - Watercraft: Boat or, for navigable waterways, a tugboat and barge tow.
 - Airborne projectiles: Shoulder-fired missiles or grenades.
 - Railroad: A train may be derailed immediately before the rail-line passes under a bridge to hit its substructure.
 - Air: An airplane or unmanned drone could be used to impact a bridge.

- Magnitude of impact force: The impact force is a function of the size and speed of the moving object hitting the bridge. The geometry of the area around, on, and under the bridge and any obstructions in the path of the movable object will have a great effect on its impact speed. The impact force of a vehicle may be computed by using principals of dynamics, which consider the mass, velocity, energy absorption, and the deceleration of the vehicle upon impact. Vessel collision forces may be calculated by using the design procedures for vessel collision as outlined in LRFD Design Article 3.14 with adjustment for velocity, aberrancy, and other factors that will be different in a deliberate attack as opposed to an accidental collision.

The provisions of LRFD Design Article 3.6.5.1 apply to the collision of highway vehicles with bridge substructures. Note that this article no longer contains requirements for train collision loads with bridge elements; the designer should consult the *AREMA Manual for Railway Engineering* (AREMA, 2019) or local railroad company guidelines for guidance on train collisions.

- Fire vulnerability (California State Transportation Agency, 2018) (LaMalva, 2018) (NFPA, 2011) (NTSB, 2018):
 - Type of material: The deterioration in the resistance of a structural component subjected to high temperature is a function of both the material and the temperature. The degree of fire protection afforded by other parts of the cross-section, such as the concrete around steel reinforcement and prestressing strands, should also be considered when determining the vulnerability of a component to fire.
 - Type of structure and accessibility for firefighters: A fire on or under a bridge is generally accessible; therefore, it may be reached by firefighters in relatively short time.
 - Determining fire effects: Given the characteristics of a threat, the effect of a fire on a structure may be determined from analyses or based on empirical data from experiments to determine the temperature and length of time a structural component can resist the applied loads safely. The analyses should include how material properties vary due to changes in temperature and the actual load on the structure.

1.5—MITIGATION MEASURES

Consideration should be given to mitigation measures to reduce identified vulnerabilities. The following four basic strategies may be combined to provide the highest practical and economically feasible degree of protection:

1. Deter
2. Deny
3. Detect
4. Defend

1.5.1—Deter

Consideration should be given to deterrence measures, such as visible closed-circuit television cameras, guard stations, cleared lines of sight to critical components, and visible structural protection measures such as barriers and armored cable protection.

1.5.2—Deny

At a minimum, consideration should be given to the following methods to deny attackers access to their target:

- Fences;
- Guarded or locked gates;
- Locked hatches on cellular equipment, such as inside box girders and bridge towers;
- Barriers, berms, and fenders around substructure units; and
- Barriers to eliminate access from the deck to the superstructure and substructure components located above the deck elevation.

1.5.3—Detect

At a minimum, detection technologies to be considered should include closed circuit television, police patrols, sirens, and alarmed doors and hatches to detect unauthorized entry to restricted spaces.

C1.5

By combining the four strategies, attacking a protected target becomes less attractive to a terrorist or other attacker as action to prevent or minimize the damage increases. This Article provides general guidelines for deploying the four strategies. Their application should be tailored to the specific structure being protected while recognizing that the threat environment may change during the structure's lifetime. As potential threat scenarios change, the protection strategies also should change. For example, a bridge that may have been initially designed on the basis of being under limited threat may require enhanced protection if traffic volume increases or a high-risk structure is built near the bridge.

C1.5.1

Deter: Visible protection measures send a strong message that the owner has taken actions to protect a bridge. The visible protections may make potential attackers realize that their chances of success are reduced and make them look for another target.

C1.5.2

Deny: The most successful method to minimize threats is to keep potential attackers as far from a target as possible. Doing so will achieve two important goals: (1) reduce the probability of occurrence for threats that require physical contact with the target, such as cutting devices and shaped charges, and (2) minimize the effects of larger threats such as car and truck bombs by increasing the standoff distance.

At times of heightened threat levels, when intelligence about a potential threat to a specific bridge is received, owners may want to employ active denial methods. Examples of active denial methods include stationing guards on or near a bridge or using lane closures to increase the standoff distance.

C1.5.3

Detect: An effective quick response to any threat includes detecting the threat before it materializes into an actual attack. Detection measures do not need to be visible to potential attackers. Detection measures are valuable in mitigating threats only if a response is possible and timely.

1.5.4—Defend (Structural Hardening)

The following general list of structural hardening measures should be considered to design or harden bridge structures. Designers should consider the effectiveness and efficiency of the overall bridge design and the lifetime construction and maintenance costs when determining the best overall design strategy for all load cases, to include these recommendations for extreme loads. Section 4 contains bridge- and component-specific measures that should be considered:

- Increase the shear resistance of concrete members most susceptible to shear distress due to extreme loads by adding shear reinforcement. Nonductile shear failure should be avoided to the extent practical.
- Decrease diaphragm spacing in cellular components, including box girders, box-type arch ribs, and box-type support columns and towers. Select diaphragm spacing that produces square or near-square panels of the box walls to produce effective load resistance because such panels tend to resist the load in two-way action. However, when the dominant demand on reinforced concrete members under other loads requires one-way reinforcement, a more economical approach may be to maintain the one-way behavior. This action, while using additional diaphragms to decrease the span without changing the reinforcement, can produce two-way behavior.
- Increase redundancy by providing multiple load paths (e.g., decreasing spacing of longitudinal girders and stringers, decreasing floor beam spacing). This will help ensure stability of the structure if it loses some members.
- Ensure stability of the structure if it loses some members, including designing cable-stayed, suspension, truss, and tied arch bridges for structural stability if one or more cable stays, truss members, or suspension cables are lost.
- Provide extra protection to tie-down piers in the back spans of cable-stayed and truss bridges. These piers can be a critical design feature because they are typically located inland, which makes them easier to reach than the main towers, which are frequently located in water.
- Provide intentionally weak members (i.e., fuses) designed to fail under high loads, thus relieving some of the load that critical structural components must resist. This strategy applies, for example, to areas of the deck that are permitted to fail to vent blast pressure and consequently reduce the demand on the supporting girders. In any case, include redundancy or alternate load paths in the design.

C1.5.4

Defend: There are measures that can improve ductility, robustness, and redundancy of structural components. These measures create desirable characteristics that can improve structural performance under extreme event loadings. However, quantifying the extra protection provided by a given strategy can be difficult. In the 2011 version of the AASHTO *Bridge Security Guidelines*, specific guidance was given only for reinforced concrete bridge columns. Now, specific guidance is available for the protective design of other components, including flexural members, reinforced concrete towers (Chiarito, Minor, et al., 2011), and steel cables (Chiarito, Ray, et al., 2011). Additional information is available in the FHWA *Bridge Security Design Manual* (Davis, Sammarco, and Williamson, 2017) on these components and others such as steel bridge towers. Some of the measures listed may run contrary to current design trends and should only be considered for highly important structures. To effectively utilize available resources, a designer must balance the sometimes-contradictory requirements of security and other extreme events.

SECTION 2 LOADS AND LOAD FACTORS

2.1—LOAD FACTORS AND COMBINATIONS

Engineering judgment should be exercised when applying blast loadings and when combining them with other loads.

2.2—CHANGE IN FOUNDATIONS BECAUSE OF LIMIT STATE FOR SCOUR

The provisions of LRFD Design Article 2.6.4.4 apply. The consequences of changes in foundation conditions resulting from the design flood for scour should be considered at strength and service limit states. The consequences of changes in foundation conditions because of scour that results from the check flood for bridge scour and from hurricanes should be considered at the extreme event limit states.

When investigating the force effects due to blast loading, the structure configuration associated with long-term scour (i.e., stream bed degradation only) should be used.

C2.1

Blast loading is considered an extreme event and corresponds to the Extreme Event II load case in LRFD Design (see Table 3.4.1-1). Because blast loads can be either accidental or stem from human-made events, historical data and typical methods for determining a return period are not suitable. Accordingly, traditional reliability-based approaches for determining load and resistance factors (or factors of safety) do not apply directly to this scenario. A guiding principle for designing bridges for blast loads may be adopted from the approach used when designing buildings subjected to blast and other types of extreme load events (e.g., those associated with disproportionate collapse). For these extreme events, it is customary to characterize the loads expected to be present at the time of an event and assess the probability of load effects occurring simultaneously.

C2.2

Statistical data show that hydraulic effects (e.g., scour, flooding, ice) are the most common reason for the failure of highway bridges in the United States (Choudhury and Hasnat, 2015) (Cook, 2014) (Den, Wang, and Yu, 2016) (Harik et al., 1990) (Lee et al., 2013) (Taricska, 2014) (Wardhana and Hadipriono, 2003) (Wesley and Barr, 2017).

Provisions concerning the effects of scour are provided in LRFD Design Section 2. Scour per se is not a force effect, but by changing the conditions of the substructure, it may significantly alter the consequences of force effects that act on structures.

Accordingly, when considering an example appropriate for the case of a bridge, the probability of blast loading occurring when the scour associated with the design or check floods exists has a low likelihood.

For guidance regarding bridge scour, see LRFD Design Article 2.6.4.4.2; for additional information when combining scour effects with blast loading, see LRFD Design Article C3.4.1.

2.3—VEHICULAR COLLISION: CT

2.3.1—Security Considerations

The owner of the bridge should establish the size and velocity of the vehicle to be used for bridge security analysis.

C2.3.1

Because intentionally ramming a vehicle into a bridge is meant to cause extensive structural damage and potential collapse, the velocity of a vehicle during an intentional collision may be higher than the normal travel speed and therefore may warrant higher velocities than used for accidental impacts. In addition to accounting for the effects of impact, consideration also should be given to the potential for vehicle-delivered explosives and subsequent fire. The maximum obtainable velocity of the vehicle should be used considering the physical limitations of both the vehicle and the approach. For example, barriers may reduce or eliminate the speed which a vehicle could obtain prior to ramming a bridge substructure on an interstate highway.

Research studies conducted by the Texas A&M Transportation Institute (TTI) and FHWA provide additional data and guidance that may be helpful to bridge designers when considering vehicle impact loads (Buth, Brackin, Chatham, et al., 2011) (Buth, Brackin, Williams, and Fry, 2011) (Buth, Brackin, et al., 2010) (Buth, Williams, et al., 2010) (FHWA, 2018b). These studies include crash probabilities based on historical accidents, data from numerical and experimental studies of large truck impacts into bridge columns, calibrations with analytical modeling, and recommended design guidelines. While the intent of the research is accidental collisions, bridge designers can apply the same principles to the case of intentional collisions. Additional information can be found at FHWA's *Primer on Impact Protection for Critical Infrastructure* (FHWA, 2018c).

2.4—VESSEL COLLISION: CV

2.4.1—Security Considerations

The owner of the bridge shall establish the size and velocity of the vessel to be used for bridge security analysis.

The vessel impact force should be determined in accordance with LRFD Design Article 3.14, as applicable.

C2.4.1

Because intentionally ramming a vessel into a bridge is meant to cause extensive structural damage and a potential collapse, the velocity of the vessel at the moment of collision is expected to be higher than the normal travel speed. In addition to accounting for the effects of impact, consideration also should be given to the potential for vessel-delivered explosives and subsequent fire. The physical limitations on the vessel's velocity should be taken into account when determining the design velocity for intentional collision. For example, the velocity of a barge tow is limited by the power of the tugboats and by the geometry of the waterway in the approach to the bridge. Similarly, the factors limiting the size of the vessel should be considered when determining the design vessel.

The probability of bridge collapse caused by the intentional collision with the design vessel at the design speed should be taken equal to PC , which should be determined using the provisions of LRFD Design Article 3.14.5.4. The design vessel and velocity are site-specific variables that the owner should select as part of a security assessment.

In case of accidental collision, determining the annual probability of collapse by using LRFD Design Equation 3.14.5-1 involves the annual number of vessels (N), the probability of vessel aberrancy (PA), and the geometric probability of a collision (PG). In the case of intentional collision, the value of each of these three variables may be taken as 1.0. Therefore, the probability of collapse in case of intentional collision is taken equal to PC .

2.5—BLAST LOADING

2.5.1—Introduction

When it has been determined that a bridge or a bridge component should be designed for intentional or accidental blast force, the following should be considered:

- Size of explosive charge,
- Shape of explosive charge,
- Type of explosive,
- Standoff distance,
- Location of the charge,
- Possible modes of delivery and associated capacities (e.g., maximum charge weight will depend on vehicle type and can include cars, trucks, and ships), and
- Fragmentation associated with vehicle-delivered explosives.

C2.5.1

The size, shape, location, and type of an explosive charge determine the intensity of the blast force produced by an explosion. For comparison purposes, all explosive charges are typically converted to their equivalent TNT charge weights.

Standoff refers to the distance between the center of an explosive charge and a target. Because of the dispersion of blast waves in the atmosphere, increasing standoff causes the peak pressure on a target to drop as a cubic function of the distance (i.e., for a given quantity of explosives, doubling the standoff distance causes the peak pressure to drop by a factor of eight). The location of the charge determines the amplifying effects of the blast wave reflecting from the ground surface or from the surfaces of surrounding structural elements. The location of the charge also determines the severity of damage to other structural components potentially impacted by fragments resulting from the spall or breach of structural components closest to the blast.

Information on the analysis of blast loads and their effects on structures can be found in *Explosion Hazards and Evaluation* (Baker et al., 1983); *Explosive Loading on Engineering Structures* (Bulson, 1997); *Introduction to Structural Dynamics* (Biggs, 1964); *NCHRP Report 645: Blast-Resistant Highway Bridges: Design and Detailing Guidelines* (Williamson et al., 2010); two U.S. Department of Defense documents, *Design and Analysis of Hardened Structures to Conventional Weapons Effects* (U.S. Department of Defense, 2002) and *Structures to Resist the Effects of Accidental Explosions* (U.S. Department of Defense, 2014); and the *FHWA Bridge Security Design Manual* (Davis, Sammarco, and Williamson, 2017).

2.5.2—Blast Load Modeling Software

The bridge owner should establish the level of analysis to be conducted based on the importance of the bridge.

C2.5.2

Several computer programs have been developed to determine blast loading and blast effects on structural components. These programs vary in complexity based on their intended use. Because of security concerns, some of these programs are not readily available for use by the design community. The bridge owner should make sure that the designer or consultant has access to and experience with these analysis tools.

Computational tools for blast analysis must consider the time-varying pressures associated with blast loadings. Equivalent static loadings are not applicable. Three levels of analysis may be used depending on the complexity and importance of the structure. The analysis levels differ in their consideration of wave propagation and the effect of surrounding surfaces that may reflect the blast wave. The inappropriate use of a method to determine blast loads may result in erroneous and unconservative results, and therefore bridge owners are strongly advised to seek guidance from qualified engineers with extensive experience and knowledge in the analysis and design for blast loads.

The first level contains methods that utilize blast phenomenology from basic equations and curves developed empirically from “ideal explosions” in free air. These ideal explosions include bare spherical charges in the air or bare hemispherical charges on the ground. Curve fits exist to allow engineers to quickly determine basic blast load parameters, such as peak overpressure, peak reflected pressure, positive phase duration, negative phase duration, time of arrival, and impulse. This type of load calculation is acceptable for simple structural configurations when the engineer expects the influence of shock reflections to be negligible because there is a direct line of sight from the charge to the target. It is also applicable for relatively large standoff calculations, but it is not acceptable for close-in detonations. Given the available curves and data are based on TNT, this type of calculation must be used with TNT equivalency values to adjust the calculations for the expected output of other explosive materials. Examples of tools in this level include the charts of shock wave parameters available in UFC 3-340-02 (U.S. Department of Defense, 2014) and several simplified computer programs, including ConWep (U.S. Army Corps of Engineers, 2001).

The second level includes those methods that consider multiple reflections and pressure magnification, often using ray-tracing methods, while not strictly employing computational fluid dynamics principles. The techniques in this group track pressure values through basic first-order principles of wave reflections as they radiate from a detonation and as they reflect off surfaces. As a result, they provide higher accuracy than the first group of load determination methods that do not consider reflections. Examples include BlastX (U.S. Army Corps of Engineers, 2013) and ATP-Bridge (Sammarco, 2014). Limitations of these methods include difficulty accurately representing loads on curved geometries, members with inclined surfaces, very complex geometries with numerous reflections from multiple surfaces, and enclosed environments that may experience quasi-static loading due to the stagnation of overpressure for extended durations. The second level of load calculation methods should not be used for scenarios with these characteristics.

The third and most sophisticated level of load determination methods are numerical codes that employ first-principle, finite element, fluid mechanics computations. These load determination methods are “high resolution” numerical codes that use the mechanics of fluids (i.e., air in the case of blast) to calculate variations in pressure, density, and velocity as a function of time and position using a custom-built, finite-element environment. As a result, this level of analysis can consider complex geometries, such as curved members, inclined members, multiple reflecting surfaces, pressure magnification, confinement, and quasi-static loading in enclosed environments. Additionally, in some cases these codes can consider venting due to structural failure and close-in detonations in simulations by coupling the fluid dynamics shock propagation code with a structural response code.

The use of the numerical codes in the third level of load determination is very complex, and the results are often code- and analyst-dependent. Furthermore, many of these codes are commercially proprietary or government restricted. Given the complexity, the accuracy provided by this level of load determination is not necessary for most design cases because the specifics of future attack scenarios are not typically known. The decision to use this level must be on a cost-benefit analysis, and it may be warranted for complex scenarios or on a large project in which the removal of even a small degree of conservatism may save large amounts of money. Therefore, bridge owners are strongly advised to seek guidance from qualified blast analysts and engineers before specifying the use of this level of load determination.