Continuing Education For Limited License Electricians

CONNECTICUT ELECTRICAL Training Center, LLC

2024 Edition

EVALUATION FORMS:

The procedure for submitting the evaluation form for electrical continuing education courses has been moved to an online format. Please access the following link to complete and submit the form:

https://portal.ct.gov/ELCeval

2024 Continuing Education for Electricians

(For All Electrical License Holders)

Part 1 - Connecticut General Statutes

Sec. 20-340. Exemptions from licensing requirements

The provisions of this chapter shall not apply to: (1) Persons employed by any federal, state or municipal agency; (2) employees of any public service company regulated by the Public Utilities Regulatory Authority or of any corporate affiliate of any such company when the work performed by such affiliate is on behalf of a public service company, but in either case only if the work performed is in connection with the rendition of public utility service, including the installation or maintenance of wire for community antenna television service, or is in connection with the installation or maintenance of wire or telephone sets for single-line telephone service located inside the premises of a consumer; (3) employees of any municipal corporation specially chartered by this state; (4) employees of any contractor while such contractor is performing electrical-line or emergency work for any public service company; (5) persons engaged in the installation, maintenance, repair and service of electrical or other appliances of a size customarily used for domestic use where such installation commences at an outlet receptacle or connection previously installed by persons licensed to do the same and maintenance, repair and service is confined to the appliance itself and its internal operation; (6) employees of industrial firms whose main duties concern the maintenance of the electrical work, plumbing and piping work, solar thermal work, heating, piping, cooling work, sheet metal work, elevator installation, repair and maintenance work, automotive glass work or flat glass work of such firm on its own premises or on premises leased by it for its own use; (7) employees of industrial firms when such employees' main duties concern the fabrication of glass products or electrical, plumbing and piping, fire protection sprinkler systems, solar, heating, piping, cooling, chemical piping, sheet metal or elevator installation, repair and maintenance equipment used in the production of goods sold by industrial firms, except for products, electrical, plumbing and piping systems and repair and maintenance equipment used directly in the production of a product for human consumption; (8) persons performing work necessary to the manufacture or repair of any apparatus, appliances, fixtures, equipment or devices produced by it for sale or lease; (9) employees of stage and theatrical companies performing the operation, installation and maintenance of electrical equipment if such installation commences at an outlet receptacle or connection previously installed by persons licensed to make such installation; (10) employees of carnivals, circuses or similar transient amusement shows who install electrical work, provided such installation shall be subject to the approval of the State Fire Marshal prior to use as otherwise provided by law and shall comply with applicable municipal ordinances and regulations; (11) persons engaged in the installation, maintenance, repair and service of glass or electrical, plumbing, fire protection sprinkler systems, solar, heating, piping, cooling and sheet metal equipment in and about single-family residences owned and occupied or to be occupied by such persons; provided any such installation, maintenance and repair shall be subject to inspection and approval by the building official of the municipality in which such residence is located and shall conform to the requirements of the State Building Code; (12) persons who install, maintain or repair glass in a motor vehicle owned or leased by such persons; (13) persons or entities holding themselves out to be retail sellers of glass products, but not such persons or entities that also engage in automotive glass work or flat glass work; (14) persons who install preglazed or preassembled windows or doors in residential or commercial buildings; (15) persons registered under chapter 400 who install safety-backed mirror products or repair or replace flat glass in sizes not greater than thirty square feet in residential buildings; (16) sheet metal work performed in residential

buildings consisting of six units or less by new home construction contractors registered pursuant to chapter 399a, by home improvement contractors registered pursuant to chapter 400 or by persons licensed pursuant to this chapter, when such work is limited to exhaust systems installed for hoods and fans in kitchens and baths, clothes dryer exhaust systems, radon vent systems, fireplaces, fireplace flues, masonry chimneys or prefabricated metal chimneys rated by Underwriters Laboratories or installation of stand-alone appliances including wood, pellet or other stand-alone stoves that are installed in residential buildings by such contractors or persons; (17) employees of or any contractor employed by and under the direction of a properly licensed solar contractor, performing work limited to the hoisting, placement and anchoring of solar collectors, photovoltaic panels, towers or turbines; (18) persons performing swimming pool maintenance and repair work authorized pursuant to section 20-417aa; and (19) any employee of the Connecticut Airport Authority covered by a state collective bargaining agreement.

Sec. 20-332-15a. Employment of apprentices

(a) Nothing in Chapter 393 of the General Statutes shall be construed to prohibit the employment of apprentices.
(b) An apprentice may perform the work for which he is being trained only in the presence and under the direct supervision of a licensed contractor or journeyman in his trade, and shall comply with all the regulations pertaining thereto.
(c) No apprentice shall at any time engage in any of the work for which a license is required without direct supervision. Direct supervision shall mean under the guidance of a licensed contractor or journeyman and within the sight and/or hearing of said licensed person.
(d) Any person who encourages or permits an apprentice or helper to so engage in the work or occupation for which a license is required without direct supervision shall also be subject to appropriate disciplinary action. The contractor who obtains the permit for the work for which a license is required shall be deemed to have encouraged or permitted the apprentice or helper to work without direct supervision for the purpose of disciplinary action by the appropriate board.

(f) How to register as an apprentice.

(1) No apprentice shall perform the work of any occupation covered by Chapter 393 of the General Statutes unless he has first obtained a card of registration from the Connecticut Department of Labor.
(2) Prior to employing an apprentice, the contractor shall communicate immediately with the Connecticut Department of Labor to request registration of said apprentice.
(3) When registration is requested for an area of the trade which is not available through the Connecticut Department of Labor, said contractor shall make his request to the appropriate board prior to the employment of the apprentice.

Sec. 20-332-16. Prohibited acts. Records. Lettering on commercial vehicles

(a) Any licensee who installs, performs or directs the performance of work in violation of any applicable state statute, state code, or state regulation, any municipal code or ordinance, any of these regulations, or who violates generally accepted basic trade practices shall be subject to disciplinary action by the appropriate board.
(b) Licensed contractors alone shall be permitted to acquire building permits to perform work covered by chapter 393 of the General Statutes and the regulations promulgated thereunder. In order to apply for a building permit to perform work covered by chapter 393 of the General Statutes and the regulations adopted thereunder a contractor shall be directly employed by the business on a regular and full time basis. In applying for the building permit to perform work covered by chapter 393 of the General Statutes and the regulations promulgated thereunder the contractor is attesting to the fact that he is responsible for and will directly supervise the work being performed under said permit. Except as provided for in Section 20-338b of the General Statutes, the licensed contractor must sign each building permit application personally and may not delegate the signing of the permit to any employee, subcontractor or other agent. Any licensed contractor who violates these regulations shall be subject to disciplinary action by the appropriate board.
(c) No licensee shall engage in or offer to engage in business under any name other than that stated on his application for a license unless he has notified the board ten days prior to using the new name.
(d) Any holder of a journeyman's license who performs work without being in the direct and regular employ of a properly licensed contractor shall be subject to disciplinary action by the appropriate board.
(e) All licensed contractors shall keep a record of all employees they employ and exhibit such records to the Commissioner or her agents upon request.
(f) No one shall perform any work beyond the limitations stated on his license regardless of the type of license his employer holds. Further, no one holding a limited

or unlimited journeyman's license can perform any work beyond the limitations of the license held by the contractor for whom he is employed.
(g) The lettering of the state license numbers required to be displayed on all commercial vehicles used in the contractor's business shall be at least one inch high and legible.
(h) Any holder of a contractor's license who installs, performs or directs the performance of work for which a building permit is required shall cause said performance of work to be performed by a person licensed or registered under the provisions of Section 20-334 of the General Statutes. The contractor who obtains the building permit shall be deemed to have caused or directed the performance of all work performed under the building permit.
(i) No person shall use solder containing mre than 0.2 per cent lead in making joints and fitting in any public or private plumbing, heating or cooling system, or fire protection system as defined in Sections 20-330 (3), 20-330- (5) and 20-330 (9) of the general statutes.

Sec. 20-332b. Hiring ratios re apprentices, journeymen and contractors. Electrical, plumbing, heating, piping and cooling, sprinkler fitter and sheet metal work. Regulations. The Commissioner of Consumer Protection shall amend existing regulations of Connecticut state agencies adopted pursuant to section 20-332 to specify the following allowable hiring ratios regarding apprentices, journeymen and contractors for the following trades:

TRADE

Electrical, Plumbing, Heating, Piping and Cooling, Sprinkler Fitter and Sheet Metal Work

Apprentices	Licensees (Journeymen or Contractors)
1	1
2	2
3	3
4	6
5	9
6	12
7	15
8	18
9	21
10	24

Ratio continues at 3 Journeypersons To 1 Apprentice

Sec. 20-332c. Apprentice, journeymen and contractor working group established. Membership. Report. (a) There is established a working group to discuss hiring ratios for apprentices, journeymen and contractors and study the hiring ratio relief process. The working group shall meet at least three times annually and shall study and make recommendations related to apprentices, journeymen and contractors.

(b) The working group shall consist of ten members, and shall be evenly divided between members of the following union and nonunion industry trade groups: The International Brotherhood of Electrical Workers, the Independent Electrical Contractors of New England, the Associated Builders and Contractors of Connecticut, Sheet Metal Local 40, Sprinkler Fitters Local 669, the Connecticut Chapter of American Fire Sprinkler Association, the United Association of Plumbers and Pipefitters Local 777, the Plumbing Heating and Cooling Contractors of Connecticut, the Connecticut Heating and Cooling Contractors and the Connecticut State Building and Construction Trades Council. Each union industry trade group member shall be either the business manager of such group or such business manager's designee

from such group. Each nonunion industry trade group member shall be either the president of such group or such president's designee from such group.

(c) Such members shall be selected as follows:
(1) Two union members appointed by the speaker of the House of Representatives;
(2) Two union members appointed by the president pro tempore of the Senate;
(3) One nonunion member appointed by the majority leader of the House of Representatives;
(4) One union member appointed by the majority leader of the Senate;
(5) Two nonunion members appointed by the minority leader of the House of Representatives; and
(6) Two nonunion members appointed by the minority leader of the Senate.
(d) All appointing authorities shall consult with the chairpersons and ranking members of the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection prior to making any appointments pursuant to this section.
(e) All appointments to the working group shall be made not later than thirty days after the effective date of this section. Any vacancy shall be filled by the appointing authority.
(f) The members of the working group shall select the chairpersons of the working group from among the members of the group. One chairperson shall be a union member and one chairperson shall be a nonunion member. Such chairpersons shall schedule the first meeting of the working group.

(g) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection shall serve as administrative staff of the working group.
(h) Not later than December 1, 2017, and annually thereafter, the working group shall submit a report on its recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection, in accordance with the provisions of section 11-4a.

Sec. 20-335. License fee. Continuing professional education requirements. Expiration and renewal. Any person who has successfully completed an examination for such person's initial license under this chapter shall pay to the Department of Consumer Protection a fee of one hundred fifty dollars for a contractor's license or a fee of one hundred twenty dollars for any other such license. All such licenses shall expire annually. No person shall carry on or engage in the work or occupations subject to this chapter after the expiration of such person's license until such person has filed an application bearing the date of such person's registration card with the appropriate board. Such application shall be in writing, addressed to the secretary of the board from which such renewal is sought and signed by the person applying for such renewal. A licensee applying for renewal shall, at such times as the commissioner shall by regulation prescribe, furnish evidence satisfactory to the board that the licensee has completed any continuing professional education required under sections 20-330 to 20-341, inclusive, or any regulations adopted thereunder. The board may renew such license if the application for such renewal is received by the board no later than one month after the date of expiration of such license, upon payment to the department of a renewal fee of one hundred fifty dollars in the case

of a contractor and of one hundred twenty dollars for any other such license. For any completed renewal application submitted pursuant to this section that requires a hearing or other action by the applicable examining board, such hearing or other action by the applicable examining board shall occur not later than thirty days after the date of submission for such completed renewal application. The department shall issue a receipt stating the fact of such payment, which receipt shall be a license to engage in such work or occupation. A licensee who has failed to renew such licensee's license for a period of over one year from the date of expiration of such license shall have it reinstated only upon complying with the requirements of section 20-333. All license fees and renewal fees paid to the department pursuant to this section shall be deposited in the General Fund.

Sec. 20-338. License as contractor and journeyman. Valid throughout state. The Department of Consumer Protection shall issue a separate license to persons qualified to engage in work as contractors and as journeymen. Any person licensed under this chapter shall be permitted to perform the work or occupation covered by such license in any town or municipality of this state without further examination or licensing by any town or municipality.

Sec. 20-338a. Work required to be performed by licensed persons. Any contractor who applies for a building permit from a local building official for any work required to be performed by a person licensed under the provisions of this chapter, shall cause such work to be performed by a person licensed under the provisions of this chapter.

Sec. 20-338b. Building permit applications. Who may sign. Any licensed contractor who seeks to obtain a permit from a building official may sign the building permit application personally or delegate the signing of the building permit application to an employee, subcontractor or other agent of the licensed contractor, provided, the licensed contractor's employee, subcontractor or other agent submits to the building official a dated letter on the licensed contractor's letterhead, signed by the licensed contractor, stating that the bearer of the letter is authorized to sign the building permit application as the agent of the licensed contractor. The letter shall not be a copy or a facsimile, but shall be an original letter bearing the original signature of the licensed contractor. The letter shall also include: (1) The name of the municipality where the work is to be performed; (2) the job name or a description of the job; (3) the starting date of the job; (4) the name of the licensed contractor; (5) the name of the licensed contractor's agent; and (6) the license numbers of all contractors to be involved in the work.

Sec. 20-338c. Work not to commence until permit obtained. No person licensed pursuant to sections 20-330 to 20-341, inclusive, shall commence work within the scope of sections 20-330 to 20-341, inclusive, unless each applicable permit with respect to the specific work being performed by such licensee has been obtained as required pursuant to local ordinances and the general statutes.

Sec. 20-340. Exemptions from licensing requirements. The provisions of this chapter shall not apply to: (1) Persons employed by any federal, state or municipal agency; (2) employees of any public service company regulated by the Public Utilities Regulatory Authority or of any corporate affiliate of any such company when the work performed by such affiliate is on behalf

of a public service company, but in either case only if the work performed is in connection with the rendition of public utility service, including the installation or maintenance of wire for community antenna television service, or is in connection with the installation or maintenance of wire or telephone sets for single-line telephone service located inside the premises of a consumer; (3) employees of any municipal corporation specially chartered by this state; (4) employees of any contractor while such contractor is performing electrical-line or emergency work for any public service company; (5) persons engaged in the installation, maintenance, repair and service of electrical or other appliances of a size customarily used for domestic use where such installation commences at an outlet receptacle or connection previously installed by persons licensed to do the same and maintenance, repair and service is confined to the appliance itself and its internal operation; (6) employees of industrial firms whose main duties concern the maintenance of the electrical work, plumbing and piping work, solar thermal work, heating, piping, cooling work, sheet metal work, elevator installation, repair and maintenance work, automotive glass work or flat glass work of such firm on its own premises or on premises leased by it for its own use; (7) employees of industrial firms when such employees' main duties concern the fabrication of glass products or electrical, plumbing and piping, fire protection sprinkler systems, solar, heating, piping, cooling, chemical piping, sheet metal or elevator installation, repair and maintenance equipment used in the production of goods sold by industrial firms, except for products, electrical, plumbing and piping systems and repair and maintenance equipment used directly in the production of a product for human consumption; (8) persons performing work necessary to the manufacture or repair of any apparatus, appliances, fixtures, equipment or devices produced by it for sale or lease; (9) employees of stage and theatrical companies performing the operation, installation and maintenance of electrical equipment if such installation commences at an outlet receptacle or connection previously installed by persons licensed to make such installation; (10) employees of carnivals, circuses or similar transient amusement shows who install electrical work, provided such installation shall be subject to the approval of the State Fire Marshal prior to use as otherwise provided by law and shall comply with applicable municipal ordinances and regulations; (11) persons engaged in the installation, maintenance, repair and service of glass or electrical, plumbing, fire protection sprinkler systems, solar, heating, piping, cooling and sheet metal equipment in and about single-family residences owned and occupied or to be occupied by such persons; provided any such installation, maintenance and repair shall be subject to inspection and approval by the building official of the municipality in which such residence is located and shall conform to the requirements of the State Building Code; (12) persons who install, maintain or repair glass in a motor vehicle owned or leased by such persons; (13) persons or entities holding themselves out to be retail sellers of glass products, but not such persons or entities that also engage in automotive glass work or flat glass work; (14) persons who install preglazed or preassembled windows or doors in residential or commercial buildings; (15) persons registered under chapter 400 who install safety-backed mirror products or repair or replace flat glass in sizes not greater than thirty square feet in residential buildings; (16) sheet metal work performed in residential buildings consisting of six

units or less by new home construction contractors registered pursuant to chapter 399a, by home improvement contractors registered pursuant to chapter 400 or by persons licensed pursuant to this chapter, when such work is limited to exhaust systems installed for hoods and fans in kitchens and baths, clothes dryer exhaust systems, radon vent systems, fireplaces, fireplace flues, masonry chimneys or prefabricated metal chimneys rated by Underwriters Laboratories or installation of stand-alone appliances including wood, pellet or other stand-alone stoves that are installed in residential buildings by such contractors or persons; (17) employees of or any contractor employed by and under the direction of a properly licensed solar contractor, performing work limited to the hoisting, placement and anchoring of solar collectors, photovoltaic panels, towers or turbines; and (18) persons performing swimming pool maintenance and repair work authorized pursuant to section 20-417aa.

Sec. 20-341. Penalties for violations. (a) Any person who wilfully engages in or practices the work or occupation for which a license is required by this chapter or chapter 399b without having first obtained an apprentice permit or a certificate and license for such work, as applicable, or who wilfully employs or supplies for employment a person who does not have a certificate and license for such work, or who wilfully and falsely pretends to qualify to engage in or practice such work or occupation, including, but not limited to, offering to perform such work in any print, electronic, television or radio advertising or listing when such person does not hold a license for such work as required by this chapter, or who wilfully engages in or practices any of the work or occupations for which a license is required by this chapter after the expiration of such person's license, shall be guilty of a class B misdemeanor, provided no criminal charges shall be instituted against such person pursuant to this subsection unless the work activity in question is reviewed by the Commissioner of Consumer Protection, or the commissioner's authorized agent, and the commissioner or such agent specifically determines, in writing, that such work activity requires a license and is not the subject of a bona fide dispute between persons engaged in any trade or craft, whether licensed or unlicensed. Notwithstanding the provisions of subsection (d) or (e) of section 53a-29 and subsection (d) of section 54-56e, if the court determines that such person cannot fully repay any victims of such person within the period of probation established in subsection (d) or (e) of section 53a-29 or subsection (d) of section 54-56e, the court may impose probation for a period of not more than five years. The penalty provided in this subsection shall be in addition to any other penalties and remedies available under this chapter or chapter 416.

(b) The appropriate examining board or the Commissioner of Consumer Protection may, after notice and hearing, impose a civil penalty on any person who engages in or practices the work or occupation for which a license or apprentice registration certificate is required by this chapter, chapter 394, chapter 399b or chapter 482 without having first obtained such a license or certificate, or who wilfully employs or supplies for employment a person who does not have such a license or certificate or who wilfully and falsely pretends to qualify to engage in or practice such work or occupation, or who engages in or practices any of the work or occupations for which a license or certificate is required by this chapter, chapter 394, chapter 399b or chapter 482 after the expiration of the license or certificate or who violates any of the provisions of this chapter, chapter 394, chapter 399b or chapter 482 or the regulations adopted pursuant thereto. Such penalty shall be in an amount not more than one thousand dollars for a first violation of this

subsection, not more than one thousand five hundred dollars for a second violation of this subsection and not more than three thousand dollars for each violation of this subsection occurring less than three years after a second or subsequent violation of this subsection, except that any individual employed as an apprentice but improperly registered shall not be penalized for a first offense.

(c) If an examining board or the Commissioner of Consumer Protection imposes a civil penalty under the provisions of subsection (b) of this section as a result of a violation initially reported by a municipal building official in accordance with subsection (c) of section 29-261, the commissioner shall, not less than sixty days after collecting such civil penalty, remit one-half of the amount collected to such municipality.

(d) A violation of any of the provisions of this chapter shall be deemed an unfair or deceptive trade practice under subsection (a) of section 42-110b.

(e) This section shall not apply to any person who (1) holds a license issued under this chapter, chapter 394, chapter 399b or chapter 482 and performs work that is incidentally, directly and immediately appropriate to the performance of such person’s trade where such work commences at an outlet, receptacle or connection previously installed by a person holding the proper license, or (2) engages in work that does not require a license under this chapter, chapter 394, chapter 399b or chapter 482.

The following is a link to Public Act 22-104

https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00104-R00HB-05330-PA.PDF

Sec. 37. (NEW) (Effective July 1, 2022) Any contractor who is licensed under chapter 393 of the general statutes and engaged to perform work on a private residence, and any person who owns or controls a business that is engaged to perform work on, or render services concerning, a private residence through persons licensed under chapter 393 of the general statutes to perform such work or render such services, shall include in the invoice or work order for such work or services, provided such invoice or work order is not signed by the consumer and therefore may constitute a contract, when complete: (1) The full legal name and license number of such licensed contractor or the licensed contractor of record for such business for such work or services, which licensed contractor or licensed contractor of record is liable for the work of any individual who performs work on such contractor's behalf related to the invoiced work or services; (2) such licensed contractor's address or, in the case of a business, the business's address and phone number; (3) a description of such work or services; (4) the labor and material costs of such work or services; (5) the date or dates on which such work was performed or services were rendered; and (6) the complete name of each licensee who performed such work or rendered such services. For the purposes of this section, "private residence" has the same meaning as provided in section 20-419 of the general statutes.

Sec. 42. Section 20-334d of the general statutes is repealed and the following is substituted in lieu thereof (Effective from passage):

(a) As used in this section:

(1) "Accredited continuing professional education" means any education of an electrician or plumber that is (A) designed to maintain professional competence in the [pursuit,] practice, pursuit and standards of electrical work or plumbing and piping work, [and that is] (B) approved by the commissioner, and [is] (C) provided (i) by an agency, institution or organization [, institution or agency that is] that has been approved by the commissioner, and (ii) in-person or through an online technology platform that includes real-time video with audio, requires participants to periodically confirm their active engagement during the educational training session and enables participants to interact with instructors in real time during the entire educational training session;

(2) "Certificate of continuing education" means a document [issued to an electrician or plumber by an organization, institution or agency] that (A) an agency, institution or organization that has been approved by the commissioner [that] and offers accredited continuing professional education [, which (A)] issues to an electrician or plumber, (B) certifies that an electrician or plumber has satisfactorily completed a specified number of continuing education hours, and [(B)] (C) bears the (i) name of such agency, institution or organization, [institution or agency, the] (ii) title of the program, [the] (iii) dates during which the program was

conducted, [the] (iv) number of continuing education hours

satisfactorily completed, and [the] (v) signature of the director of such

[organization, institution or agency or the signature of the] agency,

institution or organization or of such director's authorized agent; and (3) "Commissioner" means the Commissioner of Consumer Protection. (b) The commissioner, with the advice and assistance of the Electrical Work Board established pursuant to subsection (b) of section 20-331, shall adopt regulations, in accordance with chapter 54, to: (1) [establish] Establish additional requirements for accredited continuing professional education for electricians licensed pursuant to sections 20- 330 to 20-341, inclusive; (2) establish qualifying criteria for accredited continuing professional education programs and establish qualifying criteria for acceptable certificates of continuing education; and (3) provide for the waiver of required accredited continuing professional education for electricians for good cause. Such regulations shall require not less than four hours per year of accredited continuing professional education for such electricians, except upon request of the Electrical Work Board, the commissioner may increase such hours to a maximum of seven hours. (c) The commissioner, with the advice and assistance of the Plumbing and Piping Work Board established pursuant to subsection (d) of section 20-331, shall adopt regulations, in accordance with chapter 54, to: (1) [establish] Establish additional requirements for accredited continuing professional education for plumbers licensed pursuant to sections 20-330 to 20-341, inclusive, which regulations shall require not more than a total of seven hours of accredited continuing professional education every two years, except in the event of significant changes to the building code, as approved by the International Code Council, that relate to plumbing, the commissioner, at such commissioner's discretion, may require more than a total of seven hours of accredited continuing professional education every two years; (2) establish qualifying criteria for accredited continuing professional education programs and establish qualifying criteria for acceptable certificates of continuing education; and (3) provide for the waiver of required accredited continuing professional education for plumbers for good cause. (d) Notwithstanding the provisions of subsection (c) of this section, any person who has been issued a P-6, P-7, W-8 or W-9 license pursuant to section 20-334a and the regulations of Connecticut state

agencies shall not be required to meet the continuing education requirements established pursuant to subsection (c) of this section. (e) Notwithstanding the provisions of subsections (a) to (d), inclusive, of this section, all accredited continuing professional education offered under the provisions of this section shall: (1) Limit class size to (A) fifty attendees if such accredited continuing professional education is offered in-person, or (B) twenty-five attendees if such accredited continuing professional education is offered through an online technology platform; (2) not be offered or held at the place of business of a licensed plumbing contractor if such accredited continuing professional education is for plumbers and offered in-person; and (3) not be offered or held at the place of business of a licensed electrical contractor if such accredited continuing professional education is for electricians and offered in-person. A provider of an accredited continuing professional education course shall retain an audio-visual recording of such course for a period of not less than thirty days after completion of such course. Recordings shall be made available to the department upon the department's request for such recordings.

Sec. 20-332b. Hiring ratios re apprentices, journeymen and contractors. Electrical, plumbing, heating, piping and cooling, sprinkler fitter and sheet metal work. Regulations. The Commissioner of Consumer Protection shall amend existing regulations of Connecticut state agencies adopted pursuant to section 20-332 to specify the following allowable hiring ratios regarding apprentices, journeymen and contractors for the following trades:

TRADE

Electrical, Plumbing, Heating, Piping and Cooling, Sprinkler Fitter and Sheet Metal Work

Apprentices	Licensees (Journeymen or Contractors)
1	1
2	2
3	3
4	6
5	9
6	12
7	15
8	18
9	21
10	24

Ratio continues at 3 Journeypersons To 1 Apprentice

Sec. 20-332c. Apprentice, journeymen and contractor working group established. Membership. Report. (a) There is established a working group to discuss hiring ratios for apprentices, journeymen and contractors and study the hiring ratio relief process. The working group shall meet at least three times annually and shall study and make recommendations related to apprentices, journeymen and contractors.

(b) The working group shall consist of ten members, and shall be evenly divided between members of the following union and nonunion industry trade groups: The International Brotherhood of Electrical Workers, the Independent Electrical Contractors of New England, the Associated Builders and Contractors of Connecticut, Sheet Metal Local 40, Sprinkler Fitters Local 669, the Connecticut Chapter of American Fire Sprinkler Association, the United Association of Plumbers and Pipefitters Local 777, the Plumbing Heating and Cooling Contractors of Connecticut, the Connecticut Heating and Cooling Contractors and the Connecticut State Building and Construction Trades Council. Each union industry trade group member shall be either the business manager of such group or such business manager's designee from such group. Each nonunion

industry trade group member shall be either the president of such group or such president's designee from such group.

(c) Such members shall be selected as follows:
(1) Two union members appointed by the speaker of the House of Representatives;
(2) Two union members appointed by the president pro tempore of the Senate;
(3) One nonunion member appointed by the majority leader of the House of Representatives;
(4) One union member appointed by the majority leader of the Senate;
(5) Two nonunion members appointed by the minority leader of the House of Representatives;
and
(6) Two nonunion members appointed by the minority leader of the Senate.
(d) All appointing authorities shall consult with the chairpersons and ranking members of the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection prior to making any appointments pursuant to this section.
(e) All appointments to the working group shall be made not later than thirty days after the effective date of this section. Any vacancy shall be filled by the appointing authority.
(f) The members of the working group shall select the chairpersons of the working group from among the members of the group. One chairperson shall be a union member and one chairperson shall be a nonunion member. Such chairpersons shall schedule the first meeting of the working group.

(g) The administrative staff of the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection shall serve as administrative staff of the working group.
(h) Not later than December 1, 2017, and annually thereafter, the working group shall submit a report on its recommendations to the joint standing committee of the General Assembly having cognizance of matters relating to the Department of Consumer Protection, in accordance with the provisions of section 11-4a.

2022 Connecticut State Building Code: (Include in all course handouts to attendees for their future use and review with class.)

Building and Fire Code Adoption Process

State Building, Fire Safety and Fire Prevention Codes Update

The Department of Administrative Services, Office of the State Building Inspector and Office

of the State Fire Marshal, in conjunction with the Codes & Standards Committee and the Fire

Prevention Code Advisory Committee, intend to adopt the following new codes, effective

October 1, 2022:

- 2022 Connecticut State Building Code (CSBC)
- 2022 Connecticut State Fire Safety Code (CSFSC)
- 2022 Connecticut State Fire Prevention Code (CSFPC)

In accordance with the requirements of sections 29-252b, 29-292a and 29-291e of the

Connecticut General Statues, the agency accepted comments from the public for a period of

forty-five (45) days, beginning January 31, 2022 through the close of business March 17, 2022.

The comments received are now being considered for incorporation into the draft codes ahead

of their submission of legislative review.

Draft 2022 State Codes

• The public comment drafts of the three proposed codes are available under Documents/Forms

• The legislative approval drafts of the three proposed codes are being prepared.

Proposed Model Codes:

The following codes are proposed to be adopted into the next state codes:

• 2021 International Building Code (IBC) by the ICC

• 2021 International Existing Building Code (IEBC) by the ICC

• 2021 International Energy Conservation Code (IECC) by the ICC

• 2021 International Mechanical Code (IMC) by the ICC

• 2021 International Plumbing Code (IPC) by the ICC

• 2021 International Residential Code (IRC) by the ICC

• 2021 International Swimming Pool & Spa Code (ISPSC) by the ICC

• 2020 NFPA 70 National Electrical Code (NEC) by NFPA

• 2017 ICC A117.1 Accessible and Usable Buildings and Facilities by the ICC

• 2021 International Fire Code (IFC) by the ICC

• 2021 NFPA 101 - Life Safety Code by the NFPA

• 2021 NFPA 1 - Fire Code by the NFPA

The model codes are viewable on their publisher's web sites:

- International Code Council (ICC) Codes
- National Fire Protection Association (NFPA) Codes

https://portal.ct.gov/DAS/Office-of-State-Building-Inspector/Building-and-Fire-Code-Adoption-Process/Documents

NOTE: Always refer to the State Building Officials website indicated above for all the most currently adopted codes and "AMENDMENTS" to the codes.

2024 Continuing Education for Electricians

(For All Electrical License Holders)

Part 2 - Safety

PART II – Safety

(1/2 Hour To Review With Class And Inform Attendees Material in Handout)

(Please review with the class the top 10 OSHA Violations for 2022)

The chart below gives OSHA's preliminary data alongside the final data from FY 2021.

See recent results here: 2020 | 2019 | 2018

OSHA Standard	FY 2022 Preliminary Data	Previous Year's Data
1. Fall Protection – General Requirements (1926.501) OSHA Fall Protection Defense Guide Construction Fall Protection Standards	5,260 Violations	5,271 Violations
2. Hazard Communication (1910.1200) OSHA's Revised Hazard Communication Standard	2,424 Violations	1,939 Violations
3. Respiratory Protection (1910.134) Selecting and Using Particulate Respirators Starting a Respiratory Protection Program	2,185 Violations	2,521 Violations
4. Ladders (1926.1053) Are Your Ladders Compliant? Ladder Safety Tips	2,143 Violations	2,018 Violations
5. Scaffolding (1926.451) OSHA Scaffolding Requirements for Construction and General Industry	2,058 Violations	1,943 Violations
6. Lockout/Tagout (1910.147) When Does the Lockout/Tagout Standard Apply?	1,977 Violations	1,670 Violations
7. Powered Industrial Trucks (1910.178) Forklift Safety Training Guide	1,749 Violations	1,404 Violations

8. Fall Protection – Training Requirements (1926.503) ANSI/ASSP Z359: Fall Protection Standards System	1,556 Violations	1,660 Violations
9. Personal Protective and Life Saving Equipment – Eye and Face Protection (1926.102) PPE Requirements: Eye and Face Protection	1,401 Violations	1,451 Violations
10. Machine Guarding (1910.212) OSHA Requirements: Machine Guarding	1,370 Violations	1,105 Violations

2024 Continuing Education for Electricians

(For All Electrical License Holders)

Part 3 – 2020 National Electrical Code

Finding State Building Code Interpretations

The State Building Inspector issues formal interpretations of the State Building Code pursuant to the authority granted by Section 29-252 of the Connecticut General Statutes. These interpretations may be issued at the request of a local building official or by the general public. The final interpretations are the opinion of the State Building Inspector.

The state building code interpretations can be found at the following web address:

https://portal.ct.gov/DAS/Office-of-State-Building-Inspector/State-Building-Code-Interpretations

2020 National Electrical Code (NEC)

Errata and Tentative Interim Amendments (TIA)

Users of the National Electrical Code (NEC) should be aware that the NEC may be amended from time to time through the issuance of Tentative Interim Amendments (TIA) or corrected by Errata. Errata is a list of errors in a printed work discovered after printing and shown with corrections.

The NEC at any point in time consists of the current edition together with any Tentative Interim Amendments and any Errata then in effect.

For official, detailed information visit the National Fire Protection Association's website:

https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=70

ARTICLE 90 – INTRODUCTION

(Amd) **90.2 Scope.**

(A) Covered. This code covers the installation of electrical conductors, equipment and raceways; signaling and communications conductors, equipment and raceways; and optical fiber cables and raceways for the following:

(1) Public and private premises, including:
- a. *buildings* and structures;
- b. utility connections, *additions* and alterations to mobile homes;
- c. utility connections to recreational vehicles; and
- d. floating *buildings*.

(2) Yards, lots, parking lots, carnivals and industrial substations.

(3) Installations of conductors and equipment that connect to the supply of electricity.

(4) Installations used by the electric utility, such as office *buildings*, warehouses, garages, machine shops and recreational *buildings* that are not an integral part of a generating plant, substation or control center.

(5) Installations supplying shore power to ships and watercraft in marinas and boatyards, including monitoring of leakage current.

(6) Installations used to export electric power from vehicles to premises wiring or for bidirectional current flow.

(B) Not covered. This code does not cover the following:

(1) Installations in ships, watercraft other than floating *buildings*, railway rolling stock, aircraft or automotive vehicles other than mobile homes and recreational vehicles.

(2) Installations underground in mines and self-propelled mobile surface mining machinery and its attendant electrical trailing cable.

(3) Installations of railways for generation, transformation, transmission or distribution of power used exclusively for operation of rolling stock or installations used exclusively for signaling and communications purposes.

(4) Installations of communications equipment under the exclusive control of communications utilities located outdoors or in *building* spaces used exclusively for such installations.

(5) Installations under the exclusive control of an electric utility where such installations:
- a. Consist of service drops or service laterals, and associated metering; or
- b. Are located in legally established easements, rights-of-way or by other agreements either designated by or recognized by public service commissions, utility commissions or other regulatory agencies having *jurisdiction* for such installations; or

c. Are on property owned or leased by the electric utility for the purpose of communications, metering, generation, control, transformation, transmission or distribution of electric energy; or
d. Are located by other written agreements either designated by or recognized by public service commissions, utility commissions, or other regulatory agencies having *jurisdiction* for such installations. These written agreements shall be limited to installations for the purpose of communications, metering, generation, control, transformation, transmission, or distribution of electric energy where legally established easements or rights-of-way cannot be obtained. These installations shall be limited to federal lands, Native American reservations through the U.S. Department of the Interior Bureau of Indian Affairs, military bases, lands controlled by port authorities and state agencies and departments, and lands owned by railroads.

(C) Special permission. The State Building Inspector may grant an exception for the installation of conductors and equipment that are not under the exclusive control of the electric utilities and are used to connect the electric utility supply system to the service-entrance conductors of the premises served, provided such installations are outside a *building* or terminate immediately inside a *building* wall.

(Amd) **90.4 Enforcement.** Administration of this code shall be in accordance with the provisions of Chapter 1 of the 2021 *International Building Code* portion of the 2022 Connecticut State Building Code. For the purposes of this code, the authority having *jurisdiction* for interpreting the rules and for granting the special permission contemplated in a number of rules is the State Building Inspector. Interpretations shall be requested verbally or in writing from the Office of the State Building Inspector. Special permission shall be requested in writing using the Request for Modification of the State Building Code form available from local building departments or from the Office of the State Building Inspector, 450 Columbus Boulevard, Suite 1303, Hartford CT 06103. www.portal.ct.gov/DAS.

Where this Code contains requirements for a new product, construction, or material that has an effective date after the adoption date of the 2022 Connecticut State Building Code, those requirements are not part of this Code.

CHAPTER 1 – GENERAL

ARTICLE 100 – Definitions.

(Amd) **Authority having jurisdiction.** The organization, office or individual responsible for approving equipment, material, an installation, or a procedure. The local *building official* has the responsibility for approving *construction documents*, issuing *permits*, approving materials and procedures and for making inspections from time to time as the construction process requires. The State Building Inspector has the responsibility for administering the Connecticut State Building Code, interpreting the Connecticut State Building Code and for granting exceptions from specific rules of the Connecticut State Building Code. See the definition of "Special Permission," and Article 90.4.

(Amd) **Special Permission.** For the purposes of this code, the authority having *jurisdiction* for granting the special permission contemplated in a number of rules is the State Building Inspector. Special permission shall be requested in writing using the Request for Modification of the State Building Code form available from local building departments or from the Office of the State Building Inspector, 450 Columbus Boulevard, Suite 1303, Hartford CT 06103. www.portal.ct.gov/DAS.

CHAPTER 2 – WIRING AND PROTECTION

(Amd) **210.8 Ground-Fault Circuit-Interrupter Protection for Personnel. (F) as follows:**

(Amd) **(F) Outdoor Outlets.** All outdoor outlets for dwellings, other than those covered in 210.8 (A)(3), Exception to (3), that are supplied by single-phase branch circuits rated 150 volts to ground or less, 50 amperes or less, shall have ground-fault circuit-interrupter protection for personnel.

Exception No. 1: Ground-fault circuit-interrupter protection shall not be required on lighting outlets other than those covered in 210.8(C).

Exception No. 2: Ground-fault circuit-interrupter protection shall not be required for mini-split-type heating/ventilating/air-conditioning (HVAC) equipment and other HVAC units employing power conversion equipment as a means to control compressor speed.

(Amd) **230.46 Spliced and Tapped Conductors.** Service-entrance conductors shall be permitted to be spliced or tapped in accordance with 110.14, 300.5(E), 300.13, and 300.15. Power distribution blocks, pressure connectors, and devices for splices and taps shall be listed.

(Amd) **230.85 Emergency Disconnects.** For new one- and two-family dwelling units, all service conductors shall terminate in disconnecting means having a short-circuit current rating equal to or greater than the available fault current, installed in a readily accessible outdoor location. If more than one disconnect is provided, they shall be grouped. Each disconnect shall be one of the following:

(1) Service disconnects marked as follows:
EMERGENCY DISCONNECT,
SERVICE DISCONNECT

(2) Meter disconnects installed per 230.82(3) and marked as follows:
EMERGENCY DISCONNECT,
METER DISCONNECT,
NOT SERVICE EQUIPMENT

(3) Other listed disconnect switches or circuit breakers on the supply side of each service disconnect that are suitable for use as service equipment and marked as follows:
EMERGENCY DISCONNECT,
NOT SERVICE EQUIPMENT

Markings shall comply with 110.21(B).

(Amd) **250.50 Grounding Electrode System**. All grounding electrodes as described in 250.52(A)(1) through (A)(7) that are available at each building or structure served shall be bonded together to form the grounding electrode system. Where none of these grounding electrodes exist, one or more of the grounding electrodes specified in 250.52(A)(4) through (A)(8) shall be installed and used.
Exception: Concrete-encased electrodes of existing buildings or structures shall not be required to be part of the grounding electrode system where the steel reinforcing bars or rods are not accessible for use without disturbing the concrete.

(Amd) **250.68(C) Grounding Electrode Conductor Connections.** Grounding electrode conductors and bonding jumpers shall be permitted to be connected at the following locations and used to extend the connection to an electrode(s):

(1) Interior metal water piping that is electrically continuous with a metal underground water pipe electrode and is located not more than 1.52 m (5 ft) from the point of entrance to the building shall be permitted to extend the connection to an electrode(s). Interior metal water piping located more than 1.52 m (5 ft) from the point of entrance to the building shall not be used as a conductor to interconnect electrodes of the grounding electrode system.
Exception: In industrial, commercial, and institutional buildings or structures, if conditions of maintenance and supervision ensure that only qualified persons service the installation, interior metal water piping located more than 1.52 m (5 ft) from the point of entrance to the building shall be permitted as a bonding conductor to interconnect electrodes that are part of the grounding electrode system, or as a grounding electrode conductor, if the entire length, other than short sections passing perpendicularly through walls, floors, or ceilings, of the interior metal water pipe that is being used for the conductor is exposed.

(2) The metal structural frame of a building shall be permitted to be used as a conductor to interconnect electrodes that are part of the grounding electrode system, or as a grounding electrode conductor. Hold-down bolts securing the structural steel column that are connected to a concrete-encased electrode complying with 250.52(A)(3) and located in the support footing shall be permitted to connect the metal structural frame of a building or structure to the concrete encased grounding electrode. The hold-down bolts shall be connected to the concrete-encased electrode by welding, exothermic welding, the usual steel tie wires, or other approved means.

(3) A rebar-type concrete-encased electrode installed in accordance with 250.52(A)(3) with an additional rebar section extended from its location within the concrete footing to an accessible location that is not subject to corrosion shall be permitted for connection of grounding electrode conductors and bonding jumpers in accordance with the following:

a. The additional rebar section shall be continuous with the grounding electrode rebar or shall be connected to the grounding electrode rebar and connected together by the usual steel tie wires, exothermic welding, welding, or other effective means.
b. The rebar extension shall not be exposed to contact with the earth without corrosion protection.
c. Rebar shall not be used as a conductor to interconnect the electrodes of grounding electrode systems.

CHAPTER 3 – WIRING METHODS AND MATERIALS

(Add) **300.4.1 Drilling and notching.**

(A) Structural floor, wall, ceiling and roof members.

(1) Solid sawn lumber. Notches in solid lumber joists, rafters and beams shall not exceed one-sixth of the depth of the member, shall not be longer than one-third of the depth of the member and shall not be located in the middle one-third of the span. Notches at the ends of the member shall not exceed one-fourth the depth of the member. The tension side of members 4 inches (102 mm) or greater in nominal thickness shall not be notched except at the ends of the members. The diameter of holes bored or cut into members shall not exceed one-third the depth of the member. Holes shall not be closer than 2 inches (51 mm) to the top or bottom of the member, or to any other hole located in the member. Where the member is also notched, the hole shall not be closer than 2 inches (51 mm) to the notch.
Exception: Notches on cantilevered portions of rafters are permitted provided the dimension of the remaining portion of the rafter is not less than 4-inch (102 mm) nominal and the length of the cantilever does not exceed 24 inches (610 mm).

(2) Engineered wood products. Cuts, notches and holes bored in trusses, structural composite lumber, structural glue-laminated members or I-joists are prohibited except where permitted by the manufacturer's recommendations or where the effects of such alterations are specifically considered in the design of the member by a *registered design professional*.

(3) Studs. Any stud in an *exterior wall* or interior bearing partition may be cut or notched to a depth not exceeding 25 percent of its width. Studs in nonbearing interior partitions may be notched to a depth not to exceed 40 percent of a single stud width. Any stud may be bored or drilled, provided that the diameter of the resulting hole is no greater than 40 percent of the stud width, the edge of the hole is no closer than 5/8 inch to the edge of the stud and the hole is not located in the same section as a cut or notch.

Exception No. 1: A stud may be bored or drilled to a diameter not exceeding 60 per cent of its width, provided that such studs located in exterior walls or interior bearing partitions are doubled and not more than two successive studs are bored.
Exception No. 2: Approved stud shoes may be used when installed in accordance with the manufacturer's recommendations.

(4) Top plates. When wiring, conduit, piping or ductwork is placed in or partly in an *exterior wall* or interior bearing wall, necessitating cutting, drilling or notching of the top plate by more than 50 per cent of its width, a galvanized metal tie of not less than 0.054 inch thick (1.37 mm) (16 ga) and 1 ½ inches (38 mm) wide shall be fastened across and to the plate at each side of the opening with not less than eight 10d (0.148 inch diameter) nails at each side or equivalent. The metal tie must extend a minimum of 6 inches (152 mm) past the opening.
Exception: When the entire side of the wall with the notch or cut is covered by wood structural panel sheathing.

CHAPTER 4 – EQUIPMENT FOR GENERAL USE

(Amd) **440.14 Location –** Add exception No. 3.

(Add) Exception No. 3: Where the interior section of a factory packaged split system is fed solely from the exterior section of the system and the disconnecting means for the exterior section is capable of being locked in the open position, a separate disconnecting means for the interior section shall not be required within sight from that section. The provisions for locking or adding a lock to the disconnecting means shall remain in place with or without the lock installed.

CHAPTER 5 - SPECIAL OCCUPANCIES

(Amd) **517.13 Equipment Grounding Conductor for Receptacles and Fixed Electrical Equipment in Patient Care Spaces**. Wiring in patient care spaces shall comply with 517.13(A) and (B).

Exception No. 1: Luminaires more than 2.3 m (71/ 2 ft) above the floor and switches located outside of the patient care vicinity shall be permitted to be connected to an equipment grounding return path complying with 517.13(A) or (B).

(A) Wiring Methods. All branch circuits serving patient care spaces shall be provided with an effective ground-fault current path by installation in a metal raceway system or a cable having a metallic armor or sheath assembly. The metal raceway system, metallic cable armor, or sheath assembly shall itself qualify as an equipment grounding conductor in accordance with 250.118.

(B) Insulated Equipment Grounding Conductors and Insulated Equipment Bonding Jumpers.

(1) General. The following shall be directly connected to an insulated copper equipment grounding conductor that is clearly identified along its entire length by green insulation and installed with the branch circuit conductors in the wiring methods as provided in 517.13(A):

(1) The grounding terminals of all receptacles other than isolated ground receptacles

(2) Metal outlet boxes, metal device boxes, or metal enclosures

(3) All non–current-carrying conductive surfaces of fixed electrical equipment likely to become energized that are subject to personal contact, operating at over 100 volts

(4) Metal faceplates, by means of a metal mounting screw(s) securing the faceplate to a metal yoke or strap of a receptacle or to a metal outlet box

Exception No. 1: For other than isolated ground receptacles, an insulated equipment bonding jumper that directly connects to the equipment grounding conductor is permitted to connect the box and receptacle(s) to the equipment grounding conductor. Isolated ground receptacles shall be connected in accordance with 517.16.

(2) Sizing. Equipment grounding conductors and equipment bonding jumpers shall be sized in accordance with 250.122.

(Amd) **525.5 Overhead Conductor Clearances.** Add the following exception to (B)(2):

(Add) Exception: Tents erected and dismantled under the supervision of a licensed electrician or other person approved by the authority having jurisdiction may be placed within the 15 feet (4.5 m) space provided the finished height of the tent is a minimum of 10 feet (3.0 m) below the conductors.

CHAPTER 6 – SPECIAL EQUIPMENT

(Del) **680.4 Inspections After Installation.** Delete in its entirety without substitution.

CHAPTER 7 - SPECIAL CONDITIONS

700.3 Tests and Maintenance

(Del) **(F) Temporary Source of Power for Maintenance or Repair of the Alternate Source of Power.** Delete in its entirety without substitution.

(Amd) **700.7 Signs.** Amend (A) as follows:

(Amd) **(A) Emergency sources.** A sign shall be placed at the service-entrance equipment, at the meter location, and on any equipment up to the service entrance-equipment, indicating type and location of on-site emergency power sources.
Exception: A sign shall not be required for individual unit equipment as specified in 700.12(I).

(Amd) **701.7 Signs.** Amend (A) as follows:

(Amd) **(A) Mandated standby.** A sign shall be placed at the service entrance, at the meter location, and on any equipment up to the service entrance-equipment, indicating type and location of on-site legally required standby power sources.
Exception: A sign shall not be required for individual unit equipment as specified in 701.12(J).

(Amd) **702.7 Signs.** Amend (A) as follows:

(Amd) **(A) Standby**. A sign shall be placed at the service-entrance equipment, at the meter location, and on any equipment up to the service-entrance equipment for all installations that indicates the type and location of on-site optional standby power sources. For one- and two-family dwelling units, a sign shall be placed at the disconnecting means required in 230.85 that indicates the location of each permanently installed on-site optional standby power source disconnect or means to shut down the prime mover as required in 445.18(D).

(Amd) **725.121 Power Sources for Class 2 and Class 3 Circuits.** Amend (C) as follows:

(Amd) **725.121 (C) Marking**. The power sources for limited power circuits in 725.121(A)(3), limited power circuits for listed audio/video equipment, listed information technology equipment, listed communications equipment, and listed industrial equipment in 725.121(A)(4) shall have a label indicating the maximum voltage and rated current output per conductor for each connection point on the power source. Where multiple connection points have the same rating, a single label shall be permitted to be used. The labeling requirement shall apply to equipment with a rated current per conductor 0.3 amperes or greater.

Electrical License Types and Scope of Work

C-5 LIMITED ELECTRICAL CONTRACTOR

The holder of this license may perform only work limited to low voltage, alarm or signal work, audio and sound systems, and telephone-interconnect. The voltage of any system is not to exceed forty-eight (48) volts or eight (8) amperes where such work commences at an outlet receptacle or connection previously installed by a person holding the proper electrical license. The requirements to qualify for this license examination shall be two (2) years as a properly licensed journeyperson or at least six (6) years of equivalent experience and training.

C-6 LIMITED ELECTRICAL JOURNEYPERSON

The holder of this license may perform only work as defined for C-5 category and only while in the employ of a licensed electrical contractor. The requirements to qualify for this license exam shall be the completion of a registered apprenticeship program or at least four (4) years of equivalent experience and training.

C-7 LIMITED ELECTRICAL SIGN CONTRACTOR

The holder of this license may perform only work limited to installing, servicing, maintaining and testing electric signs where such work commences at a dedicated outlet receptacle or connection directly adjacent to such sign. The requirements to qualify for this license examination shall be two (2) years as a properly licensed journeyperson or equivalent experience and training.

C-8 LIMITED ELECTRICAL SIGN JOURNEYPERSON

The holder of this license may perform only work limited to installing, servicing, maintaining and testing electric signs where such work commences at a dedicated outlet receptacle or connection directly adjacent to such sign and only while in the employ of a contractor licensed for such work. The requirements to qualify for this license examination shall be the completion of a registered apprenticeship program or equivalent experience and training.

E-1 UNLIMITED ELECTRICAL CONTRACTOR

The holder of this license shall be permitted to do all electrical work as defined in section 20-330 of the general statutes. The requirements to qualify for this license

exam shall be two (2) years as a unlimited licensed journeyperson or at least six (6) years of equivalent experience and training.

E-2 UNLIMITED ELECTRICAL JOURNEYPERSON

The holder of this license shall be permitted to do all electrical work as defined in section 20-330 of the Connecticut General Statutes, and only while in the employment of a properly licensed contractor. The requirement to qualify for this license exam shall be the completion of a registered apprenticeship program or at least four (4) years of equivalent experience and training.

L-1 ELECTRICAL LINES CONTRACTOR

The holder of this license may perform only work limited to line construction, including distribution systems, and their allied work, for public and private companies; installation, maintenance and repair of all high-voltage cable splicing and pulling wire for all systems in excess of 2,400 volts; traffic signal and highway lighting installation, maintenance and repair. The requirements to qualify for this license examination shall be two (2) years as a properly licensed journeyperson or at least six (6) years of equivalent experience and training.

L-2 ELECTRICAL LINES JOURNEYPERSON

The holder of this license may perform only work limited to line construction, including distribution systems, and their allied work, for public and private companies; installation, maintenance and repair of all high-voltage cable splicing and pulling wire for all systems in excess of 2,400 volts; traffic signal and highway lighting installation, maintenance and repair, and only while in the employ of a contractor licensed for such work. The requirements to qualify for this license examination shall be the completion of a registered apprenticeship program or at least four (4) years of equivalent experience and training.

L-5 LIMITED ELECTRICAL CONTRACTOR

The holder of this license may perform only work limited to low voltage, alarm or signal work, audio and sound systems. The installation or repair of any telecommunication work is not authorized with the exception of the interface wiring from an alarm system to an existing telephone connection for monitoring purposes. The voltage of the system is not to exceed 25 volts or five amperes where such work commences at an outlet receptacle or connection previously installed by

a person holding the proper electrical license. The requirements to qualify for this license examination shall be two (2) years as a properly licensed journeyperson or at least six (6) years of equivalent experience and training.

L-6 LIMITED ELECTRICAL JOURNEYPERSON

The holder of this license may perform only work limited to low voltage, alarm or signal work, audio and sound systems, and only while in the employ of a contractor licensed for such work. The installation or repair of any telecommunication work is not authorized with the exception of the interface wiring from an alarm system to an existing telephone connection for monitoring purposes. The voltage of the system is not to exceed 25 volts or five amperes where such work commences at an outlet receptacle or connection previously installed by a person holding the proper electrical license. The requirements to qualify for this license examination shall be the completion of a registered apprenticeship program or at least four (4) years of equivalent experience and training.

T-1 LIMITED ELECTRICAL CONTRACTOR

The holder of this license may perform only work limited to telephone-interconnect systems where such work commences at an outlet receptacle or connection previously installed by a person holding the proper electrical license. The requirements to qualify for this license examination shall be licensed journeyperson or at least six (6) years of equivalent experience and training.

T-2 LIMITED ELECTRICAL JOURNEYPERSON

The holder of this license may perform only work as defined for the T-1 category and only while in the employ of a licensed electrical contractor. The requirements to qualify for this license examination shall be the completion of a registered apprenticeship program or at least four (4) years of equivalent experience and training or five (5) years as a registered public service technician.

PV-1 LIMITED SOLAR ELECTRIC CONTRACTOR

The holder of this license may perform only work limited to Solar Electric systems; which means the installation, erection, repair, replacement, alteration or maintenance of photovoltaic or wind
generation systems, including storage and distribution of such energy
for heat, light, power or other purposes to a point immediately inside a structure or

adjacent to an end use. The requirements to qualify for this license examination shall be two years as a solar journeyperson or equivalent experience and training.

PV-2 LIMITED SOLAR ELECTRIC JOURNEYPERSON

The holder of this license may perform only work limited to Solar Electric systems; which means the installation, erection, repair, replacement, alteration or maintenance of photovoltaic or wind generation systems, including storage and distribution of such energy for heat, light, power or other purposes to a point immediately inside a structure or adjacent to an end use and only while in the employ of a licensed electrical contractor. The requirements to qualify for this license examination shall be the completion of a registered apprenticeship program or equivalent experience and training.

* **Clarification:** The Electrical Work Examining Board has clarified "to a point inside a structure or adjacent to an end use" by unanimous vote, that a **PV-1 or PV-2 license holder is not permitted to connect to any existing panel, junction box, wiring or circuit(s) on the premises**. They are limited to properly terminating their wiring into a junction box or controller of theirs that is not in any way connected to the buildings existing electrical system or utility meter. Connection to the buildings existing electrical system or utility meter can only be performed by a licensed E-1 or E-2 license holder.

Chapter 6 Special Equipment

1

600.2 Definitions – Electric Signs and Outline Lighting

- **Four new definitions** were added to 600.2 pertaining to **retrofit kits for signs** (1) Host Sign, (2) Retrofit Kit, General Use, (3) Retrofit Kit, Sign Specific, (4) Subassembly
- Luminaires are typically standardized and are typically mass produced, whereas **signs** are typically **custom made** and have **distinctly different structural and illumination characteristics**, including multi-location corporate signage programs which are dissimilar in size
- A retrofit kit for a sign typically has **more "moving parts"** to deal with than a retrofit kit for a luminaire
- Concentrated efforts has been pursued in the sign industry to upgrade signs to achieve **greater energy efficiency** by replacing in-place illumination systems such as florescent with light emitting diodes (LED) technology

2

600.2 Definitions – Electric Signs and Outline Lighting *(cont.)*

- **Four new definitions** were added to 600.2 pertaining to **retrofit kits for signs** (1) Host Sign, (2) Retrofit Kit, General Use, (3) Retrofit Kit, Sign Specific, (4) Subassembly *(cont.)*
- An upgrade of the sign typically involves **field modifications** of the sign
- Proper adherence to **developed protocols** for these field conversions, such that when done within the testing laboratory parameters, ensures these field conversion "retrofit kits" do not compromise the safety profile of the listed sign
- These **added definitions** will aid the installer and the inspector in assuring the right retrofit kit is used with the correct host sign

3

600.2 Definitions

- Four new definitions were added to 600.2 pertaining to retrofit signs
- Host Sign - A sign or outline lighting system already installed in the field that is designated for field conversion of the illumination system with a retrofit kit.
- Retrofit Kit, General Use – A kit consisting of primary parts, which does not include all parts for a complete subassembly but includes a parts list and instructions for field assembly.

4

600.2 Definitions (Cont.)

- Retrofit Kit, Sign Specific – A kit consisting of the necessary parts and hardware to allow for field installation in a host sign, based on the included installation instructions.
- Subassembly – Component parts or a segment of a sign, retrofit kit, or outline lighting system, that when assembled forms a complete unit or product.

5

600.4(D) Visibility of Markings for Electric Signs and Outline Lighting

- Revisions now require **visibility of markings** at the time of installation, inspection, and prior to servicing, but can be installed in a location **not viewed by the public**
- Previously, 600.4(A) markings and listing labels were not required to be visible after installation, but were required to be permanently applied in a location **visible during servicing** *(rather than **prior to servicing**)*
- This marking would include such things as manufacturer's name, trademark, maximum allowable lamp wattage, input voltage, and current rating
- New *Code* text was added to clarify that "***visible after installation***" does not necessarily mean visible in a location viewed by the public
- When an installer or inspector first approaches a sign, they should be able to identify **input voltage** and **current rating** prior to opening the sign

6

600.4(D) Visibility of Markings – Electric Signs and Outline Lighting

- Signs and outline lighting systems are required to be marked with such things as manufacturer's name, trademark, input voltage and current rating, maximum allowable lamp wattage per lampholder, and other means of identification. 600.4(A) and (C).
- Markings and listing labels are required to be visible after installation and must be permanently applied in a location visible prior to servicing.
- Marking permitted not to installed in a location not in public view

7

600.5(A) Required Branch Circuit for Electric Signs and Outline Lighting

- Revision clarifies that **entrances not accessible to customers**, such as delivery doors, **do not require a sign outlet**
- At each commercial building and each commercial occupancy accessible to pedestrians, at least one outlet *(located in an accessible location)* is required to be installed at each entrance to each tenant space for a sign or outline lighting system
- A sign or outline lighting outlet **not required** at entrances for deliveries, service corridors, or service hallways that are intended to be used only by service personnel or employees
- Clarification was needed to distinguish what entry doors did and did not require this required sign outlet

8

600.5(A) Required Branch Circuit for Electric Signs/Outline Lighting

- At each commercial building and each commercial occupancy accessible to pedestrians, at least one outlet is required to be provided at an accessible location for each entrance to each tenant space for a sign or outline lighting system (required to be supplied by a 20-ampere branch circuit with no other loads).
- Sign outlet not required at delivery entrances or service corridors.

9

690.2 Definitions: ~~Functional~~ Grounded, Functionally ~~PV System~~

- The previous definition for "**Functional Grounded PV System**" was revised to "**Grounded, Functionally**"
- **Informational Note** also revised to clarify the operational purposes for a functionally grounded system and to indicate that ground faults are only one reason to employ a functionally grounded system
- Changed to "**Grounded, Functionally**" to follow the format in Article 100 as this definition is used in multiple articles such as Article 705, 706, and 712

10

690.2 Definitions: ~~Functional~~ Grounded, Functionally ~~PV System~~ *(cont.)*

- Text in the previous definition was **vague and misleading** since functionally grounded PV systems *(without a point of direct connection to a grounding electrode system)* is only permitted through the use of a **listed ground-fault protection system** that will open all of the ungrounded conductors of a system when a fault is detected in accordance with **690.41(A) or (B)**
- To accomplish this detection, an **equipment grounding connection** is necessary as a reference to a grounding system since the functionally grounded system is effectively isolated from a ground reference until a ground fault is sensed

11

690.2 Definitions: ~~Functional~~ Grounded, Functionally ~~PV System~~ *(cont.)*

- The previous definition for "**Functional Grounded PV System**" was revised to "**Grounded, Functionally**" *(cont.)*
- Most PV systems installed in the past decade or so are actually functionally grounded systems rather than solidly grounded systems as defined in Article 100
- For functionally grounded PV systems with an interactive inverter output, the ac equipment grounding conductor is connected to associated grounded ac distribution equipment
- This connection is often the connection to ground for ground-fault protection and equipment grounding of the PV array

12

690.2 Definition: Grounded, Functionally

- Grounded Functionally – A system that has an electrical ground reference for operational purposes that is not solidly grounded.
- Informational Note: A functionally grounded system is often connected to ground through an electronic means internal to an inverter or charge controller that provides ground-fault detection.

13

690.4(B) PV Equipment Listing and Evaluation

- Revision clarifies that if the **listed PV equipment** is not **listed for the application** then it must be **field evaluated** by a NRTL or Field Evaluation Body (FEB) and have a field label applied if it passes the evaluation
- Inverters, motor generators, PV modules, ac modules and ac module systems, dc combiners, dc-to-dc converters, rapid shutdown equipment, dc circuit controllers, and charge controllers **intended for use in PV systems** are now required to be listed or be **evaluated for the application** and have a **field label applied** *(function of the "field evaluation" process)*
- New *Code* language added to not just require this equipment to be "**field labeled**" but be "**evaluated**" for the intended application
- Equipment that is listed for the application means that it is intended for use in that application

14

690.4(B) PV Equipment Listing and Evaluation (cont.)

Equipment required to be listed or evaluated:

- Inverters
- Motor generators
- PV modules
- AC modules and AC module systems
- DC combiners
- DC to DC converters
- DC circuit controllers
- Charge controllers

15

690.8(A) PV Circuit Sizing and Calculation of Maximum Circuit Current

- 690.8(A) was reorganized to provide improvement to the understanding of the requirements for PV circuit sizing and current
- Maximum current for specific PV circuits are now calculated in accordance with **690.8(A)(1) through (A)(2)**, with previous 690.8(A)(2), (A)(3), (A)(5), and (A)(6) incorporated into **revised 690.8(A)(1)**
- Language was added to clarify that calculations for these circuits have **options**, however, the **secondary options** in 690.8(A)(1)(b) and 690.8(A)(1)(a)(2) contain **restrictions**

16

690.8(A) PV Circuit Sizing and Calculation of Maximum Circuit Current (cont.)

- New **690.8(A)(2)** titled, "**Circuits Connected to the Input of Electronic Power Converters**" added to provide provision pertaining to the case in stand-alone inverter input circuit currents *[previous 680.8(A)(4)]*
  - This section includes clarifying language to require an overcurrent device in accordance with **240.4(B)** to address the allowance to **round up to the next standard size**

17

690.9(A) Overcurrent Protection for PV Circuits and Equipment

- Revision reorganizes **690.9(A)** for **overcurrent protection** to eliminate previous exception with three List Items created for unique and different protection scenarios
- The previous exception was written in positive *Code* language and transformed into **new 690.9(A)(1)** *(Circuits Where Overcurrent Protection Not Required)* with two conditions that must be meet in order to not have to provide overcurrent protection
- New **690.9(A)(2)** addresses circuits connected to current limited sources
- New **690.9(A)(3)** titled "**Other Circuits**" captures all remaining options covered under this section with four protection options

18

690.12 Rapid Shutdown of PV Systems on Buildings

- The requirements for a **Rapid Shutdown** of PV systems received extensive revision again this *Code* cycle
- The **2014 *NEC*** genesis of the rapid shutdown requirements of 690.12 were launched with the United States Department of Homeland Security (DHS) Assistance to Firefighter grant program
- For the **2017 *NEC***, the rapid shutdown requirements of 690.12 was revised to emphases the primary existence of the rapid shutdown requirements is to **reduced shock hazard for emergency responders** and to answer questions regarding the functionality of the PV rapid shutdown device itself
- This pattern of revision continued for the **2020 *NEC***

19

690.12 Rapid Shutdown of PV Systems on Buildings *(cont.)*

- The requirements for a **Rapid Shutdown** of PV systems received extensive revision again this *Code* cycle *(cont.)*
- A **new product standard** has been developed by UL so that hazardous energy levels within a PV array can be reduced when firefighters or other emergency response personnel are required to enter the array area to mitigate emergency conditions
- See **UL 3741** *(Standard for Safety Photovoltaic Hazard Control)*
- Parent text of 690.12 "**emergency responders**" replaced with "**fire fighter**" to narrow down exactly who the rapid shutdown function is intended for which harmonizes this *Code* text with **UL 3741**

20

690.12 Rapid Shutdown of PV Systems on Buildings *(cont.)*

- The requirements for a **Rapid Shutdown** of PV systems received extensive revision again this *Code* cycle *(cont.)*
- Revision to **690.12(A)** *(Controlled Conductors)* define what conductors are to be controlled; **(1)** PV system dc circuits and **(2)** Inverter output circuits
- **690.12(B)** *(Controlled Limits)* revised to indicate that controlled conductors **outside** the array boundary comply with **690.12(B)(1)** and **inside** the array boundary comply with **690.12(B)(2)**
- New *Code* text added at **690.12(C)** to address cases where more than one initiation device is used on a single PV system
- Previous **informational note** following **690.12(D)**, *(inverter input circuit conductors often remain energized for up to 5 minutes with inverters not listed for rapid shutdown)* **deleted** as informational note no longer needed

21

690.13(A) PV System Disconnecting Means

- PV system disconnecting means are required to be installed at a readily accessible location
- New requirement calling for the PV disconnecting means to be **lockable or require a tool to open** under certain conditions
- New requirement calls for any PV disconnect enclosure with a door or hinged cover that exposes live parts when open to be **locked or require a tool to open** where a disconnecting means of systems **above 30 volts is readily accessible to unqualified persons**

22

690.13(A) PV System Disconnecting Means (cont.)

- Installation of PV systems has created numerous opportunities for PV disconnect switches to be located in positions that are **accessible by other than qualified personnel** *(children in some instances)*
- Same basic change occurred at **690.15(A)** for the isolating devices or disconnecting means for PV equipment and **705.20(5)** for the disconnecting means for interconnected electric power production sources

23

690.13(E) Type of PV System Disconnecting Means

- Previous (3) List Items under "**Type of Disconnect**" removed and the revision summarizes the type of disconnects that may be used as a PV system disconnect with **lockability requirements** of **110.25** included
- Previous provisions at 690.13(F)(1), (F)(2) and (F)(3) pertaining to "**backfeed**" operations has been **removed** and referenced in a **new Informational Note** following 690.13(E)
- Revision clarifies that all **non-solidly grounded conductors** must be disconnected, but the **ac grounded (neutral) conductors** *(which are solidly grounded)*, are not required to be disconnected

24

690.15 Disconnecting Means for Photovoltaic Equipment

- Requirements for **disconnecting means** for **isolating PV equipment** of PV systems received **extensive revision** to emphasis isolation of equipment from energized conductors
- The original 1984 *NEC* title was changed from "**Disconnection of Photovoltaic Equipment**" to "**Disconnecting Means for Photovoltaic Equipment**"
  - Previous title was misleading and could be interpreted to refer to disconnecting means that is discussed at **680.13**
  - Section is intended to address isolation of equipment from energized conductors (isolated)

25

690.15 Disconnecting Means for Photovoltaic Equipment *(cont.)*

- Does not necessarily have to be accomplished by an equipment disconnecting means
- Requirements for **disconnecting means** for **isolating PV equipment** of PV systems received **extensive revision** to emphasis isolation of equipment from energized conductors *(cont.)*
- Revision occurred at the parent text of **690.15** to point directly to 690.15(D) to clarify the types of disconnecting means allowed for isolation of PV equipment

26

690.15 Disconnecting Means for Photovoltaic Equipment *(cont.)*

- A provision was added at the end of **690.15(A)** requiring the disconnecting means of equipment operating above 30 volts and readily accessible to unqualified persons to be lockable and locked or require a tool to open
- **Previous 690.15(B)** titled, "Interrupting Rating" was **deleted** as this information is covered and better suited for the disconnecting means requirements of **690.13(D)** *[previously 690.13(E)]*
- Requirements for **disconnecting means** for **isolating PV equipment** of PV systems received **extensive revision** to emphasis isolation of equipment from energized conductors *(cont.)*

27

690.15 Disconnecting Means for Photovoltaic Equipment *(cont.)*

- A new **690.15(D)** added titled, "**Type of Disconnecting Means**," which is intended to clarify the requirements related to disconnection of equipment
- Two different requirements for these devices:
  - Circuits with a **maximum circuit current over 30 amperes** must have devices that comply with **new 690.15(D)** as these conversion devices can present a load to the fault current limited circuit
  - Circuits **under 30 amperes** where isolation is required for servicing equipment, *Code* language was added to make it clear that isolating devices are permitted

28

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems

- Revisions to **690.31** organized **PV wiring methods** into one section
- Wiring methods for PV installations were previously located in various areas
- New sentence added to **690.31(A)** to introducing a revised table [**Table 690.31(A)(a)**] and a **new Table 690.31(A)(b)**
  - Revision cleans up **Table 690.31(A)(a)** [formerly Table 690.31(A)] by only including correction factors for 105°C (221°F) and 125°C (257°F) as all other correction factors are in Article 310

29

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems (cont.)

- The temperature ranges above 30°C are given in 5°C increments
- New ampacity table for 105°C (221°F) and 125°C (257°F) has been added as **new Table 690.31(A)(b)**

- Revisions to **690.31** organized **PV wiring methods** into one section *(cont.)*
- Additional clarity was needed at **690.31(B)** to address the most common application of this requirement for enforcers; installation of inverter dc input conductors and ac output conductors in the **same wireway** below an inverter

30

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- **690.31(B)(2)** permitted the installation of those same conductors *(even if from different PV systems)* within the same raceway or junction box with a removable cover without a barrier or partition
- **Exception** to **690.31(B)(2)** even deleted the grouping requirement where the conductors enter the enclosure through separate means
- **690.31(B)** revised to provide needed **lines of demarcation** for conductors of dc and ac PV systems

31

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- Several of the items in 690.31 are directly related to cables and those **cable requirements** were consolidated in the new and revised **690.31(C)**
- *Code* language added to the parent text of **690.31(C)** pertaining to the listing requirement for **Photovoltaic (Type PV) wire or cable** and **Distributed Generation (Type DG) cable** with a new informational note added to direct users of the *Code* to **UL 4703** *(Standard for Photovoltaic Wire)* and **UL 3003** *(Distributed Generation Cables)*

32

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- Requirements of **690.31(C)(1)** for "**Single-Conductor Cable**" simplified to now call for single-conductor cable in exposed outdoor locations in PV system dc circuits within the PV array to be either PV wire or cable or single-conductor cable marked sunlight resistant and Type USE-2 and Type RHW-2
- Revisions to **690.31** organized **PV wiring methods** into one section *(cont.)*
- **690.31(C)(2)** deals with single-conductor PV wire or cable installed in a cable tray with revision to this list item adding single-conductor **distributed generation (Type DG) cable** of all sizes to be permitted to be installed in a cable tray installed in outdoor locations *(with conditions)*

33

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- **690.31(C)(3)** for multiconductor jacketed cables added new provisions for distributed generation (Type DG) cables
- Type DG cable is closely related to Type TC-ER, but it is better suited for the renewable energy and other distributed generation applications allowing for different variations in conductor combinations within a single jacket
- **690.31(C)(4), (5), and (6)** were existing requirements moved from previous 690.31(E),(H), and (F) respectfully with no technical change to group all single-conductor cables requirements together at **690.31(C)**

34

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- **690.31(D)** title was shortened to be more descriptive of what it covers *(Direct-Current Circuits on or in a Buildings) [was 690.31(G)]* and extensively revised
- **690.31(D)** generally requires PV system dc circuits run inside a building to be contained in a metallic wiring system
- Purpose of revision was to acknowledge that the **physical protection requirements** of **690.31(D)** are related to the ability to detect ground faults and to protect from contact with higher voltage cables

35

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- New **exception** was added for **690.31(D)** which addresses PV hazard control systems
- **Previous requirement at 690.31(G)(1)** that called for PV circuits that were embedded in built-up, laminate, or membrane roofing materials in roof areas *(not covered by PV modules and associated equipment)* to be clearly marked for its location has been **deleted** as these marking requirement referred to a wiring method that is no longer used *(embedded in building surfaces)*
- Revision also occurred at **690.31(D)(2)** *(**Marking and Labeling Required**)* by adding language to clarify that wiring methods need not be marked where their purpose is evident

36

690.31 Wiring Methods for Solar Photovoltaic (PV) Systems *(cont.)*

- **690.31(E)** titled, "**Bipolar Photovoltaic Systems**," *[was 690.31(I)]* received slight revision by replacing the term "monopole subarray" with the term "monopole circuit" as the reference is to the circuits to these monopole subarrays so the term "circuit" was added in all five locations where monopole subarray was previously used
- New **690.31(F)** added pertaining to roof-mounted PV array mounting systems and their wiring methods
  - Permits the roof-mounted PV array to be held in place with an **approved means** other than those required by 110.13 *(Mounting and Cooling of Equipment)*

37

690.33 Mating Connectors Types for PV Systems

- New allowances added for mixing and matching brands of **PV mating connectors**
- Mating connectors **not of the identical type and brand** required to be "**listed and identified for <u>intermatability</u>**," as described in the manufacturer's instructions
- "**Intermatabilty**" is a term used in **UL 6703** (*Standard for Connectors for Use in Photovoltaic Systems)*
- Mating connectors required to be of the **latching or locking type** *(not new)*

38

690.33 Mating Connectors Types for PV Systems (cont.)

- Mating connectors that are readily accessible and used in circuits operating at **over 30 volts dc or 15 volts ac** require a tool for opening *(not new)*
- Type of connector being described at 690.33 is clearly a mating connector, so the title of 690.33 was changed from "Connectors" to "**Mating Connectors**"
- Failures of connections made between mating connectors from different brands are well documented and represent a source of **electrical and fire hazard**

39

690.41(B) Ground-Fault Protection for PV Systems

- PV system dc circuits *(not just the arrays)* that exceed **30 volts** or **8 amperes** are now required to be provided with dc ground-fault protection (GFP)
- This section now consists of three subsections
  - (1) Ground-Fault Detection
  - (2) Faulted Circuits
  - (3) Indication of Faults (New)

40

690.41(B) Ground-Fault Protection for PV Systems *(cont.)*

- PV dc AFCI and GFP requirements in both **UL 1699-B** *[Standard for Photovoltaic (PV) DC Arc-Fault Circuit Protection]* and **IEC 62109-2** *(Safety of Power Converters for use in Photovoltaic Power Systems - Part 2)* acknowledge that only energy values above these levels pose an arcing or other fire risk
- PV system dc circuits *(not just the arrays)* that exceed **30 volts** or **8 amperes** are now required to be provided with dc ground-fault protection (GFP)
- PV system circuits operating at lower voltage and power levels do not pose an arcing or other fire risk, therefore permitted to be installed **without GFP**

41

690.41(B) Ground-Fault Protection for PV Systems *(cont.)*

- Previous **exception** to **690.41(B)** permitted PV arrays with not more than two PV source circuits to be installed without GFP (where solidly grounded) as long as all PV system dc circuits were not on or in buildings has been reworded into positive language suitable for inclusion into the charging paragraph without changing the existing requirements
- New **informational note** has been added after the parent text of **690.41(B)** indicating that not all inverters, charge controllers, or dc-to-dc converters include GFP

42

690.41(B) Ground-Fault Protection for PV Systems *(cont.)*

- PV system dc circuits *(not just the arrays)* that exceed **30 volts** or **8 amperes** are now required to be provided with dc ground-fault protection (GFP) *(cont.)*
- Provisions for ground-fault detection at **690.41(B)(1)** have been revised to better align with the definitions in 690.2 and in particular, with the revised definition of "**Functionally Grounded**"
  - New language clarifies that either **GFP must be included in the converter**, or the converter and the equipment providing GFP must be **identified as being compatible** such that GFP of the circuit is maintained on either side of the converter

43

690.41(B) Ground-Fault Protection for PV Systems *(cont.)*

- Revised text at **690.41(B)(2)** concerning faulted circuits improves the application of these requirements to **any device providing GFP** *(not just inverters or charge controllers)* and clarifies the circuits to be controlled
- PV system dc circuits *(not just the arrays)* that exceed **30 volts** or **8 amperes** are now required to be provided with dc ground-fault protection (GFP) *(cont.)*
- Changes at **690.41(B)(2)** also better align *NEC* requirements with those found in PV GFP equipment safety standards such as **UL 1741** *(Inverters, Converters, Controllers and Interconnection System Equipment for Use with Distributed Energy Resources)*

44

690.41(B) Ground-Fault Protection for PV Systems *(cont.)*

- New **690.41(B)(3)** added titled, "**Indication of Faults**" states that any GFP equipment must provide an "**indication of ground faults at a readily accessible location**"
- **UL 1741** requires inverters to "identify, interrupt, and provide an indication of ground faults"
- New **690.41(B)(3)** giving examples of **indication devices** such as remote indicator light, display, monitor, signal to a monitored alarm system, or receipt of notification by web-based services

45

690.51, ~~690.52~~, and 690.53 Marking Requirements of PV Modules and dc PV Circuits

- Information outlined at previous **690.51**, **690.52**, and **690.53** that is required as part of the listing requirement of this equipment has been deleted as it is being provided on the device by the manufacturer
- **690.51** revised to simply require modules and ac modules to be marked in accordance with their listing
- **Previous 690.52** was deleted entirely
- **690.53** was revised to require a permanent readily visible label indicating the highest maximum dc voltage in a PV system

46

690.56(C) Identification of Power Sources for Buildings with Rapid Shutdown

- Several changes were made to **690.56(C)** to address the updated requirements in **690.12** *(Rapid Shutdown of PV Systems on Buildings)*
- Previous 690.56(C) contained **two figures** at 690.56(C)(1) illustrating labels required for the then two different types of rapid shutdown systems for a PV installation
- Remaining text of previous **690.56(C)(1)** has been changed to **remove** the option for the label and **previous Figure 690.56(C)(1)(b)**, previously listed under **690.56(C)(1)(b)**, since this label now describes a shutdown method that is no longer *Code* compliant

47

691.1 Scope and I-Note Figure 691.1

- New **Informational Note No. 3** and **Informational Note Figure 691.1** were added to Article 691 as an aid in interpretation
- Title of **Article 691** was changed to "**Large-Scale Photovoltaic (PV) Electric Power Supply Stations**" with the **scope changed** to indicate that the article is intended to cover "the installation of large-scale PV electric supply stations with an inverter generating capacity of no less than 5000 kW, and not under exclusive utility control"
- Term "**supply station**" which was used 12 times throughout Article 691 in the 2017 *NEC* and 17 times in the 2020 *NEC*

48

691.1 Scope and I-Note Figure 691.1 *(cont.)*

- Utilizing the term "**supply station**" better aligns the *NEC* and **National Electrical Safety Code (NESC)** on this term, which is describing the same equipment set in both Codes
- Scope of Article 691 was **updated** to align with the definition of "**Generating Capacity, Inverter**" located in Article 100
- This definitions states that Inverter Generating Capacity is defined as "the sum of parallel-connected inverter maximum continuous output power at 40°C in watts or kilowatts"
- **New informational note** was **added** after the scope of Article 691 directing users of the *Code* to a **new informational figure** intended to help in identification of unique system components related to large scale PV electrical supply stations

49

691.9 Disconnection Means for Isolating PV Equipment

- **Title revised** to be consistent with usage in Article 690, particularly 690.15
- First sentence allowing isolating devices to be located remotely from equipment was revised to align more closely with the defined term "**In Sight From (Within Sight From, Within Sight)**" in Article 100
- Provisions requiring **written safety procedures** and conditions of maintenance and supervision ensuring that only **qualified persons** service the equipment was **deleted**
- New text added requiring **documentation** of the disconnection procedures and means of isolating equipment required by the engineered design of 691.6

50

Chapter Seven Special Conditions

51

725.3(O) Temperature Limitation of Class 2 and Class 3 Cables

- New text clarifies that the **temperature limitations for conductors** of 310.14(A)(3) apply to Class 2 and Class 3 cables as well *(not just conductors)*
- New **725.3(O)** *(**Temperature Limitation of Class 2 and Class 3 Cables**)* states that requirements of **310.14(A)(3)** *[previous 310.15(A)(3)] (temperature limitation of conductors)* shall apply to Class 2 and Class 3 cables
- Because Class 2 and Class 3 circuits are typically installed in a cable rather than individual conductors, some argued that the temperature limitations of conductors of **310.14(A)(3)** did not apply to Class 2 and Class 3 cables

52

725.3(O) Temperature Limitation of Class 2 and Class 3 Cables

- To put this argument to rest, a new subsection was added to Article 725 at 725.3(O)
- Same change occurred at **760.3(N)** for **fire alarm system Class 2 and Class 3 cables**

53

725.48(B)(1) Class 1 Circuits with Power-Supply Circuits

- Revision permits **Class 1 circuits** to share enclosure space with conductors of electric light, power, non–power-limited fire alarm and medium power network-powered broadband communications circuits as long as separated by a **barrier**
- Previously, Class 1 circuits and power-supply circuits were only permitted to occupy the same cable, enclosure, or raceway ***without a barrier*** only where the equipment powered was ***functionally associated*** *(still applies)*
- The "barrier" requirement for Class 1, Class 2, and Class 3 circuits is not specific as to the type of material required

54

725.144 and Table 725.144 Transmission of Power and Data

- Extensive revision occurred for 725.144, Table 725.144, 725.144(A), and 725.144(B) dealing with **transmission of power and data** on Class 2, Class 3, Class 2-LP, or Class 3-LP cables
- Requirements of parent text of 725.144 did not change, just revised for clarity
- New ***Informational Note No. 3 and No. 4*** were added to identify the unique nature of the type of conductors and cables specified at Table 725.144 and to provide the appropriate reference standards that address the cables covered in the Table
- New ***Informational Note No. 5*** was added since Power over Ethernet (PoE) lighting is a very important application covered by 725.144

55

725.144 and Table 725.144 Transmission of Power and Data *(cont.)*

- New ***Informational Note No. 6*** was added to clarify that the rated current for power sources covered in 725.144 is the output current per conductor the power source is designed to deliver to an operational load at normal operating conditions, as declared by the manufacturer
- At Table 725.144, the undefined term "Data Cables" has been replaced with "**Balanced Twisted-Pair Cables**," which is language that is consistent with relevant industry standards *(such as **ANSI/TIA-568-C.2-2009** Balanced Twisted-Pair Telecommunications Cabling and Components Standards)* and is also consistent with language in other parts of Article 725

56

725.144 and Table 725.144 Transmission of Power and Data *(cont.)*

- All the ampacity adjustment factors in **previous Table 725.144** were expressed to **one tenth values** *(i.e. 1.4, 1.7. 0.6, etc.)* except for the ampacity adjustment factors of whole numbers, such as "1, 2 and 3" amperes
- Based on **Note 2 to the table**, an ampacity of 1 ampere could be interpreted to be 1.4 amperes as this note states that where only half of the conductors in each cable are carrying current, the values in the table are permitted to be increased by a factor of 1.4
- The table ampacity adjustment factors of "1, 2 and 3" needed to be revised to "1.00, 2.00 and 3.00" respectively to avoid incorrectly interpreting these numbers

57

725.144 and Table 725.144 Transmission of Power and Data *(cont.)*

- **Table 725.144** ampacity adjustment factors are now expressed in double digit values
- Some of the ampacity values have been updated in **Table 725.144** to reflect new ampacity values for 23 AWG cables after recreating and reaffirming the data from the substantiation that generated this table in the 2017 *NEC*
- **725.144(A)**, covering the use of Class 2 or Class 3 cables to transmit power and data was **revised** to enhance the usability of this subsection by identifying applications where Table 725.144 need not be consulted

58

725.144 and Table 725.144 Transmission of Power and Data *(cont.)*

- The requirements of **725.144(B)**, titled "**Use of Class 2-LP or Class 3-LP Cables to Transmit Power and Data**" was revised with a new sentence added pertaining to **bundled LP cables**
- **725.144(B)** now states that where bundled LP cables number **192 or less** and the selected ampacity of the cables in accordance with Table 725.144 exceeds the marked current limit of the cable, the ampacity determined from the table is permitted to be used

59

760.121(B) Power Sources for PLFA Circuits *(Fire Alarm Systems)*

- New sentence added to permit the fire alarm branch-circuit disconnecting means for power limited fire alarm (PLFA) circuits to be **secured in the "on" position**
- The fire alarm circuit disconnect for non-power-limited fire alarm (NPLFA) circuits was already permitted to be secured in the "on" position *[see 760.41(A)]*
- Change provides consistency with NPLFA circuits and PLFA circuits
- While this practice was not prohibited by **760.121**, it was not specifically permitted either
- Installing **breaker locks** is already a common industry practice on fire alarm circuits

60

770.24 Mechanical Execution of Work (Optical Fiber Cable)

- Revision will require optical fiber cable to conform to **all of 300.4 and 300.11** *[not just 300.4(D) through (G)]*
- Previously, optical fiber cables were to be installed and protected from physical damage in accordance with 300.4(D) through (G) and 300.11
- Optical fiber cables not limited to communications installations and need protection against physical damage regardless if they can be a shock hazard or not
- Even if optical fiber cable is not carrying any current, the equipment being supplied by this cable in several situations are critical to **life and safety**
- The installation of these optical fiber cables should conform to **all of 300.4**

61

770.110(D) Cable Trays for Optical Fiber Cables

- New section added permitting **optical fiber cables** to be installed in metal or listed nonmetallic **cable tray systems**
- Previously, permission to install optical fiber cable in a cable tray was given in several locations across Article 770
- This revision will make it easier to find this cable tray rule with it located in the same section that permits optical fiber cables to be installed in raceways and cable routing assemblies
- New requirement limits the allowance for optical fiber cables to be installed in a cable tray to **metal and listed nonmetallic cable trays** in order to address flame spread concerns

62

770.133 Installation of Optical Fibers and Electrical Conductors

- Previous requirements of **770.133(A)** has been reorganized and relocated throughout **770.133(A)** and new **770.133(B)**
- Previous exceptions rewritten into positive *Code* language
- Previous 770.133(A) permitted optical fiber cables to occupy the same cable tray and raceway as conductors for electric light, power, Class 1, non-power-limited fire alarm, etc. *(with five exceptions)*
- Almost all of the 2017 *NEC* requirements of 770.133 are still there for the 2020 *NEC* but **relocated for a better flow of the information**

63

770.133 Installation of Optical Fibers and Electrical Conductors *(cont.)*

- Permission to allow nonconductive optical fiber cables to occupy the same cable tray as conductors for electric light, power, Class 1, non-power-limited fire alarm, etc. operating at 1000 volts or less was moved to the second paragraph of new 770.133(B)
- Previous requirements of **770.133(A)** has been reorganized and relocated throughout **770.133(A)** and new **770.133(B)** *(cont.)*

64

770.133 Installation of Optical Fibers and Electrical Conductors *(cont.)*

- First paragraph of **770.133(A)** was updated to permit **conductive optical fiber cables** contained in an armored or metal-clad-type sheath and **nonconductive optical fiber cables** to occupy the same cable tray with conductors for electric light, power, Class 1, non-power-limited fire alarm, etc. operating at 1000 volts or less
- **Conductive optical fiber cables without an armored or metal-clad-type sheath** not permitted to occupy the same cable tray as power conductors, etc. unless separated by a **permanent barrier** or listed divider

65

Chapter Eight Communications Systems

66

Article 800 General Requirements for Communications Systems

- **New Article 800** *(General Requirements for Communications Systems)* combines **common requirements** previously found in Articles 800, 820, 830 and 840 into a **new "general" article** that applies to all of these articles
- **Previous Article 800** *(Communications Circuits)* was moved to **Article 805** to make room for this new Chapter 8 article
- **Common requirements** would include such things as mechanical execution of work, abandoned cables, spread of fire or products of combustion, and temperature limitations of wires and cables

67

Article 800 General Requirements for Communications Systems (cont.)

- New article for communication circuits significantly improves clarity and usability while removing redundant requirements from each of the articles throughout Chapter 8
- 800.1 Scope – This article covers general requirements for communications systems. These general requirements apply to communications circuits, community antenna television and radio distribution systems, network-powered broadband communication systems, and premises-powered broadband systems unless modified by Articles 805, 820, 830, or 840.

68

800.2 Definitions: Communications Circuit

- **Communications Circuit.** The circuit that extends service from the communications utility or service provider to and including the customer's communications equipment.
- The definition of a "**Communications Circuit**" was revised to remove the "list" of service types offered by a communications circuit
- List was problematic as it did not allow for new technologies to be included in this definition without a *Code* change, which only happens every three years

69

800.3 Other Articles for Communications Systems

- New text was added to reinforce the **independence of Article 800 and Chapter 8** which stipulates that only those sections of Chapters 1 through 7 referenced in Article 800 shall apply to communications systems
- Opening sentence of 800.3 now reads, "**Only those sections of Chapters 1 through 7 referenced in Chapter 8 shall apply to Chapter 8**."
- Requirements of **90.3** state that Chapter 8 of the *NEC* is a **"stand-alone" article** and "is not subject to the requirements of Chapters 1 through 7 except where the requirements are specifically referenced in Chapter 8"

70

800.3 Other Articles for Communications Systems (cont.)

- In order for a requirement from Chapters 1 through 7 to apply to Chapter 8, there must be a clear reference or "**road map**" in Chapter 8 to a specific requirement in Chapters 1 through 7
- Only those sections of Chapters 1 through 7 referenced in Chapter 8 shall apply to Chapter 8

71

800.27 Temperature Limitation of Wire and Cables (Communications Systems)

- New section added to specify that no communication wire or cable be used in such a manner that its **operating temperature** exceeds that of its rating
- When the previous requirements of 800.3 were moved to new Article 800, it was felt that this **temperature limitation requirement** deserved its own section in Article 800
- Previous temperature limitations of 800.3(H) were moved to a **new 800.27** and titled "**Temperature Limitation of Wires and Cables**"

72

800.27 Temperature Limitation of Wire and Cables (Communications Systems) (cont.)

- New text at 800.27 makes it clear that this temperature limitations in Chapter 8 **apply to cables** *(not just conductors)*
- New text simplifies the *Code* by including the temperature limitation requirement **directly in Article 800**, rather than have a cross-reference in Article 800 to the temperature limitation requirements of **Article 310**
- No communications wire or cable is permitted to be used in such a manner that its operating temperature exceeds that of its rating

73

800.44 Overhead (Aerial) Communications Wires and Cables

- Requirements were added for ***all*** communications circuits pertaining attachment to **above-the-roof raceway mast** and cables extending between buildings or structures
- Previously, **Article 820** contained provisions for attaching coaxial cables to an **above-the-roof raceway mast** that did not enclose or support conductors of electric light or power circuits *(none of the other Chapter 8 article contained this mast rule)*
- Previously, **Articles 820 and 830** contained requirements pertaining to coaxial cables and network-powered broadband communications **cables extending between buildings** or structures *(other Chapter 8 articles did not have such rules)*

74

800.44 Overhead (Aerial) Communications Wires and Cables (cont.)

- These two rules were perfect candidates to be placed in **new Article 800** to prevent repeating these rules in four different articles *(needed consistency)*
- 800.44 – Overhead (Aerial) Communications Wires and Cables shall be permitted to be attached to above-the –roof raceway mast that does not enclose or support conductors of electric light and power circuits

75

805.179(D) Limited Power (LP) Cables

- Provisions were added to permit **limited power (LP) cables** to act as a **substitute** for Class 2 and Class 3 cables
- Previously, communications cables were permitted as substitutes for Class 2 and Class 3 cables, but the *Code* **did not specifically address** limited power (LP) cables as a substitute for Class 2 and Class 3 cables
- **725.144** and **Table 725.144** gives designers, installers and AHJs the assurance that 4-pair data cables can safely carry power as well as data when bundled together in cable trays or cable routing assemblies

76

805.179(D) Limited Power (LP) Cables (cont.)

- This revision recognizes the fact that an **LP cable** is a specific type of Class 2, Class 3, and communications cable and explicitly permits these cable types as **substitutes** for Class 2 and Class 3 LP cables *(vast majority of LP cables are listed as communications cables)*
- LP cables are listed under the UL product categories of Communications Cable **(DUZX)** and Power Limited Circuit Cable **(QPTZ)**

77

840.2 Definitions for Premises-Powered Broadband Communications Systems

- Two new definitions were added to 840.2 to define the terms "**Broadband**" and "**Premises-Powered**"
- **Broadband.** Wide bandwidth data transmission that transports multiple signals, protocols, and traffic types over various media types.
- **Premises-Powered.** Using power provided locally from the premises.
- Previously, neither "**Broadband**" or "**Premises-Powered**" were defined in Article 840 *(Premises-powered Broadband Communications Systems)* or the *NEC*

78

840.2 Definitions for Premises-Powered Broadband Communications Systems (cont.)

- Definition for "**Broadband**" was added to provide an appropriate description of the circuits covered under Article 840
- Term "**Premises-Powered**" had to be defined as it now applies to more than one type of system
- Premises powered basically means that the power used by the communications system is **derived from the local premises power**, and this power source has **no limits on the power crossing a premises property line** or boundary

79

840.94 and 840.102 Premises Circuits Leaving the Building

- Two new sections (840.94 and 840.102) added to provide requirements for **premises-powered broadband communication system (PPBCS) circuits** when they **leave the building** to power equipment **remote to that building**
- Previously, 840.101 contained provisions for PPBCS circuits where they **did not leave the building**, but no provisions existed for when PPBCS circuits **did leave the building**
- PPBCS circuits are being installed by utilities or service providers that provide power to exterior equipment such as an asymmetric digital subscriber line (ADSL), which is a type of digital subscriber line (DSL) technology

80

840.94 and 840.102 Premises Circuits Leaving the Building *(cont.)*

- The circuits are equipment on the network being powered from the premises which ultimately would power circuits going to **other premises**
- These circuits are derived from the premises power to avoid having to run copper cable to the exterior location, avoid establishing a meter point, and/or avoid providing backup batteries *[sometimes referred to as **"reverse powering (RP)"**]*
- These added circuits are potentially exposed to lightning events and/or electric power ground faults
- They deserve and require the same protection and grounding and bonding means as other aerial, buried, or underground communications cables entering a building

81

840.94 and 840.102 Premises Circuits Leaving the Building *(cont.)*

- 840.94 – Requires circuits leaving a building to power equipment remote to that building or outside the exterior zone of protection defined by a 46 m (150 ft) radius rolling sphere, to comply with 805.90 (Protective Devices) and 805.93 (Grounding, Bonding, or Interruption of Non-Current-Carrying Metallic Sheath Members of Communications Cables)
- 804.102 - Requires circuits leaving a building to power equipment remote to that building or outside the exterior zone of protection defined by a 46 m (150 ft) radius rolling sphere, to comply with 800.100 (Cable and Primary Protector Bonding and Grounding) and 800.106 (Primary Protector Grounding and Bonding at Mobile Homes)

82

840.160 Powering Circuits (Premises-Powered Broadband Communication Systems)

- Revised text identifies **listing provisions** for communications cables, powered communications equipment, and the power source
- Communications cables that are listed in accordance with **805.179** are permitted to carry circuits for powering communications equipment *(in addition to carrying the communications circuit)*
- Communications equipment has to be listed in accordance with **805.170**

83

840.160 Powering Circuits (Premises-Powered Broadband Communication Systems) (cont.)

- Power source required to be listed in accordance with **840.170(G)**
- Installation of listed 4-pair communications cables for a communications circuit or installation where 4-pair communications cables are substituted for Class 2 and Class 3 cables in accordance with **725.154(A)** is required to comply with **725.144** with an exception *where the rated current of the power source does not exceed 0.3 amperes in any conductor 24 AWG or larger*

84

Informative Annexes

85

Informative Annex A- Product Safety Standards

- Informative Annex A was reformatted to provide and add ***NEC* article numbers** and **appropriate product standards were added and updated**
- Previously, Informative Annex A had **two columns** of information; **(1)** the name of the product standard and **(2)** the product standard number
- Informative Annex A now has **three columns** of information; **(1)** the *NEC* article number where the referenced product standard can be found, **(2)** the product standard number, and (3) the name of the product standard

86

Informative Annex A- Product Safety Standards (cont.)

- **2017 *NEC*:** Informative Annex A referenced **236 product standards**
- **2020 *NEC*:** Informative Annex A references **352 product standards**
- Previous tabular format of Informative Annex A did not provide **correlation with various *Code* Articles** (*where can these product standard references be found throughout the NEC?)*

87

Informative Annex C - Conduit, Tubing, and Cable Tray Fill Tables for Conductors and Fixture Wires of the Same Size

- Informative Annex C revised to include conductor fill tables for **cable trays** as well and for conduits and tubing
- Previous Informative Annex C contained **26 tables** for determining the maximum number of conductors or fixture wires permitted in various conduits and tubings
- New Informative Annex C is now contains **33 tables** for determining the maximum number of conductors or fixture wires permitted in various conduits, tubings **and cable trays**

88

Informative Annex C - Conduit, Tubing, and Cable Tray Fill Tables for Conductors and Fixture Wires of the Same Size (cont.)

- Rules and tables provided in Article 392 *(Cable Trays)* for determining the sizing of various cable tray types and sizes can be intimidating and complicated to some users of the *Code*
- **New tables** in Informative Annex C allows for **simplified determination** of the maximum number of cables or conductors allowed in a particular cable tray width and serve to **enhance safety** due to reductions of errors pertaining to incorrect cable selection and erroneous cable tray sizing calculations

89

2022 SECURITY MEGATRENDS™

THE ANNUAL VISION FOR THE SECURITY INDUSTRY

SIA
SECURITY INDUSTRY ASSOCIATION

STAFF

PIERRE TRAPANESE
SIA Chair of the Board

STEVE VAN TILL
Megatrends Advisor

DON ERICKSON
SIA CEO
derickson@securityindustry.org

GEOFF KOHL
SIA Senior Director of Marketing
Author, 2022 Security Megatrends Report
gkohl@securityindustry.org

KEVIN MURPHY
SIA Director of Member Services
kmurphy@securityindustry.org

MARC BENSON
Associate Director of Membership
mbenson@securityindustry.org

JOHN COLEMAN
Manager, Member Services
jcoleman@securityindustry.org

KIM LANDGRAF
SIA Manager of Design and Production
klandgraf@securityindustry.org

MICHELLE WANDRES
Production Design

Copyright 2022 Security Industry Association. Reproduction prohibited without prior permission.

Security Industry Association
8405 Colesville Road
Suite 500
Silver Spring, MD 20910
Main: 301-804-4700
Fax: 301-804-4701
securityindustry.org

2022 SECURITY
MEGATRENDS™

THE PROMISING FUTURE

SIA's annual Security Megatrends report is a story of how our industry will be changed, but it's more a vision of how our industry will drive change. Based on industry surveys and focus groups, plus drawn from insights that speakers shared during our annual Securing New Ground (SNG) conference, this is our best forecast for what opportunities lie ahead.

Now in its sixth year serving as the industry's defining list of trends, Security Megatrends is a consistent, measured report, and if you compare this year's list to our 2021 report, you won't see a full sweep of the trends. The megatrends aren't a rally cry for the latest buzzwords; rather, these are the long-term trends that change the underlying archetypes.

Artificial Intelligence (AI) continues to reign as the #1 megatrend, and each year, this trend moves further along its developmental journey. While AI may have once been simple marketing hype from companies seeking promotional value, today the application of AI (mostly in the form of machine learning) is a real part of most company's next generation solutions, correlating data that had been heretofore uncorrelated and automating one or two more processes or steps to make a business owner or a security officer's job that much easier.

Cybersecurity likewise stayed consistent, still ranked #2 for the 2022 report, propelled perhaps by the constant fear of a security solution held hostage by ransomware or of a nation state hacking a vital government or critical infrastructure security system. Today, cybersecurity is a market differentiator, and entire segments – notably in the field of video surveillance – have been transformed by attention to cybersecurity. Before you turn the page and we reveal the full list of 2022 Security Megatrends, I do want to recognize three trends that represent a mindset shift within the industry. One is Increased Interoperability (ranked #6), one is Data Privacy (ranked #7) and the other is Health & Sustainability (ranked #10).

In recent years, the industry has been more cognizant of how security solutions shape the world, and we believe this will only increase in the future. Today we ask, are we making the world more closed, or are we helping to open the world? Asked in another way: Are we just restricting (keeping bad people out) or are we enabling (ensuring the right people can get in)? Simultaneously, the industry has made commitments to ethics, not just in how security solutions are used but in how individuals' privacy is protected in these systems.

Today, the fact that three of the top 10 trends are centered around openness, respect of individuals and how we make the world both healthier and more sustainable speaks to the level of change that has occurred in our industry. And that kind of change can only lead to an ever-brighter future!

Sincerely,
Pierre Trapanese
Chair, SIA Board of Directors

THANK YOU

SIA THANKS ITS 2021 SNG SPONSORS

ALLEGION

AMAG TECHNOLOGY

ASSA ABLOY
The global leader in door opening solutions

AXIS COMMUNICATIONS

BOSCH

brivo
simply better security

convergint

DELL Technologies

dormakaba

Genetec

Imperial Capital

intel

LENEL:S2

milestone

PROSEGUR

RAYMOND JAMES

SALIENT

INDUSTRY PARTNER

iSC

MEDIA PARTNERS

Campus Safety

SDM

SIW SECURITY INFOWATCH.COM

SECURITY SYSTEMS NEWS

SECURITY SALES & INTEGRATION

SECURITY

EXECUTIVE TAKEAWAYS

"Technology is moving at an incredible pace, and so have our customers' needs. Our customers have now really focused on innovation. We're seeing companies wanting to move to cloud-based solutions. They want to modernize their network, security infrastructure, remote capabilities. We're seeing an increase in disruptive technologies like AI and computer vision. Businesses are continuing to prioritize digital transformation initiatives and get real-time data to make better decisions."

– Bhuvana Badrinathan, CIO, Convergint

"Cybersecurity and IT generally are integral to smart buildings. These are part and parcel of the whole thing. If you want to call it a smart building, then it has to be a smart and secure building."

– Adam Chapman, Cybersecurity Manager and Product & Solution Security Officer, Siemens

"It [AI] is the natural evolution of our industry. In the end, it's about how we can drive operational efficiencies."

– Luis Orbegoso, President, Americas, Allegion

"B2B industries are way behind all the consumer product companies, so we're basically fighting for the scraps [in the supply chain]. I'd love to tell everyone that 2022 is going to be great, but I think you're going to see some struggles throughout the year, and there might be some light at the end of the tunnel, but I don't think so for another 12 months unfortunately."

– Thomas Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"80% of the spending in the security industry today is manual labor. That means guards, monitoring or even installation services. That will change."

– Fredrik Nilsson, Vice President, Americas, Axis Communications

"People don't mind change. They mind being changed. And when there's a pandemic or there's a disaster, there's going to be a lot of change."

– Bonnie Michelman Executive Director of Police, Security and Outside Services, Massachusetts General Hospital and Mass General Brigham Corporation

"I call it the 'OK, now what?' type of data, where it's the aggregation of data that triggers an action."

– Lee Odess, General Manager of New Market Development, Latch

"It's kind of the elephant in the room that when you build products, it's not entirely built by the company that you bought it from. There are a lot of third-party components, sometime open-source components. They can come from many places, so you need to track this somehow as a supplier, but also as a customer."

– Mathieu Chevalier, Principal Security Architect, Genetec

"When you think about all that's going on across some of the major sectors of the market, access control, video, even guarding, we are seeing tremendous amounts of change – business model transformations, the infusion of technology at levels that this industry has never seen before, the development of businesses like some of the SPAC companies, or the companies that have gone public through SPACS, that are very nascent in what they're doing, but they're trying to transform entire industries. So the excitement level in this space from the investment community is extremely high. It's the highest I've seen it in quite some time. For companies in the space, I think you're in a good spot. There's plenty of capital out there, so continue to go do what you're doing because you've built up the business and the industry in a very good way. There's more forward momentum and progress in our space than ever before."

– Alper Cetingok, Managing Director, Head of Diversified Industrials, Raymond James

HOW WE DEFINED AND RESEARCHED THE 2022 SIA SECURITY MEGATRENDS

Each year at Securing New Ground (SNG), senior-level industry leaders and financial partners gather, trends are discussed, connections are formed and ideas are shared openly.

In advance of SNG, as part of our annual membership survey, SIA asked hundreds of executives from SIA member companies what factors were shaping their business decisions and what trends they were watching. We then further surveyed SIA members, along with current and recent speakers and attendees of SNG about which previous trends were still relevant, which trends were no longer as impactful to the industry and which trends could be identified to be added to our report.

In addition to the survey research, the selection of these trends relies on the speakers, panel and audience members of SNG, because the conference is the ultimate proving ground for deep-dive discussions on what we can do as an industry to pave a successful future. A special poll-driven session during the 2021 SNG conference provided additional feedback related to the Security Megatrends and helped generate some of the chart data included in this report.

Through SIA's research and the vetting, validation and additional research that occurs during and after SNG, here we have, hopefully, not only captured the industry's driving forces in the 2022 SIA Security Megatrends report, but also provided you insights and action items to facilitate a successful future in the security industry.

2022 SECURITY MEGATRENDS

1 ARTIFICIAL INTELLIGENCE page 6

2 CYBERSECURITY page 10

3 SUPPLY CHAIN ASSURANCE page 14

4 SERVICE MODELS AND THE CLOUD page 15

5 WORKFORCE DEVELOPMENT page 20

6 INCREASED INTEROPERABILITY page 22

7 DATA PRIVACY page 24

8 SECURITY AS PROPTECH page 26

9 EXPANDED INTELLIGENCE MONITORING page 28

10 HEALTH & SUSTAINABILITY page 30

MEGATREND 1

ARTIFICIAL INTELLIGENCE

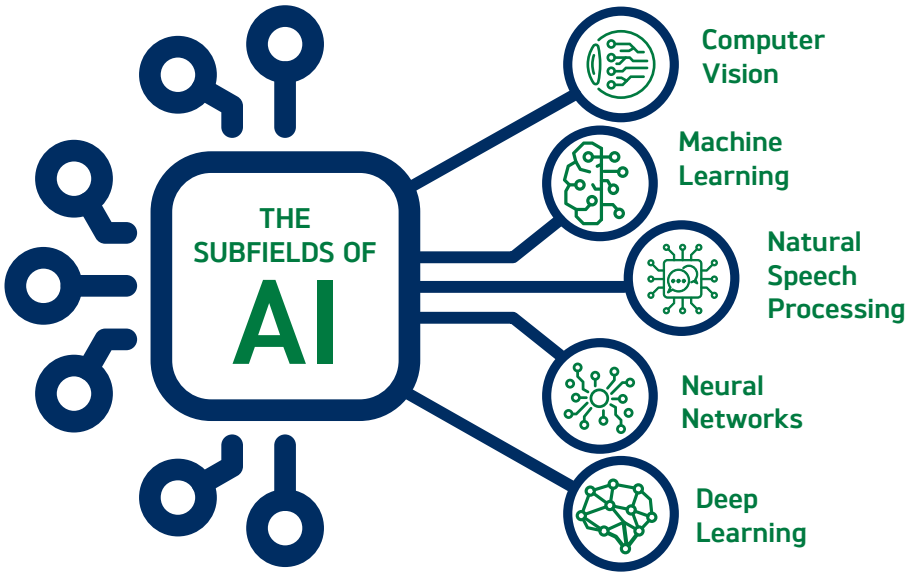
THE KING CONTINUES TO REIGN. In the 2021 Security Megatrends report, artificial intelligence (AI) rose to the position of the top-ranked megatrend, and despite coups attempted by would-be successors of cybersecurity, supply chain, RMR models and even long-term workforce development challenges, all attempts to dethrone king AI ultimately failed and AI remains atop our 2022 list. Long live the king, you might say, as industry firms have embraced the promise of AI, whether that be through advance audio analytics, complex facial recognition and cutting-edge video surveillance scene processing that can recognize human behaviors – and, of course, the world of robotics and drones.

The cynics may say it is as much a marketing trend as it a technology trend, but AI is indeed a real industry shaping (and shaking) trend today, even though the more measured and less-boosterish technologists in this space will admit that a lot of what purports to be AI today wouldn't quite meet the threshold of true "intelligence" and is fundamentally just preprogrammed algorithms doing computer vision-based object detection (e.g., vehicle in scene, license plate recognition, face mask detection). Real AI, they might say, is when a machine can far exceed the capabilities of human intelligence or can even apply the lesson learned in one situation to another, entirely different situation. Without a doubt, there are solutions today that exceed those human capabilities, like the facial recognition systems that return a high probability match from a large database nearly instantly.

AI in this industry has always existed on a spectrum, from basic smarts that can occur in a compact security camera's on-board chip to the level of intelligence that requires extensive server arrays and which can process truly massive amounts of unstructured data. Today, much of what is occurring in the industry is in the realms of computer vision, machine learning and even some natural language processing, but the

prospect of neural network-powered machine learning and deep learning means even deeper insights from more complex and less structured data.

And as we concluded last year, "AI is truly an aspirational trend. AI is that application of logic, rules and understanding that is always one step ahead of where we are now. What we may call AI today is likely to be seen as a normal feature in the future."



Source: SAS Institute

PERSPECTIVES

"Artificial intelligence would be the ultimate version of Google. The ultimate search engine that would understand everything on the web. It would understand exactly what you wanted, and it would give you the right thing. We're nowhere near doing that now. However, we can get incrementally closer to that, and that is basically what we work on."

—Larry Page, Co-Founder of Google

"The way researchers break platforms is they do things that they already know are not supposed to happen. And they wait to see what happens with the device. So how do you validate that? How do you test for all those completely oddball things? That's where AI can really help with some of the validation and be able to do these nonsensical tests on the device and help us in ways that maybe humans wouldn't have even thought of, or if we had, it would have taken a long time, and we can speed up that validation process."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

IT'S ARTIFICIAL, NOT AUTOMATIC

The machine may be learning, but who is doing the teaching? AI researchers and technology developers will tell you that the amount of work that goes into training an algorithm is often a staggering effort of not only generating a massive set or organized data for the algorithm to process, but also requires a massive human effort of providing nuanced feedback to the algorithm so that the algorithm can improve its accuracy.

As Saif Khan and Alexander Mann wrote in their 2020 paper for the Center for Security and Emerging Technology titled "AI Chips: What They Are and Why They Matter," "the success of modern AI techniques relies on computation on a scale unimaginable even a few years ago. Training a leading AI algorithm can require a month of computing time and cost $100 million."

AI SHAPING HUMAN GUARDING

Allied Universal CEO Steve Jones tells the story of how AI is making security officers even more efficient:

"We have built out a handheld technology that our officers use every day to track their performance and what they do and be kind of the checklist of things that they need to do. The AI takes all the data that we're collecting and goes through and makes recommendations on where our officers should go. In the old days we would put together all these reports manually in writing by pen and paper, and then we would consolidate these things and we'd try to present to corporate security directors and try to figure out what we need to do for our enterprise to better secure it, keep our people safe and protect and minimize risk. Now suddenly, the AI is doing that. As we are entering data on the handheld device, the AI is giving us real-time information.

"We're using it internally to operate our business, helping us drive metrics in our business and taking on menial tasks that we used to do all the time. The artificial intelligence engine is learning how we do those things day in and day out with thousands and thousands of employees. And now it's able to do it."

$15.6T
Potential contribution to the global economy by 2030 from AI

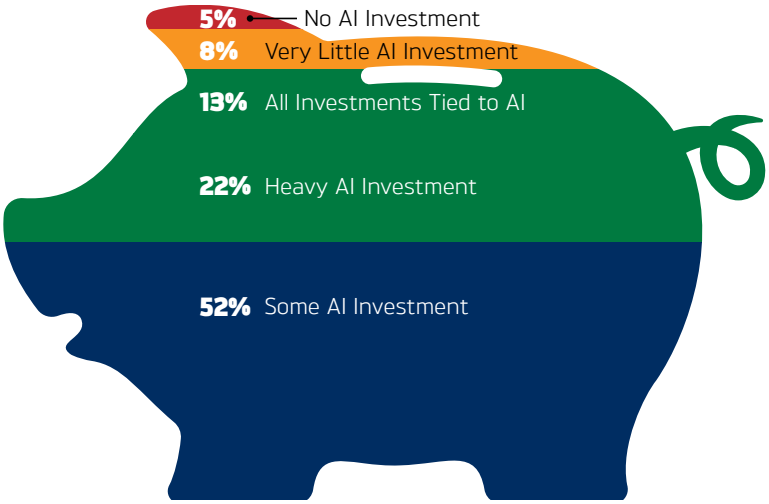
14.5%
Percentage of North America's GDP that AI could influence by 2030

Source: PwC Global Artificial Intelligence Study

SNG POLL

HOW WOULD YOU CHARACTERIZE YOUR FIRM'S R&D INVESTMENTS RELATED TO APPLYING AI TO YOUR PRODUCTS AND SOLUTIONS?

AI investment from security industry companies is exploding. When we first surveyed SIA member companies in 2019 about their R&D investments into AI, less than 2% said that all R&D investments were tied to AI. In 2020, that percentage crept up to 3%. But sometime in the last year, what started as an ember is now a raging fire of investment into AI, with 13% of companies saying that all their R&D investments are tied into AI opportunities.



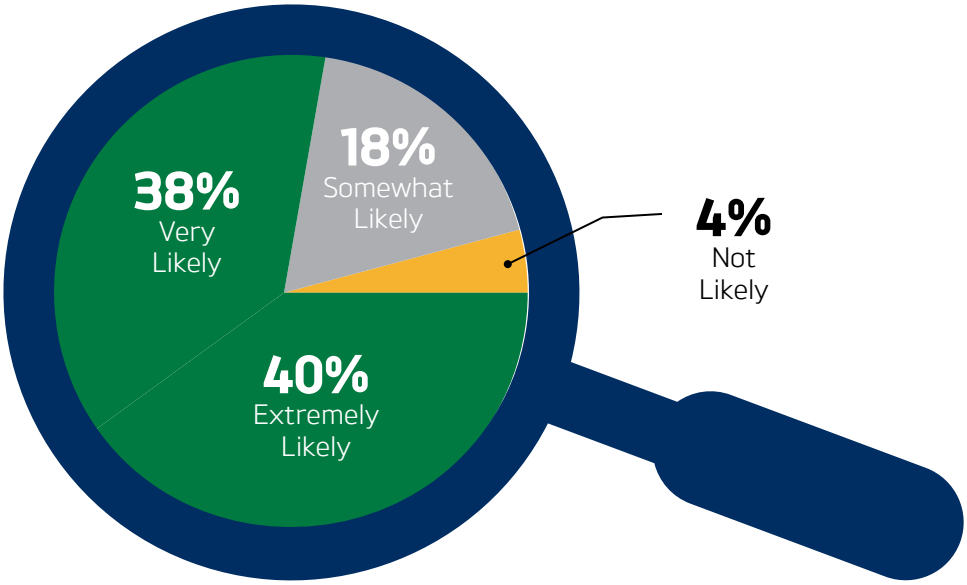
CHALLENGE

It's often claimed that Moore's Law is coming to an end, referencing the famed prediction in 1965 by Gordon Moore that the number of transistors on a chip would double every two years, effectively doubling computing power. As David Rotman noted in the February 2020 for the MIT Technology Review, the rate of development is slowing, even as our demands for computing power grow. How do we reconcile those two seemingly incongruous destinations? Experts say there are two paths. The first is to simply buy more on-demand processing, such as through cloud services. The second option is to make the algorithm or software performing the AI more efficient. Still others, particularly those in the world of chip manufacturing, will says that a slowing rate of processing power from exponential growth to sub-exponential just means computing power growth is slowing, but that the growth is far from over, and that specialized AI chipsets doing parallel, simultaneous processing (versus sequential processing) will pick up the slack that previously required the ability to shrink transistor sizes to fit more processing on a chip.

SNG POLL

DO YOU THINK PREDICTIVE DATA ANALYTICS WILL BECOME A MEANINGFUL FEATURE WITHIN YOUR PRODUCTS, SOFTWARE OR SOLUTIONS WITHIN THE NEXT YEAR?

Recognized as its own Security Megatrend in the 2021 report, for the 2022 report, predictive data analytics is included within the broader trend of AI. Predictive data analysis aligns well with the AI fields of deep learning, which promises to be able to autonomously identify patterns out of large data sets, and neural network computing which can identify patterns from undefined data. Even the simplest predictive applications can be business altering, such as recognizing when hardware needs service or will require replacement.



MEGATREND MOVEMENT

Ranked second in 2020 and fifth in 2019, artificial intelligence jumped to the No. 1 spot in 2021 as this trend was perceived as the trend that would ultimately drive most technology advances in coming years. It remains there for the 2022 report.

TAKEAWAYS

AI is not universally defined, and AI is best viewed as specific subfields of development, ranging from computer vision to deep learning.

Development of AI-specific chips is propelling new advancements.

This Megatrend promises to influence every sector of security, from guards to drones to identifying solutions through big data processing – even validating device cybersecurity by providing comprehensive scenario testing.

MEGATREND 2

CYBERSECURITY

IN LAST YEAR'S REPORT AND IN YEARS PRIOR, we named this Megatrend the "Cybersecurity of Physical Security," but we're expanding the perspective further. Maybe it was the Colonial Pipeline attack that led millions of Americans to experience fuel shortages – or other prominent ransomware attacks on companies like Acer, Brenntag, JBS Foods and even Kaseya. But our industry's concern isn't just with the cybersecurity of physical security; it's at least with cybersecurity of operational technology (OT), but truthfully, it's a concern with cybersecurity in general, because the attack vector may not always be an access control server or a security camera; it could be your own corporate servers or a piece of network infrastructure you added to build a client's security network. And what's more, while the AI megatrend may be the shiny new object that holds future promise, the cybersecurity megatrend is that nagging worry that no matter how good you are, if you make just one mistake, everything you built could be exploited for ill.

But cheer up, because awareness of cybersecurity has changed dramatically within the industry, and there are indications that many buyers – at least those with strong IT and cybersecurity focuses themselves – are asking the right questions to validate a company's cybersecurity approaches and are simultaneously willing to pay a premium for products that offer better protection.

PERSPECTIVES

"The threat landscape is evolving at an equal, if not faster pace than technology. And it's essential that companies implement best practices with respect to cybersecurity solutions in their ecosystems."

– Bhuvana Badrinathan, CIO, Convergint

"We make locks, and our expertise is with that mechanical lock and making sure that people don't get in. Now that lock is connected, our expertise has to be with cyber as well and the firmware that goes in there. I think it [cybersecurity] is going to be the ticket to play going forward. If you want to be connected, you're going to have to have a secure infrastructure or else people won't trust you."

– Luis Orbegoso, SVP & President, Americas, Allegion

"We have hundreds of some of the leading security researchers in the world, working on our platforms. We challenge them to try to break our own platform. We try to find security vulnerabilities that no one else in the world has found. And by doing that research first, when we find them, we fix those issues whether they're on our future products or even on our existing products that are out in customers' hands. We invest significantly to stay ahead of the people that are trying to do harm to the platforms. But we not only do that, we then need to work with our partners and the ecosystem to validate the fixes, to make sure that they work as they're supposed to work, and that they don't cause other damage."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

"I call it social accountability. Even if you don't have a CISO, I think it trickles down to all the employees in your enterprise. You have to start training everyone to realize that they're not only affecting themselves, but they are affecting the entire enterprise. It trickles down to the rest of the employees to empower them to say, 'Hey, look, you are ultimately responsible for any theft or any compromises or any problem that is coming from whatever you're doing.'"

– Min Kyriannis, CEO, Amyna Systems

ATTACKS TARGETING OT

Many cybersecurity analysts say that the new field of attack is OT, and attackers often pursue a strategy of ransomware on these critical systems, as the Colonial Pipeline incident of 2021 evidenced.

Why? As Genetec's principal security architect, Mathieu Chevalier, explained during SNG 2021, "OT is generally less mature from a cybersecurity perspective compared to other IT systems that we're using… Maybe you have legacy systems. Maybe they are hard to patch. Maybe the availability is super important, so you don't want them to go down, and you might not have a failover strategy."

> **"One way to defend legacy systems** is a defense-in-depth strategy that layers multiple protections to mitigate exposure."
>
> *– Wayne Dorris, Cybersecurity Business Development Manager, Axis Communications*

Wayne Dorris, cybersecurity business development manager for Axis Communications, says the problem is especially relevant in the world of interconnected building systems, where products may be installed for "7, 10, 20, even 30 years." These legacy OT systems often don't match up with typical IT considerations, and it makes it even more challenging for the responsible team – the customer, integrator and manufacturer/solution provider – to ensure that these solutions are continually sustained from a cybersecurity standpoint.

Chevalier says short of replacing old systems, one way to defend legacy systems that can't be brought up to today's cybersecurity protections is a defense-in-depth strategy that layers multiple protections to mitigate exposure of these older platforms.

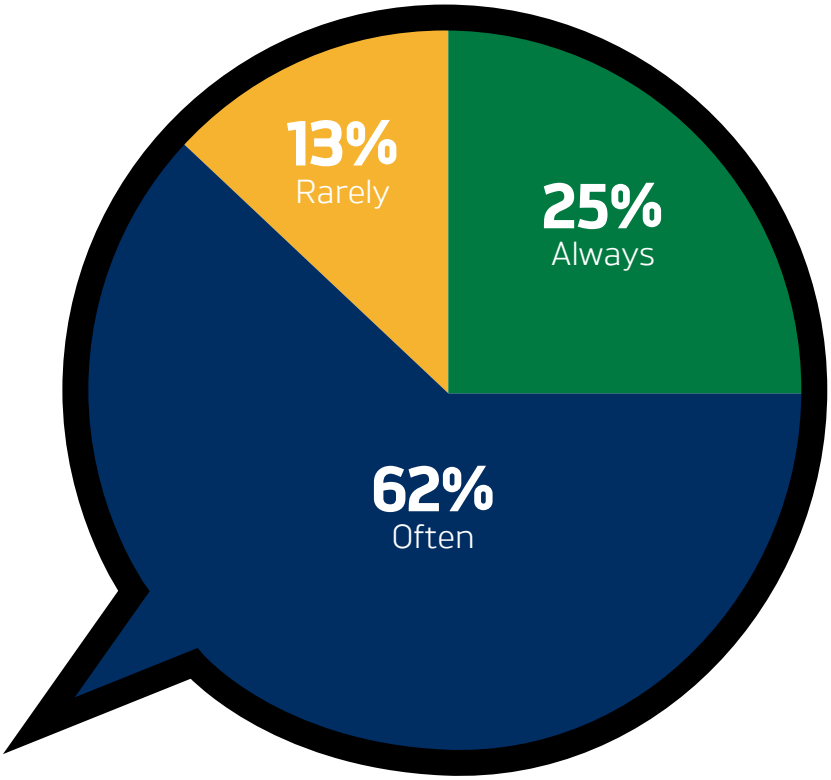
INTEROPERABLE RISK

With increased interoperability (Megatrend #6 for 2022) comes an expanded attack surface. As companies use APIs to bring in additional data sources or integrate with other platforms and software, the challenge of vetting those services intensifies, and solution and integration providers will need to disclose those API-integrated services or date sources, or at least advise their customers of those connections.

SICC™ SECURITY INDUSTRY CYBERSECURITY CERTIFICATION

MORE TRAINING, LESS RISK

While many industry leaders note that the industry is still in dire need of cybersecurity training, particularly for field installers and technicians, there are indications that security technology companies are strongly investing in cybersecurity training for employees. Simultaneously, certifications like the Security Industry Cybersecurity Certification (SICC) developed by SIA with support from PSA Security Network and Security Specifiers are gaining a foothold in the industry, along with more broad-spectrum cybersecurity certifications from organizations like (ISC)^2.



SNG POLL

HOW OFTEN IS THE CYBERSECURITY OF PHYSICAL SECURITY SOLUTIONS/SERVICES A DISCUSSION WITH POTENTIAL CUSTOMERS AND END USERS?

Cybersecurity conversations are shifting, explains Mike Dunn, chief technology officer (CTO) of Prosegur USA. He notes that as ransomware and other cyberattacks on operational technology and IoT device systems have made more news, companies like his are no longer always having to bring up the cybersecurity topic or educate and remind customers of the need for a defense strategy for their physical security systems and other operational technologies. The conversation flipped, he said. "It shifted during the pandemic at some point with them saying, 'Please, what can you give us? What do you have for services? How can you help us and protect us?'"

The chart above reflects that shift. In our previous year of tracking this benchmark question, SIA found that 2% of respondents said cybersecurity was never a discussion point; today, zero respondents indicate that cybersecurity is ever not discussed during customer calls. While a year ago, cybersecurity discussions were "often" part of the conversation 52% of the time, today that frequency has increased to 62% of the time.

AI'S PROMISE FOR CYBERSECURITY VALIDATION

While AI-enabled systems, with their extensive access to data and high value for an organization, are a rich target for cyberattacks, AI itself also has the promise of being useful for cybersecurity validation.

"Security is not about testing whether a product works the way it's supposed to work," explained Intel's Garrison. "The way researchers break platforms is they do things that they already know are not supposed to happen. And they wait to see what happens with the device. Does it fail in a certain way that maybe unlocks something that wasn't supposed to be unlocked?"

Unlike traditional cybersecurity testing, which relies upon human creativity and effort to test the cybersecurity of a device, Garrison said AI can help with validation by rapidly performing nonsensical tests that humans would not have thought of or would not have had time to test.

83%

Percentage of organizations which suffered an operational technology (OT) cybersecurity breach in the 36 months prior to November 2021

73%

Percentage of CIOs and CISOs who are "highly confident" they will not suffer an OT breach in the next 12 months

Source: Skybox Security research

MEGATREND MOVEMENT

Cybersecurity was ranked No. 1 in 2020, then slipped to No. 2 for 2021 as AI claimed the top slot. For 2022, it holds steady, indicative that cybersecurity is not something that you can ever forget about.

TAKEAWAYS

Attacks targeting operational technology (OT) are increasing.

OT systems are ripe for attack both for their business impact and because such systems are less likely to be updated, patched and refreshed at the rate of typical IT platforms.

Industry needs to retain its commitment to cybersecurity training for field workers.

MEGATREND 3

SUPPLY CHAIN ASSURANCE

THERE ARE TWO TYPES OF SUPPLY CHAIN CONCERNS shaping the industry's future.

The first is a logistics challenge – the ability to obtain source components, raw materials and even finished products. The disruption lies in many places. Temporary shutdowns for some manufacturing operations led to cascading shortages when the economy rebounded faster than anyone could predict. Complicating the situation are labor shortages that affect the entire supply, from manufacturing through shipping and distribution, to even the labor necessary to install products if you can get them.

And there's no indication that all these problems will just unravel as quickly as they formed. Inside the industry, executives are cautious to hope for any complete resolution to the logistics delays before the end of 2022, and supply chain strategists outside the industry, like Manish Sharma, group chief executive of operations services at the consulting firm Accenture, have said "Our findings indicate the disruption could be for up to three years" (New York Times, Nov. 29, 2021).

The second supply chain concern, some say, may be even more important, and it's closely related to our #2 Megatrend of cybersecurity. The concern is the ability to put full trust in the source code, firmware, system-on-chip and other hackable elements that exist with any product or solution. As addressed in the 2021 Securing New Ground keynote by Intel's Tom Garrison, the challenge today is to build transparency and traceability of the code and subcomponents of any solution, so that the end customer can trust that the installed device, software or solution is precisely what they expected.

Thus the 2022 SIA Security Megatrend of "supply chain assurance" is a blended trend that mixes logistics with cybersecurity, and the industry is paying more attention to this trend than ever before, as indicated by its first time being ranked among the industry's megatrends.

PERSPECTIVES

"The more control you have over your own supply chain, the better."

– Scott Paul, President, Alliance for American Manufacturing

"B2B industries are way behind all the consumer product companies, so we're basically fighting for the scraps [in the supply chain]. It's a struggle. I'd love to tell everyone that 2022 is going to be great, but I think you're going to see some struggles throughout the year, and there might be some light at the end of the tunnel, but I don't think so for another 12 months, unfortunately."

– Tom Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"Supply chain is the next frontier from a security standpoint."

– Tom Garrison, VP & GM, Client Security Strategy and Initiatives, Intel Corporation

DIGITAL DNA

In his keynote at Securing New Ground, Intel's Tom Garrison shared the firm's vision for the "Digital DNA" of a device.

"What we mean, quite simply, is you should understand everything about the device. If you think about something like human DNA, today we can track people's relatives and ancestors back hundreds and in some cases thousands of years. So, why can't we apply the same sort of thinking about our technology devices and be able to track back and trace back the components of the devices? And are these devices in a trusted state or not?"

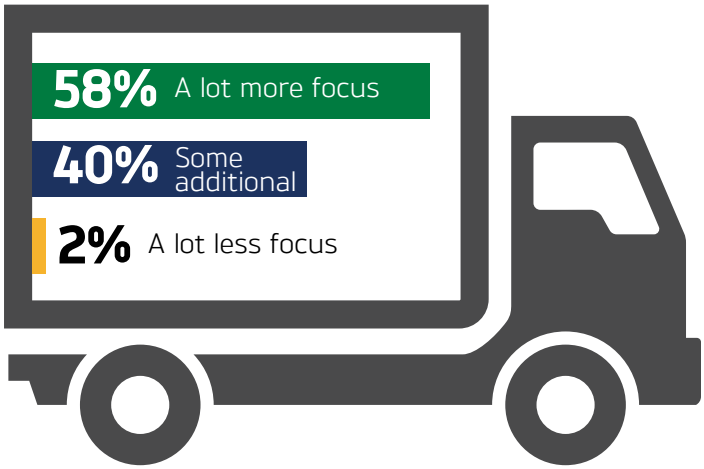
For Intel, that information will be stored on the device and protected with a cryptographic key that is individual to each device.

"We're capturing all the specific components that were built for that specific device," explained Garrison. "We're signing it with that specific endorsement key, which is unique for that platform. And by signing that information, then we can store that information in the cloud. As the device now moves its way through the transportation chain, ultimately to your site or to the end customer site, then the device can now be pulled or tested to say has anything changed in that device from when it was built? Because we can test there, locally. We compare it to the results we had when we first built it, and we say, has anything changed? If it has, we alert the user or IT and they can make a decision how to proceed or not."

SNG POLL

ARE YOU PLACING MORE FOCUS ON YOUR SUPPLY CHAIN TODAY VERSUS 2 YEARS AGO (PRE-PANDEMIC)?

Call it the "chart of no surprise," but 98% of companies in the industry have invested more time and focus on their supply chain than they did pre-pandemic, with more than half saying they're giving their supply chain "a lot more focus." In surveys of the SIA membership conducted in October and November 2021, supply chain was among the top concerns of executive respondents.



94% Fortune 1000 companies seeing supply chain disruptions from COVID-19

Source: Accenture

58% SNG attendees who said that supply chain delays is the factor most likely to negatively impact their business this year

Source: SIA, SNG 2021 research

MEGATREND MOVEMENT

A new megatrend for 2022, the supply chain has been a consistent immediate concern for SIA members in recent surveys and conversations. And while the microchips will someday be back in stock, the real lesson here is that your supply chain can never be taken for granted.

TAKEAWAYS

Supply chain delays are expected to continue throughout 2022.

Supply chain assurance has a direct relationship to cybersecurity in terms of the trust of subcomponents and code provided by outside parties.

The challenge for supply chain is to provide transparency and traceability.

Even companies that don't sell hardware, such as VMS providers, are facing challenges because the installation and integration of their software requires servers, cameras and other hardware as part of the systems.

MEGATREND 4

SERVICE MODELS AND THE CLOUD

THE "MOVE TO SERVICE MODELS" and "cloud computing" have long been included in SIA's annual Security Megatrends report as separate trends, but for 2022, based on input from survey data and commentary during Securing New Ground, we're officially connecting these two megatrends.

"The move to service models has been kind of concomitant with the move to the cloud," explains Steve Van Till, Brivo's president, "but really it [service models] is a business concept as opposed to a technical concept [cloud computing]." The fortunes of these two trends have often been tied together, and one way many firms have been able to move to as-a-service/recurring revenue models has been by delivering solutions in the cloud.

Today, this is a trend that nearly all companies in the industry are exploring, and it's becoming uncommon to see a startup company launch without a subscription delivery model and some element of the cloud, whether it's a solution delivered entirely via the cloud or whether the system uses the cloud for some processing or storage.

PERSPECTIVES

"I basically say, 'Listen, you're talking about owning and renting. You have a car; you either own the car or you lease the car.' So that's the only thing we're changing on you is that you're now leasing a product that's at your site, whether it's an NVR, DVR or a camera in our video world. And you're going to pay for that on a monthly basis or a yearly basis, instead of buying it one time, so it's OPEX versus CAPEX. And again, do I want to lease the car or do I want to own a car and deal with the maintenance? And that's typically what an IT guy understands. It's the security people that grew up in the industry [before service models]; they're the ones that are confused about [this change to a service/leasing model]."

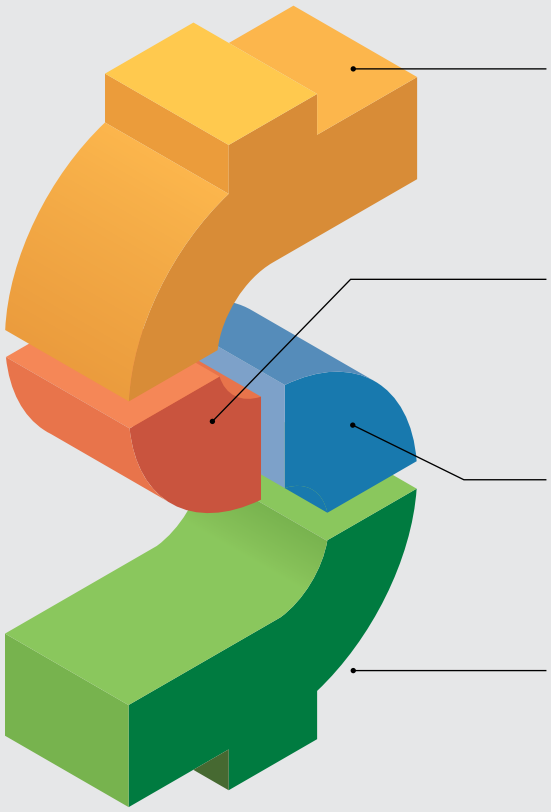
– Tom Cook, Executive Vice President of Sales & Operations, Hanwha Techwin America

"There are clearly much higher valuations for companies with recurring revenue models. Witness that security integrators with mostly one-time install revenue will trade for 0.5 - 1.5x revenue while recurring-revenue-focused alarm companies will trade for 3 - 5x annual recurring revenue or ARR. And then in the high technology SaaS businesses which are heavily recurring revenue focused, you can see revenue multiples of over 10x."

– John Mack III, EVP, Imperial Capital

SERVICE MODELS AND COMPANY VALUATIONS

Imperial Capital's John Mack III says the key variables for recurring revenue businesses to trade at higher multiples include the following attributes:



1. **Reasonable investment level to create new customers.**
   "In the alarm industry this is called 'creation cost.' In the SaaS world, this is measured with a metric known as LTV/CAC, long-term value creation/customer acquisition cost."

2. **Good gross margins for the recurring services.**
   "Typically, at least 60% but more like 70%+ and for the high technology SaaS businesses, in many cases 80%+."

3. **Low attrition (10% or less) or high retention (90% or better).**
   "In many cases, with new services sold to existing customers there is net growth in recurring revenue or net retention over 100%."

4. **High growth rates.**
   "Rates of at least 10%+ in recurring revenue per year and for the high valuations growth, rates in the 25%+ range or much higher."

MEGATREND 4 SERVICE MODELS *(continued)*

AS-A-SERVICE MODELS, NOT JUST SERVICE AGREEMENTS

Service models do not equal service agreements stresses PSA Security Network CEO Matt Barnette. Typically service agreements were a small addition on top of a one-time project-based fee. And while service agreements are a step in the right direction for integration companies looking to transition to a recurring revenue model, the real change comes when the former project-based fee is transformed into a recurring charge.

BETTER FOR BUSINESS

At SNG, Luis Orbegoso (who today leads Allegion in the Americas) tells the story of when he worked at ADT and the company made the switch to the cloud for delivering video solutions: "We actually stopped selling DVRs for the most part; [we] put all the video in the cloud. [It] drove a huge amount of retention. It was a better business model. It was easier to sell because it was less of a capital expenditure."

UPTIME, EVEN DURING BAD TIMES

As the COVID-19 pandemic sent workers home, it sent company CTOs scrambling to ensure systems remained available, whether the worker was in a cubicle on office floor 7 or working from their dining room table or a corner of their bedroom. Cloud solutions naturally exploded in popularity.

GENERATIONAL CHANGE TO RMR

Chris Meiter, president of Salient Systems, tells the story of changing from perpetual licensing to a subscription model.

"We're seeing a major transition from what we classify as the perpetual licensing agreement, to a subscription-based model," said Meiter. "The customer sees the value of the upgrades and things that come with that subscription model on an annual basis. But as we first rolled this out, we actually had some pushback by some of our integrators that were like, 'Hey, I've been selling perpetual, and we don't see the value in subscription-based.' It was literally this one company, a 50-year-old company, which had been selling perpetual licenses forever.And that was the first generation of the company speaking to us, but all of a sudden, the second generation says, 'Hey, wait. We want to build the value of this company. We want to have more equity value in this company. You can't do it just with a one-and-done sale. You need to do it with a recurring model.' And they ran that through their CFO and they could double- or triple-increase their company's value within two years by moving from perpetual licensing to subscription-based software. So, the message is getting out there and they're seeing the value."

50%
Percentage of corporate data now store in the cloud

Source: Statista

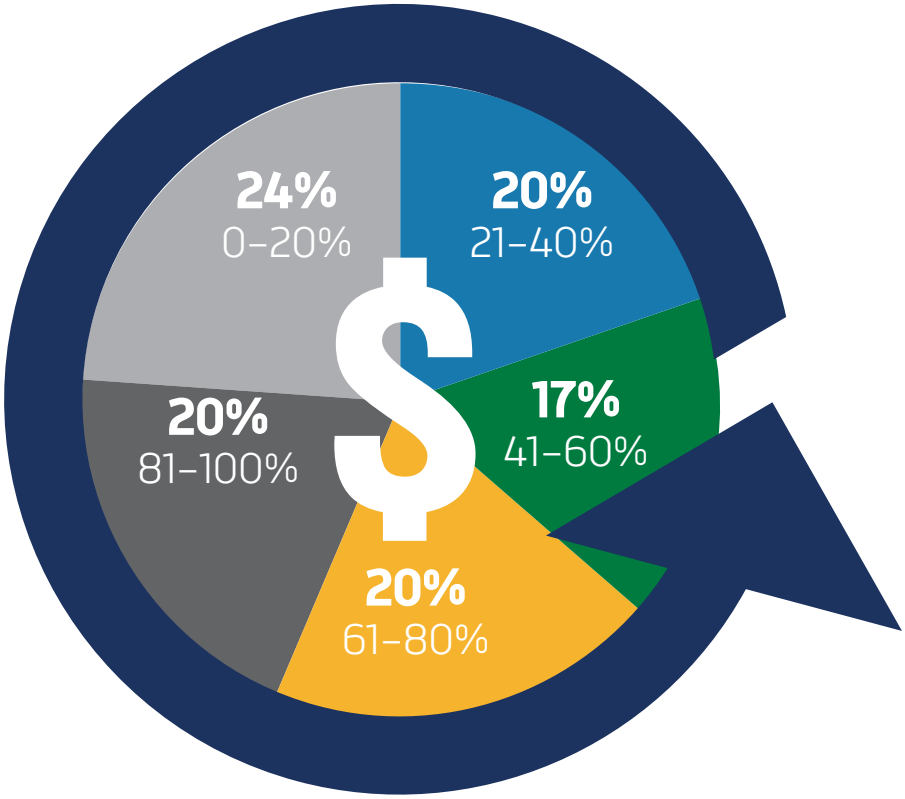
98%
Percentage of companies that had at least one cloud data breach in the past 18 months

Source: IDC

SNG POLL

WHAT PERCENTAGE OF YOUR FIRM'S TOTAL REVENUE IS FROM RECURRING REVENUE?

Business models continue to shift. A year ago, over a third of respondents said that less than 20% of their firm's total revenues were attributed to recurring revenue. A year later, that number had decreased to less than a quarter of respondents, indicating that companies were steadily transforming their business revenue from one-off sales to recurring, as-a-service income streams.



MEGATREND MOVEMENT

A long popular Megatrend, the move to service models had ranked #5 in 2017 and 2018, falling to #7 in 2019, #9 in 2020 and #10 in the 2021 report. Meanwhile, cloud computing had seen its ranking steadily climb, but the jump into the #4 position for 2022 reflects both the effect of the pandemic and conjoining of what were previously two separate megatrends.

TAKEAWAYS

Investors, equity firms and even companies making acquisitions continue to deliver higher valuations to companies which are heavily invested in cloud services and recurring revenue.

Companies with software services or access to data services can make the cloud and recurring revenue business model transition easier than hardware-only type companies.

Security end users requests for anywhere, anytime access to security solutions will further advance cloud adoption.

Many formerly "on-prem" software-and-server based security solutions now are configured to run on common cloud infrastructure platforms from firms like Amazon Web Services, Google and Microsoft.

MEGATREND 5

WORKFORCE DEVELOPMENT

IN BOTH THE SURVEY RESEARCH done for this year's Security Megatrends report and in the fall 2021 SIA Membership Survey, it was clear that one of the biggest pain points to security industry leaders and companies of all type in the industry is the ability to find the talent they need. Members said it was a broad-spectrum problem, impacting manufacturing, software development and sometimes sales. But consistently, the biggest area of pain was from integrators who were challenged to find competent installers and technicians.

That inability for integrators to find the workforce they need has a snowball effect on the industry; it limits these companies' ability to install products and complete customer job requests, which in turn can affect the security of their clients' site, and it creates a bottleneck on potential sales for every company in the security technology business ecosystem, particularly the manufacturers, solutions developers and distributors which depend on sales and project completions by the integrator channel.

The industry is also plagued by the ongoing global shortage in cybersecurity workers, which puts the cyber protection of physical security solutions at risk, and many of SIA's members have voiced the challenge of hiring competent software and application developers, too. Unfortunately, the problem of not enough technical workers – be they developers, technicians or cyber pros – isn't likely to be solved easily, as the industry is one of many competing

for workers with these skills. And the shortage is affecting the potential growth for high-tech companies – a September 2021 Gartner study found that 64% of IT executives see the talent shortage as the most significant adoption barrier to emerging technologies.

And it's not just technical talent that's causing security industry challenges. Shortages of guards are commonplace among guard services companies and corporate security teams, and shortages in non-security industries like shipping, trucking and distribution are impacting the supply chain that industry firms depend upon.

PERSPECTIVES

"I've been through lots of different economic cycles. And what I'd say is in 2019 when we had really low unemployment – some cities across the country had 2 or 3% unemployment – it was hard to find people, but you could find people. Today, it is the most dysfunctional labor market I've ever seen."

– Steve Jones, Global Chairman and CEO, Allied Universal

"The issue is labor, and I think that's really going to hit us, not only in terms of us being able to find people to install, but people to manufacture. There's a huge labor gap right now that we're experiencing and we just can't get people in fast enough."

– Luis Orbegoso, SVP and President, Americas, Allegion

TECHNOLOGY SOLVING THE WORKFORCE CHALLENGE?

As Fredrik Nilsson noted to 2021 SNG attendees, "80% of the spending in the security industry today is manual labor That means guards, monitoring or even installation services." But Nilsson noted, "That will change." As automation and AI begin to replace manual work by some humans (even Allied Universal CEO Steve Jones noted that some of the corporate security data interpretation that formerly required human input is now being handled algorithmically), technology may lessen the dependency upon human workers, but no one expects those technologies to solve the workforce shortage problem quickly.

GREAT RESIGNATION

The much-touted "Great Resignation" of 2021, which left nearly 11 million jobs unfilled, was most impactful in the areas of technology and health care according to research published in the Harvard Business Review, with technology work resignations increasing by 4.5%.

Complicating the resignation trend and the overall workforce shortage is the fact that average salary increases were not expected to match 2021's inflation rates, according to the Society for Human Resource Management (SHRM).

And even as SHRM found pay rates that weren't keeping up with inflation, ADP Research Institute's data indicated that the average wage growth of someone who switched jobs in Q3 2021 was 6.6% – and that means workers are likely to continue to resign in favor of better-paying opportunities.

CONSEQUENCES OF CYBERSECURITY STAFF SHORTAGE

32% Misconfigured systems

30% Not enough time for proper risk assessment and management

29% Slow to patch critical systems

28% Oversights in process

27% Inability to remain aware of all

27% Rushed

Source: (ISC)² Cybersecurity Workforce Study (2021)

37% Percentage of SNG poll respondents who said that worker shortages would be the factor most likely to impact their business' ability to grow in 2022

60% Percentage of (ISC)² study participants in 2021 who indicated that a cybersecurity staffing shortage is placing their organization at risk

MEGATREND MOVEMENT

Workforce development last appeared in the 2020 Security Megatrends report, coming off 2019's extremely low unemployment rates. But amid the pandemic, as companies initially laid off workers and were challenged to put workers on customer sites, the issue briefly subsided and was temporarily removed from the Megatrends. For the 2022 report, workforce development came roaring back, as companies struggled to find installers and as labor shortages struck the entire supply chain.

TAKEAWAYS

FAST Foundation for Advancing Security Talent

Despite the enormity of the problem, moves are underway through organizations like the Foundation for Advancing Security Talent to spread the word of the industry's opportunities.

Labor and talent shortages are driving supply chain issues and even inflation in some sectors.

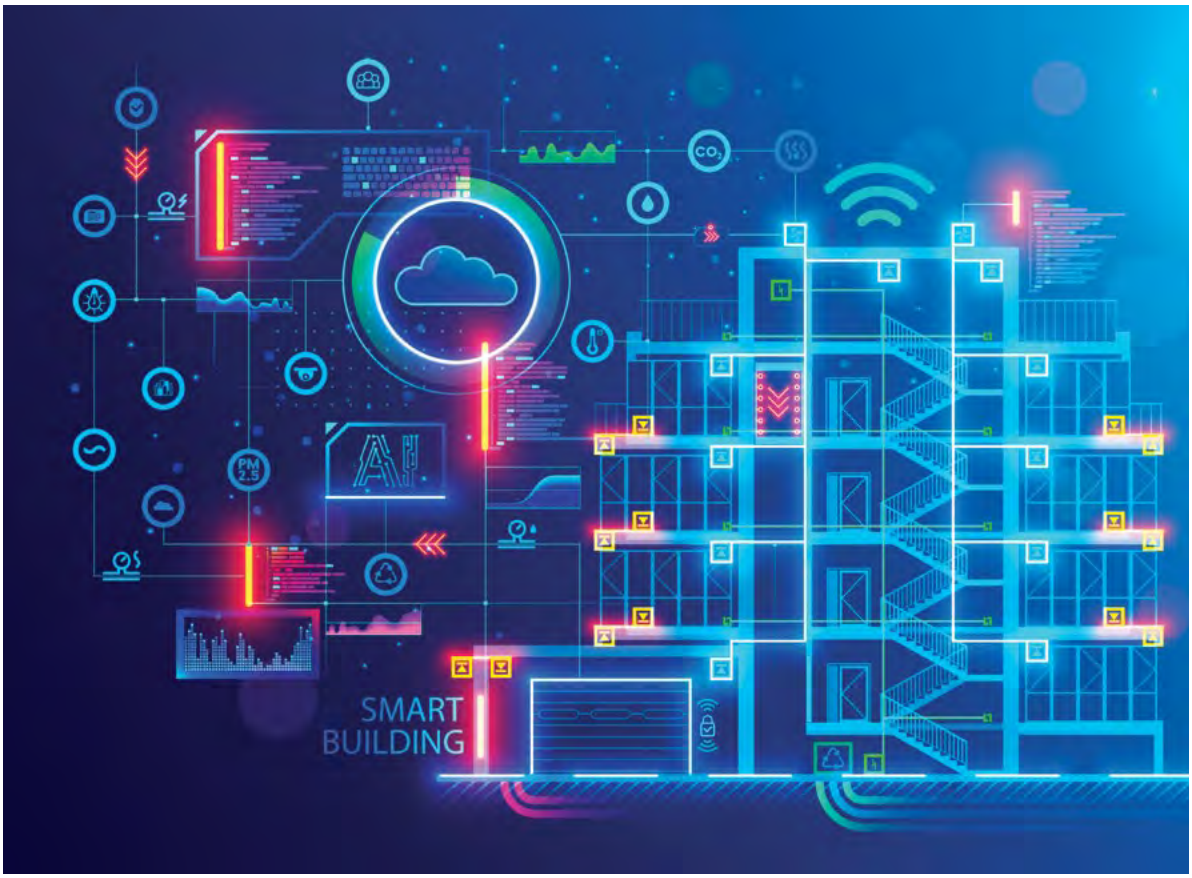
Promoting the industry as being open a diverse workforce can remove self-limiting hiring challenges.

Wage and benefits are likely to rise as companies compete for scarce talent.

Eventually, automation in some technology areas may reduce dependency on human workers.

MEGATREND 6

INCREASED INTEROPERABILITY



ASIDE FROM THOSE MANAGED by major corporate, institutional and government security users, the number of individual security systems that are integrated in the industry (such as between video and access control, or between the video system and the intrusion system) is still surprisingly low according to many systems integrators and manufacturers. That low rate of interconnectedness is changing, however, as more systems become open and as customers demand business operational insights and efficiencies that can only be determined by correlating data from multiple systems.

In the building environment, as in the security environment, the overall trend has been toward open systems or the use of common protocols that can allow communication between otherwise closed systems. With increased use of wireless technologies in the built environment and the network connected status of most control systems, advancing interoperability becomes more approachable, driving not only interconnected security platforms, but connecting security with other business systems.

THE INTEROPERABLE BUILDING

The common platforms integrated in a "smart building" type of environment include

- HVAC
- Security video
- Building access control
- Intrusion alarm systems
- Lighting
- Fire detection systems
- Mass notification systems
- Electrical power
- Elevator controls
- Parking controls

PERSPECTIVES

"Everyone wants to connect, and they want to be interconnected immediately, like yesterday."

– Michael McNeil, Chief Information Security Officer (CISO), McKesson Corporation

"We don't want things siloed separately. That doesn't really give us a clear picture of what we're dealing with. If we bring all these things together, and we've got our cameras, we've got our access control, we've got all of our monitoring technology, then we can tell what's happening at any given point in time in the airport. And that information is coming to us and we're not having to wait, or listen, or see, someone monitoring a screen all the time, or watching for an alarm to come to us."

– Megan Atkins Thoben, A.A.E., Director of Operations and Business Development, Louisville Regional Airport Authority

"Our buildings cost millions or even billions of dollars. They have the latest technology. But they don't know how many people are in them. They don't know when to turn the lights off or learn when to start warming or cooling office or meeting space. They don't reposition elevators for maximum efficiency, and they can't tell first responders where the fire is, where the medical emergency is, or what the quickest route up is. Nor can they tell occupants that the air is clean today, or that there's an elevated level of volatile organic compounds because the floors were just waxed yesterday."

– Journalist and author John Koetsier, writing for Forbes

"When you think about how you step into a building and the ecosystem that sits inside the building, whether that's the elevator system or the turnstile system or the visitor management system and the tenant amenity system platforms, we have to be able to be open in our ability to connect to all of those systems, to integrate with them, to be fully functioning inside that building. And every ecosystem will be different. And so, if you're closed off such that you cannot accommodate those, then your system will not work."

– Haniel Lynn, CEO, Kastle Systems

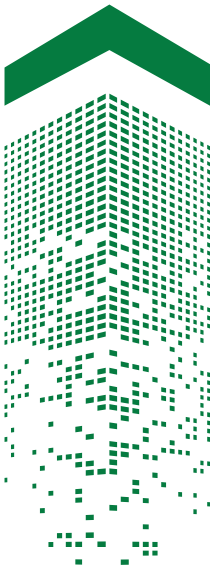
MORE BENEFITS, MORE RISK

One of the great clamors for interoperability is connecting physical security and IT systems with legacy operational technology and building systems. While McKesson Corporation CISO Michael McNeil says the demand for connection with these systems is high, it means more risk, because "most of those technologies in those types of environments are probably based on code that originally started back in the '80s."

$108B

Predicted 2030 global market value of the smart buildings IoT endpoint electronics and communications market, up from $55 billion in 2020

Source: Gartner Research



MEGATREND MOVEMENT

Increased interoperability as a singular trend may be new for the 2022 report, but it's not new to the industry. Retired from the 2022 Megatrend report were "Connectivity and the IoT of Everything" (trend #4 in 2021) and "Responsive Environments and Intelligent Spaces" (trend #8 in 2021), and both of these previous megatrends related to interoperability, whether among devices or systems.

TAKEAWAYS

Increased interoperability will require more standardization so that integration work does not require bespoke coding in most situations.

Connecting legacy building systems and OT systems brings increased risk due to legacy code bases of such systems.

Tremendous opportunity exists to simply connect disparate security systems, surprisingly few of which are commonly integrated.

MEGATREND 7

DATA PRIVACY

THE MEGATREND IS DATA PRIVACY, but underlying this trend is an overall increase of interest in individual privacy, particularly related to the public's concerns about how their data is being used and how they personally are being tracked, be it by security platforms, social media tools or even government systems.

The security industry, of course, is particularly relevant in that this industry's systems are often built to record data. Want to know who was in the building last night when the property was stolen? That's why video and access control systems exist. But with that power to collect data comes increased responsibility, and data can't simply be vacuumed up without processes and policies in place – particularly if it's data that captures individuals in environments within which they have a right to expect privacy.

This megatrend is being closely followed by legislators and regulators, and there are indications that data privacy will be more regulated by government in the future, with even some U.S. states considering or enacting their own legislation.

PERSPECTIVES

"[There is] entanglement of cyber and privacy as you can't have privacy unless you've got a secured container for all the PII. And if you're not guarding privacy, then what can you really say about the cybersecurity of your organization or your product?"

– Steve Van Till, President, Brivo

"Depending on where I have a camera, if I'm using it in a hospital or if I'm using it in a different environment, that could be considered privacy data as well. So, it's incumbent upon understanding where you're putting the product or device, what data it's generating and whether you've classified that and are saying yes, I consider this private data or privacy data, and I have to encrypt and also do things to protect it."

– Wayne Dorris, Cybersecurity Business Development Manager, Axis Communications

FIVE QUESTIONS TO ASK

1. Is it necessary to collect this information?
2. If yes, where should it be stored?
3. Who should have access to it and when?
4. Should this data ever be shared and why?
5. How long should the data be retained and how should it be safely disposed of?

For more prescriptive guidance, see SIA's guide to data privacy, "Putting Privacy Into Practice."

BREACHING NEW HEIGHTS

Loss of data privacy isn't always due to cybersecurity breaches but controlling data breaches is one way to protect your customers' data privacy. Unfortunately, according to the Identity Theft Resource Center, the number of publicly reported breaches that had been reported in the first three quarters of 2021 exceeded the total number of publicly reported breaches for the full year 2020.

GUIDING PRINCIPLES

Some 21 years ago, before data privacy was even in the lexicon of the security industry and long before GDPR was drafted or enacted, Richard Purcell was serving as the chief privacy officer for Microsoft, and in an article for Harvard Business Review, he set forth five guiding ethical principles for data privacy:

Notice: "Customers should receive full disclosure of who is collecting information about them, what is being collected, and for what purpose."

Choice: "Individuals should be allowed to choose how information will be used about them, how long that information will be retained, under what circumstances that information would be transferred to other parties, and so on.

Access: "We have to establish transparency by enabling customers to view, and even edit, the information we have so they can make sure it's accurate and relevant."

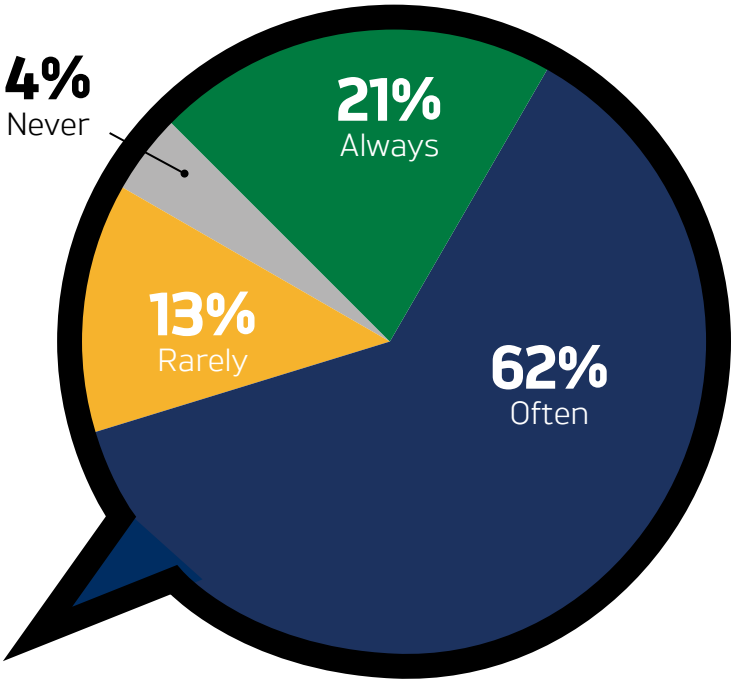
Security: "We must ensure that a customer's data are protected from unauthorized access, distribution, loss, or corruption."

Enforcement: "Some mechanism that will hold us accountable for complying with any stated policies. Third parties should be involved in maintaining that compliance."

SNG POLL

HOW OFTEN IS DATA PRIVACY A DISCUSSION WITH POTENTIAL CUSTOMERS AND END USERS?

Data privacy conversations are occurring, but are they prevalent enough? A year ago, when we asked this same question, only 53% said that they "often" had these conversations with customers. Unfortunately, the growth in those conversations "often" occurring may be coming at the expense of those who previously said they "always" had such conversations, with that number dipping from 33% in the 2021 report to just 21% today.



MEGATREND MOVEMENT

Data privacy first appeared in the Security Megatrends in 2019 (ranked #6) and has stayed ranked continually since (#4 in 2020, #9 in 2021). This megatrend naturally links to technology trends like the adoption of facial recognition and other systems which can recognize and identify an individual.

TAKEAWAYS

Increased regulation and policy changes are likely to shape data privacy.

Companies need to define an individual or team that can develop and determine the company's data privacy policies.

Protection of private data requires a base layer of good cybersecurity.

MEGATREND 8

SECURITY AS PROPTECH

LOOSELY DEFINED, PROPTECH IS ANY TECHNOLOGY RELATED TO how buildings are managed or used, or even bought, sold or rented. And when it comes to how buildings are managed and used, security solutions – particularly building access control systems – are uniquely positioned to be one of the central data sources on building occupancy and usage efficiency. Security's position at the heart of the PropTech ecosystem is leading to renewed attention and increased valuations for security solutions companies that embrace the Proptech trend.

This megatrend, buzzword-laden as it may be, is about providing business insights for building owners, property managers and tenants. Security's mission changes from a role of preventing bad things to a mission of enablement: enabling great experiences for employees, enabling better property management, and enabling tenants and building owners to more efficiently use their space.

PERSPECTIVES

"[Security solutions] are the grandfather of all Proptech."

– Haniel Lynn, CEO, Kastle Systems

"The $100B Proptech revolution is providing a huge brand uplift for the security industry as more and more analysts appreciate that we are a foundational technology for the digital transformation of real estate."

– Steve Van Till, President and CEO, Brivo

"You're seeing changing expectations from building owners. It [security and building access control] was a utility and they wanted the cheapest solution that would last the longest without much maintenance. Today, the applications for that technology and the expectations of what they can do with that technology have changed."

– Lee Odess, General Manager of New Market Development, Latch

PROVIDING VALUE FOR OWNERS, MANAGERS AND TENANTS

Tenants, property managers and even building owners are finding direct value today from data coming out of the security systems, and the most referenced data is about occupancy. Tenants are using it to determine if they still need the same amount of space, or which office locations need more space or less space; owners and property managers are using it to track their financial performance and usage of shared tenant amenities. The data also is being connected to health conditions (see Megatrend 10).

Security solutions, chiefly access control, are also at the heart of the tenant experience. As a new wave of tenant experience platforms and apps have arrived from companies like Equiem, HqO and VTS, the one platform and app component that is always present is a connection to the access control system, because a great tenant experience starts with making sure the right people have the right access at the right time.

WHAT'S NEXT FOR SECURITY AS PROPTECH?

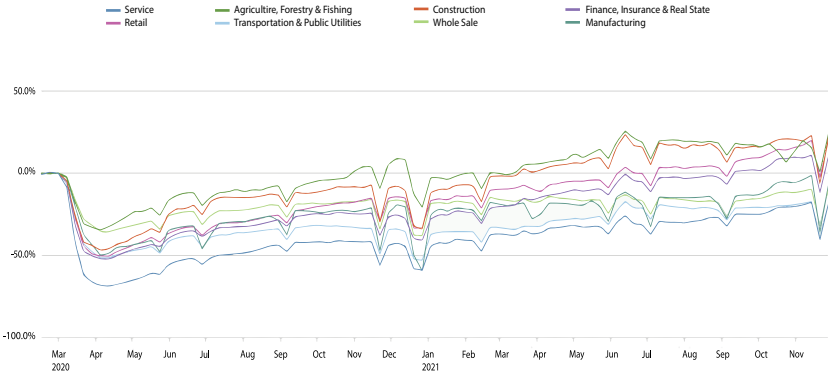
Experts expect more big-tech incursion, such as Apple's NFC credentials becoming a preferred identifying token. Third-party integrations will become even more common, particularly in the area of tenant experience apps. Data is likely to be aggregated across competing system providers and building operators to give urban planners more insights into how their cities are used. And on the business front, cloud-based access control companies may see higher valuations as they are seen fully as tech companies rather than purely security companies.

NOT JUST FOR A+

There's a common perception that Proptech is really just influential in Class A and A+ luxury office environments, but some property owners say that delivering Proptech solutions will make a Class B property tenant feel like they're receiving the Class A experience.

While initially viewed as a commercial real estate trend, Proptech is also providing data for multifamily residential properties like apartment complexes and condo towers, and at the individual residence level, Proptech is giving families insights into actions like a child arriving home from school, a package delivered or even status updates on home efficiency and comfort systems.

PERCENTAGE CHANGE IN DAILY ACTIVE USERS OF COMMERCIAL PROPERTIES BY INDUSTRY



Source: Brivo

$9.7B

Amount of new funding the Proptech sector attracted in the first half of 2021

Source: JLL 2021 Global Proptech Report

58%

Daily unique building access users compared to the pre-Covid daily average in February 2020 – an example of the level of data that access control solutions can provide.

Source: Brivo, data from Nov. 26, 2021

MEGATREND MOVEMENT

Newly ranked for 2022, this is nonetheless closely connected to the 2021 megatrend "Responsive Environments and Intelligent Space." This Proptech megatrend connects directly to the "Health & Sustainability" megatrend (Security Megatrend 10 for 2022), particularly as building owners and companies continue to navigate a return to the office.

TAKEAWAYS

Access control is at the heart of real estate property technology.

Security solutions companies, particularly those working in cloud-based access control, are seeing increased valuations and capitalization levels as the Proptech industry recognizes the value of such solutions beyond security.

The Proptech revolution and the approaches for how to use Proptech data are far from mature; new concepts for how to gain insights from Proptech data appear nearly daily, and industry players expect even more competition from big tech companies.

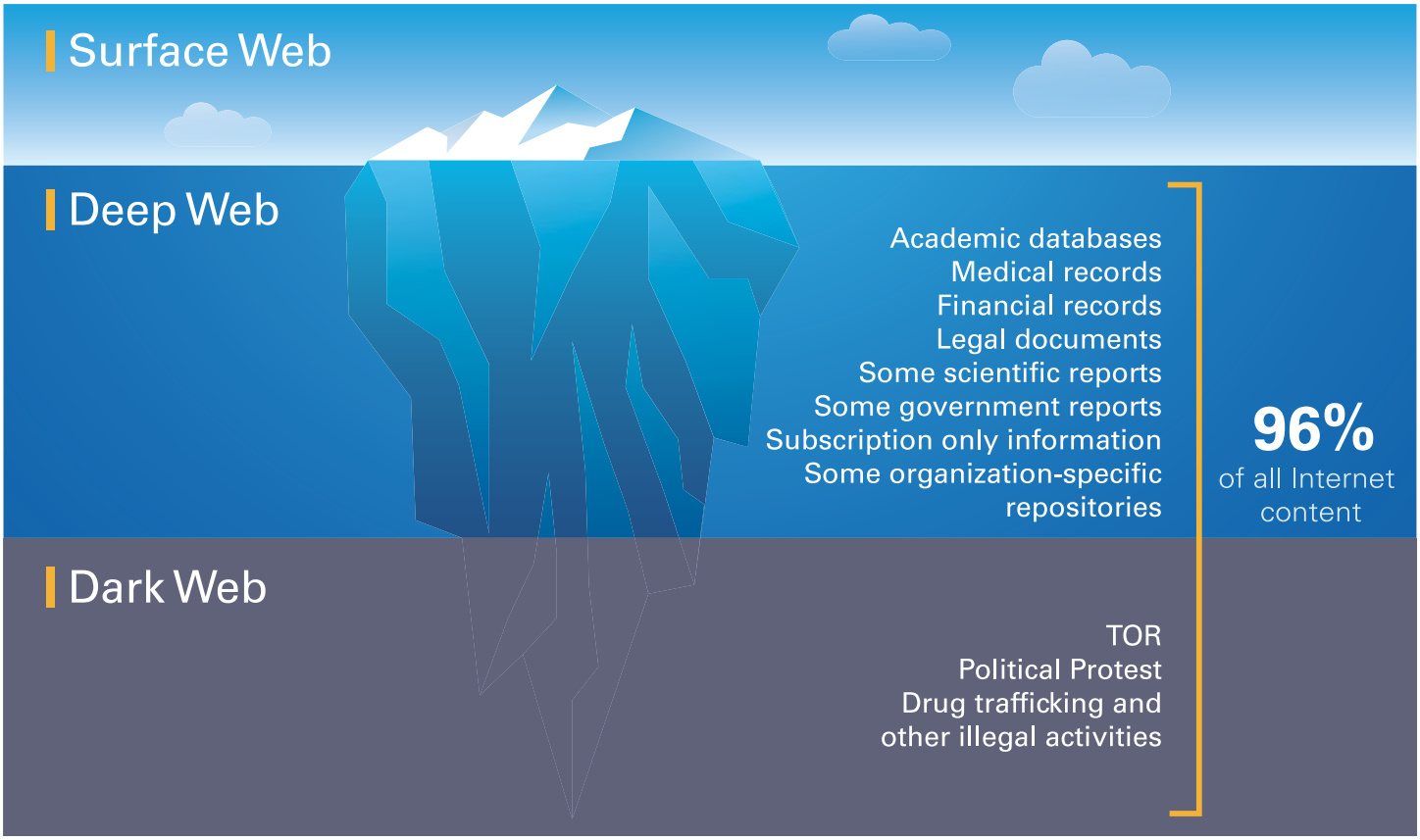
MEGATREND 9

EXPANDED INTELLIGENCE MONITORING

THE DATA YOUR CORPORATE SECURITY CLIENT WANTS is no longer limited to door alarms, card swipes and video footage. Chief security officers of the largest corporations today are seeking to mine intelligence from any public data sources that can give them an edge up in their security responses. Those intelligence sources could be social media feeds and posts that reference their brand or even their retail locations, but it's just as often public governmental data sources like U.S. Department of State informational feeds, weather data, international information related to disasters, terrorism and more. Beyond those public sources, companies are now scouring the dark web for potential threats, and all this information is now being processed and presented to savvy corporate security teams.

DEEPER AND DARKER

Expanding intelligence monitoring of public data sources on the surface web is already common, but companies and service providers are more regularly exploring reaches of the deep web and dark web to identify emerging threats or investigate stolen data.



MEGATREND MOVEMENT

Newly identified for 2022, this megatrend is as much a corporate security risk trend as it is a technological trend. It naturally relates to cybersecurity (No. 2) and data privacy (No. 7).

PERSPECTIVE

"On any one of these [social] channels, attackers might voice their intentions, spread false information concerning your organisation, or partake in more obscure but potentially equalling dangerous activities such as cyber-bullying or phishing. Because of the high number of users paired with the social nature of discussion, potential threats often emerge on these channels and forums first, even before they become a tangible risk."

– intelligence monitoring firm Signal

TAKEAWAYS

Corporate security leaders are looking to new intelligence sources to stay one step ahead of threats.

The dark web, where illicit data and content often resides, can be a resource for security executives seeking to understand emerging threats.

New firms are delivering intelligence-as-a-service, presenting the information in a coherent manner to security end users.

MEGATREND 10

HEALTH & SUSTAINABILITY

THE PANDEMIC LEFT AN INDELIBLE IMPRINT upon the security and safety industry, and while the initial response may have been to install security solutions that limited the need for touch or which could detect fevers, the conversation has expanded greatly from those early days. Our industry's role is the safety and security for people and places, so part of keeping people safe is being mindful of their health. And the second part of the conversation is whether these spaces and built environments able to sustain these occupants and if the components, devices and solutions going into these built environments are fundamentally sustainable themselves, including from an energy efficiency level. And by having these conversations and making these changes, can that make the security industry itself is more sustainable and thus more valuable?

INDUSTRY CONSIDERATIONS

- Contactless/touchless solutions
- Air quality and air control
- Detection of toxic chemicals
- Energy usage of all devices
- Minimization of material used in manufacturing and packaging
- Effect of entrances/door openings on building comfort and energy efficiency
- Interoperability with comfort systems (HVAC)
- Noise pollution
- Health-focused measurements: Contact tracing, occupant counting, mask wearing, social distancing

NOT JUST FOR COMMERCIAL

Research in 2020 by Parks Associates, and presented ESA and Resideo, indicates that consumer interest in health controls extends to the smart home, not just offices and business buildings. As the Parks Associates report notes, "The residential healthy home movement is an extension of the commercial green building movement."

PERSPECTIVES

"There's a lot of focus now on transparency and making sure that things that we're producing and that we're interacting with every day are healthy. We can provide not only sustainability goals in terms of how we make the things that we sell, but also what role they play in the building at large. For example, we want to reduce the amount of material in products. We want to reduce the amount of energy that they consume. And by doing that, it also has an outcome of positive effects in terms of delivery. If I am delivering smaller boxes that carry less weight, the carbon footprint is also reduced. And then of course, if I have openings that are more sustainably designed, that's going to reduce the amount of power; that's going to reduce the amount of emissions. It's going to have a really positive effect, even beyond the products that we make."

– Peter Boriskin, CTO, Americas, ASSA ABLOY

"As we started to see offices open up and employees coming in, whether it was full time or hybrid, we were seeing a greater involvement from real estate and workplace resources wanting to know how spaces were being utilized and the amount of time, for instance, people were congregating in a certain area, whether they were actually remaining at six foot distances from one another, and believe it or not, the amount of time they were standing versus seated."

– Henry Hoyne, CTO, Northland Controls

"We all want to minimize our carbon footprint and achieve that while now getting occupants back in a building safely with their heightened concerns."

– Joe Hudock, SVP Marketing and Sales Excellence, dormakaba

MEGATREND MOVEMENT

A new trend for the 2022 Security Megatrends report, Health & Sustainability is in some ways the evolution of the 2021 report's named trend of "touchless & frictionless solutions," which was ranked #6 in last year's report.

TAKEAWAYS

The COVID-19 pandemic created an awareness of how security solutions can be used to protect the health of employees, visitors and customers.

Leading manufacturers are considering the sustainability of the solutions they deliver, from how much energy they draw to even if devices can be made with less material or packaged more efficiently.

Driving increases in health and sustainability, particularly in building environments, will require expanded interoperability.

SECURITY INDUSTRY ASSOCIATION

8405 Colesville Rd.,
Suite 500
Silver Spring, MD 20910
301-804-4700
securityindustry.org

©2022, Security Industry Association. All rights reserved.

Lighting Trends in Electric Sign Manufacturing

Looking at the future of LED use in signage

I believe that to understand the future, you must look at the past. This is my 18th year developing products specifically for the electric sign industry, and there has been a tremendous change.

When I started developing LEDs for commercial signage in 2003, I made a statement to a newspaper reporter that neon was a dinosaur. I was subsequently lectured by a few sign makers and tube benders that I was way out over my skis and that this LED thing was a flash in the pan.

Today, end-users are looking to light everything up on or around their building.

Early LED systems were bare PCBs with wire in between. There were various voltages and power sources (everyone who has been around a while remembers the GE dip switches that set the voltage depending upon the color). As with most disruptive technologies, early systems were overpriced and underperforming; however, unlike their neon predecessor, they could adapt and create new form factors. LEDs stuck.

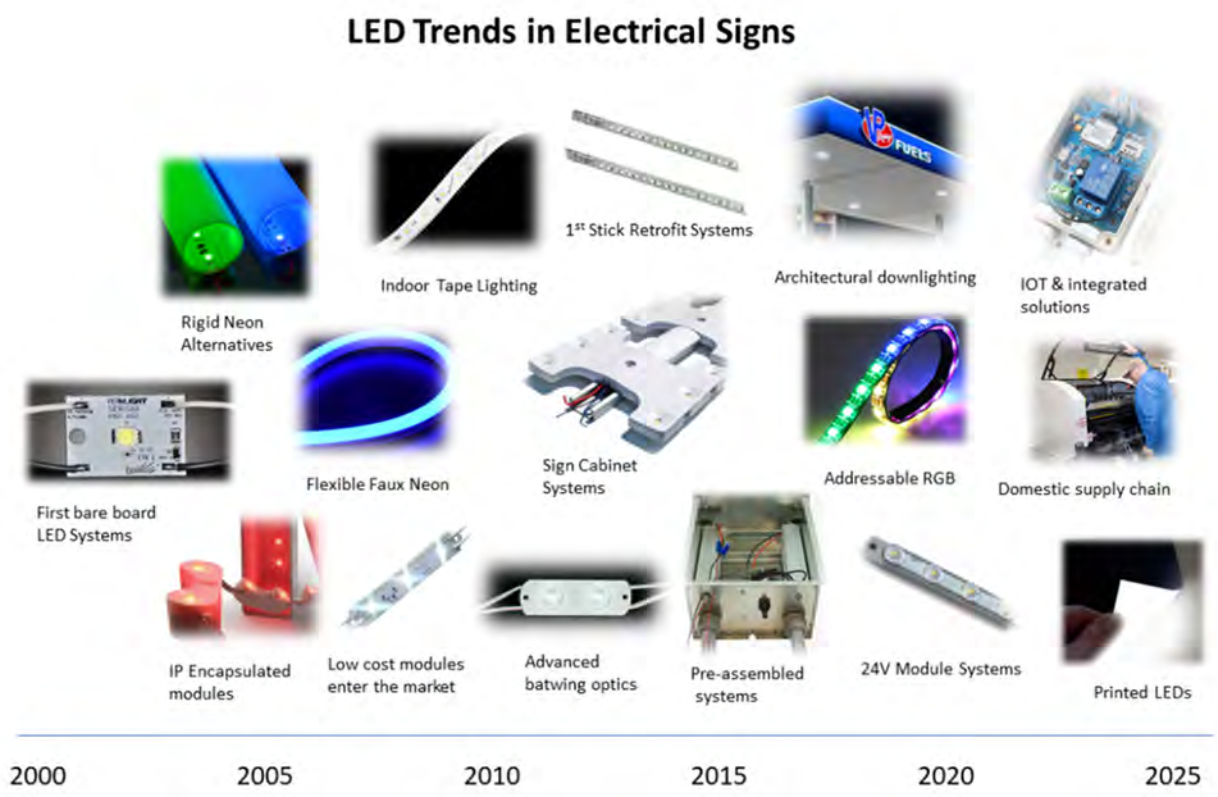
Early years

If you look back at the early years of LEDs in signs, the mission was simple: replace neon. Between 2000 and 2005, product development was focused on replacing the incumbent technology with modules in channel letters and rigid tubes in border applications. Between 2005 and 2010, flexible light tapes came onto the market to address needs in indoor signage, and flexible neon was developed as an alternative to exposed neon script. This second period really was around reducing costs, and around 2008, LEDs surpassed neon as the new lighting medium for the sign industry.

With LED manufacturers now in the pole position, they set their sights squarely on T-12 fluorescents, and again, everyone was skeptical. Just like during the heyday of LEDs in channel letters, there were a lot of systems out there for sign cabinets that varied from lattice to rail and module systems. What changed the cabinet market, particularly for sign retrofits, was when Principal LED came out with Stik that went straight into a socket. This product was preassembled in the USA, which allowed for a range of products "just in time" at a cost point that tipped the system. By the end of 2015, LEDs surpassed T-12 fluorescent lamps as the preferred technology of sign makers.

In 2015, however, technology development started to change, and between 2015 and today, direct material of LEDs and power sources began to be a smaller and smaller piece of the overall cost. It was now about system costs, and two major trends started in the industry.

The first was the development of 24V systems to reduce installation times and cost in large signs; the second was the use of kitting and preassembled systems for sign makers to reduce labor and time. Layered on top of this was a trend toward lower profile signs and the blurring of signage and architectural lighting, particularly in outdoor applications on and around building and gas canopies.



A timeline of LED trends in electrical signs. Be on the lookout for new technologies that move the cheese by creating new form factors or new manufacturing technologies and processes.

4 major trends

Now that we have looked back, it is time to look forward. I want to highlight four major trends that we'll experience over the next five years. These trends are a natural extension of application expansion and sophistication of offerings.

Growth in the domestic supply chain. With the current tariff situation and continued geopolitical risk with China, I believe more LED, and electrical manufacturers will onshore a portion of their production to North America. Domestic products mean that the just-in-time benefits that U.S. assembly created in the retrofit and kitting market can be applied at the module level. This will result in more readily available product options in stock for the sign maker, such as a full range of colors and color temperatures, spacing options, and lens choices.

Blurring of the lines between signs and lighting. As LEDs have become commoditized and the costs are a small part of the overall sign system, end users are looking to light everything up on or around their building. Sign makers are the trusted advisor for those customers. They have a great opportunity to move beyond signs into a range of interesting architectural products, including downlighting, linear lighting, and RGB and color-changing systems. With the cost-effectiveness of addressable RGB modules and IP-rated strips, sign makers can now design and create a range of unique lighting effects. Bitro Group offers full-color animation with its LightSymphony Signature system. I anticipate this area of the market will continue to grow.

LEDs have gone from replacing existing technology in neon and T-12 fluorescents to integration as a system, and now, the expansion of applications that offer a range of more sophisticated ways that they can be used.

Integrated systems and IoT. One growing trend that will continue is the integration of systems and tools for sign makers. Most LED suppliers have a range of tools to help sign makers sell to end-users. These include ROI and energy savings calculators, as well as estimating software. At Principal LED, we have a rebate group that helps sign makers take advantage of energy rebates. Sign/LED Wizard, provider of LED

layout software, now offers its integrated desktop product free of charge to sign makers. "…our production version allows sign makers to estimate costs of other materials and can be easily uploaded into a router to cut faces, and score and cut the back of the sign. We have plans to incorporate additional tools to assist in project management and sales," says Jeff Fassett, VP of business development.

Another part of integration in the future will be incorporating IoT into sign applications. The idea of smart signs that monitor energy consumption and can report outages will continue to grow. Colite has developed its own cloud system called Signalytix for monitoring and tracking of signage programs.

Printed LED technology. Interestingly, I ended up learning about and helping develop printed LEDs when I worked at Dow Chemical 20 years ago. The technology was very new and has been slow to develop. However, there is no question that end-users and sign makers want lower profile signage, and LED modules are inherently point sources. The name of the game is light distribution, and printed LEDs could be a disruptor to discreet LED modules in the sign industry over the next five years. Several companies have recently made real improvements in this space, and though not a current trend, it is something to look out for.

Trendsetting

When you look back at the history of LEDs in the sign industry (or any technology for that matter), you see a classic cycle. LEDs have gone from replacing existing technology in neon and T-12 fluorescents to integration as a system, and now expansion of applications that offer a range of more sophisticated ways that they can be used. Lines between traditional architectural lighting and signage will continue to blur, and systems will continue to be more integrated and streamlined. Finally, be on the lookout for new technologies that move the cheese by creating new form factors or new manufacturing technologies and processes.

Telecom
Trend Report

Innovation Intelligence at Your Fingertips

At **StartUs Insights**, we make the world's information on innovation, emerging companies, and technologies accessible. Our **Big Data & AI-powered Discovery Platform** covers over **2,5 million startups & scaleups globally**, making it the world's leading resource for data on emerging companies.

This technology enables you to identify what's next by quickly and exhaustively scouting startups, scaleups, emerging technologies & trends that matter.

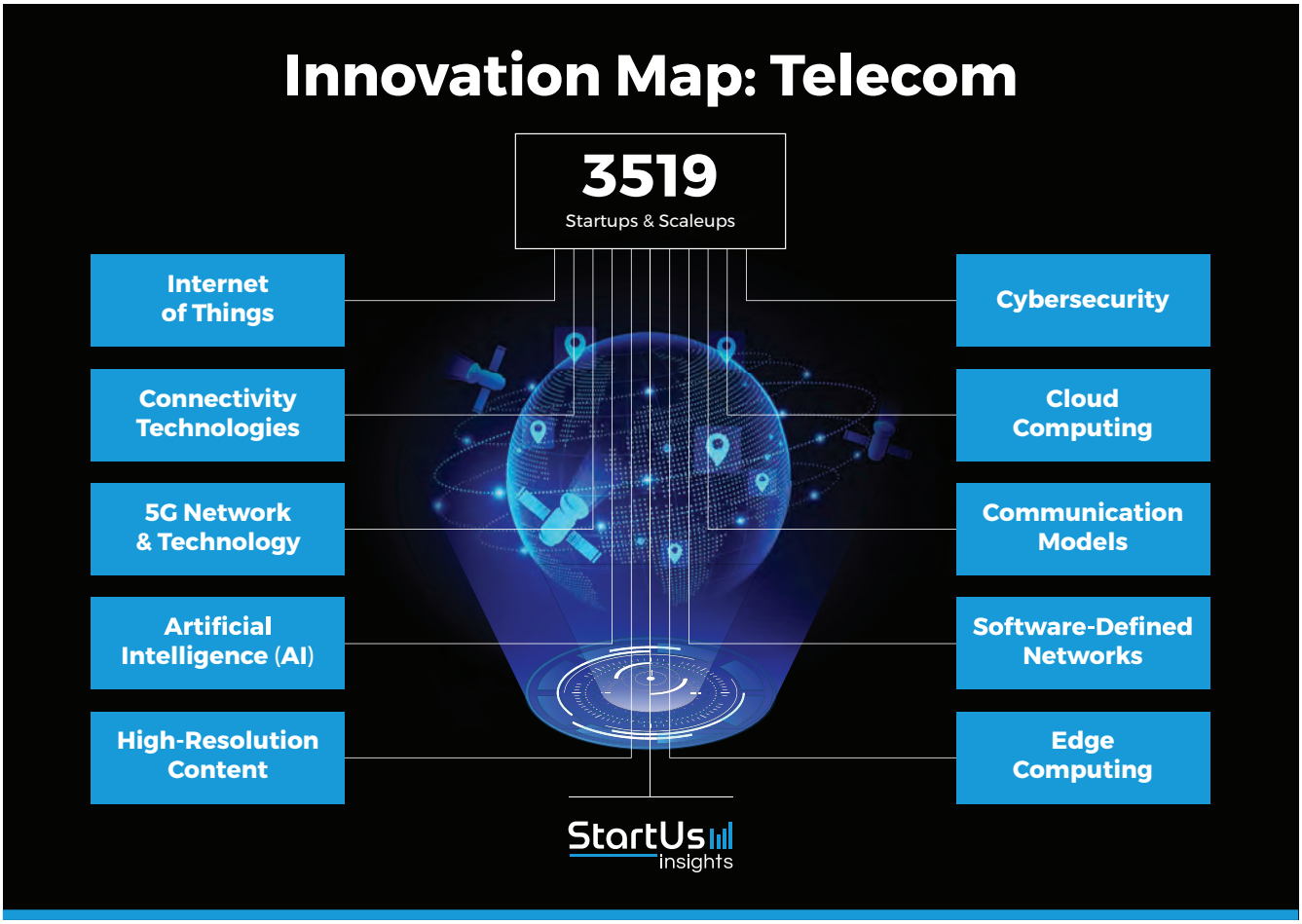
CONTENTS

5 Innovation Map: Telecom
7 Tree Map: Telecom
9 Heat Map: Telecom
10 Internet of Things
11 Connectivity Technologies
12 5G Network & Technology
13 Artificial Intelligence (AI)
14 High-Resolution Content
15 Cybersecurity
16 Cloud Computing
17 Communication Models
18 Software-Defined Networks
19 Edge Computing
20 Appendix

The telecom sector faces several looming challenges in the form of network load and infrastructure optimization, effectively addressing subscriber grievances to reduce churn, and improve security for telecommunications. The top 10 telecom industry trends directly address these challenges, in addition to improving the overall efficiency for telecom companies. Increasing global connectivity, further fuelled by the COVID-19 pandemic, presents numerous opportunities for telecom companies to reach more subscribers and offer innovative products and services. Smart factories, cities, homes, cars, and industrial workplaces require efficient and affordable cloud and 5G technology solutions, especially to address the growing number of connected people and things.

Covering over 2,5 million startups & scaleups globally, we use our Big Data and AI-powered Discovery Platform to identify innovative applications, technologies, and companies impacting the Telecom Industry. This exhaustive, data-driven startup scouting pinpoints emerging trends and technologies in the Telecom Industry. For this research, we analyzed a sample of 3 519 startups and scaleups and present the Top 10 Trends along with 20 highly relevant solutions.

In the Innovation Map below, you get an overview of the Top 10 Industry Trends & Innovations that impact telecom companies worldwide.

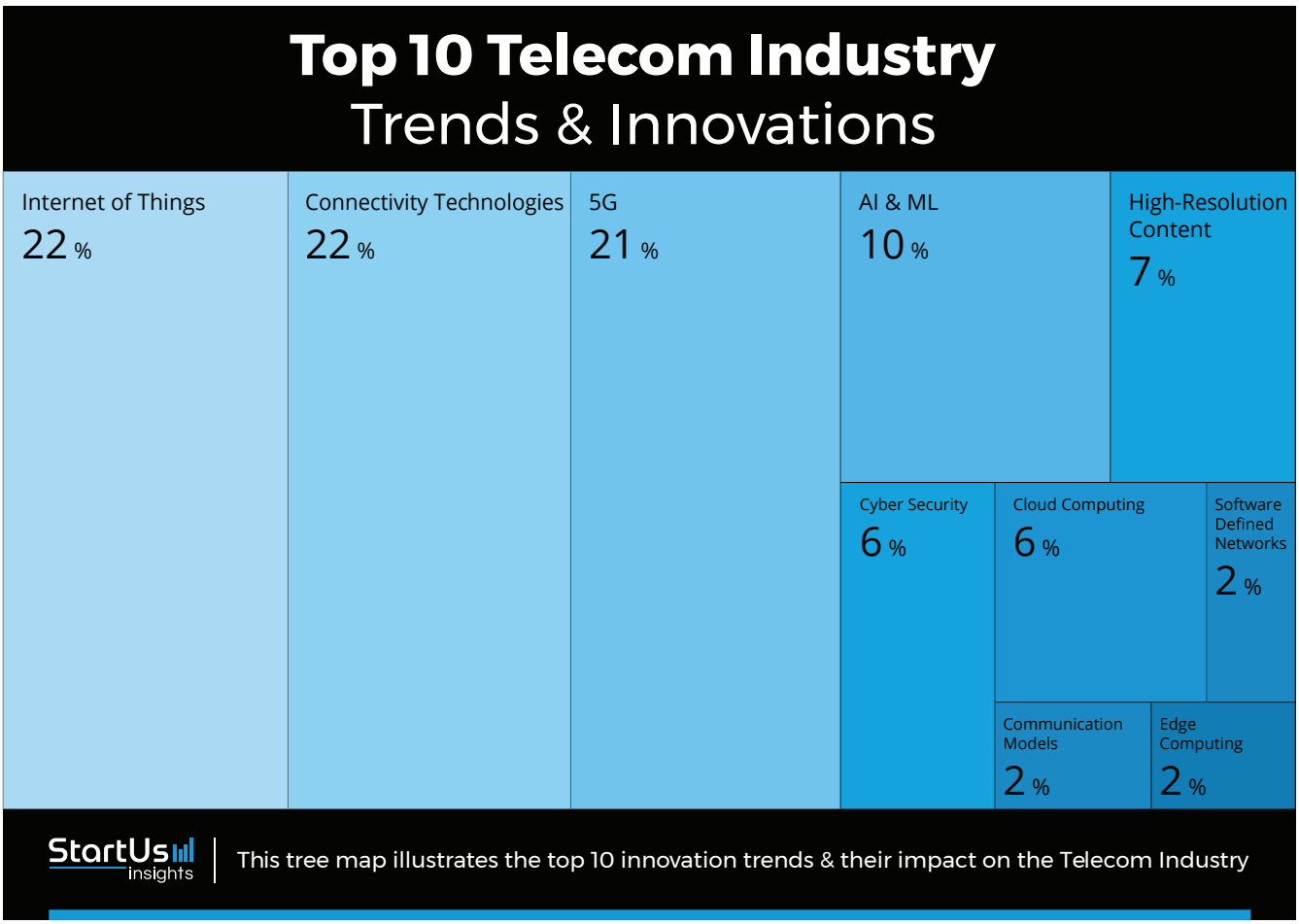


StartUs insights

Tree Map: The Impact Of Industry Trends On The Telecom Sector

Based on the Telecom Innovation Map, the Tree Map below illustrates the impact of the Top 10 Telecom Industry Trends. The internet of things (IoT) devices and sensors, connectivity solutions including next-generation WiFi and Bluetooth, as well the promise of 5G networks and technology dominate the top 10 telecom trends. Artificial intelligence (AI) algorithms influence data analytics and offer various opportunities for automation in the telecom sector. The penetration of smartphones and reliable internet generates large volumes of high-resolution content.

Telecom startups develop network solutions to manage and optimize speed and latency to further enable the growth of high-quality image and video content. In addition to these major telecom trends, the industry also sees the development of cloud and edge technologies for enabling smart industrial processes as well as solutions to improve human-to-machine and machine-to-machine communications. Get in touch with us to find relevant startups that impact your specific business.



StartUs insights

Global Startup Heat Map: Telecom Startups & Emerging Companies

The Global Startup Heat Map below highlights the global distribution of the 3.519 exemplary startups & scaleups that we analyzed for this research. Created through the StartUs Insights Discovery Platform, the Heat Map reveals that the US is home to most of these companies while we also observe increased activity in Europe as well Asia, particularly in India & Singapore.

Below, you get to meet 20 out of these 3.519 promising startups & scaleups as well as the solutions they develop. These 20 startups were hand-picked based on criteria such as founding year, location, funding raised, and more. Depending on your specific needs, your top picks might look entirely different.

StartUs insights

Internet of Things

IoT devices and sensors influence almost all industries of the technology economy. It improves people's quality of life, allows businesses to increase their profits, and improves management. IoT is also beneficial for governments looking to decrease their information technology (IT)-related expenses. Interconnection between devices, sensors, infrastructure, and computing elements further enables new ways for management. For example, decentralized operations, condition-based monitoring, and predictive maintenance ensure efficient communications between various IoT devices. In this way, IoT automates production processes and allows the implementation of Industry 4.0 concepts in the telecom sector.

Spanish startup N3uron develops highly customizable Industrial IoT and supervisory control and data acquisition (SCADA) software solutions to empower organizations to efficiently collect data. One of the startup's multiple integrated software modules, MQTT, uses special data-transfer protocols to connect thousands of field devices to any cloud or SCADA system. N3uron software runs on multiple operating systems and hardware without affecting performance. Moreover, the software's built-in networking security and data integrity checks follow industry standards of data formats. All of this allows companies to efficiently create and operate IIoT device networks.

British startup Iothic creates a communication protocol for the internet of things. The main benefit of the startup's solution is interoperability. The communication protocol enables companies to work on different devices and operating systems that are compatible with existing infrastructure. Further, a high level of security, with support for real-time low-latency operations, suits next-gen IoT applications, together with resistance to quantum decoding. The IoT standard helps manufacturers and customers by helping them reduce production and operational expenses.

Connectivity Technologies

Connectivity technologies are constantly evolving and include both wired and wireless communications. The development of communications technology is critical in today's IT-environment, with increasing data volumes, IoT devices, and people using the internet. Further, users increasingly share high-quality digital data, such as videos, photos, and music. All of these factors, along with the increasing use of satellite communications, contribute to the emerging telecom trends with innovation in connectivity technologies.

German startup FiSens manufactures Fiber Bragg Gratings (FBG) sensors for measuring strain, temperature, and pressure. The startup leverages the FBG effect, which allows creating chains without breaking fiber optics for data transmission. FiSens embeds sensors in the fiber optics, allowing up to 30 sensors in a single fiber. The startup produces FBGs for almost all possible spectral configurations. Additionally, these sensors are immune to electromagnetic interference and are safe in environments that involve radiation or explosions.

Sateliot is a Spanish satellite telecom operator for global continuous IoT connectivity, merging satellite and terrestrial networks under 5G protocols. Their hardware does not require any customization on the device side since satellite constellations act as a cell tower for IoT devices. Moreover, satellites handle messages in a secure and transparent way, ensuring customers' data is safe. Sateliot's connectivity solutions find applications in a wide range of industries, including utilities, maritime, oil & gas, and agriculture.

5G Network& Technology

5G technology is the next big upgrade for telecommunication networks and devices. It provides a much higher speed, than previous cellular broadband network standards, and, most importantly, has much lower latency. Latency is very important for cloud gaming as well as VR content streaming. Massive machine-type communications (mMTC) that 5G networks provide enable the creation of high-density IoT networks, from IIoT to smart homes. Such wide-spread applications make 5G one of the most important upcoming technology trends for the telecommunication sector.

US-based startup Aarna Networks provides a multi-cluster orchestration platform – AMCOP. AMCOP automatically manages cloud infrastructure and connected networks, such as Edge networks. AMCOP supports 5G radio access networks (RAN), and 5G Core (5GC) orchestration, as well as network slicing, data analytics, and self-organizing networks (SON). Also, AMCOP is built on vendor-agnostic open-source software, helping businesses optimize their expenditures on network infrastructure and increase security.

Simnovus is an Indian startup, building efficient UE simulators for 5G networks. Based on software-defined radio (SDR) technology, the startup allows transforming traditional x86 hardware into a UE simulator. This agile and cost-effective solution is suitable for testing telecommunication equipment and developers of such equipment. The UE simulator provides testing with realistic patterns of traffic for different network technologies, extensive logging, and elaborate statistics. Further, the simulator's licencing supports up to 1000 devices.

Artificial Intelligence (AI)

Artificial intelligence (AI) and machine learning (ML) are other big telecom trends impacting the industry. Digital transformation requires the extraction of meaningful information from data, gathered by IoT sensors and devices. At the same time, the expansion and complication of the internet create the need for high speeds and low latencies, prompting new solutions for internet connection management. To this end, startups develop AI solutions that resolve numerous problems related to network performance.

NetOp is a startup from Israel, creating a critical network health utility tool using proprietary machine learning algorithms. The solution automatically analyzes the network, searching for any vulnerabilities. Using AI-powered advanced automation, NetOp proactively predicts and remediates network issues as they arise, which is beneficial for businesses wanting to improve their security and reduce operating costs.

The US-based startup IoT/AI offers an IoT platform that combines network connectivity, cybersecurity, and analytics operating in Edge networks. The platform analyzes the data from the mesh network locally using ML algorithms. In addition to military-grade cybersecurity, IoT/AI's sensor platform is suitable for the industrial, healthcare, defense, energy industries.

High-Resolution Content

The penetration of smartphones and reliable internet leads to increased consumption of high-quality, and often heavy-to-transfer, content. The growth in high-resolution content, in turn, drives improvements in the quality of traditional information media such as videos, pictures, and music. Novel telecommunications help businesses adapt to new types of information media, such as virtual, augmented, and mixed reality- (VR/AR/MR) and cloud-based gaming. These new types of content require not only high-speed transmission but also low latency, prompting startups to develop high-capacity telecommunication networks.

Subspace is a US-based startup building networks specifically for online multiplayer games. To reduce lag and create a seamless experience for gamers, the startup uses a combination of hardware and software solutions. These include custom network routing hardware built for accelerating games and software to protect the integrity of the game. Together, these measures lead to higher player retention, matchmaking pools, and revenue for studios as well as publishers.

US-based startup echoAR creates tools to facilitate 3D application development, improve its deployment, and manage related procedures. The tools focus on cross-platform AR/VR programs development. While most AR/VR applications today support single-user, single-device static experiences, the startup's flexible cloud infrastructure makes content management & delivery simple. By making possible AR/VR products, deployable everywhere, the solution benefits brands and enterprises seeking to improve their consumers' experiences.

Cybersecurity

The increasing number of cyber-attacks and low-security IoT devices, new central processing unit (CPU) hardware vulnerabilities, and the growing dependence on computing infrastructure make tackling security risks challenging. In any industrial network, systems are continuously managed in an attempt to stay ahead of evolving cyber threats, but these methods often conflict with the network's core requirements of reliability and availability. Startups innovate industrial networks by allowing systems to remain dynamic when faced with attacks or vulnerabilities.

Cybersenshi is a startup from Saudi Arabia developing a cybersecurity tool that discovers and fixes customers' website & network security weaknesses. The database covers over 130.000 cybersecurity weaknesses of websites, networks, systems & databases. It is suitable for both small businesses, without deep knowledge in cybersecurity as well as for medium and big businesses.

US-based startup Quantum Xchange develops Phio TX and Phio Quantum Key (QK). Phio TX works on current network infrastructure, improving communications security and making existing key infrastructure quantum-safe. For a higher security level, quantum keys are used in combination with Phio TX over any type of data transmission. Further, Phio TX requires low infrastructure, which is beneficial for companies looking to bolster security.

Cloud Computing

Cloud computing is a fast-growing technology trend within telecommunications. The spreading of IoT devices and the use of more sophisticated ML algorithms leads to the high demand for computing power. There are many benefits of migrating data, applications, and other business elements to a cloud computing environment. From equipment, platforms, infrastructure, and company functions, startups bring greater connectivity and integration solutions for businesses. All connected environments, from cities and factories to houses and cars, require improvements in cloud integration technologies.

Swedish startup Cloud Backend provides a platform for subscription, data policies, and resource budget allocation using a web-based dashboard. The dashboard's architecture scales to multiple edge nodes, providing automatic synchronization and caching to secure network operations in case of failure. Cloud Backend's architecture is also suitable for enterprises expanding or optimizing their networks and systems.

Purestake is a US-based startup developing an Infrastructure-as-a-Service (IaaS) platform that delivers consistent uptime and availability. The startup combines the best practices in network architecture and security operations. The platform disperses nodes globally and, based on an automated multi-pop and multi-cloud approach, the service spans Amazon Web Services (AWS), Microsoft Azure, and Google environments. Further, the security of blockchain networks allows companies to build resilient, auto-managed networks for their needs.

Communication Models

The spread of smart and IoT devices also leads to an increase in communication channels, such as machine-to-machine (M2M), vehicle-to-everything (V2X), device-to-device (D2D), human-to-machine. Communication models differ in the connectivity technologies they use from hardware to software. Communication models are combined under include next-generation WiFi & Bluetooth, which are the basis for new products and technologies for a wide range of companies – from large banks and car manufacturers to startups and scaleups.

Indian startup M2Cloud creates device-to-cloud (D2C) solutions. They produce both simple and advanced vehicle tracking devices, aimed at creating an intelligent transport system to optimize existing public transport infrastructure. Additionally, M2Cloud produces wall-mounted sensors, both ultrasonic and infrared, for measuring body temperature. It is especially useful for establishments to check their customers and workers during the COVID-19 pandemic. M2Cloud tracking devices also use eSIMs to easily connect to the cloud.

Angoka is a British startup providing hardware solutions for managing cybersecurity risks inherent in M2M communication networks. The startup aims to improve security for connected and autonomous vehicles, smart city services, electrical grids, and banking networks. The solution provides hardware authentication using a decentralized cryptographic protocol. Angoka's solution also enables silicon devices fingerprinting based on their physical properties, which then allows for generating cryptographic keys and secure device identity.

Software-Defined Networks (SDNs)

In today's increasingly digital environment, business applications require high-performing and extensive networking operations. Particularly for cloud computing, it is essential for businesses to deploy, manage, and support connectivity across a variety of environments. Typically, complex tools are required to build and manage modern software-defined networking technology. Some vendors only provide solutions that work on their equipment, which then limits the extent of communications capabilities. . Startups develop SDN to improve network performance, monitor its performance, and enable centralized control.

UK-based startup EdgeNEXUS develops network load-balancing solutions for SDNs. edgeNEXUS optimizes routing changes based on a number of factors including load volume and application performance, thus adding a layer of intelligence between applications, networks, and SDN controllers. The startup's Global Server Load Balancer (GSLB) provides tools for multi-datacenter, multi-cloud, and hybrid cloud load balancing and failover. GLSB is suitable for enterprises looking to control their application delivery service depending on user or region.

Ethica is a Canadian startup providing CloudAccess, an easy-to-deploy and inexpensive Software-Defined Wide Area Network (SDWAN) solution focusing on SMEs. The solution reduces the downtime of the network by aggregating multiple internet connections and using them when they are available. Also, CloudAccess provides Quality of Service (QoS) by prioritizing more important types of traffic which is useful, for example, in distributed teams using video calls. Further, all the solution's features are manageable through a cloud-hosted orchestration utility.

Edge Computing

Edge computing brings data computation and data storage closer to the source of data instead of a centralized remote cloud. This reduces latency, increases bandwidth, and simplifies maintenance while it allows industrial manufacturing companies to expand their computing capacity by combining devices with edge data centers at lower costs. Lower latencies and high speeds are required for modern applications, like cloud gaming and VR. Edge Computing greatly improves the quality of experience for end-users and lowers data exchange requirements.

Belgian startup Edgegap provides Edge network-based game hosting services. By locating online game-hosting servers in close proximity to the actual players, the startup ensuring low latencies. Edgegap currently has 220 hosting locations available. Moreover, the services are easily scalable and reliable. Edgegap provides equal latencies for all players connected to a single game, ensuring fairness, which is very important in competitive gaming.

US-based startup Axellio builds FabricXpress – a high-performance, high-density computing and storage platform for heavy applications. This solution is suitable for Edge networks that have a high density, high bandwidth, and low latency requirement. In addition to improving network performance, the startup achieves this with a small energy footprint and low costs.

What Does This Mean For Telecom Companies?

The innovation areas outlined in this research on 10 Telecom Industry Trends only scratch the surface of what we found during our analysis. 5G networks and technology implementation, flexible networks for high- and low-latency requirements, and faster modes of communication are all areas bound to significantly impact telecom companies one way or the other. Identifying new opportunities and emerging technologies to implement into your business early on goes a long way in gaining a competitive advantage and becoming an industry leader.

The Telecom Industry Trends & Startups outlined in this report only scratch the surface of trends that we identified during our in-depth research. Among others, AI, 5G, and connectivity innovations will transform the sector as we know it today. Identifying new opportunities and emerging technologies to implement into your business early on goes a long way in gaining a competitive advantage. Get in touch to easily and exhaustively scout relevant technologies & startups that matter to you.

StartUs insights

Identify What's Next

The StartUs Insights Discovery Platform covers over **2,5 million startups & scaleups globally** – making it the world's largest resource for data on emerging companies. The SaaS Platform enables you to **easily**, **quickly**, **and exhaustively scout relevant companies**, **technologies**, **& trends** for your innovation activities. This saves your time and increases efficiency, which is why more than 650 leading corporate partners including Samsung, Kyocera, and Nestlé already trust our technology.

Schedule Free Demo

(D) Installations Not Covered by NEC

- Installations of communications equipment under the exclusive control of communications utilities located outdoors or in building spaces used exclusively for such installations

- Installations under the exclusive control of an electric utility where such installations

- a. Consist of service drops or service laterals, and associated metering, or

- b. Are on property owned or leased by the electric utility for the purpose of communications, metering, generation, control, transformation, transmission, energy storage, or distribution of electric energy, or

- c. Are located in legally established easements or rights-of-way, or

- d. Are located by other written agreements either designated by or recognized by public service commissions, utility commissions, or other regulatory agencies having jurisdiction for such installations. These written agreements shall be limited to installations for the purpose of communications, metering, generation, control, transformation, transmission, energy storage, or distribution of electric energy where legally established easements or rights-of-way cannot be obtained. These installations shall be limited to federal lands, Native American reservations through the U.S. Department of the Interior Bureau of Indian Affairs, military bases, lands controlled by port authorities and state agencies and departments, and lands owned by railroads.

Highlights of the next edition of the National Electrical Safety Code

Beyond the Service Point

As the definitive safety standard for more than a century, the National Electrical Safety Code® (NESC®) continues to be the go-to standard for electric and telecom utility companies of all sizes and ownership of structures. Within the utility environment, the NESC is used by a myriad of users, including business leaders, operations management, engineering and line designers, crew supervisors, safety trainers, and others. The 2023 version, edited by the IEEE Standards Association (IEEE SA), will be published in August 2022 and will become effective on February 1, 2023.

by Nelson G. Bingel III, Chairman, NESC, and Dr. Lawrence M. Slavin, Contributor, NESC

Purpose and Format

Published exclusively by IEEE SA and typically updated every five* years to keep the Code current with changes in the industry and technology, the NESC sets the ground rules and guidelines for the practical *safeguarding of utility workers and the public* during the installation, operation, and maintenance of electric supply, communication lines, and associated equipment. (*This time around, the COVID-19 pandemic caused a delay in the typical release cycle)

Like previous versions, the 2023 edition will be available in digital, printed, e-Learnings, and mobile-app formats. The edition consists of initial sections covering scope, purpose, and grounding methods, followed by sections that include specific rules for electric supply stations, overhead lines, underground lines, and safety-related work practices.

A companion document, the 2023 NESC Handbook, will be published at the same time as the Code. The Handbook includes all of the rules of the code but also provides insights and commentary on the rules and how to apply them from the experts who helped develop the Code. The new handbook format will be more user-friendly, as the handbook text is interspersed with the code rules to include historical notes and provide context for revisions and additions. The previous edition of the handbook, the 2017 edition, is available in Spanish and Chinese, and the 2023 handbook will be translated in the near future.

2023 NESC Highlights

Revisions in the 2023 NESC are intended to provide clarity and ease of use, which ultimately point back to its purpose – safety. Goals of the revision process include modernizing and keeping the Code relevant, making it more intuitive and easier to understand, and accommodating the emergence of new technologies such as solar and wind energy, distributed energy/microgrids, battery technologies, energy storage, and wireless small cell networks.

Online e-Learning courses, originally introduced with the 2017 edition, will be updated to include the new changes on grounding methods, electric supply stations, overhead lines – clearances and strength & loading, underground lines, and work rules. The new courses will be available on August 1, 2022.

Before diving into some of the Code revisions, notable changes have been made to units of measurement intended to help prevent mistakes in applying the safety rules. All stand-alone tables for

metric measurements will be removed from the main code body and moved to Annex 1. For tables that include both English and metric values, the revised Code presents numerical values in the customary "inch-foot-pound" system first and the corresponding metric values following in parentheses. These and other changes were introduced to help prevent users from making serious errors caused by misreading a value as being metric when, in fact, they are U.S. values.

A few notable revisions to the Code include:

- In the Clearances section, as well as in the specification of the Grade of Construction in Table 242-1, the Code further clarifies the use of non-hazardous fiber optic cables as telecom providers continue to expand their networks.
- Revisions in the Strength & Loading sections include modified Rule 250C, which addresses extreme wind loading for overhead lines. Two wind maps are now provided instead of the previous single one. A map for Grade B, the highest grade of construction, with a Mean Recurrence Interval (MRI) of 100 years (corresponding to a one percent annual probability of occurrence) is provided in place of the previous 50–90-year MRI map. For Grade C construction, a separate 50-year MRI (two percent annual probability of occurrence) map is now provided. In the previous Code, a factor was applied to the 50–90-year MRI map for application to Grade C. Changes were also made to the method of determining the corresponding wind loads, consistent with the latest engineering practices.
- As an example of a Code revision focused on public safety, the ground end of *all* anchor guys adjacent to regularly traveled pedestrian thoroughfares, such as sidewalks, and similar places where people can be found must include a substantial and conspicuous marker to help prevent accidents. The previous Code did not require the marking of every such anchor guy.

Addressing Recent and Emerging Technologies

Just as it has done for more than a century, the NESC is continuously evolving and being refined to embrace new technologies. Today, this includes emerging technologies such as solar and wind energy, distributed energy/microgrids, batteries and energy storage, and wireless small cell networks – while addressing both the opportunities and any safety issues they present. The potential impacts of recent and emerging technologies are reflected in the new Code, including the following:

- Significant revisions were made in Section 14 covering batteries. Previous editions of the code were based on lead-acid technology and batteries only used for backup power. The 2023 Code incorporates the new battery technologies and addresses energy storage and backup power.
- A new Section 19 of the code covers photovoltaic generating stations, with sections addressing general codes, location, grounding configurations, vegetation management, DC overcurrent protection, and DC conductors. These new rules accommodate large-scale solar power projects.
- In the Clearances section, all rules for wireless antenna structures have been consolidated in the equipment section (Rule 238 and 239), which makes the Code more user-friendly.

To further address new technologies in subsequent editions of the Code:

- A new subcommittee was created focusing on generating stations, with the original subcommittee continuing to address substations.
- A working group is investigating Fault Managed Power Systems (FMPS) cables as the technology may be used for 5G networks. The team is looking at possible impacts, including clearances and work rules.

These are just a few of the highlights of the 2023 NESC, which is the product of hundreds of contributors and peer reviewers and the careful editing of the IEEE Standards Association. For more information, please visit standards.ieee.org to learn more information about the NESC and NESC Products. We welcome you to join our efforts by joining the NESC!

Limited License Random Questions

1.) The NEC governs the installations under the exclusive control of an electric utility.
True
False

2.) A PV license holder can make connections to an existing panel, junction box, wiring, or circuits on the premises.
True
False

3.) A C5 license holder can work on and install circuits that exceed 48 volts or 8 amperes.
True
False

4.) The scope of the L5 license limits work to a system voltage not to exceed 25 volts or 5 amperes.
True
False

5.) Class 1 remote control and signaling circuits can exceed 300 volts.
True
False

Limited License Random Questions Answer Key

1.) The NEC governs the installations under the exclusive control of an electric utility.
True
False

2.) A PV license holder can make connections to an existing panel, junction box, wiring, or circuits on the premises.
True
False

3.) A C5 license holder can work on and install circuits that exceed 48 volts or 8 amperes.
True
False

4.) The scope of the L5 license limits work to a system voltage not to exceed 25 volts or 5 amperes.
True
False

5.) Class 1 remote control and signaling circuits can exceed 300 volts.
True
False

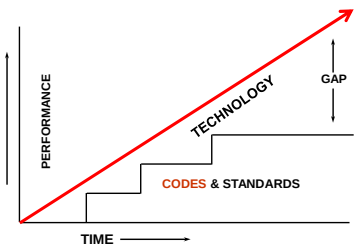
Brain – Calisthenics

1. Circuits – What are they ?
1. How do the CT Limited Low Voltage License's define power?
2. NEC 2020 Defines Broadband and Premise Powered circuits in Chapter 7 or Chapter 8?
3. How are the Connecticut Model Building Codes integrated into the NEC 2020.
4. What are the top three OSHA violations.?

1

2

Design & Technology Integration



3

Standards

- Are established as a basis to compare, measure, or judge:

- Capacity
- Quantity
- Value
- Quality

- Performance
- Limits
- Interoperability

4

Safety Codes

- Code adoption and compliance is intended to protect the health, safety and general welfare of the public through legislation or statues.

- ***Enforceable***
  - Established by a regulatory or legislative body
  - Construction guidelines & practices
  - Can carry Fines & Penalties
  - Occupational & Trade Licensure qualifications

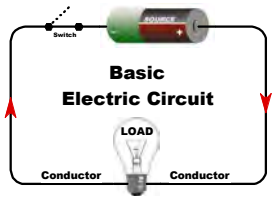
5

Basic Electricity – Another View

Electricity flowing through a wire is like water flowing through a garden hose. The amount of water that can fit through the hose depends on the diameter of the hose (amps). The pressure of the water depends on how far open the faucet is (volts). The amount of work that can be done (watts) depends on both the amount and the pressure of the water (volts x amps = watts).

6

Circuits



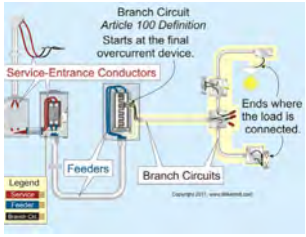
A circuit provides the path for current to flow.

Conductor

Material that allows the flow of an electrical current

7

Electrical Branch Circuit



What is a Communications Circuit??

8

Article 800 General Requirements for Communications Systems

800.1 Scope. This article covers general requirements for communications systems. These general requirements apply to communication circuits, and equipment community antenna television and radio distribution systems, network-powered broadband communication systems, and premises-powered broadband communication systems unless modified by Articles 805, 820, 830, or 840.

9

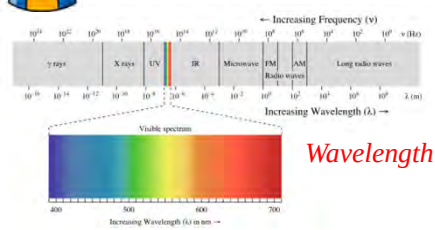
800.2 Definitions: Communications Circuit

- **Communications Circuit.** The circuit that extends service from the communications utility or service provider to and including the customer's communications equipment.
- The definition of a "**Communications Circuit**" was revised to remove the "list" of service types offered by a communications circuit
- List was problematic as it did not allow for new technologies to be included in this definition without a *Code* change, which only happens every three years

Copyright © IAEI 2020

10

Frequency



Wavelength

Visible Spectrum

11

11

Bandwidth – Signal Processing – Hertz

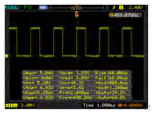
Analog

Bandwidth – Computer Processing - Bit Rate - bits per second (bps)

Shannon Capacity - The amount of error free digital data that can be sent over a continuous ***analog communications channel.*** Measured in bits per second (bps)

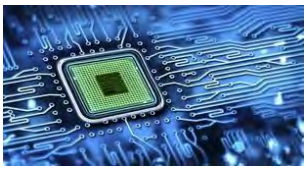
$$C = B\log_2\left(1+\frac{S}{N}\right)$$

Digital



12

Sorcery of Silicon

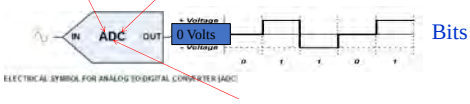


13

Power/Voltage

Converter

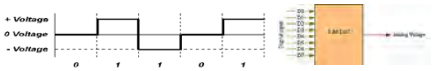
Analog



Bits

Digital

Power/Voltage



14

14

Communication Fundamentals

Transmit

Analog

Digital

Information

Transport Method

Receive

Copper

- Twisted Pair
- Coax
- Hybrid

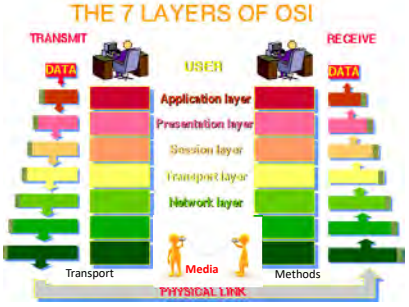
Fiber

- Single Mode
- Multi-Mode

15

15

Communication Fundamentals

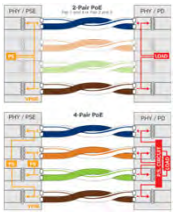


16

Power and Data

Over the Same Pair Simultaneously

- **Power delivered via center tap of data transformer combining power and data**
- **Both conductors of one pair are (+) while both conductors of the other pair are (–)**
  - 2 pair PoE: pairs 1 & 4 or 2 & 3 used
  - 4 pair PoE: pairs 1 & 4, AND 2 & 3 used
- **Data "rides on top" of DC voltage – DC voltage does not interfere with data**

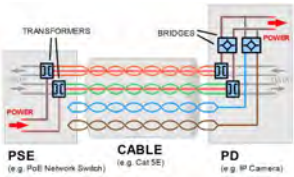


17

Power over Ethernet – PoE

PoE Ready Devices

- Normally, the data pairs are used to carry the PoE power, and the spare pairs remain unused. The example illustrates how electrical power can be connected to the data pairs in the cable, and the path it follows.
- Electrical transformers can be used to separate the signals at either end. Bridge circuits in the PD correct the electrical polarity and allow power to be received from either the data or spare pairs, while preventing current from being able to flow back down the unused wires.



Power Sourcing Equipment (PSE) **Powered Devices (PD)**

18

Current PoE IEEE Standards

19

PoE Performance & Current Limits

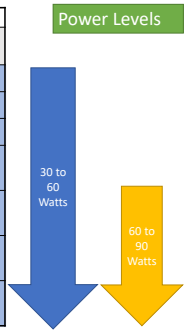
Type	Standards	Maximum Current	Number of Energized Pairs	Power at Source	Power at Device	Maximum Data Rate	Standard Ratified
PoE	IEEE 802.3af (802.3at Type 1)	350 mA	2	15.4 W	13 W	1000BASE-T	2003
PoE+	IEEE 802.3at Type 2	600 mA	2	30 W	25.5 W	1000BASE-T	2009
PoE ++ HPoE	**IEEE 802.3.bt Type 3 IEEE 802.3.bt Type 4**	**600 mA 960 mA**	**4**	**60 W 99 W**	**51 W 71 W**	**10GBASE-T**	**2011/2018**
No IEEE standard	Cisco UPOE HDBaseT (www.hdbaset.org)	600 mA 1000 mA	4	60 W 100 W	51 W 100 W	Varies	Exists today – no official ratification

20

Category ratings and frequency range

Performance Evolution of "Category Rated" Cabling and Components

Category	MHz	Mb/s	Cable Type	Date of Introduction
Cat 3	16 MHz	10 Mb/s	UTP	1993
Cat 4	20 MHz	16 Mb/s	UTP	1994
Cat 5	100 MHz	100 Mb/s	UTP	1995
Cat 5e	100 MHz	1000 (1G) Mb/s	UTP	2000
Cat 6	250 MHz	1000 (1G) Mb/s	UTP	2002
Cat 6a	500 MHz	10,000 Mb/s	UTP, F/UTP	2006
Class F, Cat 7	1000 MHz (1GHz)	40Gbs	S/FTP	ISO/IEC



21

Category Ratings and Frequency range

Performance Evolution of "Category Rated" Cabling and Components

Category	MHz	Mb/s	Cable Type	Date of Introduction
Class F, Cat 7 A	2 GHz	40Gb/s	S/FTP	ISO/IEC Europe (under development)
Cat 8 * *(distance limits)	2 GHz	40Gb/s 25Gb/s	S/FTP	TIA North America 2016

Power Levels

30 to 90 Watts

Challenges - Cable Diameter

Challenges - Wire Gauge (24 ga. / 23 ga.)

Challenges - 60 Watts PoE = Heat

22

90W Revolutionizing Workspaces

BEFORE

Today : Workspace powered by UPOE+ 90W

PoE powered workspaces

- Automated height adjustable desk*
- PoE powered desktop switch
- All-in-one computers / Displays
- Daisy-chained PoE Lights
- IP phones
- Ethernet to USB-C for laptops/Tablets/Phones

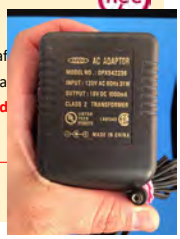
23

What Else Can I Do With 90 Watts ?

24

Chapter 7 – Special Conditions
NEC Article 725 - Class 1, Class 2, Class 3 Remote Control, Signaling, and Power-Limited Circuits

- Class 2 Power
  - Defined within National Electrical Code (NFPA 70)
  - 30VAC, 60VDC, 100VA
  - Due to its power limitations, a Class 2 circuit is considered saf
    standpoint and provides acceptable protection from electrica
- Class 2 and 3 systems **do not** require the same **wiring method**
  Class 1 systems



Power Limited Circuit

25

Chapter 8 – Communications Systems

800.1 Scope. *This article covers* ***communications sytems*** *and equipment.*

Informational Note No. 1: See 90.2(B)(4) for installations of communications circuits and equipment that are not covered.
Informational Note No. 2: For further information for remote- control, signaling, and power-limited circuits, see Article 725.
Informational Note No. 3: For further information for fire alarm systems, see Article 760.

N **-800.2 Definitions** Part 1 of Article 100 shall apply throughout Chapter 8.

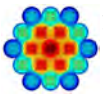
N**- Communications Circuit.** *The* ***circuit*** *that extends service* ***communications utility or service provider*** *up to and including the customer's communications equipment.*

26

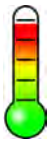
Chapter 8 – Communications Systems
Cable Heating & Bundle Sizes

Table 725.144 –Ampacity Table – ***pg.70-640***

805.179 (D) - ***LP Cable Types*** – ***pg.70-680***



The heat or thermal energy is either dissipated or "trapped" and can be measured in watts.



What Contributes to Heat Generation?

Bundle Size
Power Source
Ambient Air temperature
Environmental Conditions
Type of Pathways
Firestopping
Number of energized conductors/pairs
Cable Construction
Workmanship
Installation Practices

27

Table 725.144

Table 725.144 Ampacities of Each Conductor in Amperes in 4-Pair Class 2 or Class 3 Omni Balanced Twisted-Pair Cables Based on Copper Conductors at an Ambient Temperature of 30°C (86° F) with All Conductors in All Cables Carrying Current, 60°C (140°F), 75°C (167°F), and 90°C (194°F) Rated Cables

	Number of 4-Pair Cables in a Bundle																	
	1-7			8-19			20-37			38-61			62-91			92-192		
	Temperature Rating			Temperature Rating			Temperature Rating			Temperature Rating			Temperature Rating			Temperature Rating		
AWG	60°C	75°C	90°C	60°C	75°C	90°C	60°C	75°C	90°C	60°C	75°C	90°C	60°C	75°C	90°C	60°C	75°C	90°C
26	1.00	1.23	1.42	0.71	0.87	1.02	0.55	0.68	0.78	0.46	0.57	0.67	0.45	0.55	0.64	N/A	N/A	N/A
24	1.19	1.46	1.69	0.81	1.01	1.17	0.63	0.78	0.91	0.55	0.67	0.78	0.46	0.56	0.65	0.40	0.48	0.55
23	1.24	1.53	1.78	0.89	1.11	1.28	0.77	0.95	1.10	0.66	0.80	0.93	0.58	0.71	0.82	0.45	0.55	0.63
22	1.50	1.86	2.16	1.04	1.28	1.49	0.77	0.95	1.11	0.66	0.82	0.96	0.62	0.77	0.89	0.53	0.63	0.72

Note 1: For bundle sizes over 192 cables, or for conductor sizes smaller than 26 AWG, ampacities shall be permitted to be determined by qualified personnel under engineering supervision.

Note 2: Where only half of the conductors in each cable are carrying current, the values in the table shall be permitted to be increased by a factor of 1.4.

Informational Note No. 1: Elevated cable temperatures can reduce a cable's data transmission performance. For information on practices for 4-pair balanced twisted pair cabling, see TIA-TSB-184-A and 6.4.7, 6.6.3, and Annex G of ANSI/TIA-568-C.2, which provide guidance on adjustments for operating temperatures between 20°C and 60°C.

Informational Note No. 2: The per-contact current rating of connectors can limit the maximum allowable current below the ampacity shown in Table 725.144.

Copyright © IAEI 2020

28

805.179(D) Limited Power (LP) Cables

- Provisions were added to permit **limited power (LP) cables** to act as a **substitute** for Class 2 and Class 3 cables
- Previously, communications cables were permitted as substitutes for Class 2 and Class 3 cables, but the *Code* **did not specifically address** limited power (LP) cables as a substitute for Class 2 and Class 3 cables
- **725.144** and **Table 725.144** gives designers, installers and AHJs the assurance that 4-pair data cables can safely carry power as well as data when bundled together in cable trays or cable routing assemblies
- This revision recognizes the fact that an **LP cable** is a specific type of Class 2, Class 3, and communications cable and explicitly permits these cable types as **substitutes** for Class 2 and Class 3 LP cables *(vast majority of LP cables are listed as communications cables)*
- LP cables are listed under the UL product categories of Communications Cable **(DUZX)** and Power Limited Circuit Cable **(QPTZ)**

Copyright © IAEI 2020

29

805.179(D) Limited Power (LP) Cables

Provisions added at to permit limited power (LP) cables to act as a substitute for Class 2 and Class 3 cables as well as the previous provisions allowing communications cables as substitutes for Class 2 and Class 3 cables

CMR-LP (D-6A) (75C) 23 AWG 4 pair

Cable Sample Courtesy of Belden

Copyright © IAEI 2020

30

31

Abandoned Cable Review

NEC 2020 - Definitions

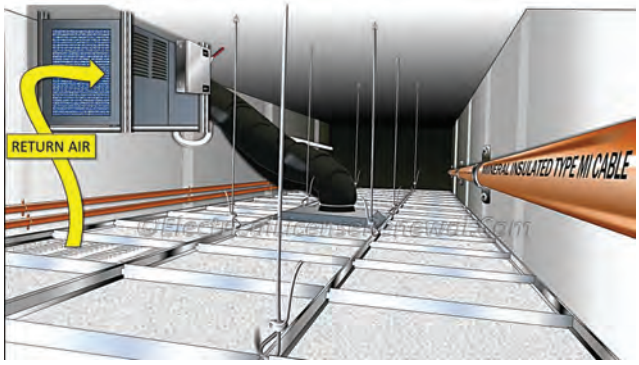
Articles 640
Articles 645
Articles 725
Articles 760
Articles 770
Articles 800

NFPA-90A
NFPA-75
NFPA-76

Abandoned Cable & Plenums

What is a Plenum ?

- Article 100 – Definitions - pg 70-39
- Section 800.113 (C) - pg.70-668



Abandoned Cable & Plenums

- Understand the background of abandoned cable issue ie "Fuel Load"
- Understand NEC Code requirements governing the removal of abandoned cables
- Understand relative fire safety performance of available network cabling products

Why is it important to consider the fire safety performance of network cable?

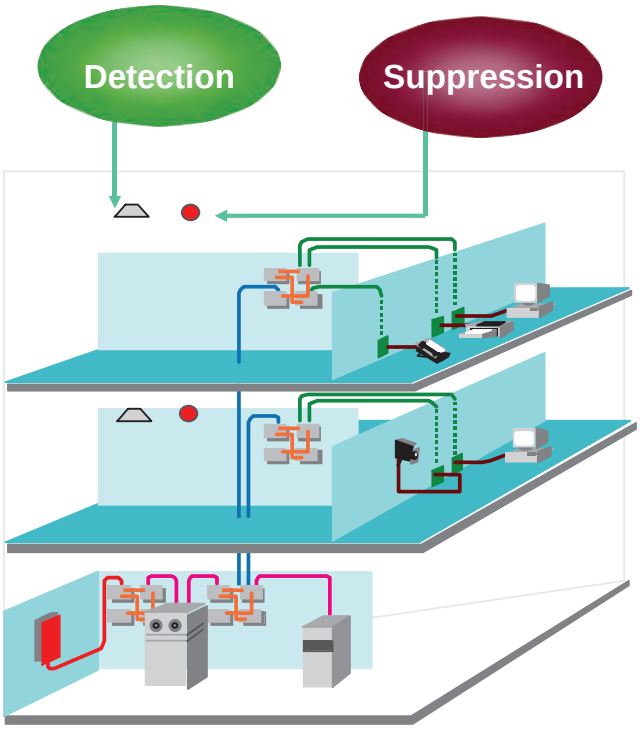
- A small fire caused by electrical failure can ignite cables
- Certain cables burning generate large amounts of thick black smoke which can hamper evacuation.
- Cables can provide fuel to a fire allowing the fire to spread rapidly through concealed spaces.
- Smoke generated by burning cables is particularly damaging to electronics

Fire Investigations: Lessons Learned

- Ignition source is often electrical failure
- Cables can add significant fuel load and spread fire rapidly
- Mechanism of fires spread by following cable pathways and spaces
- Small fires can cause extensive smoke damage
- Combustible materials in concealed spaces are of great concern.

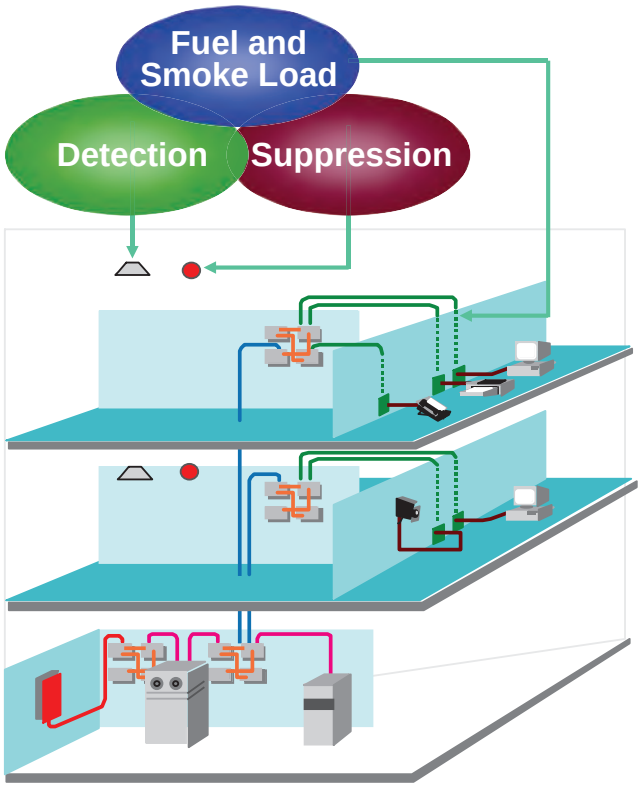
Investments in building safety

- To prevent or minimize the effects that a fire will have on their business, companies should invest in safety measures to protect their people, facilities, and equipment.
  - Passive and active systems
  - Evacuation procedures and drills
  - Safe practices
  - Contingency and disaster recovery plans



Reducing the hidden hazard from communications cabling should be a part of our investment in protecting people, facilities, and equipment. Removal of abandoned cable from plenums is one key step.

Fuel Load & Smoke



Abandoned Cable Makes Headlines

Buildings

Wired in to NEC Changes?
Ensure Your Facilities Are Code-compliant

National Real Estate Investor
Abandoned Cable Issue Could Trip Up Owners

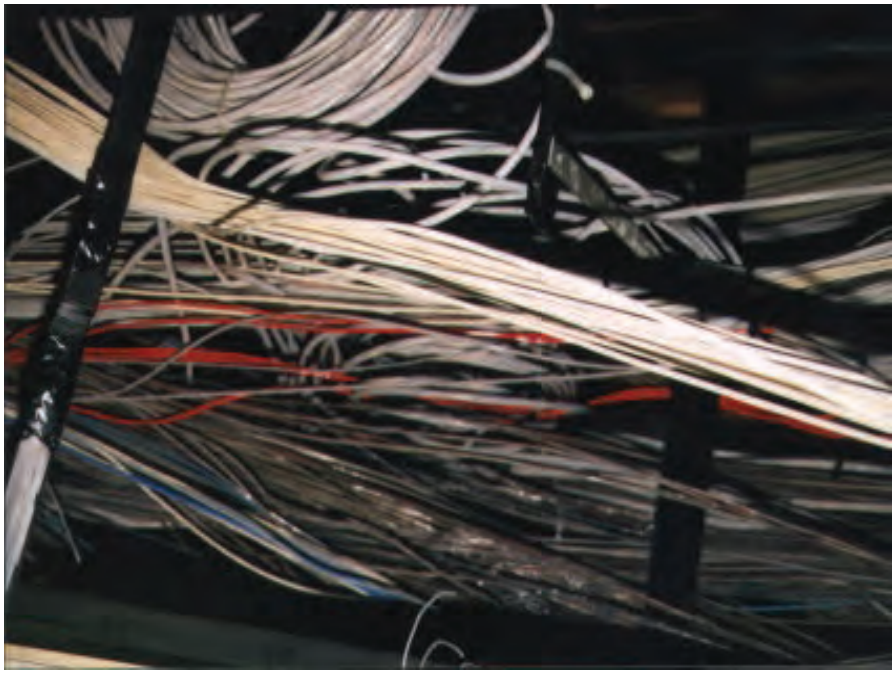
Atlanta Business Chronicle
Abandoned cable is fire hazard; removal onerous

The New York Times
Landlords and Tenants Wrestle With Wiring

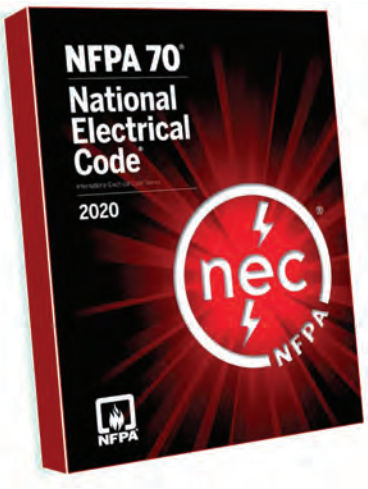
What lurks beneath?

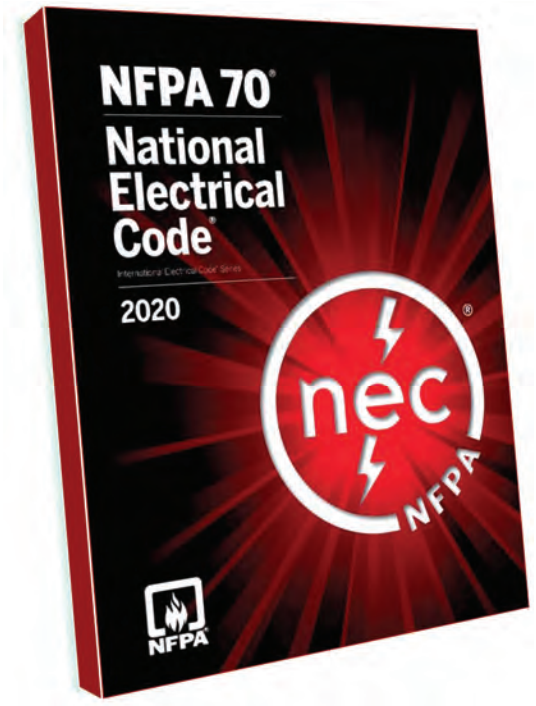
Or – in our case -- What lurks above?

Hidden Hazards - Above ?



NFPA codes and standards represent a set of minimum fire safety requirements for the protection of buildings.





NFPA 70 is responsible for plenum cable products and applications.

- NFPA 70 – National Electrical Code (NEC):
  - Recognizes hazards associated with cables in plenums
  - Requires removal of abandoned cable from plenums
  - Fine Print Note (FPN) points to NFPA 13 requirements for plenum sprinklers where there is combustible loading

National Electric Code Fire Safety Hierarchy for Copper Communications Cable

Cable Type	Insulation	Jacket
CMP - Plenum	FEP	LS-PVC*
CMR - Riser	PE	FR-PVC*
CM – General Purpose Communication	PE	PVC*

*Different PVC compounds

The miracles of science

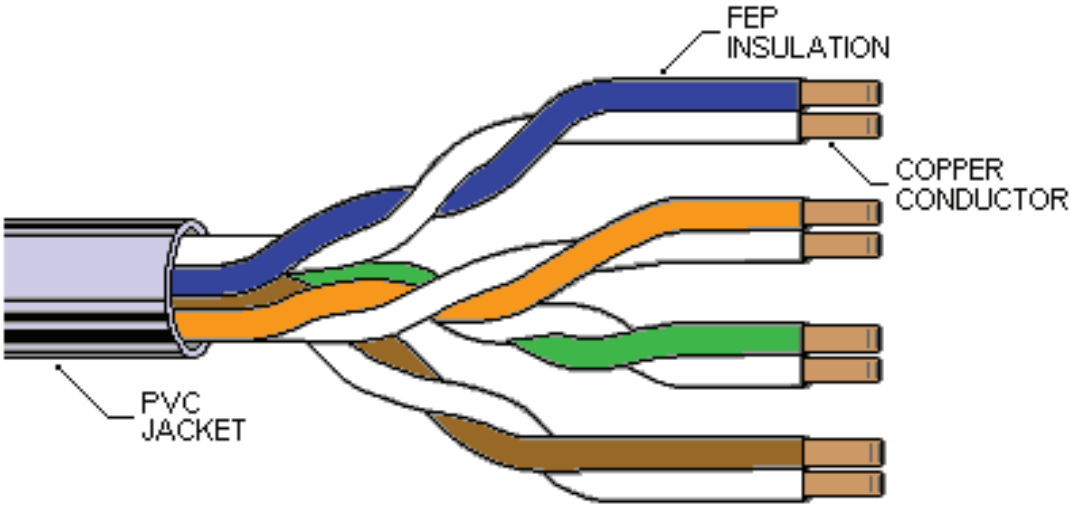
National Electric Code Fire Safety Hierarchy for Copper Communications Cable

Cable Type	Insulation	Jacket
LCC – Limited Combustible FHC 25/50 CMP	FEP	FEP or FP Compound
CMP - Plenum	FEP	LS-PVC*
CMR - Riser	PE	FR-PVC*
CM – General Purpose Communication	PE	PVC*

*PVC compounds containing different levels of flame retardant and smoke inhibitors

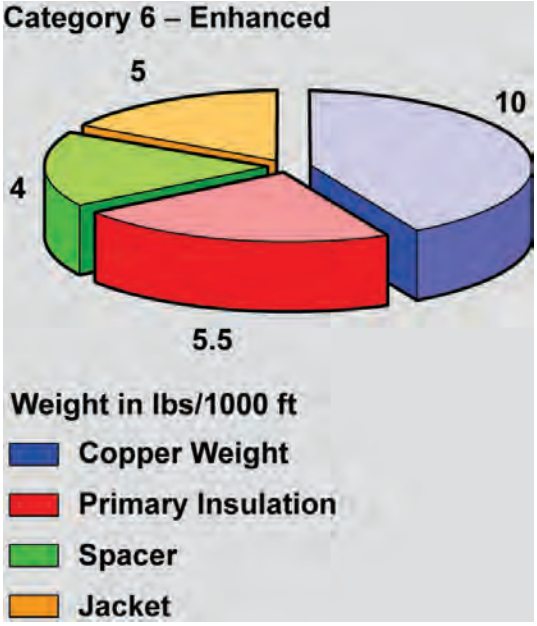
The miracles of science

What is Plenum Cable?



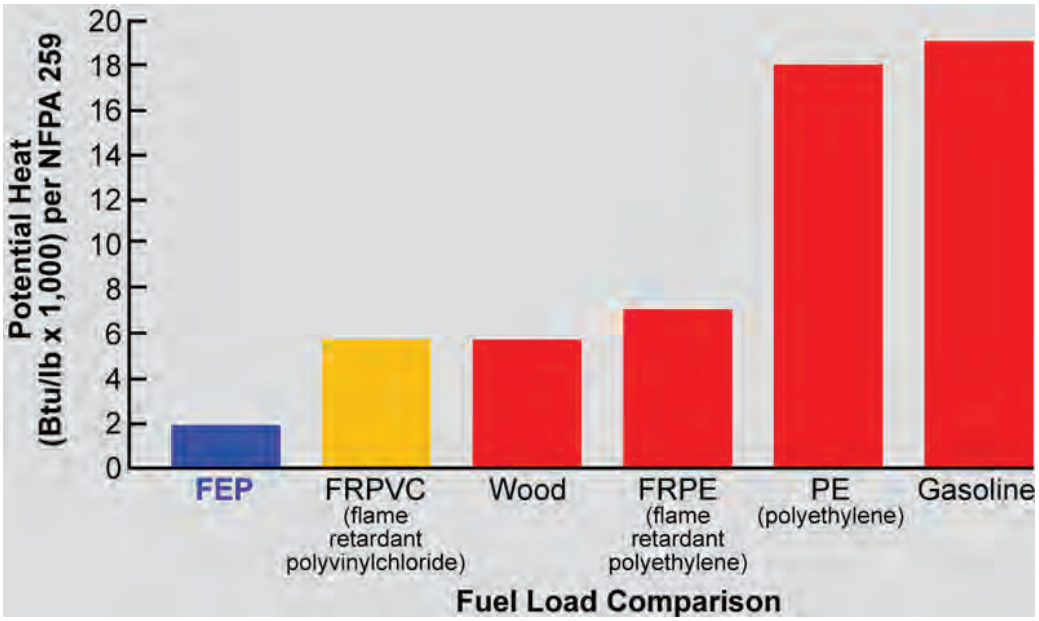
4-Pair UTP Plenum Rated Cable (CMP)

Typical composition of 4-pair UTP Cables



- Composed of >50% plastics by weight
- Represents 1,500 lbs of potentially combustible material for every 100,000 feet of installed cable

Insulation and jacket materials have a significant impact on the level of fire safety performance



Burning Characteristics of Communications Cables

Cable Fire Research

The miracles of science

CMR

CMP

LCC

The miracles of science

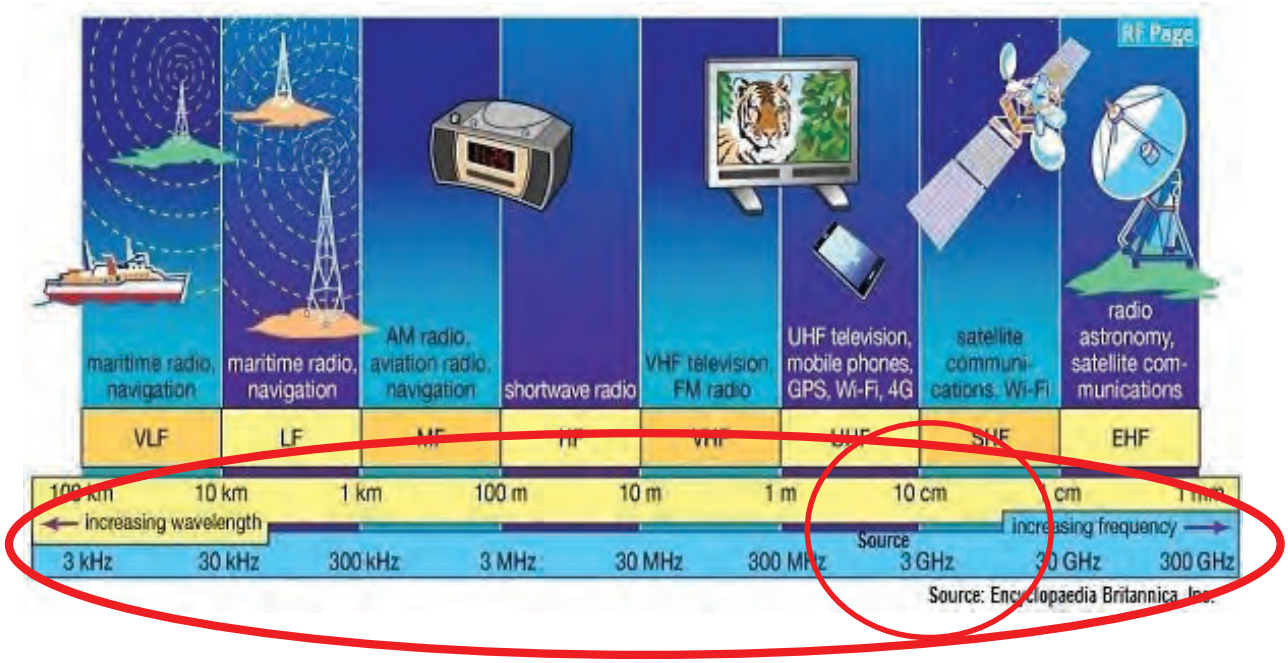
Environmental Concerns

- U.S. Green Building Council (USGBC)
  - LEED
- California
  - Proposition 65 (Lead)
- European Directives
  - Restriction of Hazardous Substances (RoHS)
  - Waste Electrical and Electronic Equipment (WEEE)

Increasing attention is being paid to the impact of electrical and electronic wastes, including cable

- **Which cables offer greater environmental sustainability?**
- Should not contain any substances or components regulated under the RoHS and WEEE Directives.
- Be Free of heavy metals (lead) and phthalates.
- Be Free of hazardous substances such as PBB and PBDE.
- Comply with California Proposition 65 (requires no warning labels on product).
- Offer more complete recyclability of both copper and plastics at end-of-life.
- Contain post-industrial recycled content today, with options for post-consumer content in the future.

Wireless & Radio Frequency Bands (RF)



300MHZ – 30GHZ

WiFi - Technology

Radio Frequency (RF) Transmission

Public Band – 2.4GHZ & 5GHZ - Competition

- **Cordless Phones**
- **Microwaves**
- **Radio controlled toys**
- **Access devices**
- **Wireless LANS (WLANS)**

WiFi - Technology

Radio Frequency (RF) Transmission

"Wi-Fi" radios

- **Efficient encoding techniques**
- **Allow "frequency hopping"**
- **Powered devices (repeaters) can be inserted into the system.**

WiFi- Standards

- IEEE 802.11 a,b,g.
  "Wi-Fi" Certified (1991-2003)
- IEEE 802.16 & IEEE 802.16a
  "WiMAX" MAN Networks
- Bluetooth
- HomeRF
- RFID
- IEEE 802.1X - security

First Gen - IEEE/WiFi Standards

IEEE 802.11

Speed – 2Mbps
Band – 2.4GHZ

Comments
Extended to 802.11b

IEEE 802.11b

Speed – Up to 11Mbps
Band – 2.4GHZ

Comments
"Wi-Fi" Certified
14 Channels (11 US)
Not interoperable with 802.11a
Susceptible to RF interference

First Gen - IEEE/WiFi Standards

IEEE 802.11g

Speed – Up to 54Mbps
Band – 2.4GHZ
Comments
"Wi-Fi" Certified
14 Channels (11 US)
Improved security over 802.b
Susceptible to RF interference

IEEE 802.11a

Speed – Up to 54Mbps
Band – 5GHZ
Comments
"Wi-Fi" Certified
8 Channels
Less susceptible to RF
More susceptible to obstructions
Better for high bandwidth APPS - video
Long range "drop-outs"

Other Notable IEEE Standards

IEEE 802.16

IEEE 802.16a

Speed – Up to 54Mbps

Band – 10 to 66GHZ (802.16)
2 to 11GHZ (802.16a)

Comments

"WiMAX"

MAN networking

Security and compatibility with WLAN products an issue

Bluetooth

Speed – Up to 2.4Mbps

Band – 2.4GHZ

Comments

No IP support yet

Short distances – 10 meters

Susceptible to RF

More - Standards

HomeRF

Speed – Up to 10Mbps

Band – 2.4GHZ

Comments

No longer support

Some legacy equipment exists

RFID

Multiple Bands

125KHz- animal tags

915MHz(UHF) - logistics

2.4GHZ – ISM apps for Active devices (transponders)

Comments

Auto-ID segment

Needs cables for antennas and data collection devices

Next Generation of Standards

Generation of network connection	Sample user interface visual
Wi-Fi 6 (802.11ax)	6
Wi-Fi 5 (802.11ac)	5
Wi-Fi 4 (802.11n)	4

Next Generation of IEEE Standards

802.11n (Wi-Fi 4) - *2009*

- Speed – Up to 600Mbps
- Bands – 2.4GHZ
- Interim between 802.11g and 802.11ac
- Introduced MIMO

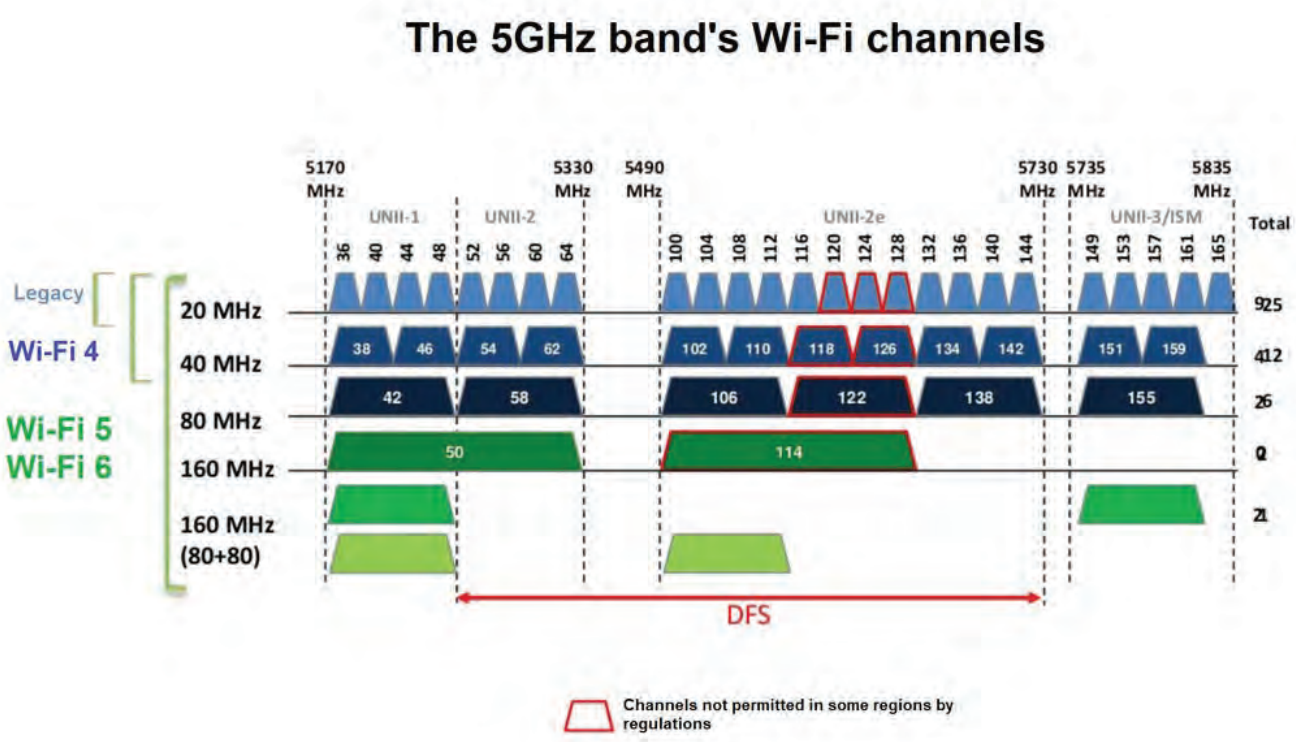
802.11ac- (WiFi-5) – *2014*

- Speed – Up to 1,300 on 5GHZ & 450 on 2.4 GZ
- Dual Bands – 2.4GHZ & 5GHZ
- Backward compatible
- Introduced MU-MIMO – 4 devices simultaneously
- Being replaced by 802.11ax

Next Generation of Standards

802.11ax (WiFi-6)- *2019*

- Speed – Up to 10G
- Dual Bands – 2.4GHZ & 5GHZ
- Backward compatible
- Multiple Channels
- MU-MIMO – Devices communicate simultaneously
- OFDMA - data to multiple devices
- POE +(30-watts)
- Cable recommendation is (2) two- Cat6/Cat6A
- Devices & Adoption rates



FCC Opened the 6GHZ band to the public

802.11ax (WiFi-6E)- *2020*

"In layman's terms, if the 2.4GHz band is a one-lane country highway and the 5GHz band is a three-lane interstate, picture the 6GHz band as a shiny, new seven-lane superhighway, and only 6E devices get access to the onramp." *

- Not a new protocol but expands on WiFi 6 by adding more bandwidth
- Compatibility
- Devices coming to market now

Implementation Challenges

Still in the public band 2.4GHZ

Range vs Speed

Speed decreases as distance increases

Ex: 802.11a at 100' was 12Mbps

802.11b at 100' was 1Mbps

To maintain higher through puts more access points are needed. = More Cabling

Security – encryption methods ($$$)

Implementation Challenges

WAP – Dual Bands - saturation

WAP – increase power- bleeding

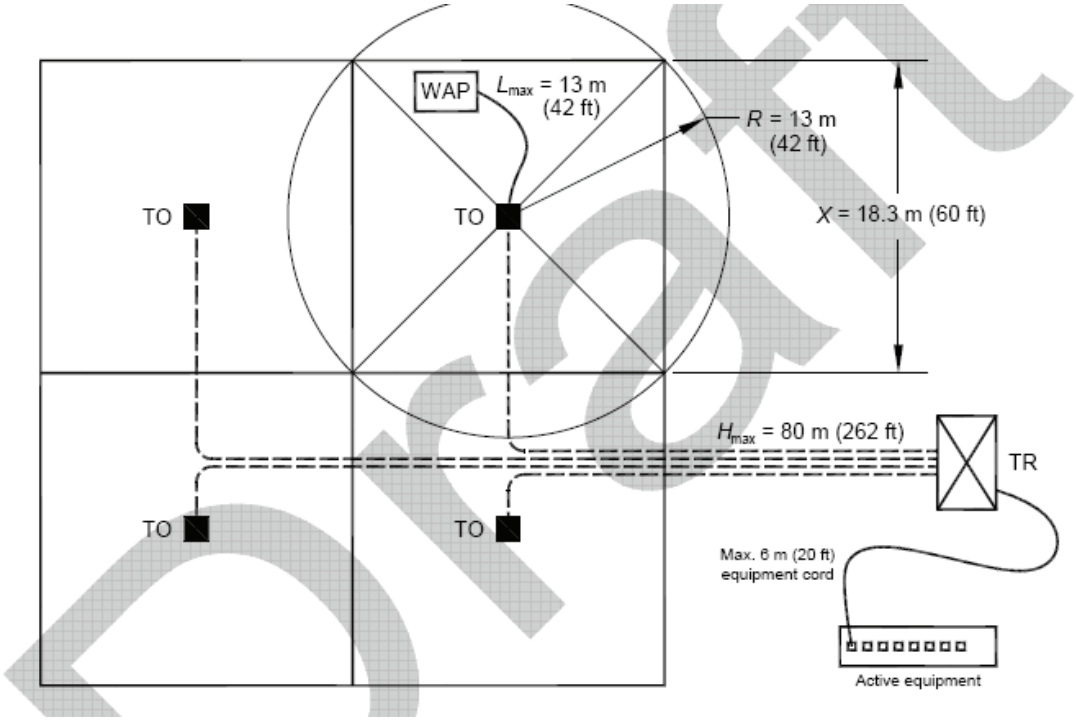
Network performance – more users fighting for bandwidth

Changing Standards (802.11n)

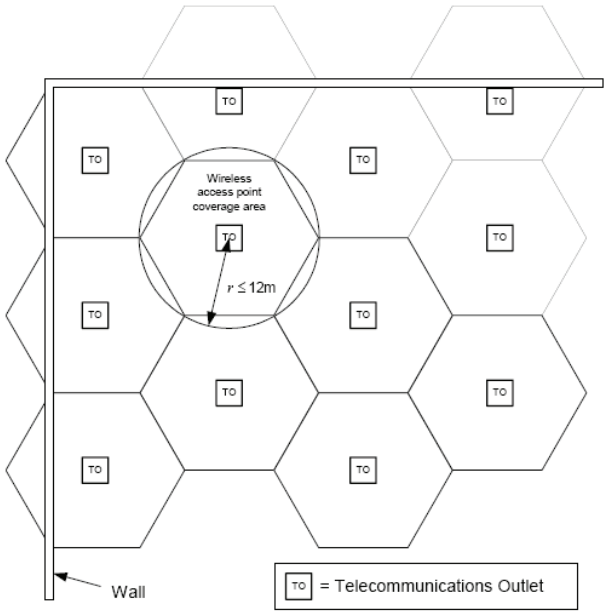
Cable "Enabler"

Standards	Standards
TIA TSB-162 (Draft3.1)	**ISO/IEC 247-004**
Grid approach TO every 250 to 360 sq/ft (60' grid)	**"Honey Comb" approach** TO every 12meters
Estimated cable increase 5-7%	**Estimated cable increase 5%**
Less testing than ISO	**Pre-testing and post-testing highly recommended**

Cable "Enabler" TSB-162



Cable "Enabler" ISO/IEC 24704-2016



NOTE 1 A "Honeycomb" grid provides the most efficient coverage. Other grid shapes such as squares or rectangles may be used.

NOTE 2 Under normal circumstances, the optimum mounting location for a wireless access point or antenna is at the centre of the cell.

Figure 1 – Grid of telecommunications outlets for wireless coverage areas

Distributed Antenna Systems (DAS)

Active Das

Passive DAS

Micro Cells (eRAN)

Tunxis Community College

Education That Works For A Lifetime

Understanding Cellular Coverage

- **Cell phone signals are Radio Waves.** Like AM/FM they operate in a certain frequency /wavelength. They require a Transmitter and a Receiver.
- **Decibel-milliwatts** or **dBm** measures the strength of the wave and are expressed in negative numbers. (-65 dBm) The closer to "0" the stronger the wave.
- **RSRQ** – The "Quality" of the cell signal received by the device.

Signal Strength	General Results
-50 to -79 dBm	Considered **great signal** (4 to 5 bars)
-80 to -89 dBm	Considered **good signal** (3 to 4 bars)
-90 to -99 dBm	Considered **average signal** (2 to 3 bars)
-100 to -109 dBm	Considered **poor signal** (1 to 2 bars)
-110 to -120 dBm	Considered **very poor signal** (0 to 1 bar)

Measuring Signal Strength -RSRQ

RF Conditions	RSRP (dBm)	RSRQ (dB)	SINR (dB)
Excellent	>=-80	>=-10	>=20
Good	-80 to -90	-10 to -15	13 to 20
Mid Cell	-90 to 100	-15 to -20	0 to 13
Cell Edge	<=-100	<-20	<=0

What Causes Poor Cell Reception?

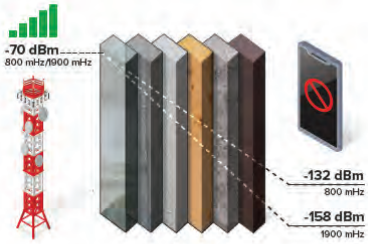
Physical Obstruction - Natural or man-made obstacles located between a phone and the nearest cell phone tower can also have a significant impact on overall signal strength. Common obstructions include:

Geographic Barriers - When a phone or cellular device isn't near a cell tower, signal can be weak or even undetectable. This is common when living or working in remote or rural areas faraway from cell towers.

Vegetation
Trees, shrubbery, and other kinds of foliage can absorb and weaken cell signals.

Man-made Objects
In urban settings, buildings obstruct cell signal that can't easily penetrate metal, brick, concrete, energy-efficient glass, and foam insulation. While inside cell reception can be spotty, you can also experience poor connectivity outside when surrounded by tall buildings.

Typical Building Scenario



Signal Amount Blocked

Material	800 mHz	1900 mHz
Low-E Glass Window	▼ 34 dB	▼ 34 dB
6" Concrete Wall	▼ 10 dB	▼ 19 dB
1/2" Drywall	▼ 2 dB	▼ 2 dB
Solid Pine 1/2"	▼ 2 dB	▼ 5 dB
Venetian Plaster	▼ 8 dB	▼ 16 dB
Solid Wood Door	▼ 6 dB	▼ 12 dB
TOTAL BLOCKED	**▼ 62 dB**	**▼ 88 dB**

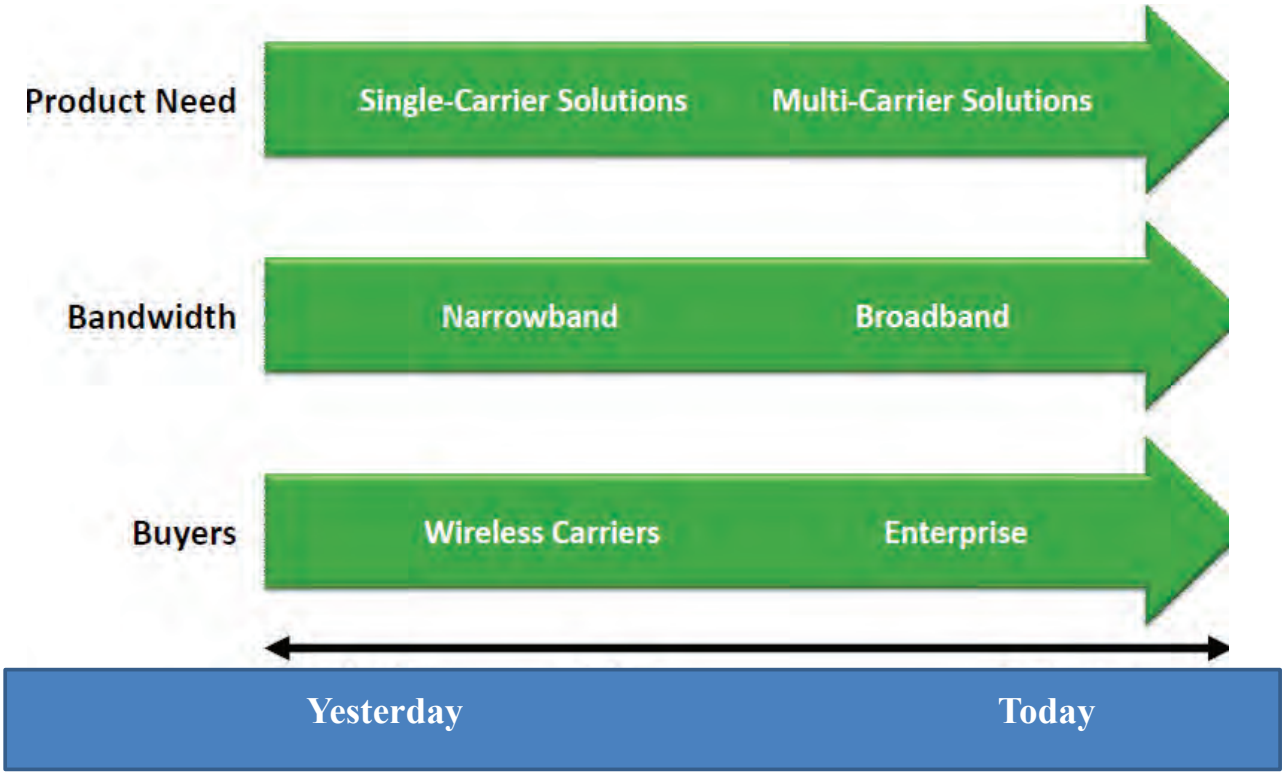
Distributed Antenna Systems

First, what is a DAS?

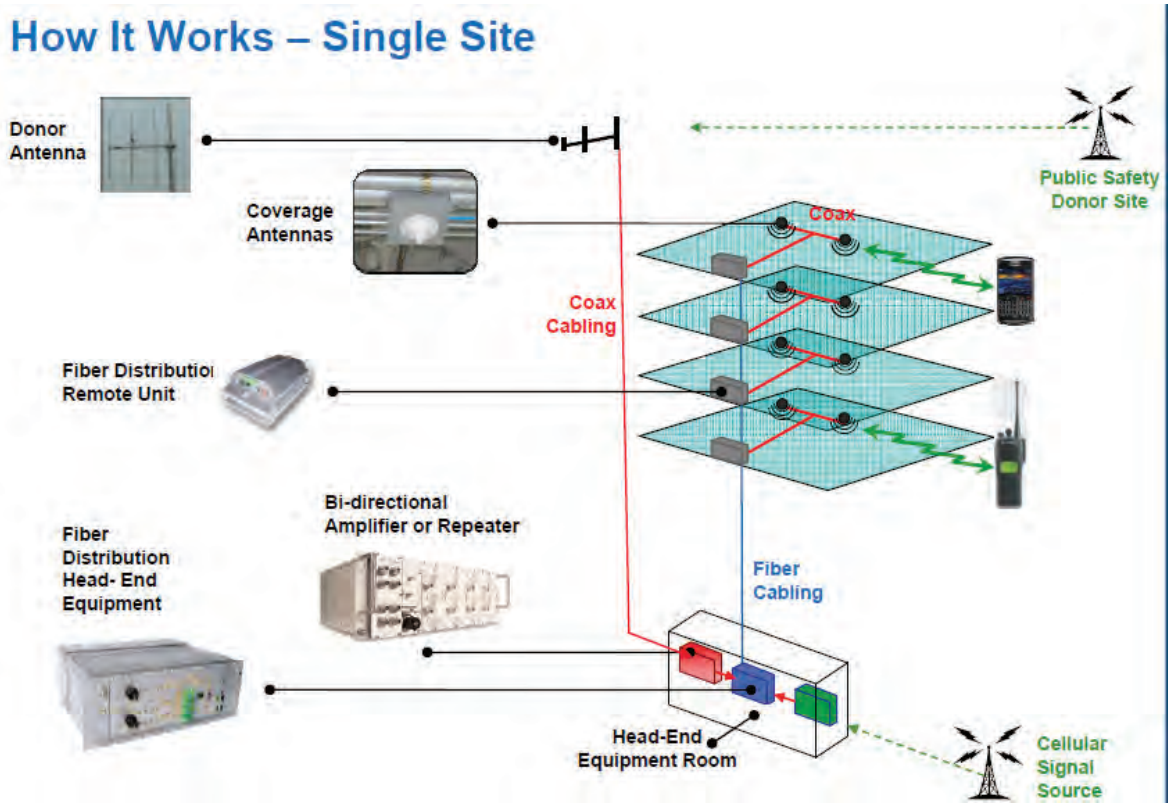
A ***Distributed Antenna System*** or DAS, is a network of spatially separated antennas connected to a transport medium – typically coax or fiber-optic cable -- that provides wireless service within a building or structure.

The DAS can be driven by a direct connection to a radio base station or an "off-air" repeater/signal booster.

Distributed Antenna Systems

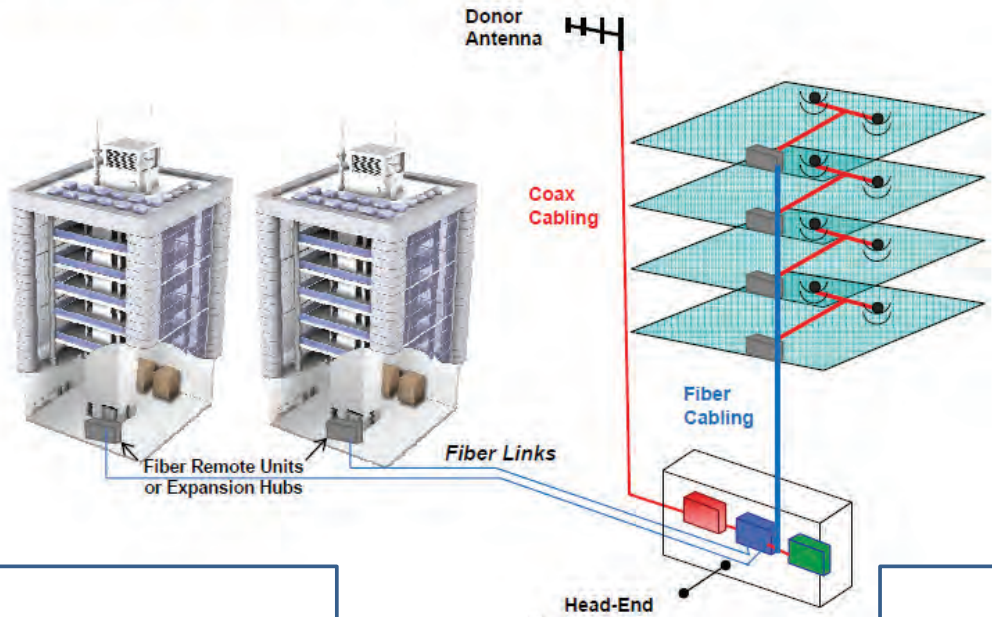


Distributed Antenna Systems



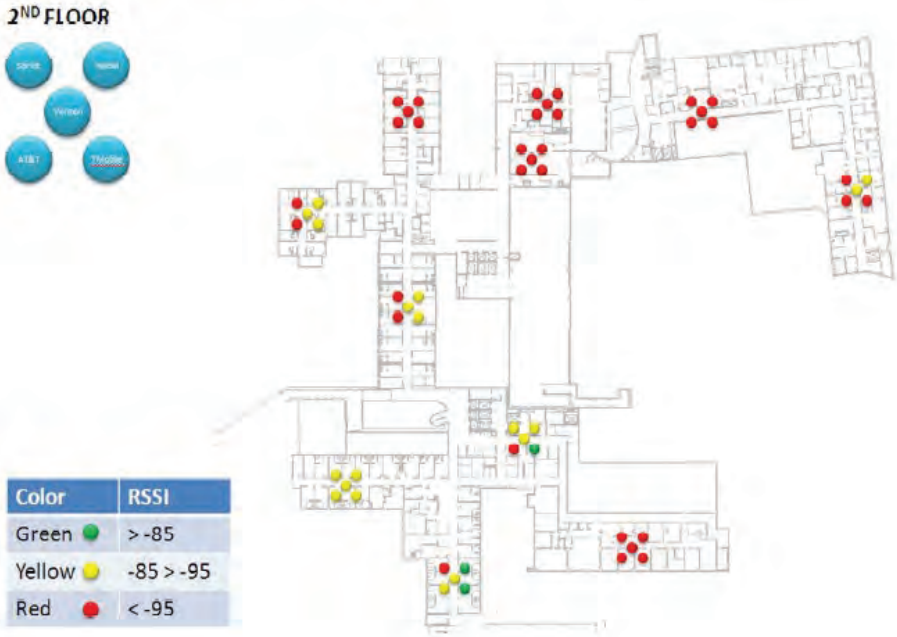
Distributed Antenna Systems

DAS in multi-site or Campus setting



Distributed Antenna Systems

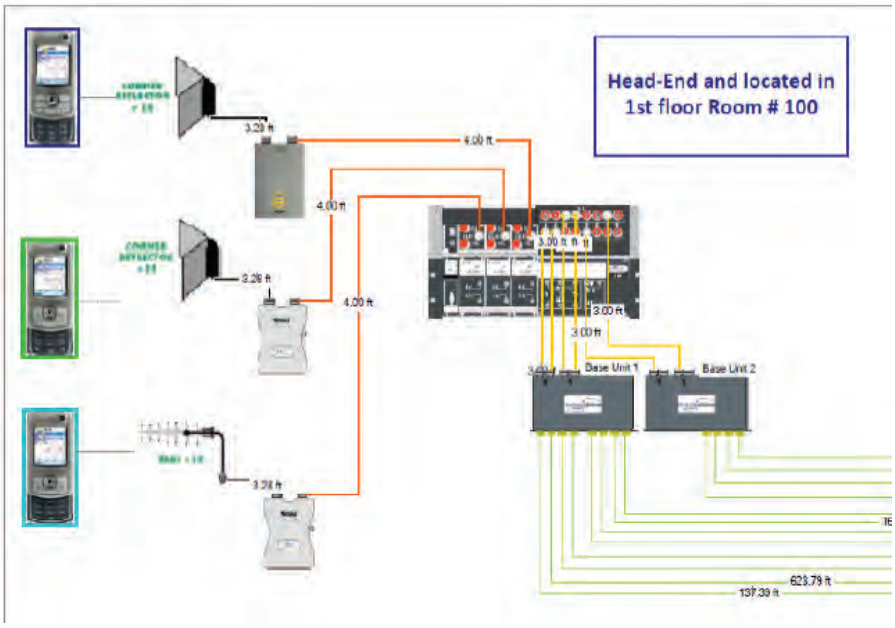
Coverage Needs Analysis



Color	RSSI
Green	> -85
Yellow	-85 > -95
Red	< -95

Distributed Antenna Systems

Design



Distributed Antenna Systems

Design: Typical Frequency Bands & Technologies

- AT&T: 850/1900 MHz — GSM and UMTS/WCDMA
- Verizon: 700/850/1900 MHz — LTE,CDMA and EVDO
- Nextel: 800/900 MHz — iDEN/SMR
- Sprint PCS: 1900 MHz — CDMA and EVDO
- T-Mobile: 1900/2100 MHz — GSM and AWS
- Public Safety: VHF(150-174MHz), UHF(450-470MHz), 700/800 MHz
- Federal Government: VHF & UHF

Distributed Antenna Systems

Carrier Coordination

- Necessary to obtain permission from wireless service providers
- Purchased frequencies from FCC/US Government
- Re-transmission agreements
  - Repeaters or microcell/base station
- Potential RF issues generated
  - Noise floor, oscillation, frequency-specific, etc
- Carrier monitoring/database
- Coexisting with Public Safety systems

What Industry Solutions Are Available for Cellular Coverage ?

Wi-Fi Calling

Many businesses believe that Wi-Fi calling is an immediate fix for cellular connectivity problems

Network Extender

A network extender, sometimes called a femtocell or microcell. The device plugs into an existing broadband internet connection and works like a mini cell tower in your home or office.

Digital Apps

Digital applications may be the most commonly used cellular connectivity alternative. Offerings like Skype, Google Hangouts, and FaceTime boast accessible Voice over Internet Protocol (VoIP) and digital video communications solutions.

Active DAS

The most robust and infrastructure-intensive cellular connectivity solution is an active Distributed Antenna System (DAS). Active DAS offers a carrier- grade, high-capacity infrastructure solution for large venues.

An active DAS creates cell coverage within a building, using its own cellular signal. The system distributes signal between a centralized signal - "head end" source and "remote nodes" placed around a building

Passive DAS

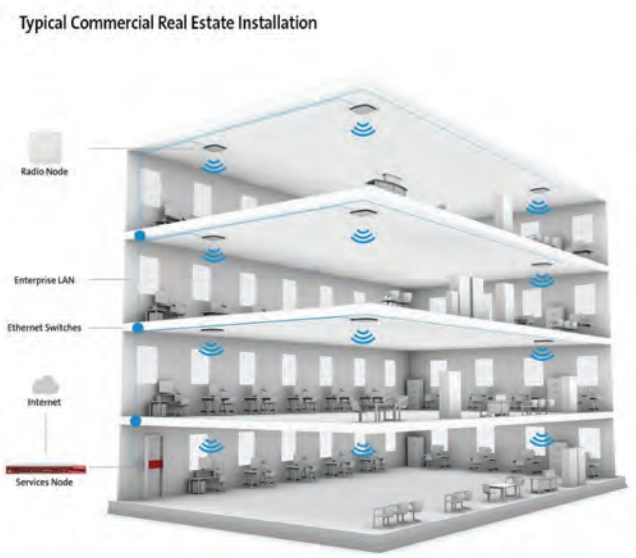
Passive DAS, also known as a cell signal booster system or bi-directional amplifier (BDA), enhances an existing signal with passive components and amplifiers. Antennas on the outside of a building capture the cellular signal and send it to a booster that amplifies the signal.

Less equipment than an active DAS, a passive DAS is a financially viable option for a wide range of users. **It is important to note that a passive DAS relies on the strength and quality of the available signal at the site to provide optimal cell coverage.**

Comparative Analysis of Systems

	WI-FI	NETWORK EXTENDER	DIGITAL APPLICATION	ACTIVE DAS	PASSIVE DAS
CARRIER AGNOSTIC	YES	NO	YES	NO	YES
BUILDING SIZE	Unlimited	<7,500 sq ft	Unlimited	>500,000 sq ft	Unlimited
USER CAPACITY/ RELIABILITY	Low	Low	Low	High	High
SECURITY	Low	Low	Low	High	High
BUDGET	$	$	$	$ $ $ $	$ $
EASE OF INSTALLATION	Easy	Easy	Easy	Difficult	Moderate

Hybrid Solutions for Cell Coverage



What is an enterprise radio access network (E-RAN)? An E-RAN system is made up of one services node that manages a group of radio nodes (access points) that are attached to it. All of the radio nodes are powered by Ethernet, which makes them quick
and easy to install.

How does E-RAN work?

- PoE+-powered radio nodes install on ceiling or wall
- Radio nodes connect to services node over Ethernet LAN and internet
- Services node connects to operator network over internet
- Reliable cellular coverage and capacity inside buildings

PoE- Enabled System

E-RAN Platform

An E-RAN system is made up of one rack-unit-sized services node that manages multiple single-carrier or dual-carrier radio nodes operating in 3G, LTE, and unlicensed spectrum.

Services Node

The services node lies at the heart of the SpiderCloud® E-RAN solution. It ensures that the E-RAN system is easy to deploy and manage and that it delivers the performance mobile operators expect. The services node is access technology agnostic, supporting UMTS, LTE, and LTE-LAA. It orchestrates the self-organizing network (SON) process, controls the operation of different radio nodes during neighbor discovery, gathers information from different radio nodes, and creates optimized neighbor lists based on information received from the neighbor scans.

Hybrid Solutions for Cell Coverage

Radio Nodes

Like Wi-Fi access points, radio nodes are small with low profiles. An E-RAN platform offers a wide range of radio nodes for
many different applications and mobile operator configurations. All models are powered by PoE+ (802.11at) Ethernet switch ports.

Installation is quick and easy using commonly available PoE+.

1. Pull a structured cable (CAT 5e or greater).
2. Attach the radio to wall or ceiling.
3. Connect Ethernet patch cords at both ends.

Radio Node Family

Similar to a WiFi Access Point