

Розкрийте потенціал Інтернету речей

Дослідження головних викликів тестування пристроїв через призму концепції «5G+1» для IoT

Переклад: Вадим Потапенко

Редагування: Віктор Бутирін, директор, Юнітест

E-mail: Victor_Butyrin@unifitest.com

Впровадження IoT диверсифікувалися: від споживчого використання до критично важливих застосунків для громадської безпеки, реагування на надзвичайні ситуації, промислової автоматизації та автономних транспортних засобів. Критично важливі застосунки використовують зручність, низьку вартість, тривалий час автономної роботи технологій IoT та наявну бездротову інфраструктуру. Ці технології покращують зручність, взаємодію та взаємозв'язок, що дозволяє в режимі реального часу контролювати та керувати критично важливими пристроями та системами.

Інтернет речей (*Internet of Things, IoT*) стрімко розвивається в усіх галузях (рис. 1). Прогнозується, що до кінця 2025 року кількість підключених пристроїв IoT

досягне 30.9 мільярда, чому сприятимуть нові технологічні стандарти, як-от 5G.

Глобальні витрати на IoT досягли 159.8 мільярда доларів ще в кінці

2021 року і зростають із середньорічним темпом зростання (CAGR) 26.7% у період між 2022 і 2025 роками.

Оскільки кількість критично важливих застосунків зростає, пристрої та системи Інтернету речей повинні витримувати суворі умови реального світу. Інженери-розробники стикаються з величезними технічними викликами. Вони змушені робити критичні оцінки конструкції, враховувати аспекти тестування та йти на компроміси протягом усього життєвого циклу продукту — від раннього проектування до виробництва. Цілком зрозуміло, що вирішення багатогранних завдань проектування та тестування IoT вимагає комплексного підходу.

РОЗУМНЕ МІСТО

Понад 40 міст у всьому світі стали «розумними» до 2020 року

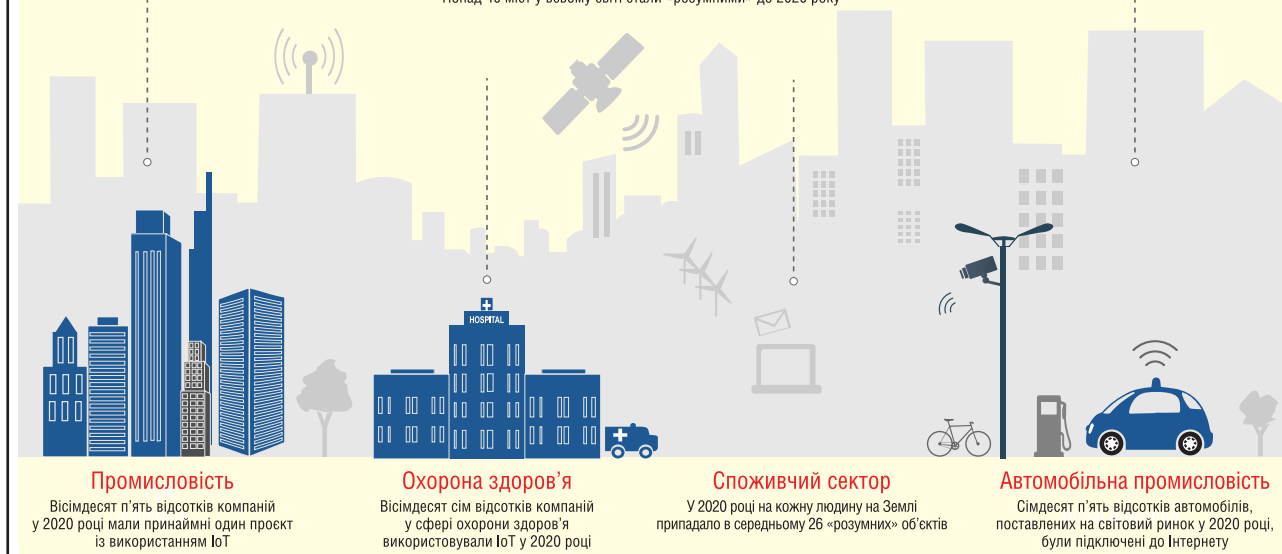


Рис. 1. IoT стрімко розвивається в усіх галузях

КОМПЛЕКСНИЙ ПІДХІД ДО ВАШОГО БАГАТОГРАННОГО ЗАВДАННЯ У ПРОЄКТУВАННІ ПРИСТРОЇВ ІОТ

Хоча пристрої IoT пропонують велику зручність, розміщення великої їх кількості на малому просторі ускладнює проектування, тестування, продуктивність та безпеку. Тестування цих пристроїв є одним із найбільших викликів для інженерів-розробників та виробників пристроїв. Їм необхідно вирішувати виклики «5C+1» (рис. 2.) протягом усього життєвого циклу пристрою IoT:

- **Зв'язність (Connectivity)** забезпечує підключення ваших пристроїв IoT до інших пристроїв IoT, хмари та навколишнього світу.
- **Безперервність роботи (Continuity)** вимагає, щоб ваші пристрої IoT мали тривалий час автономної роботи для виконання своїх завдань.
- **Відповідність вимогам (Compliance)** вимагає, щоб ваші пристрої IoT відповідали глобальним нормам.
- **Сумісність (Coexistence)** забезпечує гармонійну роботу ваших пристроїв IoT у переповнених середовищах IoT.
- **Кібербезпека (Cybersecurity)** захищає ваші дані від кіберзагроз.

Хоча ці технічні аспекти є важливими, врахування потреб та поведінки користувачів у дизайні та тестуванні продукту на ранніх етапах життєвого циклу є першочерговим для задоволення та утримання клієнтів. Окрім «5C» для IoT, важливим є тестування **клієнтського досвіду (Customer experience)**.

ПЕРШЕ «С»: ЗВ'ЯЗНІСТЬ (CONNECTIVITY)

В IoT бездротовий зв'язок є ключем до забезпечення безперебійного потоку інформації до пристрою та від нього, до інфраструктури, хмари та застосунків. Через складність систем та щільність розгортання пристроїв, зв'язність є головним викликом, з яким стикаються розробники пристроїв. Пристрої повинні працювати надійно, без збоїв, навіть у найсуворіших умовах. Стандарти бездротового зв'язку, що швидко розвиваються, додають складності у розробку та тестування пристроїв. Розробники та інженери пристроїв IoT стикаються з типовими викликами в цих сферах:

- **Брак знань у сфері РЧ (радіочастот).** Багато компаній розробляють свої перші бездротові продукти. Часто їм не вистачає власних фахівців для



Рис. 2. Виклики «5C+1» для IoT

вибору відповідних рішень для тестування на етапах розробки та виробництва. Традиційне обладнання для РЧ-тестування занадто дороге та складне в експлуатації. Створення методологій тестування для отримання точних та надійних результатів вимагає значних знань у сфері РЧ та програмування.

- **Неможливість керувати тестованим пристроєм (ТП).** Мініатюризація електроніки означає, що конструкції друкованих плат зменшуються, антени вбудовуються в плати, а порти вводу/виводу зникають. Розробники стикаються з викликами щодо того, як керувати ТП без фізичного з'єднання для імітації реальних режимів роботи. Як виміряти радіочастотні (РЧ) характеристики «по повітрю» (*over-the-air, OTA*)?
- **Недостатній обсяг РЧ-тестування.** Які РЧ-параметри потрібно охопити на етапах досліджень і розробок та виробництва? Під час розробки продукту пристрій, ймовірно, повинен пройти повний набір тестів згідно з відповідним стандартом бездротового зв'язку для забезпечення відповідності вимогам. На виробництві не повинно бути необхідності в додаткових прецизійних РЧ-тестах. Але які РЧ-тести допомагають відфільтрувати виробничі дефекти?
- **Висока вартість тестування.** Поширення пристроїв IoT означає, що попит на них зростатиме експоненційно. Виробникам потрібна високомасштабована та надійна система виробничого тестування, яка легко впорається з цим обсягом, що зростає.
- **Ненадійні результати тестування.** При розгортанні пристроїв IoT у критично важливих застосунках таких як «розумні» мережі, підключені автомобілі та критично важливі медичні пристрої, традиційні низьковартісні методи виробничого тестування з використанням допоміжних пристроїв, як-от метод «еталонного» радіомодуля, є недостатніми для забезпечення якості пристрою. Такі методи пропонують обмежене покриття тес-

тування, що може призвести до катастрофічних збоїв у роботі та навіть до дорогих відкликань продукції.

Для вирішення цих проблем необхідний ретельний вибір конструкції та тестового рішення, яке буде гнучким, налаштованим і масштабованим.

- Тестове рішення має бути гнучким, щоб тестувати багато пристроїв із різними форматами радіозв'язку, та оновлюваним для підтримки нових версій або форматів.
- Програмне забезпечення повинно мати можливість керувати як тестованим пристроєм (ТП), так і тестером, щоб переводити пристрій у різні режими роботи для оцінки реальних РЧ-характеристик.
- Апаратні засоби повинні забезпечувати можливість РЧ-вимірювання «по повітрю» (*over-the-air, OTA*) без необхідності фізичного підключення до пристрою або програмного забезпечення для керування спеціалізованим чипсетом.
- Тестова система має бути простою, недорогою та застосовною як для валідації конструкції, так і для виробництва, щоб мінімізувати проблеми з кореляцією вимірювань на цих різних етапах.
- Рішення має бути високомасштабованим та реконфігурованим, щоб зробити можливим тестування кількох ТП для потенційного розширення виробництва.

ДРУГЕ «С»: БЕЗПЕРЕРВНІСТЬ РОБОТИ (CONTINUITY)

Час автономної роботи є важливим параметром для пристроїв IoT. Він забезпечує величезну конкурентну перевагу та враховується споживачами при прийнятті рішення про покупку. «Розумні» лічильники або промислові бездротові датчики повинні працювати протягом тривалого часу між заряджаннями — часто 10 років або більше. Для медичних пристроїв, таких як кардіостимулятори, час автономної роботи може означати різницю між життям

і смертю. Групи, що займаються стандартами бездротового зв'язку, також визначають нові режими роботи з низьким енергоспоживанням, такі як NB-IoT, LTE-M, LoRa та Sigfox, які пропонують обмежений час активної роботи.

Розробники інтегральних схем (IC), проєктувальники пристроїв та інженери з тестування стикаються з викликами, коли йдеться про час автономної роботи пристроїв IoT:

- Щоб задовольнити вимоги до тривалого часу автономної роботи, розробники повинні створювати IC з режимами глибокого сну, які споживають мінімальний струм, знижувати тактову частоту та набори інструкцій, а також реалізовувати низькі напруги живлення.
- Розробники пристроїв, які інтегрують сенсорні, обчислювальні, керувальні та комунікаційні компоненти в кінцевий продукт, повинні розуміти, як периферійні пристрої поведуться та споживають енергію. Зрештою, їм доведеться оптимізувати мікропрограму та програмне забезпечення пристрою, щоб спростити роботу та зменшити споживання енергії.
- Розробники пристроїв та інженери з тестування повинні вимірювати струми, що сильно змінюються, на кожному етапі життєвого циклу пристрою. Пристрої IoT з низьким енергоспоживанням більшу частину часу проводять у режимі сну або очікування і лише зрідка «прокидаються» для передачі та приймання даних.
- Споживання енергії пристроями IoT значно коливається — від мікросекунд до секунд, і від пікоамперів до амперів. Вимірювання цього швидкозмінного та широкого діапазону струмів є викликом для розробників пристроїв та інженерів-тестувальників. На рисунку 3 показано приклад пристрою з низьким енергоспоживанням та вимоги до вимірювань.

Щоб вирішити ці проблеми, розробники IC, проєктувальники пристроїв та інженери-тестувальники повинні:

- Візуалізувати споживання струму від наноамперів до амперів (від нА до А), що відповідає широкому діапазону струмів пристроїв IoT від режиму сну до активного режиму.
- Автоматично співвідносити свої графіки споживання струму з подіями підсистем (наприклад, увімкнення радіомодуля, насоса, дисплея), щоб виявити слабкі місця в конструкції. Це дає розробнику краще розумін-

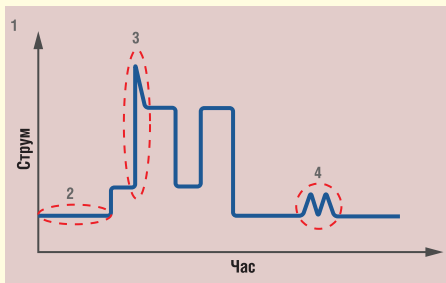


Рис. 3. Приклад пристрою з низьким енергоспоживанням та вимоги до вимірювань

1. Бажання перевірити профіль струму та оптимізувати його порівняно з імітацією
2. Необхідність оцінити та зменшити споживання струму в режимі сну
3. Бажання точно виміряти перехідний струм під час роботи пристрою
4. Необхідність не пропустити малі сигнали та стрибки, корисні для налагодження

ня внеску підсистем пристрою в загальне споживання струму.

- Здійснювати сигнальне керування пристроєм «по повітрю» (OTA) для імітації реальних операцій та вимірювання споживання струму під час цих операцій.
- Автоматично розраховувати загальний витрачений час, визначати струм, споживаний кожною підією або підсистемою, та оцінювати час автономної роботи пристрою, імітуючи реальні операції.

Завдяки цим можливостям розробники та інженери-тестувальники можуть виявляти слабкі місця в конструкції на ранніх етапах, прискорювати цикл розробки продукту та максимізувати час автономної роботи.

- Тиск часу виходу на ринок: розробники пристроїв часто намагаються вкластися в стислі графіки впровадження продукції та забезпечити плавне проникнення на світовий ринок, дотримуючись при цьому останніх нормативних вимог.
- Складність нормативного тестування: нормативні акти час від часу змінюються, що ускладнює нормативне тестування. Повільне оновлення від постачальника тестового обладнання створює додатковий тиск на терміни.
- Високі капіталовкладення: комплексна система нормативного тестування часто вимагає значних капітальних інвестицій.

ЧЕТВЕРТЕ «С»: СУМІСНІСТЬ (COEXISTENCE)

Стрімке зростання кількості підключених пристроїв зробило бездротове середовище щільним і перевантаженим. Органи зі стандартизації розробили методології та техніки уникнення колізій для підвищення продуктивності роботи пристроїв у присутності інших сигналів — адаптивне перелаштування частоти, прослуховування перед передачею та спільне уникнення колізій.

ТРЕТЄ «С»: ВІДПОВІДНІСТЬ ВИМОГАМ (COMPLIANCE)

Відповідність означає забезпечення того, що ваші пристрої IoT відповідають радіостандартам та глобальним нормативним вимогам перед виходом на ринок (рис. 4).

Виробники пристроїв IoT часто стикаються з викликами у дотриманні різних вимог у різних країнах світу.



Рис. 4. Дві основні категорії сертифікаційних тестів

Наскільки вони ефективні в середовищі змішаних сигналів? Якщо радіоформи не розпізнають інші сигнали, це може призвести до колізій та втрати даних. Споживчі пристрої, такі як бездротові навушники та носимі пристрої, можуть зіткнутися з дратівливими затримками або паузами. Однак медичний пристрій, такий як інфузійний насос, що перестав працювати через завади від мобільного телефону, є небезпечним для життя.

Хоча тестування на сумісність є важливим, для нього бракує режиму відповідності чи сертифікації. У США Федеральна комісія зі зв'язку (FCC) регулює випромінювання бездротових пристроїв, а Управління з санітарного нагляду за якістю харчових продуктів і медикаментів (FDA) регулює безпеку медичних пристроїв. Однак саме виробники повинні брати на себе відповідальність і проводити відповідне тестування. Інститут інженерів з електротехніки та електроніки (IEEE) встановив деякі рекомендації в ANSI (Американський національний стандарт для оцінки сумісності бездротових пристроїв) C63.27, щоб надати ключові аспекти для тестування на сумісність, такі як процес оцінки, налаштування тесту та рівні тестування на основі ризиків (рис. 5).

Завдяки цим рекомендаціям виробники можуть оцінити потенційний ризик та здатність свого пристрою успішно підтримувати його функціональні характеристики у присутності непередбачених сигналів у робочому середовищі.

П'ЯТЕ «С»: КІБЕРБЕЗПЕКА (CYBERSECURITY)

Кібератаки можуть відбуватися на багатьох рівнях — від пристроїв і комунікаційних мереж до хмари та застосунків. Будь-який підключений пристрій може потенційно діяти як шлюз до систем, що мають більшу цінність. Наприклад, хакер може використати пристрій IoT, щоб отримати доступ до національного центру розподілу електроенергії або оборонної системи та вивести її з ладу.

Щоб мінімізувати ризик кібератаки, підприємства тепер усвідомлюють, що їм потрібно вживати надзвичайних заходів для створення надійної інфраструктури IoT. Ось рекомендований багаторівневий підхід.

Безпека на рівні пристрою

Усунення прогалин у безпеці починається на рівні пристрою. Більшість порушень безпеки виникають на



1. Схарактеризуйте цільове середовище

- Які джерела завад присутні? Які їхні частоти, протоколи та потужність сигналу?



2. Визначте функціональні характеристики бездротового пристрою

- Що він повинен передавати? Як часто має відбуватися зв'язок? Яка максимальна допустима затримка? Яка необхідна стійка швидкість передачі даних?



3. Розробіть план тестування

- Оберіть налаштування тесту — коаксіальне, з використанням камер чи на відкритому повітрі?
- Визначте рівні ризику. Збої 1-го рівня становлять значний ризик, такий як смерть або серйозна травма, тоді як збої 4-го рівня мають незначний ризик, що переважно призводить до незручностей або дискомфорту
- Визначте критерії проходження/непроходження тестування. Це може бути швидкість передачі даних, затримка або частота помилок



4. Виконайте тест

- Моніторте РЧ-середовище та сигнал до та від тестованого пристрою
- Протестуйте без завад, щоб встановити еталонну продуктивність
- Тестуйте з завадами, поки не відбудеться збій



5. Створіть звіт

Рис. 5. Ключові кроки для виконання належного тестування на сумісність, спираючись на рекомендації, надані в ANSI C63.27

кінцевих пристроях. Розробники пристроїв повинні враховувати безпеку на самому ранньому етапі розробки пристрою та проводити постійну перевірку протягом усього життєвого циклу продукту, щоб забезпечити безпеку та якість обслуговування.

Безпека на рівні мережі

Впровадьте систему інформаційної безпеки — низку політик і процедур, які допомагають підприємствам знизити ризики та вразливість. Наприклад, Національний інститут стандартів і технологій (NIST) виділяє п'ять ключових напрямків діяльності в рамках своєї програми «основи ефективної безпеки»:

- Визначте дані та процеси, які потрібно захистити, і проведіть належну оцінку ризиків.
- Захистіть ці активи за допомогою фізичних та адміністративних засобів контролю.
- Постійно виявляйте загрози в мережі.
- Реагуйте на загрози за допомогою задокументованого та перевіреного плану реагування на інциденти.
- Відновлюйте усі втрачені активи, якщо це можливо.

Безпека на рівні підприємства

Навчання всіх співробітників важливості безпеки даних — мабуть, найменш витратний захід безпеки — забезпечує найвищу віддачу від інвестицій. Керівники вищої ланки та ради директорів, а не лише IT-відділ, повинні усвідомлювати ризик кібератаки для організації.

Навіть після впровадження всіх рекомендованих заходів, мережа все ще

може бути скомпрометована. Справжній тест полягає в тому, скільки часу знадобиться на відновлення. Сійка мережа захищатиметься від загроз і мінімізуватиме фінансові втрати організації.

БІЛЬШЕ НІЖ «5С» ДЛЯ ІОТ: КЛІЄНТСЬКИЙ ДОСВІД (CUSTOMER EXPERIENCE)

Перші п'ять «С» — зв'язність, безперервність роботи, відповідність вимогам, сумісність та кібербезпека — усі важливі. Однак додаткове «С», клієнтський досвід, виведе ваш пристрій на перше місце серед конкурентів. Для складних продуктів важливе наскрізне тестування клієнтського досвіду, щоб переконатися, що продукт досягає вершини своєї продуктивності, задовольняє потреби клієнтів і витримує реальні сценарії використання.

На щастя, існують інтегровані рішення, які можуть вирішити проблеми проектування та валідації, з якими сьогодні стикаються інженери. Найкращим підходом до тестування наскрізного клієнтського досвіду є інтелектуальне рішення для тестування на основі моделей, яке може допомогти оптимізувати продукт. Рішення, що включає ці чотири компоненти, забезпечує всебічне тестування всього спектру потенційних шляхів користувачів.

- Фізичне моделювання пристрою з інтерфейсом керування вимірюваннями для створення цифрового двійника тестованого приладу.
- Обладнання з розвинутою автоматизацією, яке замінює ручні дії люди-

ни, дозволяючи прискорити та підвищити точність розробки.

- Моделювання програмного забезпечення або застосунків, яке імітує реальні сценарії користувача для тестування повного шляху клієнта, щоб забезпечити швидку та ефективну валідацію всієї системи.
- Хмарне програмне моделювання із застосуванням алгоритмів аналізу даних на основі машинного навчання для профілювання поведінки користувача з метою покращення досвіду кінцевого користувача.

ПОГЛЯД НА «5C+1» У ПЕРСПЕКТИВІ

Інтернет речей відкриває двері для захопливих нових застосунків та можливостей для багатьох галузей промисловості. Але це також приносить безпрецедентні виклики, які вимагають нового мислення для задоволення критично важливих вимог. Візьмемо, наприклад, кардіостимулятори. Припустимо, хірург імплантує кардіостимулятор

під шкіру пацієнта для моніторингу та управління його серцебиттям. За допомогою бездротового з'єднання лікар може стежити за діяльністю серця пацієнта та планувати подальше лікування.

Попри свій потенціал, успіх кардіостимулятора та інших критично важливих пристроїв IoT тісно пов'язаний з «5C+1»:

- енергоефективність кардіостимулятора, оскільки заміна вбудованої батареї означає операцію на грудній клітці;
- величина струму витоку, який може спричинити надмірну стимуляцію м'язів;
- надійність зв'язку для забезпечення безперебійної передачі даних у будь-якому середовищі;
- захист переданої інформації;
- здатність швидко проходити тривалі нормативні та клінічні процеси FCC та FDA;
- всебічне охоплення тестуванням усього шляху використання кардіостимулятора пацієнтом.

Дослідники все ще працюють у всіх цих напрямках. Завдяки ретельній оцінці викликів «5C+1», дистанційний моні-

тинг пацієнтів за допомогою імплантованих бездротових кардіостимуляторів допоможе поліпшити якість їхнього життя. З огляду на це, рівень впровадження бездротових кардіостимуляторів, ймовірно, стрімко зростатиме.

Успішне впровадження IoT вимагає від розробників та інженерів подолання технічних викликів. Глибоке розуміння технічних викликів та ключових аспектів проектування й тестування створить міцну основу для зниження ризиків розробки та розгортання IoT у всій екосистемі. Використання правильних інструментів проектування, валідації, тестування на відповідність вимогам та виробництва протягом усього життєвого циклу продукту також допоможе забезпечити виконання обіцянок IoT.

Щоб отримати додаткову інформацію, звертайтеся, будь ласка, в компанію Юнітест:

**04053, м. Київ,
вул. Олеса Гончара, 6,
тел. +38 (044) 272-60-94,
e-mail: web@unitest.com
www.unitest.com**

CN

СУЧАСНЕ КОНТРОЛЬНО-ВИМІРЮВАЛЬНЕ ОБЛАДНАННЯ ВІД КОМПАНІЇ KEYSIGHT TECHNOLOGIES ДЛЯ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО!

Співпраця між міжнародною високотехнологічною компанією **Keysight Technologies** та **Факультетом електроніки КПІ ім. Ігоря Сікорського (ФЕЛ)** триває з 2023 року. Завдяки цій співпраці університет отримав:

- 8 комплектів обладнання для навчально-наукової лабораторії «Електричних кіл та силової електроніки», в якій здійснюватиметься освітній процес (осцилографи, генератори сигналів, блоки живлення, цифрові мультиметри тощо);
- 2 комплекти наукового контрольно-вимірювального обладнання загальною кількістю 50 одиниць (осцилографи, електронні навантаження, LCR-метри, пробники струму та диференційні пробники).

Обладнання було передано за участі Дугласа Бейні (корпоративний директора Keysight Technologies з питань освіти) та Віктора Бутиріна (директор **ТОВ «Юнітест ЛТД»**, авторизованого дистриб'ютора Keysight Technologies в Україні).

Завдяки такій підтримці студенти КПІ отримують ще більший доступ до передових технологій світового масштабу та освіти за міжнародними стандартами.

ФЕЛ КПІ ім. Ігоря Сікорського щиро дякує партнерам за довіру та підтримку!

<https://uadd.me/kpiua>
www.unitest.com



Сучасне контрольно-вимірювальне обладнання від міжнародної високотехнологічної компанії Keysight Technologies (США) для КПІ ім. Ігоря Сікорського

СПІВПРАЦЯ