10. Pastukh O., Petryk M., Bachynskiy M., Mudryk I., Stefanyshyn V. Processing of Cerebral Cortex Neurosignals from EEG Sensors and Recognizin Specific Types of Mechanical Movements Elements of Pacient Limbs under the Cognitive Feedback Influenses // International Workshop on Computer Information Technologies in Industry 4.0. 2023. №3468. С. 61–70.

УДК 621.396.674.37

Г.П. Химич, ст. викл., С.П. Дуда, асистент
Тернопільський національний технічний університет імені Івана Пулюя, Україна

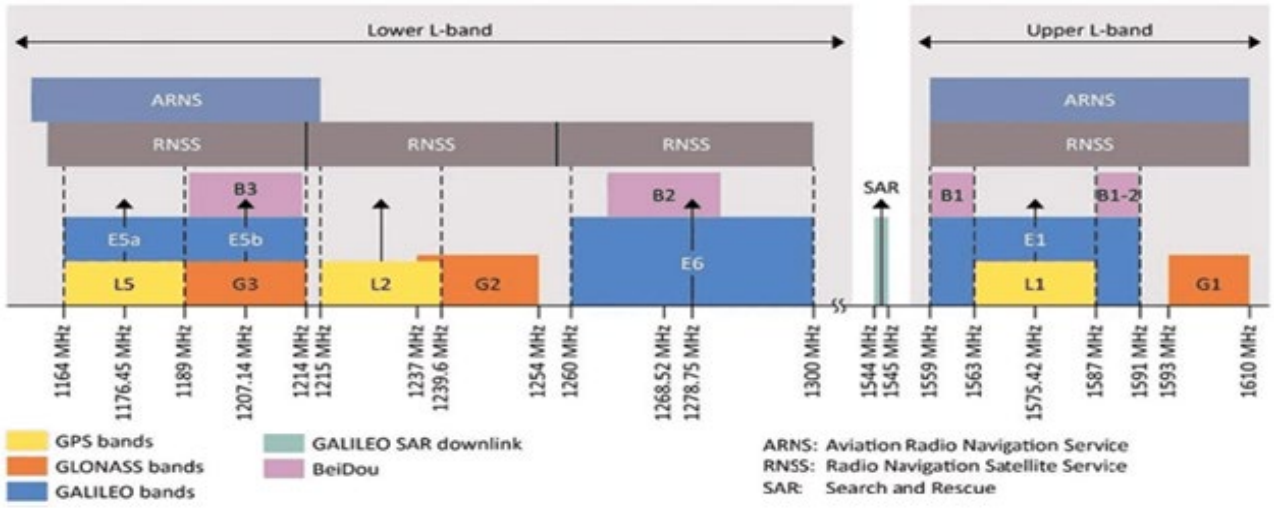
ПОВНОДІАПАЗОННА ПАТЧ АНТЕНА ДЛЯ СУПУТНИКОВОЇ НАВІГАЦІЇ

H. Khymych, senior lecturer, S. Duda, assistant

FULL-BAND PATCH ANTENNA FOR SATELLITE NAVIGATION

У статті представлена широкосмугова патч антена пасивного типу для високоточного моніторингу та прийому сигналів від всіх існуючих супутникових систем навігації (GNSS — Global Navigation Satellite System). Дана антена входить в наземний комплекс і призначена для позиціонування в просторі (місцезнаходження в географічній системі координат), у часі і визначення параметрів руху (швидкості, напрямку та ін.) для швидкісних повітряних об'єктів. Відповідно до рекомендацій ITU-R (раніше CCIR) з номерами 1901-1906, для GNSS, табл. 1, виділено п'ять діапазонів частот, з яких використовуються три:
(1559-1610) МГц, позначається як L1, E1, B1;
(1215-1300) МГц, позначається як L2, E6, B3, L6;
(1164-1215) МГц, позначається як L5, E5, B2, L3;
(1200-1250) МГц, змішаний діапазон частот L2b, який включає:
G3 (1202,025 МГц), E5b/B2b/B2I (1207,140 МГц), L2 (1227,600 МГц)
G2/L1 (1242,937-1248,625 МГц).
Існують інші сигнали за межами цих діапазонів:
-1381,05 МГц (L3 GPS), який використовується для моніторингу ядерного вибуху;
-1379,9133 МГц (L4 GPS), використовується для дослідження іоносфери.

Таблиця 1



Для антени вибрана кубічна 3D конструкція з трьох сендвіч-панелей на основі фольгованого склотекстоліту FR-4,8. Така конструкція забезпечує широкосмуговість (1160 – 1610) MHz, кращий прийом на низьких кутах, хорошу оглядовість, низьке відношення сигнал/шум, придушення ефекту багатопроменності. Дана система підтримує індустріальні стандарти прийому сигналів для забезпечення високої точності, достовірності та продуктивності.

Так як два діапазони L2 і L5 фактично перекриваються по частоті, то оптимізація розрахунку антени проводилась для їх загальної центральної частоти - 1230 МГц.
Попередню оцінку параметрів спроєктованої антени проведено в середовищі MATLAB.
Так як врахування діелектричних властивостей плати викликає програмні складнощі, аналіз проводився для МПЛ без заповнення, рис. 1. Подальше проєктування антени виконано з врахуванням діелектричних властивостей підложки. Виміряний коефіцієнт стоячої хвилі (SWR) за напруженістю антени (узгодженості)показано на рис. 2. Дослідницький взірець патч антени показаний на рис. 3.

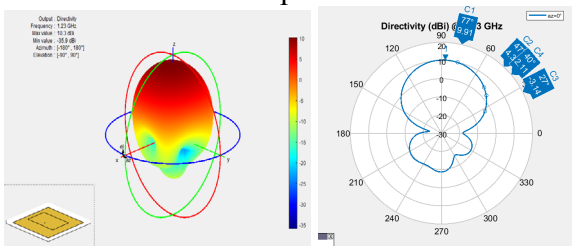


Рисунок 1. Кутомісна діаграма з маркерами зміни коефіцієнта підсилення.

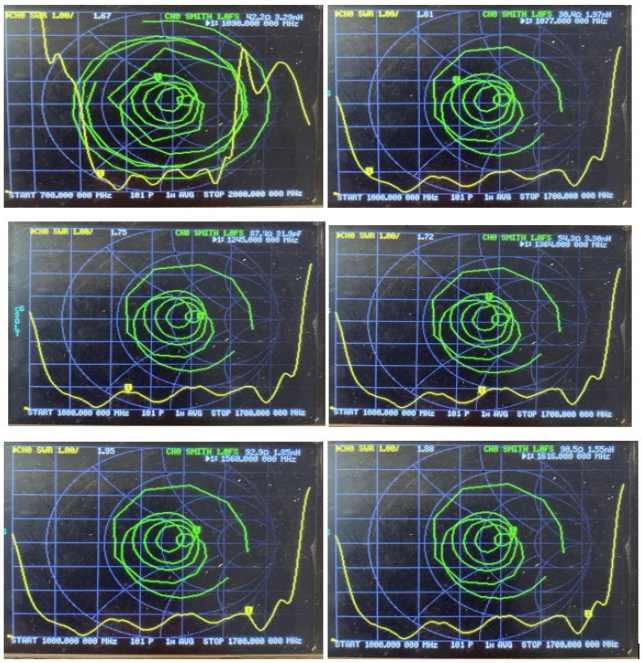


Рисунок 2. Спектрограми КСХн.

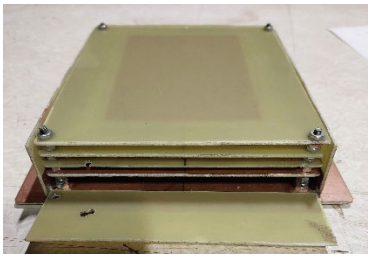


Рисунок 3. Взірець патч антени

У якості матеріалу вибрані склотекстоліт FR4 товщиною 1,5 мм, та ФЛАН 2,8 товщиною 1 мм. Теоретичні розрахунки і оціночні (практичні) параметри сформовані в табл.2.

Таблиця 2

Конструктивні розміри і параметри	ФЛАН 2,8 t=1 mm,	FR 4,8 t=1,5 mm	ФЛАН 2,8 t=1 mm,	FR 4,8 t=1,5 mm
	оціночно		теоретично	
F – частота, MHz	1208,0			
L - довжина патча	73,9	56,5	73,9	56,5
W - ширина патча	90	72,9	90,1	72,9
g - зазор	2,1	1,24	2	1,3
Xo - глибина зазору	23,3	18,9	23,6	18
Wt - ширина лінії живлення	2,3	2,1	2,6	2,7
Lекр - довжина екрану	149	114	150	115
Wекр - ширина екрану	165	131	165	130
Zp - хвильовий опір патчу	165	204	264	327
Wf - ширина 50 Ом, (розрах.)	2,6	2,7	2,6	2,7

Дана антена включає в себе три окремі патчі на різні діапазони частот згідно рекомендацій ITU-R, систему узгодження та фільтрування цих патчів, умовний суматор, фідерну вихідну лінію. Нижній патч виконує також роль екрануючої підложки для всієї антени. Вихідними даними для розрахунку глибини вставки в патч служить цільовий вхідний імпеданс, який повинен дорівнювати імпедансу фідерної лінії в напрямку смужкової антени (зазвичай 50 Ом). Фідерна лінія проникає в антену на певну глибину, а відношення глибини до зазору (D/S)

впливає на вхідний імпеданс. Рівняння, що зв'язує глибину вставки, імпеданс антени та імпеданс фідерної лінії, має вигляд:

$$D = \frac{L}{\pi}\cos^{-1}\left(\sqrt[4]{\frac{Z_{Feedline}}{Z_{Antenna}}}\right)$$

Дослідний взірець антени пройшов натурні випробування на літаючому швидкісному об’єкті.

Література

1. Mbinack, Clement, E. Tonye and D. Bajon. Microstrip-line theory and experimental study for the characterization of the inset-fed rectangular microstrip- patch antenna impedance. Microwave and Aptical Technology Letters, #2, 2015.
2. Kumar Girish. Broadband microstrip antennas/Girish Kumar and K.P. Ray. Artech House antennas and propagation library. ISBN 1-58053-244-6, 2003.

УДК 004.056

В.Г. Хомишин, Н.В. Загородна, к.т.н., доц., М.А. Стадник, к.т.н., доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

БЕЗПЕКА SCADA СИСТЕМ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

V.H. Khomyshyn, N.V. Zagorodna, Ph.D., Assoc. Prof., M.A. Stadnyk, Ph.D., Assoc. Prof.

SCADA SYSTEM SECURITY AT CRITICAL INFRASTRUCTURE FACILITIES

Системи диспетчерського управління та збору даних (SCADA) є основними компонентами моніторингу та управління на об’єктах критичної інфраструктури, такими як енергетика, телекомунікації, транспорт, тощо. Застарілі SCADA-системи працювали в ізольованих мережах й були менш вразливими до інтернет-загроз. Проте все частіше підключення корпоративних мереж, включаючи SCADA-системи, до мережі Інтернет створює серйозні проблеми з безпекою. При цьому спостерігається зростання кількості інцидентів безпеки щодо цих критичних інфраструктур. Кібератака на систему SCADA може мати руйнівні наслідки. Зловмисник, скомпрометувавши таку систему, може відключити послуги електропостачання, газу та водопостачання або знищити критично важливу військову інфраструктуру [1].

У 2015-2016 роках серія кібератак на українську енергосистему спричинила перебої в електропостачанні. Атаки проводило хакерське угруповання Sandworm. Зловмисники надіслали документ Microsoft Excel, у якому було шкідливе програмне забезпечення, що здійснювало атаки типу «відмова в обслуговуванні» на контролери SCADA й призвело до виведення з ладу підстанцій, відключення електроенергії та видалення інформації на жорстких дисках заражених систем.

Існують певні вразливості, які зловмисник використовує, щоб скомпрометувати SCADA системи. Такі системи часто побудовані на загальних комп'ютерних протоколах та функціях, таких як передача файлів по мережі або віддалений доступ. Незашифрований обмін даними може бути скомпрометований зловмисником з метою отримання конфіденційної інформації. Крім того, системні програми та служби вимагають певних відкритих мережевих портів. Зловмисник може використовувати ці порти для отримання доступу до системи SCADA, збору інформації про неї та отримання адміністративних привілеїв. Крім того, зловмисник може завантажити шкідливий код, який експлуатує вразливу програму, й отримати несанкціонований доступ. Таким чином, атака на мережі зв'язку може перерости в атаку на всю систему.

Однією з основних проблем захисту таких систем є відсутність зрілих інструментів для аналізу безпеки, адаптованих до вимог SCADA-систем. На відміну від традиційних